

THIRD DISTRICT COURT-FILED  
2011 AUG -8 PM 4:12

FILED BY \_\_\_\_\_

David R. Olsen (2458)  
E-mail: [doles@dkolaw.com](mailto:doles@dkolaw.com)  
Ralph L. Dewsnap (876)  
E-mail: [rdews@dkolaw.com](mailto:rdews@dkolaw.com)  
Paul M. Simmons (4668)  
E-mail: [psimm@dkolaw.com](mailto:psimm@dkolaw.com)  
DEWSNUP, KING & OLSEN  
36 South State St., Suite 2400  
Salt Lake City, UT 84111-0024  
Telephone: 801-533-0400  
Facsimile: 801-363-4218

*Attorneys for Cisero's, Inc. and Theodora McComb*

---

**IN THE THIRD JUDICIAL DISTRICT COURT  
IN AND FOR SUMMIT COUNTY, UTAH**

---

ELAVON, INC.,

Plaintiff,

vs.

CISERO'S, INC. and THEODORA MCCOMB,

Defendants.

---

CISERO'S, INC. and THEODORA MCCOMB,

Counterclaim Plaintiffs,

vs.

ELAVON, INC.,

Counterclaim Defendant.

**MOTION FOR LEAVE TO FILE  
AN AMENDED ANSWER AND  
COUNTERCLAIM**

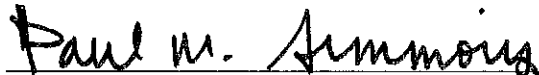
Civil No. 100500480

Judge Keith Kelly

Defendants and Counterclaim Plaintiff, Cisero's, Inc., and Theodora McComb, move the Court under Utah Rules of Civil Procedure 13(g) and 15(a) for leave to file an amended answer and counterclaim, on the grounds that the Defendants and Counterclaim Plaintiff are now represented by new counsel who, upon review of the pleadings and the evidence, have determined that amendment is necessary to join an indispensable party, to raise all of their legal and factual theories arising out of the events alleged in the Complaint, and to properly frame the issues for trial. This motion is supported by an accompanying memorandum of points and authorities. A copy of the proposed Amended Answer and Counterclaim is attached as Exhibit A.

DATED this 8th day of August, 2011

DEWSNUP, KING & OLSEN



David R. Olsen

Ralph L. Dewsnup

Paul M. Simmons

DEWSNUP, KING & OLSEN

36 South State St., Suite 2400

Salt Lake City, UT 84111-0024

Telephone: 801-533-0400

Facsimile: 801-363-4218

*Attorneys for Cisero's, Inc., and Theodora McComb*

**CERTIFICATE OF SERVICE**

I hereby certify that on this 8<sup>th</sup> day of August, 2011, I caused a true and correct copy of the foregoing **MOTION FOR LEAVE TO FILE AN AMENDED ANSWER AND COUNTERCLAIM** to be served by U.S. mail, first-class postage prepaid, on the following:

Cameron Hancock  
Todd Weiler  
DORSEY & WHITNEY LLP  
136 S. Main Street, Suite 1000  
Salt Lake City, UT 84101-1655  
*Attorneys for Plaintiff*

Paul M. Simmons

DEWSNUP, KING & OLSEN  
David R. Olsen (2458)  
E-mail: [doles@dkolaw.com](mailto:doles@dkolaw.com)  
Ralph L. Dewsnup (876)  
E-mail: [rdews@dkolaw.com](mailto:rdews@dkolaw.com)  
36 South State St., Suite 2400  
Salt Lake City, UT 84111-0024  
Telephone: (801) 533-0400  
Facsimile: (801) 363-4218

CONSTANTINE CANNON LLP  
W. Stephen Cannon  
Todd Anderson  
Richard Levine  
One Franklin Square  
1301 K Street, N.W., Suite 1050 East  
Washington, DC 20005  
(202) 204-3500

A. Owen Glist  
David A. Scupp  
335 Madison Avenue  
New York, NY 10017  
(212) 350-2700  
*Pro hac vice applications forthcoming*

*Attorneys for Cisero's, Inc. and Theodora McComb*

---

**IN THE THIRD JUDICIAL DISTRICT COURT  
IN AND FOR SUMMIT COUNTY, UTAH**

---

ELAVON, INC.,

Plaintiff,

vs.

CISERO'S, INC. and THEODORA MCCOMB,

Defendants.

---

CISERO'S, INC. and THEODORA MCCOMB,

Counterclaim Plaintiffs,

vs.

ELAVON, INC., and U.S. BANK NATIONAL  
ASSOCIATION,

Counterclaim Defendants.

**AMENDED ANSWER AND  
COUNTERCLAIM**

Jury Demanded

Civil No. 100500480

Judge Keith Kelly

Defendants, Cisero's, Inc. and Theodora McComb (referred to together as "Cisero's"), answer plaintiff's Complaint as follows:

1. Cisero's admits the allegations in paragraph 2 of the Complaint.
2. Cisero's denies the allegations in paragraphs 1 and 3 of the Complaint for lack of knowledge.
3. Cisero's denies the allegations in paragraphs 6, 10-15.
4. In response to paragraph 4, Cisero's notes that the "contract" speaks for itself. To the extent the allegations of paragraph 4 differ from the terms of the contract, the allegations are denied.
5. In response to paragraph 5, Cisero's acknowledges it had an agreement with U.S. Bank but notes that the copy of the "Merchant Agreement" attached to the Complaint as Exhibit A is largely illegible and, on that basis, denies the allegations in paragraph 5 for lack of knowledge.
6. Cisero's notes that paragraphs 7-9 state legal conclusions not requiring a response.
7. In response to paragraph 16, Cisero's admits Theodora McComb has, in the past, guaranteed certain obligations but denies the remaining allegations.

Any paragraphs or allegations in the Complaint not referenced in the preceding paragraphs of this Answer are denied.

#### **FIRST AFFIRMATIVE DEFENSE**

The Complaint fails to state a claim upon which relief may be granted.

## **SECOND AFFIRMATIVE DEFENSE**

Plaintiff's claims are barred in whole or in part for the reasons stated in defendants' Amended Answer and Counterclaim.

## **THIRD AFFIRMATIVE DEFENSE**

Plaintiff's claims are barred because there was no meeting of the minds between Cisero's and U.S. Bank regarding material terms purportedly incorporated by reference into the merchant agreement.

## **FOURTH AFFIRMATIVE DEFENSE**

Plaintiff's claims are barred because the terms of the merchant agreement were materially changed without providing consideration to Cisero's.

## **FIFTH AFFIRMATIVE DEFENSE**

Plaintiff's claims are barred because the merchant agreement between Cisero's and U.S. Bank is an unconscionable contract of adhesion.

## **SIXTH AFFIRMATIVE DEFENSE**

Plaintiff's claims are barred because the merchant agreement between Cisero's and U.S. Bank is void as against public policy.

## **SEVENTH AFFIRMATIVE DEFENSE**

Plaintiff's claims are barred because the fines and assessments for which U.S. Bank and Elavon seek indemnification are unenforceable penalties.

#### **EIGHTH AFFIRMATIVE DEFENSE**

Plaintiff's damages, if any, were caused by third parties over whom defendants had no control and for whose conduct defendants have no responsibility.

#### **NINTH AFFIRMATIVE DEFENSE**

Plaintiff's claims are barred by laches.

#### **TENTH AFFIRMATIVE DEFENSE**

Plaintiff's claims are barred by unclean hands.

#### **ELEVENTH AFFIRMATIVE DEFENSE**

Plaintiff's claims are barred by waiver.

#### **TWELFTH AFFIRMATIVE DEFENSE**

Plaintiff's claims are barred by estoppel.

#### **THIRTEENTH AFFIRMATIVE DEFENSE**

Defendants presently have insufficient knowledge or information upon which to form a belief whether there may be additional, as yet unstated, defenses and reserve the right to assert additional defenses in the event that discovery indicates that such defenses are appropriate.

**WHEREFORE**, Cisero's requests that plaintiff's Complaint be dismissed with prejudice and on the merits, that plaintiff take nothing thereby and that Cisero's be awarded its costs and reasonable attorney's fees.

## **AMENDED COUNTERCLAIM**

Cisero's, Inc. and Theodora McComb (collectively, "Cisero's") assert counterclaims against Elavon, Inc. ("Elavon"), and against U.S. Bank National Association ("U.S. Bank"), as follows:

### **INTRODUCTION**

1. Cisero's, a small Park City restaurant, brings this Amended Counterclaim to recover damages from U.S. Bank and Elavon for wrongfully confiscating funds from Cisero's bank account. U.S. Bank and Elavon confiscated these funds without legal basis and imposed unwarranted harsh fines and penalties on Cisero's, while denying the restaurant and its owners proper notice and the opportunity to contest the false assumptions underlying the penalties. The fines and penalties are based upon alleged technical violations of security rules and a supposed data security breach at Cisero's, even though there is no proof that a data breach occurred or that any fraud losses actually resulted.

2. In 2001, Cisero's and U.S. Bank entered into an agreement whereby U.S. Bank would act as Cisero's "acquiring bank" for payment card transactions, enabling Cisero's to accept Visa and MasterCard payments. Elavon, U.S. Bank's affiliate and one of the largest payment processors in the country, acted as U.S. Bank's agent providing Cisero's with payment processing services under the agreement.

3. Cisero's agreement with U.S. Bank was a non-negotiable contract of adhesion. Its relevant terms were typical of contracts between acquiring banks and smaller merchants, such as restaurants, who must accept Visa and MasterCard to compete. The contract incorporated



Visa's and MasterCard's complex and onerous rules by reference, subjecting Cisero's to rules that were not publicly available and could change at any time without notice.

4. The contract gave U.S. Bank unilateral discretion to change the terms of the agreement at any time, often without notice to Cisero's. It granted U.S. Bank broad indemnification rights against Cisero's, allowing U.S. Bank to satisfy any claimed indemnity by withdrawing funds directly from Cisero's account at U.S. Bank, without giving Cisero's any recourse. Despite these onerous terms, Cisero's executed the Merchant Agreement because otherwise it could not accept Visa and MasterCard payments.

5. As a small restaurant, Cisero's did not have expertise in the rules or technical issues surrounding the protection of cardholder data. Cisero's therefore depended upon U.S. Bank and Elavon's knowledge of Visa and MasterCard rules and payment technology expertise to ensure that Cisero's complied with the payment networks' rules.

6. U.S. Bank and Elavon did nothing to apprise Cisero's of these rules – which were changing in material ways during the relevant time period – educate it about technical issues, or help ensure compliance. The first substantive communication about these rules that Cisero's received from U.S. Bank or Elavon was when Elavon notified Cisero's that it might have violated them.

7. In 2008, U.S. Bank and Elavon demanded indemnification from Cisero's for fines and penalties assessed by Visa and MasterCard arising from an alleged data breach at Cisero's. These fines and penalties were assessed pursuant to Visa's and MasterCard's complex, evolving standards regarding the storage of cardholder data. Prior to informing Cisero's in March 2008 of

a potential data breach, neither U.S. Bank nor Elavon had ever provided Cisero's with proper notice – much less education or guidance – regarding those standards. Nor had U.S. Bank or Elavon made any attempt to verify or ensure that Cisero's complied with the standards.

8. After an investigation that yielded no proof of a data breach or resulting fraud loss, both Visa and MasterCard nevertheless asserted that Cisero's had violated the networks' standards and imposed fines upon U.S. Bank. U.S. Bank and Elavon agreed to pay these fines to Visa and MasterCard, demanded indemnification from Cisero's, and seized payment from Cisero's bank account. They did so despite the fact that:

- Neither the alleged data breach nor any resulting fraud loss has ever been proved;
- Cisero's was not given an opportunity to challenge the assessments or present evidence in its defense;
- Visa did not follow its own rules in assessing liability; and
- The fines and penalties were punitive in that they bore no relationship to the non-existent harm to Visa or MasterCard.

9. Although U.S. Bank and Elavon blamed Cisero's, Visa's and MasterCard's fines and penalties were the result of U.S. Bank and Elavon's own negligence. Nevertheless, U.S. Bank and Elavon helped themselves to more than \$10,000 from Cisero's bank account before Cisero's was able to close its account with U.S. Bank and find a new acquirer and processor in September 2008. Some or all of the funds withdrawn by U.S. Bank and Elavon were unrelated to the Merchant Agreement, such as funds deposit pursuant to Cisero's agreement with American Express.

10. As a result of U.S. Bank and Elavon's conduct, Cisero's faces some \$90,000 in fines, a substantial amount for a merchant of its size. Cisero's and Ms. McComb have suffered financial and reputational harm. Cisero's brings this Counterclaim to obtain a declaration of its rights under the Merchant Agreement and to recover the damages it sustained.

### **PARTIES**

11. Counterclaim plaintiff Cisero's, Inc. is a Utah corporation with its principal place of business in Summit County, Utah. Cisero's operates a restaurant and nightclub in Park City, Utah.

12. Counterclaim plaintiff Theodora (Cissy) McComb is an owner of Cisero's, Inc.

13. Counterclaim defendant U.S. Bank is a national banking association with its principal place of business in Minneapolis, Minnesota. U.S. Bank was at all times mentioned herein doing business in Summit County, Utah.

14. Counterclaim defendant Elavon, formerly known as Nova Information Systems, is a Georgia corporation doing business in Utah, with its principal place of business in Atlanta, Georgia. Elavon and U.S. Bank are subsidiaries of U.S. Bancorp, a financial services holding company. In its pleadings and its correspondence with Cisero's counsel, Elavon claimed to be a subsidiary of U.S. Bank. Elavon purports to be the assignee of U.S. Bank's right to collect the alleged debt owed by Cisero's to U.S. Bank. Elavon was at all times mentioned herein doing business in Summit County, Utah.

## FACTS

15. Cisero's is a small Park City restaurant founded in 1985 by Stephen and Cissy McComb. It is a family restaurant managed directly by the McCombs and frequented by locals and tourists alike. Since its opening, and prior to the events described below, Cisero's processed millions of dollars of Visa and MasterCard credit and debit card transactions without incident.

### **Background**

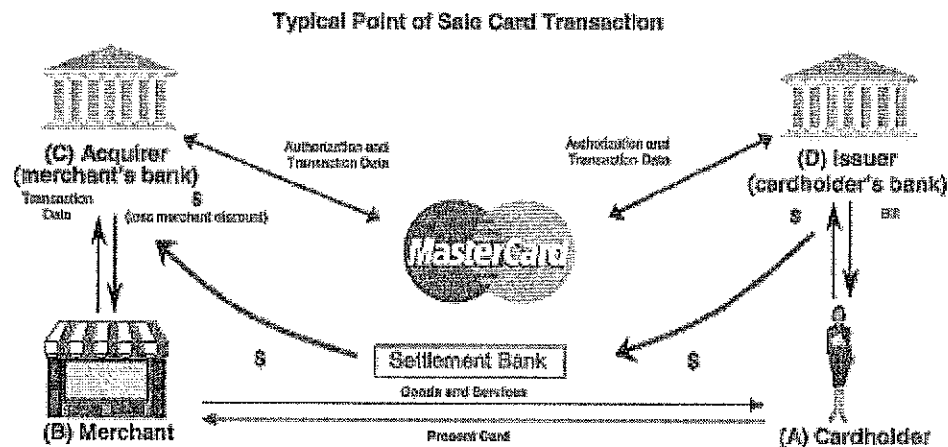
16. Visa and MasterCard payment card services are provided by means of "four-party" networks. As depicted in the diagram below, the four parties are:

- Cardholder. A cardholder is a consumer who makes a purchase from a merchant using an electronic payment card.
- Merchants. When a cardholder makes an in-person transaction, the cardholder's credit or debit card is swiped at a merchant's point-of-sale ("POS") terminal.
- Acquirers. Acquirers are merchants' banks, such as U.S. Bank, that "acquire" transactions by providing merchants with access to the payment networks and maintaining amounts due to the merchant. Acquiring banks usually contract with a processor, such as Elavon, to provide merchants with authorization, clearance, and settlement transactional services.
- Issuers. Issuers are cardholders' banks, such as Bank of America or Wells Fargo, that issue credit and debit payment cards to retail customers.

17. This process works as follows:<sup>1</sup>

---

<sup>1</sup> This graphic is taken from MasterCard's 2005 Annual Report filed with the SEC. The process is the same for both Visa and MasterCard. MasterCard, Inc., SEC Form 10-K for 12/31/05 (filed 3/16/06).



18. The diagram shows how, in a typical transaction, a cardholder (A) purchases goods or services from a merchant (B) using a payment card. After the transaction is authorized by the issuer (D) using the MasterCard (or Visa) network, the acquirer (C) pays the amount of the purchase, net of a fee, to the merchant. The acquirer typically holds the merchant's funds in an account called the settlement account.

**Cisero's Was Forced to Accept a Contract of Adhesion, Binding Cisero's to Non-Public Rules That Could Change Without Notice at Any Time**

19. Like most other businesses, restaurants must be able to accept electronic payments from Visa and MasterCard cardholders to stay in business. This need is magnified for restaurants such as Cisero's whose livelihood is heavily dependent on tourist customers. Not accepting Visa and MasterCard payments is simply not an option for Cisero's. Visa and MasterCard control 78% of payment card transactions – and approximately 90% of Cisero's restaurant customers use payment cards.

20. To accept credit and debit cards, a merchant must contract with an acquiring bank. In turn, this acquiring bank often contracts with a payment processor to handle its day-to-

day interaction with merchants. Under Visa's and MasterCard's rules, the acquirer is responsible for the merchant, including its compliance with Visa's and MasterCard's rules. Visa and MasterCard typically levy fines against acquirers when their merchants violate these rules, and acquirers, as discussed below, almost always pass these fines along to merchants. Upon information and belief, the relevant terms of merchant processing contracts of acquirers are substantially similar and typically include many if not all of the onerous terms. Small merchants like Cisero's have no choice but to accept the terms as offered to be able to accept Visa and MasterCard payments.

21. On or about November 28, 2001, Cisero's and U.S. Bank entered into the Merchant Agreement, whereby U.S. Bank agreed to act as Cisero's acquirer for the processing of electronic payments through the Visa and MasterCard networks.

22. The Merchant Agreement states "Merchant agrees to abide by the terms and conditions set forth in the [Merchant Terms of Service ("MTOS")], the Merchant Processing Guide and this Merchant Agreement, as they may be amended by U.S. Bank from time to time."

23. The MTOS purports to give U.S. Bank broad discretion in changing the terms of the agreement:

U.S. Bank may charge the Merchant Discount Fees or one or more of the other fees and charges, or amend any terms and conditions set forth in this MTOS or included on the Merchant Agreement upon prior written notification to Merchant. Further, any such fees and charges or any other part of this MTOS may be amended by U.S. Bank at any time without notice to Merchant if such change is due to National Association [Visa and MasterCard] rules.  
TENDER OF ANY SALES DRAFT BY MERCHANT AFTER  
THE EFFECTIVE DATE OF ANY CHANGES IN THE

DISCOUNT RATE, ANY FEES OR CHARGES, OR ANY CHANGES TO THIS MTOS CONSTITUTES ACCEPTANCE OF SUCH CHANGES. IF MERCHANT DOES NOT AGREE TO SUCH CHANGES, MERCHANT'S SOLE REMEDY SHALL BE TO CEASE TENDERING SALES DRAFTS PRIOR TO THE EFFECTIVE DATE OF SUCH CHANGE AND NOTIFY U.S. BANK IN WRITING OF MERCHANT'S INTENTION TO TERMINATE MERCHANT PROCESSING SERVICES PURSUANT TO SECTION 12.I OF THIS MTOS.

MTOS at 1 (underline added; capital letters in original).

24. Visa's and MasterCard's rules mandate that each acquirer include in its merchant agreement provisions requiring that merchants, in turn, also obey network rules. Accordingly, the MTOS includes a requirement that Cisero's comply with Visa's and MasterCard's rules:

Merchant will comply with all other Merchant Program rules and regulations as established and amended from time to time by U.S. Bank and by Visa U.S.A., Inc., Visa International, MasterCard International and any other national card association, regional debit network or other regulatory organization designated by U.S. Bank (collectively, the "National Associations"), which rules and regulations, together with the Merchant Processing Guide, are hereinafter referred to as the "Operating Regulations" and are incorporated herein and made part of the Agreement by this reference. Any breach of the Operating Regulations shall constitute a breach of this MTOS.

25. Cisero's payment card transactions were thus subject to Visa's and MasterCard's complex sets of rules, regulations, and standards. However, at the time Cisero's and U.S. Bank entered into their contract, these arcane operating rules – over 1,000 pages in length – were not publicly available to merchants and did not contain provisions regarding data security, as discussed below, relevant to this case. In fact, relevant Visa and MasterCard data security rules were not enacted until years later, unbeknownst to Cisero's.

26. Until 2008, these rules were treated as proprietary to the payment networks, issuers, and acquirers. In a May 8, 2008 press release, Visa announced that it “will for the first time make its Visa International and Regional Operating Regulations available publicly, effective May 15, 2008.” As discussed below, this was after the alleged data breach at Cisero’s.

27. Even when made available, the regulations were not necessarily available in full or in a timely fashion. According to the October 2008 public version of Visa’s rules, Visa intentionally omitted sections from its public release of its rules:

[W]e have omitted certain proprietary and competitive information from this manual. As such, a reader of this manual may observe non-sequential section numbering, and information that may seem out of context or incomplete regarding the subject. Visa makes no representations or warranties as to the accuracy or completeness of the text contained in this manual. . . . Visa reserves the right to amend, modify, delete or otherwise change the *Visa Operating Regulations* at any time, and such changes, if made after the publication date noted in this version of the *Visa Operating Regulations* . . . will not appear in this manual. The contents of this manual will be updated in accordance with the normal publication cycle of the *Visa Operating Regulations*. In the event of any discrepancy between the text in this manual and the *Visa Operating Regulations*, the text contained in the *Visa Operating Regulations* takes precedence.

Visa U.S.A. Inc., *Operating Regulations--Volume I, General Rules* at i (Public Edition, Nov. 15, 2008) (“VOR”).

28. Thus, Cisero’s entered into the Merchant Agreement with U.S. Bank in 2001, and was purportedly bound by Visa’s and MasterCard’s rules for *years* before those rules were made publicly available. Even then, the publicly available rules were incomplete and, by the terms of the MTOS, could change at any time, without notice to Cisero’s. Cisero’s was not even given notice that the rules had been made publicly available. Yet Cisero’s was compelled to accept



these terms – which, upon information and belief, are found in almost all small merchants' contracts with acquirers – in order to accept Visa and MasterCard payments.

29. The MTOS also grants U.S. Bank broad indemnification rights:

[Cisero's] hereby indemnifies and releases U.S. Bank, its affiliates and Correspondent, and agrees to defend and hold U.S. Bank, its affiliates and Correspondent harmless, from and against any and all claims, causes of action, demands, judicial and administrative proceedings, losses, liabilities, damages, costs and expenses, including without limitation court costs and reasonable fees and expenses of attorneys and consultants, arising out of or directly or indirectly related to . . . (2) any non compliance by Merchant with this MTOS, applicable laws, or rules of any National Association [Visa or MasterCard]; . . . (5) U.S. Bank's provision of services hereunder or Merchant's participation or activities hereunder.

MTOS § 7.A.

30. Upon information and belief, almost all contracts between acquirers and merchants have such indemnification clauses. These clauses provide acquirers like U.S. Bank with virtually no incentive to dispute any of the fines assessed against them by Visa or MasterCard for supposed infractions committed by their merchants. Acquirers can instead agree to pay fines levied by Visa and MasterCard without worrying about whether the fines are supported by evidence, are consistent with the card networks rules, or are even legal under applicable state law, because acquirers know that they will be indemnified by the merchant.

31. Moreover, under most merchant agreements, acquirers can simply withdraw the amount of the fines from the merchant's account without notice or consent. Cisero's Merchant Agreement is no exception. Section 11.A. of the MTOS provides that Cisero's establish a reserve account that "shall serve as a fund available to U.S. Bank to enforce any and all

obligations and liabilities of [Cisero's] to U.S. Bank arising under this MTOS." Section 11.B. states that "U.S. Bank may withdraw funds from the Reserve Account at any time without notice to Merchant in the amount of any obligation or liability of Merchant to U.S. Bank hereunder."

32. At various points throughout the parties' relationship, the terms of Cisero's merchant agreement were materially changed without Cisero's consent, and without providing Cisero's with adequate notice, through changes in the card networks' rules that the Agreement required Cisero's to obey – sight unseen. These material changes include, but are not limited to, the implementation of various card security rules, and fees and fines related to alleged security breaches.

**Visa and MasterCard Impose Penalties for Non-Compliance  
with PCI DSS Standards Created by the Networks**

33. In 2005, approximately four years after Cisero's and U.S. Bank entered into the Merchant Agreement, both Visa and MasterCard adopted card data protection standards developed by the Payment Card Industry ("PCI") Council known as the PCI Data Security Standards ("PCI DSS"). The Council was created and is controlled by the five major card brands: Visa, MasterCard, American Express, Discover and JCB.

34. Because these standards were made part of Visa's and MasterCard's rules, they were incorporated by reference into Cisero's merchant agreement. Neither U.S. Bank nor Elavon ever apprised Cisero's of these new standards.

35. Visa and MasterCard have additional programs that mandate acquirer validation of a merchant's PCI DSS compliance. Visa calls its program the Customer Information Security

Program (“CISP”), while MasterCard labels its program the Site Data Protection (“SDP”) Program. Through these programs, Visa and MasterCard impose “fines,” “penalties,” and “compliance assessments” on acquirers for their merchants’ violations of the PCI rules. As discussed below, these are punitive fines that bear no relation to any amount of actual losses. In fact, Visa and MasterCard will impose these fines even though there has been no fraud loss at all because these fines are profitable to them. Ultimate liability for the fines flow to merchants like Cisero’s through the indemnification provisions contained in standard merchant agreements. Neither U.S. Bank nor Elavon ever informed Cisero’s of material changes to the CISP or SDP programs, including changes that addressed merchant compliance with PCI DSS.

36. Visa’s and MasterCard’s fines and assessments are penal in nature. In fact, Visa’s rules provide for increasingly severe penalties for “willful,” “repetitive,” or “egregious” violations.

37. On February 9, 2011, Bob Russo, the General Manager of the PCI Security Standards Council admitted at the 2011 Hospitality Law Conference in Houston, Texas, that the PCI fine amounts were “arbitrary.”

38. The penalties are completely at the discretion of interested parties –namely, Visa and MasterCard – that profit from this system. They are imposed on acquirers, which, pursuant to the indemnification provisions in typical merchant agreements, then help themselves to reimbursement from merchant bank accounts. Merchants have no recourse. There is no process directly available to merchants to challenge the fines, demand proof of non-compliance, or present exonerating evidence. The acquirer (but not the merchant) may appeal the imposition of

a penalty in writing, with an appeal and supporting material to be received by Visa within 30 days of the acquirer's receipt of a notice of violation. VOR § 1.10.G.1.

**Visa's Account Data Compromise Recovery Process Imposes Fines  
for Alleged Data Breaches, Even If Unproven**

39. On or about October 1, 2006, five years after Cisero's and U.S. Bank entered into the Merchant Agreement, Visa implemented its Account Data Compromise Recovery ("ADCR") process. According to Visa, this program enables issuers that claim to have suffered losses related to data breaches to recover against the acquirer whose merchant purportedly stored compromised cardholder data. As evidenced by the fines on Cisero's, Visa imposes ADCR fines without regard to proof of a data breach, fraud loss, or a causal link between the two.

40. The ADCR process is a matter of contract among Visa and its authorized issuers and acquirers. Like fines for violations of the PCI DSS standards, the ultimate responsibility for fines and penalties assessed through the ADCR process flows directly to merchants. Merchants have no right to be heard when Visa determines merchant liability or calculates the amount of allowed recovery.

41. Under ADCR, Visa uses a "common point of purchase" ("CPP") procedure that purportedly identifies merchants where an "account compromise event" may have occurred. For an account compromise event to qualify for the ADCR process, the event must involve a minimum of 10,000 U.S. Visa account numbers. If fewer than 10,000 account numbers are compromised at a merchant location, an issuer cannot pursue recovery of its supposed financial losses from the merchant's acquirer through ADCR.

42. Visa will determine whether a breach occurred, and assess ADCR fines against the acquirer (and therefore, the merchant), based on the results of a CPP procedure. No direct proof of a data breach, nor any proof of actual fraud loss on the part of the issuers, is required. Visa does not require proof that any of the alleged fraud loss was caused by the supposed data breach.

43. MasterCard has an issuer reimbursement program substantially similar to ADCR, called the Account Data Compromise Issuer Recovery (“IR”) program.

44. Cisero’s is subject to these programs by virtue of the terms of its Merchant Agreement incorporating Visa’s and MasterCard’s rules, including the provisions that enable U.S. Bank to pass along any fines imposed due to violations of the rules.

45. CISP, SDP, ADCR and IR fines are a substantial revenue source for the payment networks, especially in light of the high rates of counterfeit payment card fraud in the U.S. resulting from the outdated security features of American credit and debit cards. In the U.S., Visa and MasterCard and issuing banks like U.S. Bank utilize payment cards with 1970s vintage fraud-prone magnetic stripe technology. Counterfeiters can easily write magnetic stripe data and clone payment cards. Outside of the U.S., countries use EMV [Europay-MasterCard-Visa] “smart cards” that contain an embedded microchip. Smartcards are extremely difficult to copy and use without authorization. As a consequence, counterfeit payment card fraud is substantially more prevalent in the United States than in countries that use EMV smart cards (which includes every OECD country other than the U.S.), and the POS systems of U.S. merchants – who have no control over payment card technology – are constantly targeted by hackers and counterfeiters.

### **Cisero's Enhanced Its Data Security System in 2005**

46. Cowan's Retail Systems, Inc. ("Cowan's") is a local distributor, installer, and maintenance provider of POS systems used by merchants to accept credit and debit card payments. Since 1985, Cisero's has retained and relied on Cowan's to provide, install, and maintain a POS system at Cisero's to accept payment by debit and credit cards.

47. Cisero's system had the same security features as many other restaurants across the country. The particular system that Cisero's used is also used by restaurants such as T.G.I. Fridays and Pizza Hut.

48. On or about October 24, 2005, Cowan's sent Cisero's a letter advising it to upgrade to a POS system that was compliant with the PCI Data Security Standards and to ensure magnetic stripe data from payment cards would not be stored on Cisero's point-of-sale system.

49. Cisero's immediately asked Cowan's to take the steps needed to upgrade the POS system Cowan's had installed. Cowan's accordingly instructed Cisero's concerning how to adjust the settings on its POS system's software so that it would not store full track magnetic stripe data. Cisero's followed Cowan's instructions and changed the settings accordingly.

50. After these adjustments, Cisero's needed to contact Merchant Link, a third party payment gateway through which payment card transactions are processed, to obtain cardholder information, such as to reprocess payments or for refunds. Because it needed to call out to an external service, Cisero's thus reasonably assumed that no magnetic stripe data was stored or could be stored on its system. Indeed, Cisero's had no idea such data was being stored, nor would any average computer user -- a point confirmed by two subsequent forensic audits. Even

Visa's alert to acquiring banks in October 2007, discussed below, stated that, "Often times, payment applications store prohibited data, post-authorization, without the merchant's or agent's knowledge."

51. At no point did U.S. Bank or Elavon ever check to ensure that Cisero's and its POS system was compliant with the PCI DSS standards.

#### **Elavon Notifies Cisero's of an Alleged Data Breach**

52. In March 2008, Elavon notified Cisero's that payment cards used at Cisero's may have been accessed, counterfeited, and fraudulently used elsewhere. This notification was based on notice from Visa to U.S. Bank.

53. Cisero's took immediate action. Ms. McComb called the Park City Police Department. Mr. McComb drove to U.S. Bank in Park City and spoke with bank employees about the supposed breach. None of these employees knew anything about the alleged data breach or PCI DSS compliance.

54. Cisero's contacted Cowan's and ultimately paid \$41,000 to replace its POS system with a new POS system.

55. Cisero's conducted two separate, comprehensive security audits of all records for evidence of any "internal" fraud – such as card-skimming. These audits found no evidence of internal fraud. Elavon requested, and Cisero's promptly produced, information concerning Cisero's data security, including a comprehensive "Merchant Action Plan" and an "Internet Security Policy."

### **Two Forensic Audits Found No Evidence of a Data Breach**

56. Elavon requested that Cisero's undergo a forensic investigation and provided the names of six forensic companies approved and certified by Visa and MasterCard. Cisero's selected Cybertrust.

57. The Cybertrust forensic investigation resulted in a report that Cisero's shared with Elavon.

58. Cybertrust noted that "[a]nalysis revealed no concrete evidence that the POS server suffered a security breach which led to the compromise of cardholder data indicated by the CPP [common point of purchase] analysis." The report also stated that Cybertrust's "[a]nalysis of the original POS server's two hard drives revealed no evidence of intrusive, malicious, or unauthorized activity that may have resulted in a security breach." While Cybertrust did point out certain alleged PCI violations, including storage of magnetic stripe data, the report does not contain any evidence demonstrating a data breach at Cisero's.

59. In or about January 2009, Cisero's hired a second company, Cadence Assurance ("Cadence"), to perform a forensic investigation of its POS server and network. Cadence confirmed Cybertrust's conclusion that no direct evidence existed demonstrating a data breach at Cisero's. Cadence also found that card data was located in complex, hidden database files that would not be readily apparent to hackers (let alone Cisero's employees). Neither report provided any evidence to suggest that a typical authorized user of Cisero's POS system would be aware that the system was storing cardholder data.



**Forensic Audits Find No Evidence That 10,000 Individual Visa Account Numbers Were Involved in the Alleged Breach**

60. Visa's ADCR process – and the associated liability for substantial fines – is not triggered if fewer than 10,000 individual Visa account numbers are “involved” in the alleged breach. Because of this threshold, U.S. Bank and Elavon should have required Cybertrust to report the number of unique Visa account numbers involved. Instead, Cybertrust reported an inflated number of “instances” of account numbers stored on the server, including 22,700 “instances” of Visa cards, rather than the number of unique accounts.

61. Each transaction record is an “instance” for a single account, and when a restaurant customer uses a payment card, a transaction record – or “instance” – may be generated multiple times. Cadence de-duplicated the data and found there were only 8,107 “unique” Visa account numbers on the POS hard drive. Had Cybertrust or Visa de-duplicated the data, Visa would have found fewer than 10,000 individual Visa account numbers involved, and the ADCR process would not have been initiated against Cisero's.

**Without Challenge, U.S. Bank and Elavon Agreed to Pay Fines and Assessments Visa Unilaterally Imposed on Cisero's**

62. In late June 2008, Elavon advised Cisero's that it would withdraw \$5,000 from Cisero's operating account at U.S. Bank containing deposits from payment card settlements. Elavon further advised Cisero's that it had to complete a “Self Assessment Questionnaire” and a “Certificate of Compliance” with PCI standards by July 18, 2008, or additional fines could be assessed and withdrawn from Cisero's U.S. Bank account.

63. Although the deadline offered little time to comply, on July 9, 2008, Cisero's completed and returned the Questionnaire and Attestation of Compliance and other requested documents to Elavon.

64. Cisero's subsequently learned that Elavon's requests were made in response to a June 20, 2008 letter from Visa to U.S. Bank, which was only made available to counsel for Cisero's on September 11, 2008. In that letter, Visa stated that it had assessed a "fine of \$5,000" following its determination that Cisero's had been found "non-compliant" with Visa's CISP security program. The letter demonstrated the punitive nature of these fines:

If Cisero's Ristorante and Nightclub does not demonstrate CISP compliance within 30 days from the date of this letter, U.S. Bank will be assessed a monthly fine of \$5,000. If Cisero's Ristorante and Nightclub does not demonstrate CISP compliance within 90 days from the date of this letter, U.S. Bank will be assessed a monthly fine of \$10,000. Monthly fines may be subject to further escalation if Cisero's Ristorante and Nightclub does not demonstrate CISP compliance within 180 days of this letter.

These escalating fines would be assessed whether or not Visa or its issuers suffer any fraud losses due to Cisero's non-compliance.

65. In response to Visa's letter, U.S. Bank unilaterally deducted the \$5,000 Visa fine from Cisero's funds on deposit at the bank on July 7, 2008.

66. On July 18, 2008 – again without notice to Cisero's – Visa advised U.S. Bank that its ADCR review committee had reviewed the facts and had preliminarily determined that the alleged data breach qualified for ADCR processing. Visa alleged that the process was based on a review of 32,581 accounts claimed to have been stored on the Cisero's system. This number, which was not explained, differed considerably from Cadence's finding of only 8,100 account

numbers and even from Cybertrust's count of 22,700 "instances" of Visa credit and debit card account numbers.

67. Using its own unexplained methodology, Visa then estimated the "actual fraud" caused by Cisero's non-compliance to be \$1.26 million, which number it then apparently adjusted based on a "baseline" of the ordinary amount of fraud across the Visa system. Visa arrived at an estimate of this "incremental fraud" caused by Cisero's non-compliance and added recovery for operating expenses for issuers, for a total of \$521,600. Visa then "capped" U.S. Bank liability at \$55,000, "assuming Cisero's Ristorante and Nightclub . . . and US Bank and any related agents fully cooperate with the compromise investigation (e.g., providing information within the requested timeframes, demonstrating satisfactory progress toward remediation of PCI DSS violations)."

68. In October 2008, Visa performed its "final ADCR liability calculations." Visa calculated the "total event fraud" to be \$1.33 million and Cisero's "total pre-cap liability" to be \$511,513.41. Visa once again failed to explain how it arrived at these calculations or provide any supporting documentary evidence. These various shifting numbers based on unexplained calculations demonstrate that the ADCR process is little more than a scheme to extract steep financial penalties from small merchants such as Cisero's for the benefit of Visa.

69. Accompanying Visa's Qualification Summary forwarded to Cisero's counsel in September 2008 was "What Every Merchant Should Know About the New Account Data Compromise Recovery Program." This was the first time Cisero's was made aware of the existence and contents of this document.

70. On July 31, 2008, MasterCard advised U.S. Bank that although it could have imposed a “non-compliance assessment of up to USD 100,000 for the storage of magnetic strip data” at Cisero’s, it was imposing an assessment of only \$15,000. In contrast to Visa’s invocation of its ADCR program, the letter stated that, “MasterCard has elected not to administer an issuer reimbursement process” as allowed by MasterCard rules, for costs from the alleged violation.

**U.S. Bank and Elavon Agree to Pay MasterCard Issuers for Damages  
Arising from the Alleged Data Breach Without Challenging the Claims**

71. Although MasterCard did not invoke the IR process, in September and October 2008, multiple MasterCard issuers, including RBS Citizens Bank (“RBS”) and Chase, initiated “compliance cases” against U.S. Bank to recover damages alleged to be the result of fraud at other merchant locations allegedly caused by Cisero’s. These fraudulent cards were allegedly counterfeited using cardholder data stolen from Cisero’s system.

72. Compliance cases such as these are filed with MasterCard and ultimately presented to the acquiring bank. If the acquiring bank challenges the claim, it goes through an adjudication process. U.S. Bank and Elavon thus had an opportunity to challenge the claims, but Cisero’s is unaware of any evidence that U.S. Bank or Elavon did so. Rather, it appears that they simply agreed to pay the claims without question. In fact, Elavon sent Cisero’s “pre-compliance” letters alerting it to some of the claims. In some instances, these letters were sent to Cisero’s after the purported date to contest the claims. Cisero’s responded to Elavon’s letters, denying that the claims had anything to do with Cisero’s. RBS’s and Chase’s alleged damages

totaled \$13,849.80. Of this amount, Elavon unilaterally deducted approximately \$5,172 from Cisero's funds on deposit with U.S. Bank, and in this action Elavon asserts U.S. Bank's claim for the remainder.

73. Cisero's was never given a meaningful opportunity to provide evidence on its behalf. This was prejudicial to Cisero's because Cadence later found that most of the claimed chargebacks reported by RBS and Chase involved credit cards that were not even found in the data files located on the Cisero's POS server hard drives.

74. The reimbursement claims initiated by RBS and Chase were not adjudicated pursuant to MasterCard's compliance process. Upon information and belief, U.S. Bank and Elavon are not required to reimburse those issuers outside of the MasterCard-adjudicated compliance processes.

**U.S. Bank and Elavon Failed to Give Cisero's an Opportunity  
to Defend Itself or Appeal the Fines**

75. At no time has Elavon, U.S. Bank, Visa, MasterCard, or any other entity proven that a data breach occurred at Cisero's, that issuers actually suffered fraud losses, or that any such losses were caused by a data breach at Cisero's.

76. Notwithstanding these facts, neither U.S. Bank nor Elavon ever gave Cisero's an opportunity to present evidence in its defense before Visa and MasterCard assessed the fines.

77. Moreover, Visa's June 20, 2008 letter to U.S. Bank notifying it of the \$5,000 Cisero's fine and Visa's July 18, 2008 letter notifying U.S. Bank of the preliminary ADCR liability carried with them 30-day appeal rights. Remarkably, to appeal this \$5,000 fine, U.S.

Bank would have first had to pay a non-refundable \$5,000 fee, which would be added to a merchant's indemnification liability.

78. To make matters worse, Elavon first notified Cisero's of these appeal rights after the time for such appeals had expired.

79. In a September 11, 2008 letter to Cisero's counsel, Elavon attempted to rationalize its failure to provide Cisero's with the opportunity to appeal the card networks' assessments, or timely notice that any opportunity for appeal existed, stating:

[A]ny appeals in connection with assessments would have had to have presented along with the non-refundable filing fees within 30 days of the original notice of the fine or assessment . . . however, given the nature of the ADCR assessment and the MasterCard determination to not initiate an issuer reimbursement process, along with the absence of any new facts or circumstances bearing on the original decision and determination, the merits of any appeals of these fines would have been highly questionable at best.

80. This explanation is incorrect, as the merits of Cisero's appeal would have been strong. Upon information and belief, it is also a pretext. Rather than facilitate a meaningful appeal, Elavon agreed to pay the fines without protest knowing it would be fully indemnified by Cisero's.

81. Elavon had good reason to question the suspicious amount of fraud reported by Visa, which was far out of proportion to figures reported by other networks. Visa reported an "actual total fraud for the event" of \$1.26 million, resulting in fraud liability plus operating expense recovery of \$521,600. By contrast, MasterCard issuers only submitted documentation for claims of approximately \$13,850. American Express and Discover made no assessments,

presumably because there were no actual fraud losses despite the fact that, in the case of American Express, thousands of cards were supposedly stored on Cisero's server – more than the number of MasterCard cards.

**U.S. Bank and Elavon Failed to Give Cisero's Adequate  
Information Regarding Network Data Security Rules**

82. Before Elavon notified Cisero's in March 2008 of a potential data breach, no one at U.S. Bank ever mentioned anything about PCI DSS to Ms. McComb. This is despite the fact that, dating from the commencement of the Merchant Agreement, Ms. McComb made hundreds of visits to U.S. Bank and had frequent business interactions with its employees.

83. In September 2008 correspondence with Cisero's counsel, Elavon claimed that it had provided Cisero's with adequate notice of the PCI standards as well as the Visa CISP and MasterCard SDP security programs. This notice consisted of inconspicuous cross-references to these programs and web site addresses on a total of six monthly hard copy U.S. Bank statements scattered throughout the period of March 2005 to October 2007, sent via U.S. mail to Cisero's. Yet the restaurant keeps detailed accounting records electronically and reconciles its balances on a daily basis based on electronic banking data. U.S. Bank's monthly statements are not used by Cisero's.

84. In an October 29, 2008 letter, Elavon claimed that "compliance with the card associations' rules and regulations as well as securing the cardholder data associated with the acceptance of a credit card remained *solely* a merchant responsibility. Compliance with the involved card association's security is not and has never been an acquirer responsibility . . . ."

(Emphasis added.) Elavon is wrong. The card networks expressly hold acquirers responsible for their merchants' compliance with their security rules and require affirmative acquirer outreach to merchants to ensure such compliance.

85. For example, in May 2007, Visa issued a Bulletin to its acquirers (such as U.S. Bank) reminding them that the Visa CISP "requires acquirers to ensure that their merchants maintain compliance with the . . . CISP . . . ." Visa instructed acquirers to submit a merchant compliance plan for merchants such as Cisero's by July 31, 2007. Indeed, Visa told its acquirers to give restaurants priority in those compliance efforts because "over the past year, Visa has found restaurants to be targeted [by those seeking account data] more than any other merchant industry segment."

86. In October 2007, Visa issued alerts termed "a call to action for all acquirers" concerning the fact that many POS systems were "designed to store" full magnetic stripe data. The alerts stated that "corrective action must be taken immediately" and that it was "critical that acquirers ensure that their merchants and agents do not use payment applications known to retain prohibited data elements and that acquirers take corrective action to address any identified deficiencies as these applications are at risk of being compromised." The alerts noted that "merchants are at high risk of being compromised" and that "[h]ackers, who know that many merchant systems store prohibited data, are targeting agents and merchants using vulnerable payment applications, and exploiting vulnerabilities to find this data."



87. The Visa alerts also contained a list of widely used POS systems that stored magnetic stripe data. Elavon and U.S. Bank should have verified whether Cisero's POS system was on this list.

88. Visa stated that the alerts were "confidential" and were not to be made publicly available.

89. As with Visa, MasterCard's Rules dated October 2008 state "[t]he Acquirer is responsible for ensuring that each of its Merchants complies with the Standards, and the Acquirer is itself responsible to the Corporation and to other Members for any Merchant's failure to do so. The Acquirer must take such actions that may be necessary or appropriate to ensure the Merchant's ongoing compliance with the Standards."

90. MasterCard's July 31, 2008 letter notifying U.S. Bank of its \$15,000 non-compliance assessment also contained the following admonishment: "As a best practice, your organization [U.S. Bank] should consider an SDP [Site Data Protection] Program implementation process for your entire merchant base to minimize the risk of future account data compromise events."

91. Tellingly, Elavon attempted to cover up its failure to have such a program in place by redacting this admonishment when it provided a copy of the MasterCard letter to Cisero's counsel on September 11, 2008. Cisero's only received an unredacted copy of this letter as part of discovery in subsequent litigation.

### **U.S. Bank and Elavon Disregard the Cadence Report**

92. In addition to undermining Visa's claim that there are more 10,000 account numbers involved, the Cadence report also concluded:

- a. No evidence exists supporting a conclusion that Cisero's systems had been hacked.
- b. No evidence exists supporting a conclusion that Cisero's employees stole payment card data.
- c. No evidence exists supporting a conclusion that payment card data of any kind was improperly taken from Cisero's systems.

Cisero's provided a copy of the Cadence report to Elavon in January 2009, and Elavon purportedly forwarded the report to Visa and MasterCard.

93. Nevertheless, in a May 6, 2009 letter, Elavon disregarded the Cadence report:

We have been advised by Visa and MasterCard that the fines as issued and assessed will stand and there will be no reduction, mitigation, waiver, or elimination of the fines as placed against the Cisero's merchant relationship. . . . Also, as had been previously communicated, Cadence Assurance is not a certified forensic examiner for either Visa or MasterCard and their analysis comes appreciably after the fact and long after the intrusion events giving rise to the data compromise and the original investigation and analysis completed by Cybertrust.

Consequently, Elavon insisted that it be paid the outstanding amount of fines, penalties, assessments and chargebacks.

94. Elavon improperly discounted the Cadence report. For years, Cadence has provided a wide range of high-quality internal audit and PCI compliance services and is now certified by the PCI council as a Qualified Security Assessor. Moreover, Elavon's statement that Cadence's analysis "comes long after the intrusion events" is wrong – neither Cybertrust nor

Cadence found any evidence of “intrusion,” and Cadence performed its analysis on the same system that Cybertrust analyzed, which had been disconnected and stored securely as soon as Cisero’s was notified of the alleged breach.

### **Damages and Cisero’s Potential Exposure**

95. As a result of Elavon’s and U.S. Bank’s conduct, Cisero’s has suffered significant financial harm for a business its size. Elavon withdrew approximately \$10,172.02 from Cisero’s bank account without Cisero’s consent. Cisero’s also faces potential liability for the remainder of the CISP, SDP, and ADCR fines from Visa, MasterCard, and issuer reimbursement claims, which total approximately \$78,677.78. Cisero’s also incurred \$5,456.25 in expenses for hiring Cadence.

96. Cisero’s has suffered from lost productivity of its owners and employees. U.S. Bank’s and Elavon’s conduct has taxed Cisero’s management. The time expended by Cisero’s trying to resolve the dispute, necessitating hundreds of emails and phone calls, was time that should have been devoted to managing Cisero’s.

97. Cisero’s has suffered reputational harm as a consequence of U.S. Bank and Elavon’s misconduct.

98. As a result of U.S. Bank and Elavon’s actions, Cisero’s actual or threatened damages include:

- a. Liability for fines from Visa totaling \$60,000;
- b. Liability for fines from MasterCard totaling \$15,000;
- c. Issuer claims totaling approximately \$14,000;

- d. Payment to Cadence totaling approximately \$5,456.25;
- e. Lost productivity of Cisero's owners and employees;
- f. Damage to Cisero's and Ms. McComb's reputation;
- g. Emotional distress to Ms. McComb;
- h. Interest;
- i. General, special, and punitive damages; and
- j. Attorney's fees, costs, and legal expenses.

### **FIRST CAUSE OF ACTION**

#### **AGAINST U.S. BANK AND ELAVON**

##### **(Declaratory Judgment)**

99. Cisero's incorporates by reference all preceding allegations.

100. Cisero's is entitled to a declaratory judgment that Cisero's is exonerated as an indemnitor to U.S. Bank and Elavon.

101. There are several bases for this declaratory judgment, including: (a) that there was no meeting of the minds; (b) that the Merchant Agreement is an unenforceable contract of adhesion; and (c) that U.S. Bank and Elavon breached its duty of good faith good faith to Cisero's, as further explained below.

102. The MTOS grants U.S. Bank broad indemnification rights against Cisero's.

103. An indemnitee owes a duty of good faith to its indemnitor. Any act of the indemnitee which prejudices the rights of the indemnitor will release his obligation to the extent of the prejudice.

104. U.S. Bank and Elavon breached their duties of good faith to Cisero's, exonerating it as an indemnitor, in the following ways:

a. Neither U.S. Bank nor Elavon ever gave Cisero's an opportunity to defend itself in the initial phase before the CISP, SDP, and ADCR fines were assessed. Nor did U.S. Bank or Elavon appeal the fines. In fact, Elavon informed Cisero's of the fines only after the 30-day appeal window had elapsed.

b. U.S. Bank and Elavon agreed to pay the fines to Visa and MasterCard without demanding proof of a data breach, fraud losses, or a causal connection between the two, because U.S. Bank and Elavon knew they would be indemnified by Cisero's.

c. Neither U.S. Bank nor Elavon should have paid the ADCR assessments. The ADCR process should not even have been triggered. Visa's ADCR process is only triggered where the account compromise involves at least 10,000 Visa account numbers, and, as explained above, that threshold was not reached. Elavon apparently paid the fees nevertheless.

d. Prior to agreeing to pay the ADCR fines, U.S. Bank and Elavon should have investigated the suspicious amount of fraud reported by Visa, which was out of proportion to the other card associations' numbers. Visa reported "total event fraud" to be a staggering \$1.33 million and Cisero's "total pre-cap liability" to be \$511,513. Yet MasterCard imposed no equivalent ADC IR fines, and the RBS and Chase chargebacks allegedly resulting from a data breach at Cisero's totaled approximately \$14,000.

American Express and Discover made no claims at all, presumably because there were no

actual fraud losses despite the fact that, in the case of American Express, thousands of cards were supposedly implicated (more than the number of MasterCard cards). Further, the ADCR assessments are unenforceable penalties because they are punitive assessments, and are neither damages nor a reasonable approximation of damages.

e. U.S. Bank and Elavon should have refused to pay the CISP and SDP fines because they are unenforceable penalties. They are imposed for violating a security standard regardless of whether a data breach actually occurred or any cardholder information was actually stolen, and, upon information and belief, are imposed as punishment and bear no relation to any financial damages actually sustained by issuers, Visa or MasterCard.

f. U.S. Bank and Elavon should have refused to pay the RBS and Chase claims because they were not brought as the result of a MasterCard compliance process adjudication.

g. U.S. Bank and Elavon should have refused to pay the RBS and Chase claims absent proof of a data breach at Cisero's. As explained in the Cadence report, most of the claimed chargebacks reported by RBS and Chase were against credit cards that were not found in the data located on the Cisero's POS server hard drives. Nevertheless, U.S. Bank and Elavon agreed to reimburse Chase and RBS for all of the claimed chargebacks without further question.

h. U.S. Bank and Elavon should have verified that Cisero's payment system complied with standards established by Visa and MasterCard regarding data security.

105. Based on the above, Cisero's is entitled to a declaratory judgment that Cisero's is not required to indemnify U.S. Bank or Elavon for fees paid or owed to Visa, MasterCard, RBS, or Chase because U.S. Bank and Elavon breached its duty of good faith to Cisero's, its indemnitor.

**SECOND CAUSE OF ACTION**  
**AGAINST U.S. BANK AND ELAVON**  
**(Negligence)**

106. Cisero's incorporates by reference all preceding allegations.

107. U.S. Bank is the fifth largest commercial bank in the country, and is a top five domestic merchant acquirer and a top-ten global merchant acquirer. U.S. Bank is also the seventh largest payment card issuer in the United States.

108. As one of the country's largest payment processors, Elavon had expertise in data processing and data security. Elavon's merchant customers, especially merchants like Cisero's who do not have any payment processing expertise, rely on Elavon to keep them informed and educated regarding their payment processing and security obligations. Elavon acknowledges this on its website, noting that "[e]very day, more than 1 million merchants trust us to efficiently and securely manage their payments business." Elavon also claims on its website that "[w]hen you choose us as your payments processor, you're getting a partner you can count on, backed by a team of professionals dedicated to meeting your needs."

109. Cisero's reasonably relied on U.S. Bank and Elavon to inform Cisero's of its obligations regarding Visa's and MasterCard's data security standards, and ensure that Cisero's met these standards because U.S. Bank and Elavon had a duty to do so.

110. U.S. Bank and Elavon breached this duty. From the commencement of the Merchant Agreement until Elavon notified Cisero's of the PCI-related fines in 2008, Ms. McComb made hundreds, perhaps more than a thousand, visits to U.S. Bank and had frequent interaction with its executives. At no point did anyone at U.S. Bank mention anything about PCI DSS standards to Ms. McComb, even though the network rules were not public.

111. At the same time, Visa did not publicly release its operating rules until *after* the alleged data breach.

112. The only notice Elavon or U.S. Bank provided to Cisero's of the networks' requirements concerning data security were inconspicuous references contained on six monthly statements.

113. Nor Elavon nor U.S. Bank did anything to "securely manage" Cisero's system or to verify that Cisero's payment system was secure and compliant with network rules.

114. U.S. Bank and Elavon also had a duty to provide Cisero's with an opportunity to present exonerating evidence or contest the fines imposed by Visa and MasterCard, and to inform Cisero's of its appeal rights in connection with the fines.

115. U.S. Bank and Elavon breached this duty by failing to inform Cisero's of the fines until after they were assessed and after the 30-day appeal period had expired.



116. The fees Visa and MasterCard assessed purportedly against U.S. Bank (but in reality, against Cisero's) were based on Cisero's alleged non-compliance with Visa and MasterCard data security standards and because of alleged data breaches that supposedly led to issuer losses.

117. The fees assessed against Cisero's were the foreseeable result of U.S. Bank and Elavon's negligence. If not for their negligence, Cisero's could have complied with Visa's and MasterCard's security standards and/or could have successfully contested the CISP, SDP, and ADCR fines. Neither U.S. Bank nor Elavon demanded proof that the supposed data breach or alleged fraud losses originated at Cisero's.

118. U.S. Bank and Elavon were also negligent in agreeing to reimburse RBS and Chase for their purported financial losses. RBS's and Chase's claims were not made pursuant to a MasterCard compliance adjudication, and neither U.S. Bank nor Elavon demanded proof that the supposed data breach or alleged fraud losses originated at Cisero's. In fact, the Cadence report later confirmed that most of the claimed chargebacks could not have been the result of a data breach at Cisero's.

119. As a result of U.S. Bank and Elavon's negligence, Cisero's has been damaged in an amount to be proved at trial.

### **THIRD CAUSE OF ACTION**

#### **AGAINST U.S. BANK AND ELAVON**

#### **(Breach of the Covenant of Good Faith and Fair Dealing)**

120. Cisero's incorporates by reference all preceding allegations.

121. U.S. Bank and Elavon's assessment of fines based on Cisero's purported failure to comply with Visa's and MasterCard's rules violates the covenant of good faith and fair dealing because U.S. Bank and Elavon unjustly hindered Cisero's ability to comply with those rules.

122. Visa's and MasterCard's fees assessed against U.S. Bank are the result of U.S. Bank and Elavon's failure to inform Cisero's of its obligations regarding data security. With respect to the fines assessed by Visa and MasterCard, U.S. Bank and Elavon failed to perform their good faith obligations, including: (a) promptly informing Cisero's of the fines; (b) affording Cisero's an opportunity to present exonerating evidence or contest the fines; (c) challenging the fines; (d) informing Cisero's of the 30-day time limit to appeal the fines; and (e) failing to demand proof that the supposed data breach or alleged fraud losses originated at Cisero's. The RBS and Chase claims assessed against U.S. Bank and Elavon are also the result of U.S. Bank and Elavon's failure to inform Cisero's of its obligations regarding data security. U.S. Bank and Elavon failed to perform their good faith obligations to challenge the compliance cases and seek an adjudication.

123. Had U.S. Bank and Elavon not failed in their good faith obligations, Cisero's would have been able to successfully contest the fines, and Elavon could have successfully contested RBS and Chase's compliance claims.

124. Despite U.S. Bank and Elavon's frustration of Cisero's ability to perform under the contract, they assessed fines against Cisero's, pursuant to the MTOS's indemnification provision, based on Cisero's purported failure to comply with Visa and MasterCard rules.

125. As a result of U.S. Bank and Elavon's breach of the implied covenant of good faith and fair dealing, Cisero's has been damaged in an amount to be proved at trial.

#### **FOURTH CAUSE OF ACTION**

#### **AGAINST U.S. BANK AND ELAVON**

#### **(Breach of Contract)**

126. Cisero's incorporates by reference all preceding allegations.

127. Cisero's entered into the Merchant Agreement, which incorporates by reference the MTOS, with U.S. Bank.

128. Section 11.A. of the MTOS states that Cisero's reserve account "shall serve as a fund available to U.S. Bank to enforce any and all obligations and liabilities of [Cisero's] to U.S. Bank arising under this MTOS."

129. Section 11.B. states that "U.S. Bank may withdraw funds from the Reserve Account at any time without notice to Merchant in the amount of any obligation or liability of Merchant to U.S. Bank hereunder."

130. U.S. Bank and Elavon therefore could only deduct funds from the Reserve Account to enforce Cisero's obligations to U.S. Bank, and only in an amount of that obligation or liability.

131. U.S. Bank and Elavon withdrew funds from Cisero's U.S. Bank account, not the Reserve Account. This account contained funds unrelated to the Merchant Agreement, such as funds deposit pursuant to Cisero's agreement with American Express.

132. In addition, despite the MTOS's indemnification clause, Cisero's was not required to indemnify U.S. Bank or Elavon for the fines and penalties levied on U.S. Bank by Visa and MasterCard because (a) Cisero's was never given notice of changes to the card association's non-public rules; (b) the card association rules were changed without Cisero's consent; (c) upon information and belief, Elavon did not actually pay the fines to Visa and MasterCard; (d) the fines are unenforceable penalties; and (e) neither U.S. Bank nor Elavon demanded proof that the supposed data breach or alleged fraud losses originated at Cisero's.

133. Elavon nevertheless withdrew funds from Cisero's bank account, without notice to Cisero's and without Cisero's permission, as purported indemnification for Visa's CISP and ADCR fines, MasterCard's SDP fines, and chargeback claims from issuers.

134. Elavon's withdrawal of funds was a breach of the Merchant Agreement.

135. As a result of U.S. Bank and Elavon's breach of contract, Cisero's has been damaged in an amount to be proved at trial.

### **FIFTH CAUSE OF ACTION**

#### **AGAINST U.S. BANK AND ELAVON**

##### **(Conversion)**

136. Cisero's incorporates by reference all preceding allegations.

137. Cisero's maintained a merchant bank account at U.S. Bank into which Cisero's funds from its customers' electronic payments were deposited and held, along with funds from other sources.

138. At various times from June 2008 through October 2008, U.S. Bank and Elavon improperly withdrew, and converted for their own use, a total of \$10,172.02 from Cisero's account. Cisero's was at the time, and still is, entitled to possession of those funds.

139. U.S. Bank and Elavon willfully interfered with Cisero's ability to possess and use the funds.

140. U.S. Bank and Elavon's interference was without lawful justification.

141. As a result of U.S. Bank and Elavon's conversion, Cisero's has been damaged in an amount to be proved at trial.

#### **SIXTH CAUSE OF ACTION**

#### **AGAINST U.S. BANK AND ELAVON**

#### **(Breach of Fiduciary Duty)**

142. Cisero's incorporates by reference all preceding allegations.

143. By virtue of their relationships with Cisero's, U.S. Bank and Elavon owed Cisero's a fiduciary duty.

144. U.S. Bank and Elavon breached that fiduciary duty.

145. U.S. Bank's and Elavon's breaches of fiduciary duty were the actual and proximate causes of damages to Cisero's in an amount to be proved at trial.

**WHEREFORE**, Cisero's and Ms. McComb demand judgment against U.S. Bank and Elavon as follows:

- A. On the First Cause of Action, for a declaratory judgment that Cisero's is exonerated as an indemnitor to U.S. Bank and Elavon.

- B. On the Second Cause of Action, for damages in an amount to be proven at trial, plus pre- and post-judgment interest, costs, and reasonable attorney's fees.
- C. On the Third Cause of Action, for damages in an amount to be proven at trial, plus pre- and post-judgment interest, costs, and reasonable attorney's fees.
- D. On the Fourth Cause of Action, for damages in an amount to be proven at trial, plus pre- and post-judgment interest, costs, and reasonable attorney's fees.
- E. On the Fifth Cause of Action, for damages in an amount to be proven at trial, plus punitive damages, pre- and post-judgment interest, costs, and reasonable attorney's fees.
- F. On the Sixth Cause of Action, for damages in an amount to be proven at trial, plus punitive damages, pre- and post-judgment interest, costs, and reasonable attorney's fees.

## **JURY DEMAND**

Cisero's reaffirms its demand for trial by jury on all issues so triable.

DATED this 8th day of August, 2011

DEWSNUP, KING & OLSEN

---

David R. Olsen  
Ralph L. Dewsnap  
DEWSNUP, KING & OLSEN  
36 South State St., Suite 2400  
Salt Lake City, UT 84111-0024  
Telephone: (801) 533-0400  
Facsimile: (801) 363-4218

- and -

CONSTANTINE CANNON LLP  
W. Stephen Cannon  
Todd Anderson  
Richard Levine  
One Franklin Square  
1301 K Street, N.W., Suite 1050 East  
Washington, DC 20005  
(202) 204-3500  
*Pro hac vice applications forthcoming*  
A. Owen Glist  
David A. Scupp  
335 Madison Avenue  
New York, NY 10017  
(212) 350-2700  
*Pro hac vice applications forthcoming*

*Attorneys for Cisero's and Theodora McComb*