LITIGATION UPDATE: THE *CISERO'S* CASE

CHALLENGING CARD NETWORK ENFORCEMENT MECHANISMS

By
W. Stephen Cannon
Richard O. Levine
Constantine Cannon LLP

The Hospitality Law Conference
February 8, 2012

ABOUT THE AUTHORS

W. Stephen Cannon is Chairman of Constantine Cannon LLP and the Managing Partner of Constantine Cannon's Washington, DC office. Constantine Cannon is a law firm with extensive experience in electronic payments matters, and served as lead counsel for U.S. merchants in the *Visa Check/MasterMoney* debit card litigation and the resulting settlement. The firm served as counsel to the Merchants Payments Coalition regarding its submission of comments to the Federal Reserve Board in its rulemakings implementing the payment card provisions of the Dodd-Frank Consumer Financial Protection and Regulatory Reform Act of 2010. Prior to joining the firm in 2005, Steve served as General Counsel of Circuit City Stores, Inc. for 11 years. Prior to Circuit City, Steve was a partner in a Washington law firm, and previously served as deputy assistant attorney general in the Antitrust Division of the U.S. Department of Justice, and Chief Antitrust Counsel to the U.S. Senate Judiciary Committee. He has testified before the Senate and House Judiciary Committees regarding payment card interchange fees on behalf of the Merchants Payments Coalition. Mr. Cannon can be reached at 202-204-3502, scannon@constantinecannon.com.

Richard O. Levine is of counsel to Constantine Cannon LLP. A former Director of the Office of Policy Planning of the U.S. Department of Justice's Antitrust Division, Richard's practice focuses on the intersection of competition law, government economic regulation, and technological change. He has been active in payment card issues since joining the firm in 2005. Mr. Levine can be reached at 202-204-3511, rlevine@constantinecannon.com.

Note: Constantine Cannon represents Cisero's, Inc., in the litigation discussed in this paper.

TABLE OF CONTENTS

I. INTRODUCTION AND OVERVIEW

Our 2009 *PCI Compliance Newsletter* article[1] and paper submitted for the 2010 Hospitality Law conference[2] analyzed how the major card networks—Visa and MasterCard—have made payment card acceptance an expensive and burdensome proposition. This paper reports on current litigation that seeks to challenge one such burden, the contractual provisions used by networks' to enforce their data security rules that allocate to merchants the ultimate responsibility for costs associated with alleged data security breaches.

Our prior work explained that the authentication systems used by Visa and MasterCard for credit and debit card transactions place merchants in significant financial jeopardy through the imposition of fines and assessments administered by Visa and MasterCard for alleged violations of payment card industry data security standards ("PCI-DSS"). These liabilities are then imposed on merchants through the indemnification clauses of the "merchant agreement" between the merchant and its acquiring bank (which serves as the member of the Visa and MasterCard networks) and the processor—often an affiliate of the acquiring bank—that actually processes a merchant's card authentication and sales transactions.

Card network operating rules, which are agreements between the networks and their member banks, require that acquirers' merchant agreements mandate merchant adherence to the networks' rules, including those related to PCI-DSS. In turn, the network operating rules expressly hold the acquiring bank responsible for their merchants' rule violations.

Nevertheless, the acquiring bank routinely will seek to place merchants at the bottom of a "liability cascade" and hold the merchant liable for network fines and assessments through indemnification provisions in their merchant agreements. Further, related provisions in merchant agreements permit these amounts automatically to be deducted from merchants' card acceptance cash flows.

In essence, standard provisions in merchant agreements effectively turn acquiring banks into the networks' enforcement arms. Most troubling is that in assessing penalties and liabilities, the card systems have simply presumed themselves to have governmental powers of punishment, as prosecutor, judge, and jury, based on card system operating

---

[1] W. Stephen Cannon, Constantine Cannon LLP and Michael McCormack, Palma Advisors, LLC, *"The Currency of Progress?" Visa and MasterCard arrogate Governmental Powers In the Name Of Card System Security,* PCI Compliance Newsletter for Hotels and Restaurants, Dec. 2009.

[2] W. Stephen Cannon, Constantine Cannon LLP and Michael McCormack, Palma Advisors, LLC, *The U.S. Payment Card Industry: Select Challenges and Issues from a Hospitality Industry Perspective* (2010 Hospitality Law Conference).

rules that merchants' may not have the right to see. Liability may be found through, e.g., Visa's Account Data Compromise Recovery program ("ADCR") on the basis of "common point of purchase" investigations (i.e., the most "common" merchant among a group of cards with reported fraud) and use of algorithms comparing "actual" versus "expected" fraud associated with cards used at a merchant so identified.[3] And a merchant's ability to contest a network's decision may be dependent on the actions of its acquirer.[4] This situation is particularly troubling, given Visa and MasterCard's market power—there is no practical alternative to acceptance of those systems' cards.

The legality of acquiring banks' invocation of indemnification clauses to recover such Visa and MasterCard assessments is questionable however, since network fines and "non-compliance" assessments are unenforceable penalties, designed to have an *in terrorem* effect, rather than to compensate for damages.[5] Further, impositions claiming to be damage-related (such as the Visa ADCR program) give the merchant *no* procedural rights, and thus bear the indicia of contractual unconscionability.

Indeed, use of indemnity clauses as a vehicle to collect liabilities imposed by card networks due to claimed violations of their security rules and standards is "procedurally" unconscionable because of, among other things, the bargaining disparity between merchants and the card networks (which require merchant agreements to mandate adherence to the networks' rules) and the lack of merchant input, notice, or consent, with respect to their changing requirements. They are "substantively" unconscionable because of, for example: (a) the lack of any merchant procedural rights to challenge card network analytic methods, findings, and conclusions; (b) the absolute discretion the networks have over the amount of fines, assessments, and liabilities imposed; and (c) the lack of any right of merchants to challenge card network liability determinations and financial penalties.[6]

---

[3] *See, e.g.,* Visa, Inc., "What Every Merchant Should Know About the New Account Data Compromise Process" (2006); http://usa.visa.com/merchants/operations/adcr.html#anchor_5; MasterCard, *Security Rules and Procedures- Merchant Edition* § 10.2.4.3, ADC Operational Reimbursement and ADC Fraud Recovery (Jan. 29, 2010).

[4] *See* Visa, *Visa International Operating Regulations,* at 752 (Public Ed., Apr. 1, 2010).

[5] *See Wetzler v. Roosevelt Raceway, Inc.,* 622 N.Y.S.2d 232, 235 (1st Dept. 1995) ("It is well settled that the imposition of a penalty is exclusively the prerogative of the sovereign and that a contractual provision that operates as a penalty is unenforceable."); *Leonard v. Northwest Airline, Inc.* 605 N.W. 2d 425, 431 (Minn. App. 2000) ("The rule against contract penalties is an equitable doctrine arising from a public policy against compulsion and has at its foundation the unconscionability doctrine.").

[6] *See, e.g., Resource Management Co. v. Weston Ranch and Livestock Co., Inc.,* 706 P.2d 1028, 1041 (Utah 1985) ("'Unconscionable' is a term that defies precise definition. Rather, a court must assess the circumstances of each particular case in light of the twofold purpose of the doctrine, prevention of oppression and of unfair surprise. … Recognition of these purposes has led to an analysis of unconscionability in terms of 'substantive' and 'procedural' unconscionability. 'Substantive unconscionability'

It is for this reason that we concluded our 2009 *PCI Compliance Newsletter* article with a call to action: Merchants "should be ready to challenge any effort to impose fines and penalties for claimed violations, and to prevent any automatic withholding of settlement funds as acquiring banks offset the amounts assessed on them by the card systems. One day, the test case will arise, and merchants should be prepared to act."

One such opportunity arose in 2010 when Elavon, Inc., the card-processing subsidiary of U.S. Bank, filed a collection action in Utah state court against Cisero's, Inc., a small restaurant in Park City, Utah.[7] The collection action grew out of allegations in 2008 by Visa and MasterCard that storage of account information on the restaurant's point of sale system had lead to the compromise of that data and fraud loses through the counterfeiting of cards using compromised account information. The restaurant had switched processors before the fines and assessments imposed on the acquirer by Visa and MasterCard automatically could be deducted from the restaurants' bank accounts, resulting in an amount that was claimed to be a balance due.

On September 7, 2011 Cisero's filed an Amended Answer and Counterclaim against U.S. Bank and Elavon seeking declaratory relief against invocation of the indemnification provision and damages based on claims of negligence, breach of U.S. Bank and Elavon's duty of good faith and fair dealing, breach of contract, conversion as a result of the withdrawal of funds from Cisero's account's prior to its switch of processors, and breach of fiduciary duty. U.S. Bank and Elavon moved to dismiss the negligence, conversion, and breach of fiduciary duty claims, and the motion remains pending.

The remainder of this paper describes the facts giving rise to Cisero's counterclaim and the legal theories that underlie it. The paper concludes by setting out implications of success for the counterclaim with respect to acquiring bank indemnification actions arising from card networks security standard enforcement efforts. In short, judicial resolution of key issues raised could:

- Limit acquirers' right to "self help" indemnification and create stronger financial incentives on the part of acquirers and processors to pro-actively assure merchants' compliance with data security standards;

- Lead to greater merchant procedural and substantive rights in challenging networks' data breach liability findings and damage assessments;

---

examines the relative fairness of the obligations assumed. 'Procedural unconscionability' focuses on the manner in which the contract was negotiated and the circumstances of the parties.").

[7] *Elavon, Inc. v. Cisero's, Inc. and Theodora McComb* and *Cisero's, Inc. and Theodora McComb* (counterclaim plaintiffs) *v. Elavon, Inc. and U.S. Bank National Association,* Civil No. 100500481 (Third Judicial District, Summit County).

- Determine the lawfulness of elements of the networks' enforcement process, including the imposition of fines and penalties; and

- Guide merchants in signing card processing merchant agreements.

The original Elavon complaint and Cisero's amended answer and counterclaim are attached.

II. THE FACTS BEHIND CISERO'S COUNTERCLAIM AND DEFENSES AGAINST U.S. BANK AND ELAVON

A. The Merchant Agreement

On November 28, 2001, Cisero's and U.S. Bank entered into a Merchant Agreement, in which U.S. Bank agreed to act as Cisero's acquirer for the processing of electronic payments through the Visa and MasterCard networks. Elavon, U.S. Bank's affiliate, acted as U.S. Bank's agent in providing Cisero's with payment processing services.

The one-page Merchant Agreement incorporates by reference U.S. Bank's 27-page Merchant Terms of Service ("MTOS"), which operates as a contract of adhesion. The MTOS purports to give U.S. Bank broad discretion to change the terms of the agreement, stating that U.S. Bank may "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."

The MTOS includes a requirement that Cisero's comply with Visa's and MasterCard's rules. 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 relevant to this case. Until May 2008 – after the alleged data security breach at Cisero's – these rules were treated as proprietary to the payment networks, accessible only by member issuer and acquirer banks.

The MTOS also purports to grant U.S. Bank broad indemnification from Cisero's for any claims or damages "directly or indirectly related to" any breach of the MTOS or Visa or MasterCard's rules.

Finally, the MTOS establishes Minnesota (U.S. Bank's headquarters state) as the choice-of-law jurisdiction with respect to issues of contract interpretation.

B. Visa and MasterCard's Data Security Standards and Penalties

In 2005, four years after Cisero's and U.S. Bank entered into the Merchant Agreement, both Visa and MasterCard adopted data protection standards developed by the Payment Card Industry ("PCI") Council, a group founded by the five major payment networks. Visa and MasterCard incorporated the standards into their rules, which were in turn incorporated by reference into the Merchant Agreement. Neither U.S. Bank nor Elavon apprised Cisero's of these new standards; rather, on six occasions, Elavon's billing statements contained references to the websites of the Visa and MasterCard data security programs, which Elavon claims merchants had an "obligation to investigate."

Visa and MasterCard also established programs that require acquirer validation of a merchant's compliance with PCI data security standards. U.S. Bank and Elavon failed to apprise Cisero's of these related programs. Visa and MasterCard fine acquirers for violations of Visa's and MasterCard's rules, including violations by merchants.

There is no process directly available to merchants to challenge the fines, demand proof, 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.

C. Elavon Notifies Cisero's of an Alleged Data Breach

In March 2008, Elavon notified Cisero's that, based on information received from card networks, payment cards used at Cisero's may have been counterfeited and used at other locations. Elavon then requested that Cisero's undergo a forensic investigation and provided the names of forensic companies approved and certified by Visa and MasterCard. Cisero's selected Verizon's Cybertrust unit.

While Cybertrust did point out certain alleged PCI violations, including storage of magnetic stripe data, the report did not contain any evidence demonstrating a data breach at Cisero's. Indeed, Cybertrust's report 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."

In 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. 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.

Further, Visa's ADCR process – and the associated liability for substantial assessments – is not triggered if fewer than 10,000 individual Visa account numbers are "involved" in the alleged breach. Cybertrust reported only the number of "instances" of account numbers stored on the server, including 22,700 "instances" of Visa cards, rather than the number of unique accounts. 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 Assurance de-duplicated the data, however, and found there were only 8,107 "unique" Visa account numbers on Cisero's POS hard drive.

D. Visa and MasterCard Impose Assessments on U.S. Bank

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. 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.

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 suffered any fraud losses due to Cisero's non-compliance.

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. 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.

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 . . . and U.S. 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)."

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 card-issuing banks' claimed costs from the alleged violation.

Although MasterCard did not invoke the issuer reimbursement process, in September and October 2008, multiple MasterCard issuers, including RBS Citizens Bank 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.

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.

E. Elavon and U.S. Bank Did Not Give Cisero's an Opportunity to Appeal And Attempted to Avoid the Burden for Merchant Compliance That Visa and MasterCard Place on Acquirers

Neither U.S. Bank nor Elavon gave Cisero's an opportunity to present evidence in its defense before Visa and MasterCard assessed the fines and recoveries. 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

Cisero's merchant's indemnification liability. Further, Elavon first notified Cisero's of these appeal rights after the time for such appeals had expired.

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.

Further, 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).

In fact, 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. For example, in May 2007, Visa issued a Bulletin to its acquirers 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."

As with Visa, MasterCard's Rules 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." *Rules* § 5.2.2.

MasterCard's July 31, 2008 letter notifying U.S. Bank of its $15,000 non-compliance assessment related to Cisero's 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." Elavon attempted to hide this admonishment from Cisero's by redacting this language 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.

F. Elavon Files a Collection Action and Cisero's Counterclaims

In sum, from June through October 2008, Visa and MasterCard assessed approximately $90,000 in fines and liabilities on U.S. Bank due to Cisero's claimed violation of network rules. Invoking the indemnification clause in their merchant agreement with Cisero's, U.S. Bank and Elavon unilaterally withdrew over $10,000 from Cisero's merchant account.

In response to these actions, Cisero's changed its card processor in October 2008. The result was that U.S. Bank no longer was receiving the cash flow from Cisero's card transactions from which it could deduct the networks' assessments. In May 2010, Elavon, claiming to be the assignee of U.S. Bank, filed suit in Utah state court in Summit County (Park City) to collect the remaining balance that was alleged to be due at the time Cisero's changed its payment card processor.

At no time during this entire process did Elavon, U.S. Bank, Visa, MasterCard, or any other entity prove that a data breach occurred at Cisero's, that card issuers actually suffered fraud losses, or that any such losses were caused by a data breach at Cisero's.

III. THE LEGAL ISSUES AT STAKE IN THE CISERO'S COUNTERCLAIM

A. Overview: An Unconscionable System Places Merchants at Risk

Based on the events set out in Section II, Cisero's September 7, 2011 Amended Answer and Counterclaim raises legal issues affecting: (1) the ability of an acquiring bank and its processor to seek indemnity from a merchant for fines, assessments, and other forms of financial liability imposed on an acquiring bank by the card networks; and (2) the lawfulness of Visa's and MasterCard's enforcement mechanisms as applied to merchants through the indemnification mechanism.

1. The Networks' Denial of Merchant Due Process Rights

Merchants' have no due process rights under the card networks' enforcement system as implemented by acquiring banks and processors through their merchant agreements. For example, merchants have no such rights with respect to the:

(a) Development of the PCI security standards,

(b) Development of networks rules for investigation and determination of a violation, including mandated merchant hiring of "approved" third-party incident investigators;

(c) Development an implementation of the procedures for the assessment of fines and penalties for violation;

(d) Development of the procedures for identification of the specific cards that may have been the subject of breach and of fraud that may have resulted from the alleged breach and the calculations used in a specific incident;

(e) Application of network "common point of purchase" algorithms in the case of an alleged breach and a network's determination that a merchant is causally linked to any subsequently claimed fraud or requests for card issuer reimbursement

(f) Network determinations of the actual expense and fraud reimbursement levels that will be assessed, based on network rules and data submitted by issuers;

(g) Application of network rules that grant a network broad discretion to reduce assessments based on their subjective judgment regarding a merchants' conduct before, during, and after an alleged incident, as well as the size of any potential liability compared to the merchants business or payment card volumes;[8] and

(h) Appeal of network findings, fines, and financial assessments, the ability to initiate which is vested in the acquiring bank, and which (if allowed by the acquiring bank) afford the merchant no discovery or hearing rights with respect to the card network staff members determining the appeal.

Notwithstanding this lack of due process rights, the card networks require acquiring banks' merchant agreements to incorporate provisions mandating merchant adherence to their network rules and requirements—even though those rules may be amended without notice to a merchant and without their input or consent. And, indeed as relevant to Cisero's counterclaim, without those regulations even being made publicly available. In turn, acquiring banks and processors, through the indemnification provisions of their merchant agreements, simply act as the networks' enforcement agents.

This lack of due process rights raises issues of the unconscionability of the card networks' enforcement mechanisms as applied to merchants, especially smaller businesses. In this regard, the mechanisms are procedurally unconscionable because of, among other things, the lack of merchant input, notice, or consent, with respect to their changing requirements, and they are substantively unconscionable because of, for

[8] For example, MasterCard *Security Rules and Procedures* § 10.2.4.2 states that "MasterCard may consider any actions taken by the compromised entity [the merchant] to establish, implement, and maintain procedures and support best practices to safeguard MasterCard account data prior to, during and after the ADC [Account Data Compromise] Event or Potential ADC Event, in order to relieve, partially or fully, an otherwise responsible Member [the acquirer] of responsibility with respect to" any assessments, reimbursements, fraud recoveries and/or investigative costs imposed by MasterCard.

example, the lack of any procedural rights to challenge any of their analytic methods, findings, and conclusions, the absolute discretion the networks have over the amount of fines, assessments, and liabilities imposed, and lack of any merchant appeal rights.

The Visa fine and MasterCard "non-compliance assessment" impositions are further unlawful because they are unlawful penalties: they arrogate the sovereign power to punish conduct, rather than to seek damages (which the networks attempt to do as well), and they are assessed without regard to damages (if any) in amounts that increase for repeat or continuing claimed non-compliance.

2. The Indemnity Clause and the Liability Cascade

In an apparent attempt to insulate themselves from attacks by merchants on the lawfulness of this system, the networks formally claim that they have no responsibility to the merchant for the financial consequences of this enforcement system—notwithstanding the networks' role in requiring merchants to obey their rules and imposing financial liabilities on an acquirer if the network believes that merchant-customer of the acquiring bank has violated those rules.

In the networks' view, the passing through of those liabilities is simply a matter of contract between a merchant and its acquiring bank. Indeed, Visa expressly incorporates this "plausible deniability" subterfuge into its rules, which proclaim:

> All fines imposed by Visa are fines imposed on Members. A Member is responsible for paying all fines, regardless of whether it absorbs the fines, passes them on, or increases them in billing its customer (e.g., Cardholder, Merchant). A Member must **not** represent to its customer that Visa imposes any fine on its customer.[9]

In turn, acquirers similarly attempt to insulate themselves from the consequences of the enforcement systems' flaws by invoking the merchant agreements' indemnity provisions. According to acquirers, merchants agreed to obey the networks' rules, the networks claim the merchant did not, and the merchants signed contracts saying they would reimburse the acquirer for damages arising from any liability imposed on the acquirer related to the merchant's violation (including automatic deduction of these amounts from the merchant's accounts).

As demonstrated by the conduct of U.S. Bank and Elavon, as set out in Section 2, above, invocation of the indemnity clause and automatic seizure of merchants' funds has permitted acquirers and processors to avoid their responsibilities to ensure merchant compliance with network security requirements, to not act as a merchant's advocate in dealing with networks in case of an alleged data compromise event, and to fail to invoke on merchants' behalf the limited appeal rights afforded to acquirers.

---

[9] Visa International Operating Regulations, ID#: 010410-010410-0001054 (Emphasis in original) (Apr. 2011).

Cisero's Counterclaim thus seeks damages from U.S. Bank and Elavon for their conduct in responding to the alleged security incident at Cisero's. The Counterclaim argues that this conduct both "exonerates" Cisero's from indemnifying them for penalties and assessments imposed by Visa and MasterCard. It also gives rise to U.S. Bank's and Elavon's liability to Cisero's for return of funds already taken, and for damages for negligence, breach of contract, conversion of Cisero's funds, and breach of fiduciary duty. Section B discusses Cicero's causes of action; Section C describes U.S. Bank's and Elavon's partial motion for dismissal; and Section D briefly notes current discovery efforts.

B. Cisero's Counterclaim Causes of Action

1. Declaratory Judgment as to Cisero's Exoneration as an Indemnitor

An indemnitee owes a duty of good faith to its indemnitor. Consequently, actions by an indemnitee that prejudice the rights of the indemnitor will release its obligation to the extent of the prejudice. The Counterclaim argues that, in dealing with the alleged security incident at Cisero's, U.S. Bank and Elavon breached their duties of good faith to Cisero's, exonerating it as an indemnitor, including that:

a. Neither U.S. Bank nor Elavon ever gave Cisero's an opportunity to defend itself in the initial phase before the Visa and MasterCard 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 Visa Account Data Compromised issuer expense and fraud recovery assessments. The Visa recovery process should not even have been triggered. The Visa process is only triggered where the account compromise involves at least 10,000 Visa account numbers, and, as discussed in Section II(C), that threshold was not reached. Elavon apparently paid the fees nevertheless.

d. Prior to agreeing to pay the Visa damage recovery assessments, U.S. Bank and Elavon should have challenged the high amount of fraud reported by Visa, which was out of proportion to the other card associations' numbers. Visa reported "total event fraud" to be $1.33 million and Cisero's "total pre-cap liability" to be $511,513. In contrast, actual MasterCard "compliance case" charge backs totaled around $14,000 and American Express and Discover made no claims at all. Further, the Visa 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 Visa and MasterCard non-compliance 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 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 specific MasterCard compliance claims because they were not brought as the result of a MasterCard compliance process adjudication, nor should they have been paid because there was no proof of a data breach at Cisero's.

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

The facts giving rise to Cisero's exoneration as an indemnitor similarly serve as an affirmative defense in Elavon's collection action under the merchant agreement's indemnification clause.[10]

2. U.S. Bank's and Elavon's Negligence

The Counterclaim also argues that 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 to ensure that Cisero's met these standards. The need to inform was particularly important in this instance because the networks did not publicly release their operating rules until *after* the alleged data breach. Further, neither Elavon nor U.S. Bank did anything to verify that Cisero's payment system was secure and compliant with network rules, notwithstanding the fact that the networks' operating rules squarely place the responsibility for ensure merchants' compliance with the rules on a merchant's operating bank.

In this context, the law imposes an obligation of care on service providers independent of contractual obligations. Imposition of an obligation of care is particularly appropriate in this instance because not only did the networks impose an obligation on U.S. Bank and Elavon to assure merchant compliance with the data security rules, U.S. Bank and Elavon knew that the networks would (and did) impose fines if U.S. Bank and

[10] Other affirmative defenses raised by Cisero's include that the Cisero's merchant agreement is unenforceable because it is an unconscionable contract of adhesion and void as against public policy, and that Elavon's claims are barred because the fines and assessments for which U.S. Bank and Elavon seek indemnification are unenforceable penalties.

Elavon failed in their obligations and the networks concluded merchants such as Cisero's had violated their rules. Indeed, U.S. Bank and Elavon knew that they would themselves inflict injury on their customers by withdrawing the networks' fines and penalties from merchants' accounts.

Notwithstanding this duty of care, U.S. Bank and Elavon were negligent in failing to inform Cisero's of the data security rules, in failing to assure Cisero's compliance with them, in interacting with the card networks once allegations of a data compromise were raised, and in withdrawing funds from Cisero's accounts in response to claims and assessments filed against U.S. Bank by the networks and card-issuing banks. Their negligence also included failing to provide Cisero's with timely notice of the Visa and MasterCard fines, and failing to contest those fines and to inform Cisero's of its ability to appeal.

3. Other Causes of Action

U.S. Bank's and Elavon's conduct also violated other legal obligations to Cisero's. In particular, they violated the covenants of good faith and fair dealing implicit in the merchant agreement by failing promptly to informing Cisero's of fines and assessments, and by failing to give Cisero's the opportunity to contest any findings and present exonerating evidence, to appeal the fines, and to demand proof that any losses were the result of a data breach at Cisero's. U.S. Bank and Elavon also violated specific contractual requirements regarding the accounts and manner in which funds could automatically be withdrawn to satisfy, e.g. indemnification claims. Because U.S. Bank and Elavon had no legal basis for withdrawing those funds, the parties' actions amounted to unlawful conversion of the funds so withdrawn.

Finally, the nature of the relationship between the parties created a fiduciary duty on the part of U.S. Bank and Elavon, particularly due to their control over, and access to all of Cisero's funds, as well as their "superior position" to Cisero's in the relationship to Visa and MasterCard. In turn, their actions, as set out above, constituted a breach of that duty.

B. Discovery Efforts

Discovery efforts with respect to Cisero's Counterclaim will continue during 2012. The interrogatories and document requests address not only U.S. Bank's and Elavon's interactions with Visa and MasterCard with respect to the alleged data compromise at Cisero's, but also U.S. Bank's and Elavon's administration of their responsibilities under the Visa and MasterCard data security programs.

Areas of inquiry include their record of merchants' appeals, and their steps, if any, to ensure that merchants did not use point-of-sale systems that had been identified to acquiring banks by the card networks as having potential security vulnerabilities. Discovery may also shed light on the actual procedures and considerations used by the card networks in determining that a data compromise has occurred, assessing related

fines, and calculating the issuer fraud and expense recoveries for which acquiring banks would be held responsible.

It is anticipated that depositions and the production of any expert reports will take place later in 2012.

IV. POTENTIAL IMPLICATIONS OF THE CISERO'S LITIGATION FOR THE HOSPITALITY INDUSTRY

At this early stage of litigation, of course, it is unknown what issues will proceed to final resolution and what evidence will emerge through the discovery process. However, Cisero's Counterclaims and its affirmative defenses to the U.S. Bank/Elavon collection action have the potential to help resolve key issues regarding the use of merchant agreement indemnity clauses to enforce network security regulations. Such a result may be of particular value to those in the hospitality industry, where, for example, restaurants are a frequent source of data breach claims.

Enhancing acquirer and processor incentives to work with merchants to ensure compliance with data security rules and to serve as a merchant's advocate if it desires to obtain indemnification. The ability of acquirers and processors automatically to withdraw from merchants' accounts any fines and assessments related to alleged data breaches removes any meaningful incentive to comply with their obligation under network rules to assure that their merchants are in compliance with all data security requirements. Moreover, once the networks allege that a "data compromise" may have occurred, their right of automatic indemnification against any consequent fines and assessments reduces acquirers' and processors' financial motivation to challenge network findings, act as a merchant's advocate, and work with a merchant to formulate an appeal of adverse network actions.

By affirming the fulfillment of an acquirer's "good faith" obligation as a prerequisite to invoking an indemnification clause, a favorable outcome on this issue not only would increase acquirers' incentives to assure merchant compliance with security rules and to act as the merchant's advocate with the card networks, it would also establish a precedent that could facilitate other merchants' ability to contest indemnification claims when good faith conduct is absent. Similarly, by affirming a merchant's ability to hold an acquirer responsible for negligence (and breach of fiduciary duty) apart from any contractual obligations, the litigation offers the promise of recoveries (including return of automatically seized amounts) where acquirers and processors fail to take reasonable actions in responding to network actions following an alleged data compromise. In particular, holding an acquirer responsible for missed deadlines or late notifications affecting appeal rights or challenges to data breach "compliance" claims will incentivize them to ensure the opportunity for timely and effective merchant responses.

Promoting greater merchant procedural rights to understand and challenge adverse network determinations in alleged data compromises. The procedures for developing network data security standards—as well as procedures for enforcing those

standards—are very much an "inside game" among the networks and their acquirers and issuers. In particular, the rules empowering the networks to fine acquirers and allocate claimed fraud losses among issuers and acquirers are contained in the card networks rules,' which are as contracts between the networks and their members.[11]

Given the existence of indemnification provisions as a pass-through escape mechanism for acquirers' liability, it is not surprising that acquirers have not insisted on greater procedural protections. And it is not surprising that, as non-parties to the network rules, merchants have not been given a formal due process channels to contest network determinations. A judicial finding that this absence of merchant rights—agreed to by acquirers and networks without merchant participation—renders merchant agreement indemnification provisions unenforceable could well serve as a catalytic event for change. Potentially, the result would be a more transparent and less arbitrary network process with greater merchant rights, and with greater acquirer incentives to advocate on merchants' behalf.

Limiting the ability of acquirers to enforce unlawful penal sanctions. Because Visa "fines" and MasterCard "non-compliance assessments" are intended to operate as punitive sanctions, rather than compensate for damages, they are unenforceable "penalties." The fact that they are imposed in the absolute discretion of the card networks, without any right of a merchant to respond, demonstrates that the networks are arrogating the powers of the sovereign to punish. Moreover, they are imposing these punishments as prosecutor, judge, and jury in ways that would be a due process violation if undertaken by a government agency. Judicial recognition that acquirers cannot seek indemnification for the networks' punitive sanctions would provide additional clarity regarding the scope of acquirers' indemnity powers, separate from the limitations on acquirer invocation of indemnity clause, discussed above.

Guiding merchants' negotiation of their agreements with acquirers and processors. Lawyers for acquiring banks and their processors appear to be increasingly concerned that merchants may "get wise" to the legal flaws in the application of indemnity provisions to the card networks' security enforcement mechanisms. Consequently, form agreements that have been introduced in the past few years may contain provisions that purport to have merchants acknowledge and accept the networks' enforcement procedures, and to allow the acquirer and/or processor to automatically invoke indemnification powers with respect to any resulting financial liabilities imposed on them. For example, one card processor's 2009 form merchant agreement (Chase Paymentech) contains the following provision:

> You understand that your failure to comply with the Payment Brand Rules, including the Security Standards, or the compromise of any Payment Instrument Information, may result in assessments, fines, and/or penalties by the Payment

[11] "The *Visa International Operating Regulations* are set and modified by Visa … and represent a binding contract between Visa and all Members." Visa Regulation ID#: 050411-010410-0020308 (2011).

> Brands, and you agree to indemnify and reimburse us immediately for any such assessment, fine, or penalty imposed on us or the Member [bank] and any related loss, cost, or expense incurred by us or the Member.

Regardless of the outcome of the Cisero's litigation, merchants should negotiate to limit the scope of indemnity provisions based on the legal objections raised in the Counterclaim. Further, merchants should seek as a predicate to invocation of indemnification the processor/acquirer's: (a) compliance with network rules mandating that they take steps to assure merchant awareness of, and compliance with network security rules; (b) providing access to all information given to—or received from—a card network with respect to an alleged breach; and (c) recognition and fulfillment of its obligation affirmatively to act as the merchant's advocate in any network compliance proceeding and to provide timely notification of any merchant opportunities to appeal.

* * *

As we concluded in our paper to the 2010 Hospitality Law Conference: "Simply put, those in the hospitality industry should resist being at the bottom of the hill as liability cascades downward from all others in the card processing chain." This advice remains true today. Hospitality industry counsel should monitor litigation for any resulting precedents to assist in this effort.