

LITIGATION UPDATE: THE *CISERO'S* CASE

CHALLENGING CARD NETWORK ENFORCEMENT MECHANISMS

Presenter



- W. Stephen Cannon, Chairman, Constantine Cannon LLP
- Former General Counsel, Circuit City Stores, Inc.; former Deputy Assistant Attorney General, Antitrust Division, U.S. Department of Justice; former Chief Antitrust Counsel, Senate Judiciary Committee
- Active involvement in payment card issues, including testimony before the Senate and House Judiciary Committees on behalf of the Merchants Payments Coalition and representation of the Coalition in Federal Reserve Board rulemaking proceedings
- Representation of merchants in disputes regarding Visa and MasterCard data compromise fines and assessments

Electronic Payments Today: Merchants and the Liability Cascade

Networks Impose High Fraud Costs

- Merchants face significant compliance, monitoring, and liability costs as a result of card networks' Payment Card Industry data security standards (PCI-DSS)
- Liability includes charge-backs and "Account Data Compromise" systems of fines, penalties and assessments for PCI violations or claimed data breaches
 - Unilaterally imposed by Visa and MasterCard based on "common point of purchase" and "expected fraud" algorithms
 - Limited appeal rights dependent on acquirers
 - Collected through indemnification provisions of merchants' agreements with their acquirers and processors

Unconscionable System Places Merchants at Risk

- Card networks
 - Develop security standards and enforcement mechanisms without merchant input or consent
 - Arrogate governmental powers to impose punishments, fines, and penalties
 - Determine merchant liability for a breach and amount of damages without any due process
- Acquirers and processors serve as “gatekeepers” to network officials in security enforcement procedures

Merchant Agreements

- Required by networks to mandate merchant adherence to network rules
 - Merchants bound by rules without notice or consent
 - Some rules secret to this day
- Contain indemnification clauses that hold merchants liable for network fines and assessments from alleged rule violations
 - Do not impose reciprocal obligations on processors to assist merchant
 - Authorize acquirers automatically to seize funds from merchants' payment card cash flow: the reserve account

Avoiding Responsibility

- Network rules:
 - Acquirers expressly told not to say that networks impose assessments on merchants; rather it's up to acquirers as to how to recover them
 - Acquirers and processors held responsible by networks for merchants' compliance with security and other standards, and for taking reasonable steps to ensure it
- However, under indemnity clause, acquirers treat fines and assessments as just between merchants and networks
- At last year's Conference, the PCI Council's Bob Russo acknowledged that PCI fines are "arbitrary"

Two Years Ago, A Call to Action

- “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.”
- “One day, the test case will arise, and merchants should be prepared to act.”

Cisero's



Steve and Cissy McComb



The *Cisero's* Case

- A family-owned restaurant in Park City Utah has been sued by U.S. Bank's card processor
- Initiated as a 2010 collection action arising from an alleged 2008 data breach
- Counterclaims filed by Cisero's against U.S. Bank and Elavon in September 2011
- In early motions practice and discovery

Some Factual Background

- Cisero's notified of possible compromise of payment card data in early 2008
- Forensic investigation conducted as requested by networks
- Card data found to be stored on POS server, but no evidence at all of a breach, "malware," or unauthorized access
- Verizon Cybertrust found 22,000 "instances" of stored Visa accounts
- However, Cadence Assurance review found
 - only 8,100 "unique" Visa accounts stored
 - 70% of accounts identified by MasterCard not on Cisero's hard drive

The Networks' Response

- MasterCard
 - Imposed \$15,000 “non compliance assessment”
 - Cost recovery procedure not instituted
 - Individual issuer “compliance cases” of \$14,000
- Visa
 - Imposed \$5,000 fine
 - Instituted ADCR process based on 32,000 compromised accounts (10,000 required)
 - Found \$1.26 million in “actual” fraud and \$521,000 in “incremental’ fraud; but capped liability at \$55,000 if current PCI-DSS compliance demonstrated

Elavon's Response

- Claimed Cisero's had been advised of PCI rules through web site references on six billing statements
- Did not notify Cisero's of networks' actions until too late for any appeals
- Stated "Compliance with ... card association's security is not and has never been an acquirer responsibility"
- Redacted MasterCard admonishment that Elavon "As a best practice ... should consider implementation" of merchant site protection programs to minimize risk of future incidents
- Automatically deducted amounts from Cisero's accounts pursuant to indemnification clause until Cisero's switched processors

September 2011:
Cisero's Countersues Elavon and
U.S. Bank

Counterclaims and Defenses

- A declaration that Cisero's is "exonerated" as an indemnitor by U.S. Bank/Elavon's lack of "good faith"
 - Failed to give Cisero's opportunity to defend or appeal network action
 - Failed to take steps to ensure Cisero's aware of and in compliance with data security standards
 - Paid fines and assessment without demanding proof of breach and causal connection to losses, questioning disparate Visa and MasterCard fraud amounts, and verifying that more than 10,000 unique Visa accounts at risk
- Indemnity clause as applied to network fines and assessments is an unconscionable contract of adhesion
- Penalties are unenforceable

Counterclaims (cont'd)

- Damages to Cisero's as a result of U.S. Bank and Elavon's:
 - Negligence
 - Failure to inform Cisero's of security standards and take steps to ensure compliance
 - Conduct during investigation and network imposition of fines and assessments
 - Breach of contractual covenant of good faith and fair dealing
 - Breach of contract provisions regarding deductions
 - Conversion of amounts deducted from Cisero's accounts
 - Violation of fiduciary obligations

Discovery Underway

- Includes U.S. Bank and Elavon's administration of Visa and MasterCard data security programs, including appeals
- Seeks information relating to networks' actual methods and procedures for determining existence of a data breach, assigning liability, and allocating losses


Recent Press Coverage

- **WIRED** (January 12)- “Rare Legal Fight Takes on Credit Card Company Security Standards and Fines”
 - A small celebrity-friendly restaurant in Utah is finally doing what many merchants have only dreamed of doing for a long time — taking on a part of the payment card industry’s powerful but flawed system for securing card data by fining merchants for failing to secure their data.
 - “All it takes is for one case to drive a truck through a provision of the contract, and all other contracts written like this one are suddenly put into question,” says Andrea Matwyszyn, a law and business ethics professor at the University of Pennsylvania’s Wharton School.
 - The fact that merchants are liable for a third-party agreement their banks make with Visa and MasterCard is also problematic because it disempowers merchants and prevents them from being able to “negotiate the kinds of balanced provisions we would expect to see between two parties to a contract.”




Recent Press Coverage (cont'd)

- **Bloomberg** (January 9)- “Park City Eatery Balks at Credit Card Fines in Rare Court Fight”
 - Cissy McComb: “We find ourselves in a position to do nothing but defend ourselves and try to change the way merchants are treated.”
 - “There’s a suspicion among many merchants that PCI is a near scam wrapped in good intentions,” [Mallory] Duncan said by phone from Washington. “The dissatisfaction with PCI and the financial consequences of it in the retail industry are rampant.”
- **Rolling Stone** (Matt Taibbi, January 9)- “Credit Card Firms: They Don’t Just Steal From Cardholders”
 - “Nobody minds banks and creditors being greedy. But we can't live with big firms simply taking money out of bank accounts for no reason, and daring people to sue to get the money back. That's theft by bureaucratic force, not mere greed.”


Recent Press Coverage (cont'd)

-  (January 19)- “Breached Merchant Sues Processor”
 - [M]ost merchants don't take acquiring banks and card networks on in court. "They usually walk away and pay the fines, even if they think the fine's unfair."
 - The mere fact that Cisero's filed a counter suit against U.S. Bank makes its case unique. If Cisero's is successful in its legal quest to have U.S. Bank's indemnification ruled illegal, it could set a legal precedent that puts a contractual shift in motion for the ways response and liability are handled in the wake of card breaches.

Recent Press Coverage (cont'd)

-  techsecuritytoday (January 11)- “Restaurant Refuses to Accept Credit Card Fines”
 - The broader implications of Cisero’s countersuit are obvious: If the court finds in favor of Cisero the responsibility for data breaches will rest with the card processor, not the retailer. How long do you think the banks and Visa/MasterCard will sit still for that?
 - I can easily see Visa/MasterCard taking such a decision all the way to the U.S. Supreme Court.
-   (January 12)- “PCI Security Standards in the Dock”
 - At the moment, merchants like the McComb's have no choice but to sign up to the PCI compliance standards and accept the provisions dictated by the card schemes. If they win their court case, the implications for the future of the PCI scheme - and the security blanket it provides to the payment cards industry - could be very grave.

Recent Press Coverage (cont'd)

-  (January 26)- “Who is PCI Really Protecting?”
 - The PCI Council is not a world government, merchant banks are not the IRS, and neither have any legal right (beyond those rights they give themselves in the small print of the one-sided contracts they issue to uninformed merchants) to levy fines or to seize assets or funds. The fact that they give themselves these powers is, frankly, terrifying.
 - PCI should be protecting all parties involved in the payment process. Not just the big dogs and not just the consumers, but everyone involved. Until that happens, we have to side with Cisero’s.

Potential Outcomes of *Cisero's* Litigation

- Enhance processor incentives to ensure merchant compliance with data security rules and to serve as a merchant's advocate to networks in data security proceedings
- Promote greater merchant procedural rights to understand and challenge adverse network determinations in alleged data compromises
- Limit the ability of acquirers to enforce unlawful penal sanctions

A Warning to Hospitality Industry Counsel

- Recent indemnification clauses attempt to preempt merchant challenges:

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 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.

Chase Paymentech

Actions Counsel Can Take

- Negotiate to require as a predicate to indemnification the acquirer's or processor's-
 - compliance with network rules mandating acquirer's assurance of merchant awareness of, and compliance with network security rules
 - providing all information provided to—or received from—networks with respect to an alleged breach
 - recognition and fulfillment of its obligation to act as the merchant's advocate in any network compliance proceeding and to provide timely notification of any merchant opportunities to appeal

Session Evaluation



Scan or Visit TheHLC.co