

“THE CURRENCY OF PROGRESS?”
VISA AND MASTERCARD ARROGATE GOVERNMENTAL POWERS IN THE
NAME OF CARD SYSTEM SECURITY

By W. Stephen Cannon, Constantine Cannon LLP and
Michael McCormack, Palma Advisors, LLC

January 1, 2010 marks the effective date of a new Nevada law establishing the Payment Card Industry’s Data Security Standard (“PCI DSS”) as the required method by which merchants and those in the payment system processing chain are to protect sensitive payment card data from unlawful access and misuse. In particular, the new law establishes a safe-harbor defense: a “collector” of card data “shall not be liable for damages for a breach of the security” of its system if it is in compliance with the latest PCI DSS standard and the breach is not the result of gross negligence or intentional misconduct. 2009 Nev. Stat. ch. 355 § 1(3).

While some commentators have labeled this first-in-the-nation PCI-DSS legislative effort as a “game-changer” in the privacy and data protection area,¹ merchants’ *already* are subject to significant financial jeopardy arising from a detailed system of penalties and liabilities administered by Visa and MasterCard for alleged PCI-DSS violations. This arrogation of governmental power to police payment system security (without the accountability of a government-run system) should not come as a surprise: A recent Visa advertising campaign claims its payment systems are “The Currency of Progress,” far superior to mere cash and checks. And exactly decade ago, December 14, 1999, Visa’s attorneys advocated that courts should view Visa a “private Federal Reserve.”²

But this privatization of law enforcement demonstrates a further downside for merchants to the card systems’ effort to achieve de facto privatization of America’s payment system—beyond having to pay their high interchange fees for card acceptance. As set out below, Visa and MasterCard have set themselves up as prosecutor, judge, and jury to penalize merchants and others with expressly denominated “fines,” potentially amounting to hundreds of thousands of dollars—amounts that automatically can be deducted from payments owed to merchants from their card acceptance cash flow.

And unlike the forthright way Nevada has adopted liability rules, the card systems have simply presumed themselves to have governmental powers of punishment through mandated compliance with card system Operating Rules that no merchant ever signs directly. This situation is particularly troubling, given Visa and MasterCard’s market power—there is no practical alternative to acceptance of those systems’ cards.

¹ See “Is Nevada’s New Privacy Law a ‘Game-Changer?’” *Bank Info Security* (July 6, 2009).

² See L. Constantine, G. Schnell, R. Cyr & M. Peters, “Repairing the Failed Debit Card Market: Lessons From an Historically Interventionist Federal Reserve and the Recent *Visa Check/MasterMoney Antitrust Litigation*,” 2 *NYU Journal of Law and Business*, 147, 198 n. 187 (2005).

The card systems' penalty mechanisms. At the heart of the card systems' power of punishment are the agreements Visa and MasterCard have with each of their "members," which include not only the banks that issue credit, debit, and stored-value cards, but the banks (denominated "acquirers") that provide card acceptance and processing services to merchants. Under their agreements with the card systems, members must require that merchants and processors agree to be bound by the card systems' operating rules, and these rules, in turn, require adherence by merchants to PCI-DSS requirements and to each card system's auditing, testing, and investigation procedures associated with PCI-DSS compliance. Visa calls its package of standards and compliance measures the "Cardholder Information Security Program" ("CISP"), while MasterCard calls its effort the "Site Data Protection Program" ("SDP Program"). These programs require more than just compliance: for most merchants they require an annual self-certification and quarterly security scans for systems connected to the Internet; larger merchants may need to have an annual onsite audit by a "Qualified Security Assessor."

Both programs are enforced against acquirers, processors, and merchants with a system of fines and penalties. Visa's CISP web site is careful to warn participants of these sanctions, but is vague as to their actual level:

If a member, merchant or service provider does not comply with the security requirements or fails to rectify a security issue, Visa may fine the responsible member. Visa may waive fines in the event of a data compromise if there is no evidence of non-compliance with PCI DSS and Visa rules. *To prevent fines a member, merchant, or service provider must maintain full compliance at all times, including at the time of breach as demonstrated during a forensic investigation. Additionally, a member must demonstrate that prior to the compromise the compromised entity had already met the compliance validation requirements, demonstrating full compliance.*³

Note that Visa's approach is to fine the "member," i.e., the acquiring bank, if there is a merchant violation; as discussed below, the acquirer's merchant agreements permit recovery of those fines from the merchant. According to Visa's US Operating Regulations,⁴ a member is assessed a "fine" of up to \$50,000 for the first violation in a rolling 12-month period, up to \$100,000 for the second, and "At the discretion of Visa U.S.A." for additional violations. Given that the count apparently includes violations by merchants and processors, it would not be a surprise if the "discretionary" level were easily reached.

MasterCard is more specific. The July 2009 release of its *Security Rules and Procedures- Merchant Edition*⁵ specifies "assessments" for merchant non-compliance ranging from up to \$10-25,000 for the first violation in a calendar year to up to \$80-200,000 for the fourth, dependent on merchant transaction volume (the smallest merchant class, Level 4, appears to be exempt from assessments). Further, acquirers may be liable

³ See http://usa.visa.com/merchants/risk_management/cisp_overview.html#anchor_7 (emphasis added).

⁴ Section 1.7.D.27.

⁵ Section 10.5.4.

to card issuers for various loss claims resulting from a compromise, including \$25 per reissued card and for other costs.

Merchant agreements provide the collection mechanism for the penalties. The fact that card systems impose fines and “assessments” on their members might be of limited concern for merchants, since merchants normally would have no direct agreements with Visa and MasterCard. However, the agreements that merchants do sign with acquiring banks and/or their processors provide the link between card systems and merchants. The Wells Fargo agreement⁶ appears typical: “you agree ... to comply with all applicable Association [e.g., Visa and MasterCard] Rules.”⁷ In turn, the agreement requires compliance with the Visa CISP and MasterCard SDP programs: “The Associations or we may impose fines or penalties ... if it is determined that you are not compliant with applicable data security requirements.”⁸ Next, the Agreement requires indemnification of the bank against all “liabilities” growing out of a merchant’s use of the bank’s acquiring services, “including any third-party indemnifications we are obligated to make as a result of your actions (including any indemnification of any Association or Issuer).”⁹ Finally, the agreement gives the bank a right of offset against all funds deposited into a merchant’s settlement account from payments from the issuing banks for cardholders’ purchases. In particular:

We may also debit your Settlement Account or settlement funds in the event we are required to pay Association fees, charges, fines, penalties, or other assessments as a consequence of your sales activities. Such debits shall not be subject to any limitations of time specified elsewhere in the Agreement.¹⁰

In short, should Visa or MasterCard decide a merchant has violated elements of their CISP or PDD programs, it has large discretion to assess a fine within the parameters outlined above, based on the result of an investigation of a claimed breach incident. The fine and other related assessments (e.g., reimbursement for card reissues) are assessed to the acquirer, which then may automatically deduct them from the merchant’s settlement fund cash flow. Keep in mind that the evidence of “breach” may merely be from a statistical analysis of “common merchants” used by cardholders whose cards have been the subject of fraudulent activity.¹¹ A merchant in this group found to be in PCI-DSS non-compliance may be deemed to be the cause of the breach, and subject to any resulting fines and penalties—and automatic offset from funds due to the merchant from payment card purchases.

But is this system of card system-imposed fines and penalties really legal? This is a good question, which does not appear to have been answered definitively. It is

⁶ Denominated as the Wells Fargo Program Guide, available at www.wellsfargo.com/downloads/pdf/biz/merchant/program_guide.pdf.

⁷ Section 15.

⁸ Section 4.1.

⁹ Section 26.1.

¹⁰ Section 10.2.

¹¹ E.g., MasterCard, “Common Point of Purchase (CPP) Investigations,” *Security Rules and Procedures-Merchant Edition*, section 10.4.

Hornbook law that contractual “penalties” are unenforceable. That is, contracts may not contain provisions that provide *in terrorem* payment of money to deter a breach, rather than to compensate the other party should a breach occur. The reason is one of public policy: “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.”¹² As the highest court in Maryland recently summarized:

As Professor Williston has noted, “a liquidated damages provision will be held to violate public policy, and hence will not be enforced, when it is intended to punish, or has the effect of punishing, a party for breaching the contract...” We have long recognized that “one of the most difficult and perplexing inquiries encountered in the construction of written agreements” is determining whether a contractual clause should be regarded as a valid and enforceable liquidated damages provision or as a penalty. Thus, “if there is doubt whether a contract provides for liquidated damages or a penalty, the provision will be construed as a penalty.”¹³

The contract law of many states evidences a similar hostility to penalties.¹⁴

However, the analysis required to determine whether a “fine” imposed by Visa or MasterCard is a “penalty,” does not seem to require a “difficult and perplexing” inquiry at all. First, the penalty schedule effectively imposed on merchants does not represent a negotiated arrangement between merchants and Visa and MasterCard. The only contract that merchants have is with the acquiring bank or its processor agent. Merchants simply are compelled to abide by each card system’s rules, whatever they might be. And, given the acquirers’ right to indemnity from merchants, there is little incentive for an acquirer—the entity in actual contractual privity with the card systems—to resist changes in the level of the penalties, which the acquirers simply can deduct from a merchant’s settlement account.

Second, the financial penalty is self-admitted to be just that—a “fine,” “penalty,” or “assessment” imposed by the card association to penalize and deter violations—with the amount of the fine increasing as the number of alleged violations per year increases. This is just like the fines associated with a traffic ticket, e.g., the greater the number of times a motorist is caught using a “high occupancy” lane while driving solo, the higher the fine. Third, the card systems are not damaged by a violation of the rules at all. The card issuers are separately to be reimbursed for cards reissued and other expenses, and the party being investigated must absorb the cost of the investigation.¹⁵ So the penalties are just that, “penalties;” they do not even purport to be liquidated damages since they

¹² *Wetzler v. Roosevelt Raceway, Inc.*, 622 N.Y.S. 2d 232, 235 (1st Dept., 1995).

¹³ *Barrie School v. Patch*, 933 A. 2d 382, 390 (Md., 2007) (citations omitted).

¹⁴ *See, e.g., Williston on Contracts* § 65.3 (May 2009 update).

¹⁵ For example, Visa requires that a “compromised” merchant or Visa member should engage a “Qualified Incident Response Assessor” (“QIRA”). “However, Visa has the right to engage a QIRA to perform a forensic investigation as it deems appropriate, and will assess all investigative costs to the client [Visa member] in addition to any fine that may be applicable.” Visa, *What to do If Compromised* at 12 (December 2008).

clearly are intended to deter violations and have no relationship to the cost to the card system, itself, of a claimed violation.¹⁶

Of course, it is not surprising that a card system, claiming to be the “Currency of Progress,” has sought to act in a manner heretofore held to be “exclusively the prerogative of the sovereign.” But much as they would like it to be so, the card systems are not the government—at least not yet. Even the Nevada PCI legislation only opened the door to damages; it did not impose fines for claimed PCI violations.

So, what to do? We commend merchants to be alert to the merchant agreements they sign and understand precisely the surprises that the card systems have in store for them, should a merchant be deemed to be in violation of the CISP and SDP programs. And they 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.

W. Stephen Cannon is Chairman of Constantine Cannon LLP, a law firm based in New York and Washington, D.C. Mr. Cannon can be reached at 202-204-3502, scannon@constantinecannon.com. Michael McCormack is President of Palma Advisors, LLC, a Fort Lauderdale-based consultancy specializing in the payments transaction industry, including card, electronic and paper based payments. Mr. McCormack can be reached at 954-713-7549, mike.mccormack@palmaadvisors.com.

¹⁶ The card systems have claimed that other fees paid by merchants, such as the interchange fee and card system processing fees, are, in part, used to reimburse the card systems and issuers for the underlying fraud detection capabilities imbedded in the payment system.