2021 The Banking Law Journal § 2021-9.04

The Banking Law Journal > 2021 The Banking Law Journal > Volume 138, Number 9 The Banking Law Journal October 2021 > Payment Card Issuers Face Mixed Results Seeking Loss Recovery on Merchant Data Breaches

Author

Jennifer Hall[*]

§2021-9.04 Payment Card Issuers Continue to Face Mixed Results Seeking Loss Recovery on Merchant Data Breaches

In this article, the author explains that, with losses mounting due to cybercrime, issuer banks—dissatisfied with the remedies available via Visa and Mastercard—have sought redress through the courts, albeit with only limited success.

Despite, or perhaps because of, the COVID-19 pandemic, 2020 proved to be another record-breaker for cybercrime. According to a year-end report, "the total number of records compromised in 2020 exceeded 37 billion, a 141 percent increase compared to 2019 and by far the most records exposed in a single year since we have been reporting on data breach activity."[1] Consistent with prior years, credit cards accounted for approximately 12 percent of the total data breaches; the average stolen credit card now sells for just $12-$35 on the dark web, including pin.[2] With losses mounting, issuer banks—dissatisfied with the remedies available via Visa and Mastercard—have sought redress through the courts, albeit with only limited success.

THE PAYMENT CARD SYSTEM

---

[*] Jennifer Hall is an attorney with the law firm of Emmet, Marvin & Martin, LLP, in New York. Ms. Hall principally practices in the area of commercial real estate finance, representing national banks in commercial loan transactions and related litigation and bankruptcy matters. She may be contacted at *jhall@emmetmarvin.com*.

[1] RiskBased Security, *2020 Year End Report: Data Breach QuickView*, *https://pages.riskbasedsecurity.com/en/en/2020-yearend-data-breach-quickview-report*.

[2] Welivesecurity, Amer Owaida, August 3, 2020, *https://www.welivesecurity.com/2020/08/03/how-much-is-your-personal-data-worth-dark-web/*.

The United States has two principal credit card networks: Visa and Mastercard. Each network operates through five additional players: the issuer bank, the merchant, the retail customer, the acquiring bank, and the card processor (together, the "Card Network Players"). The system works as follows: a bank (a/k/a the "issuer bank") issues a credit card to a retail customer. When the customer thereafter uses that credit card to make a purchase from a merchant, a payment processor transmits the retail customer's card information first to the merchant's bank (a/k/a the "acquiring bank") and then to the issuer bank, which makes the payment.

Cybersecurity standards for customer data are set by Visa and Mastercard through a protocol known as the Payment Card Industry Data Security Standard ("PCI DSS"). The PCI DSS applies to all parties involved in the processing, holding, or securing of credit card data. As security weaknesses in merchant and card processor systems have increasingly compromised retail customers' card information, disputes over loss allocation have arisen.

COST RECOVERY PROCESS FOR MERCHANT NEGLIGENCE

As one court observed, the Card Network Players are all tied together by a "complex web of relationships … governed by both individual contracts and exhaustive regulations promulgated by Visa and other card networks."[3] These regulations include a cost recovery process, whereby an issuing or acquiring bank can ask Visa or Mastercard to resolve a rules violation that caused it to incur a financial loss. In particular, the Visa and Mastercard regulations "specifically contemplate the possibility of a data breach. They specify procedures for issuer banks to make claims when such data breaches occur through private dispute-resolution systems."[4]

Mastercard's current Compliance Case Filing procedures are found in Chapter 7 of its May 4, 2021 Chargeback Guide.[5] The issuer bank initiates the recovery process against the merchant by filing a pre-compliance case and alleging that a rule (in the case of a data breach, the PCI DSS) was violated and the issuer suffered a loss as a result. Supporting documents must be included. The merchant, in turn, may accept or reject the pre-compliance

---

[3] *Banknorth, N.A. v. BJ's Wholesale Club, Inc., 394 F.Supp.2d 283, 287 (D. Me. 2005)*.

[4] *In re Heartland Payment Systems, Inc. v. Heartland Bank and Key Bank, N.A., 834 F.Supp. 2d 566, 588 (S.D. Texas 2011)* (citing *Sovereign Bank v. BJ's Wholesale Club, Inc., 533 F.3d 162, 165 (3d Cir. 2008)* (describing "comprehensive provisions for resolving disputes between Visa members" that allow Visa to decide disputes "in accordance with risk allocation judgments made by Visa"); *Cumis Ins. Soc'y, Inc. v. BJ's Wholesale Club*, (Mass. Super.Ct. June 4, 2008) (noting that Visa and Mastercard regulations "provide for an elaborate dispute resolution procedure and for fines for non-compliance"), *aff'd*, *455 Mass. 458 (2009)*).

[5] *See* Mastercard Chargeback Guide dated May 4 2021, which can be found at: *https://www.mastercard.us/content/dam/mccom/global/documents/chargeback-guide.pdf*. Visa has comparable rules. *See* Visa Core Rules and Visa Product and Service Rules dated April 17, 2021, which can be found at: *https://usa.visa.com/dam/VCOM/download/about-visa/visa-rules-public.pdf*.

case, with a rebuttal to be filed within 30 calendar days of commencement. If the merchant does nothing, then after 30 days, the pre-compliance case is automatically rejected. The issuer must then escalate the matter to a compliance case, and Mastercard will issue its ruling. Mastercard generally refuses to review a case if any of the filing requirements are not met.

COST RECOVERY PROCESS FOR MERCHANT FRAUD

Mastercard has a separate process for security breaches caused by a merchant's fraudulent conduct. The procedures are set forth in Chapter 8 of Mastercard's February 14, 2019 Security Rules and Procedures: Merchant Edition (the "Rules"). Through its Questionable Merchant Audit Program ("QMAP"), an issuer bank may recover half of any "actual fraud losses" that are properly reported, if the merchant meets the criteria of a questionable merchant. Under Chapter 8.4.1 of the Rules, a merchant may be deemed a "Questionable Merchant" if, for example, its "fraud-to-sales" ratio was at least 70 percent; at least 20 percent of its transactions were declined by the issuer; and the merchant's dollar amount of fraudulent transactions and declines was greater than its total dollar amount of approved transactions. Mastercard has "sole discretion" to determine whether a merchant should be considered a "Questionable Merchant."

Chapter 8.4.2 of the Rules further provides that the issuer "must promptly notify Mastercard" if it "has reason to believe that a Merchant may be a Questionable Merchant." The issuer must provide specific information about the merchant, including its member ID and address, the name of the acquirer, the number of transactions conducted affecting the cardholders, the dates and times of the transactions, and the total dollar volume of the issuer's losses. If Mastercard determines that a merchant should be deemed a Questionable Merchant, then the issuer will be notified of its eligibility for partial recovery. The Rules preclude recovery to the issuer bank if, among other things, the issuer recovers by pursuing remedies outside Mastercard.

THE HEARTLAND DATA BREACH

Following one of the decades' largest data breaches, card issuers were able to recover over $100 million through the recovery channels of Mastercard and Visa.

In 2008, the computers of a card processor, Heartland Payment Systems, Inc., were compromised, and hackers obtained approximately 130 million customers' credit card data.[6] In 2010, Heartland settled with both Visa and Mastercard. The Mastercard settlement required Heartland "to fund up to $41.4 million of 'alternative recovery offers' to be made to eligible Mastercard card issuers to settle their claims for operational costs and fraud losses alleged to have been incurred by them as a result of the breach."[7] The Visa settlement, in turn, required Heartland

---

[6] "5 of the biggest-ever credit card hacks," *CNN Business*, Jan. 12, 2014, by Julianne Pepitone, *https://money.cnn.com/gallery/technology/security/2013/12/19/biggest-credit-card-hacks/2.html*.

to pay $60 million to Visa-branded credit and debit card issuers—"the largest known settlement amount ever paid to Visa."[8] Both settlements were contingent on 80 percent of the card issuers accepting the deal. The settling issuers also had "to forgo any other remedies or recoveries they might otherwise be able to obtain from Heartland and its acquirers by reason of the Heartland data security breach, and to release Mastercard, Heartland and Heartland's acquiring banks from all legal and financial liability associated with the breach."[9]

Rather than participating in the foregoing settlement, a number of bank issuers affected by the Heartland data breach chose to pursue common law remedies against the card processor in federal court. The ensuing litigation was an uphill battle for the issuer banks due to a few seemingly unsurmountable defenses, especially the economic loss rule ("ELR"). ELR is a common law doctrine that prohibits parties from recovering in tort when the negligence of others results in purely economic losses for which contractual remedies are available.

The issuer banks based their negligence and breach of contract claims against Heartland on Heartland's alleged failure to comply with the PCI DSS. The card issuers' breach of contract claim was dependent on a third-party beneficiary theory, as the litigating parties were not in contractual privity. The issuers argued that Heartland's contracts with the acquiring banks "required Heartland to take 'appropriate steps to safeguard the sensitive financial information'" of the card issuers' customers.[10]

The U.S. District Court for the Southern District of Texas, however, rejected the issuers' third-party beneficiary theory, finding that it lacked "a clear expression of intent to benefit the third party—in this case, the [issuers]."[11] While Heartland had contracted with acquiring banks to "safeguard" confidential information "from disclosure to unauthorized persons," it did not "state an intent to benefit anyone other than the contracting parties" such as the issuers.[12]

---

[7] "MasterCard Reaches Settlement with Heartland Payment Systems to Provide Issuers Worldwide up to $41.4 Million for Data Breach Claims," by Chris Monteiro, *https://newsroom.mastercard.com/press-releases/mastercard-reaches-settlement-with-heartland-payment-systems-to-provide-issuers-worldwide-up-to-41-4-million-for-data-breach-claims/*.

[8] "Heartland, Visa Announce $60 Million Settlement," January 8, 2010, by Linda McGlasson. *https://www.bankinfosecurity.com/heartland-visa-announce-60-million-settlement-a-2054*.

[9] *See supra* note 7.

[10] *Heartland Payment Sys., 834 F.Supp.2d at 577*.

[11] *Id. at 579*.

[12] *Id.*

The district court also dismissed the issuer banks' negligence claims, holding that Heartland did not owe them a duty in tort because their relationship was "governed by the Visa and Mastercard regulations."[13] Accordingly, the district court held that the ELR barred the issuers' claims in tort, as their alleged damages were purely economic, and they already had contractual remedies available to them through Visa and Mastercard:

> To participate, issuer banks must accept the Visa and MasterCard regulations. By participating in the Visa and MasterCard networks, the Financial Institution Plaintiffs entered into the web of contractual relationships that included not only issuer and acquirer banks but also third-party businesses, such as Heartland, that process transactions for network members. Heartland agreed to follow the Visa and MasterCard regulations.[14]

On appeal, the U.S. Court of Appeals for the Fifth Circuit reversed the district court's dismissal of the negligence claims and held in favor of the issuer banks, ruling that governing New Jersey law permitted recovery for economic losses "where the defendant causes an identifiable class of plaintiffs to which it owes a duty of care to suffer economic loss that does not result in boundless liability."[15] The court of appeals stated that: "New Jersey law does not preclude the Issuer Banks' negligence claim against Heartland at the motion to dismiss stage."[16]

As the Fifth Circuit explained, "it is unclear whether Heartland has contracts with Visa and MasterCard, let alone what the contents of such contracts may be.[17] This uncertainty in the record leaves open the issue of the Issuer Banks' bargaining power with respect to Heartland's participation in the Visa and MasterCard networks."[18]

Following remand, the case settled with no further substantive rulings, leaving the ultimate legal issues to be resolved.

OTHER DATA BREACH LITIGATION

Outside of the *Heartland* case, issuer banks have met with less litigation success. In cases preceding *Heartland*, the U.S. Courts of Appeals for the First and Third Circuits held that the ELR required dismissal of credit card data breach negligence claims brought by issuers.

---

[13] *Id. at 587*.

[14] *Id. at 588*.

[15] *Lone Star Nat. Bank, N.A. v. Heartland Payment Sys., Inc., 729 F.3d 421, 424 (5th Cir. 2013)*.

[16] *Id. at 426* (quoting *People Express Airlines, Inc. v. Consol. Rail Corp., 495 A.2d 107, 116 (N.J. 1985))*.

[17] *Id.*

[18] *Id.*

The First Circuit case of *In re TJX Companies Retail Security Breach Litigation* dealt with a major data breach in 2005 that affected millions of cardholders due to the merchant's and its processor's alleged failure to "follow security protocols prescribed by Visa and Mastercard to safeguard personal and financial information."[19]

The court of appeals affirmed the district court's dismissal of the issuers' negligence claims, holding that governing Massachusetts law, "which is not alone, holds that purely economic losses are unrecoverable in tort and strict liability actions in the absence of personal injury or property damage."[20] The breach of contract claims were also dismissed because, the First Circuit held, the issuers were not intended beneficiaries of the contract between the acquiring bank and the merchant.[21]

In the Third Circuit case, *Sovereign Bank v. BJ's Wholesale Club*, an issuer bank brought suit against a merchant, BJ's Wholesale Club, and its affiliated processor after a major credit card data breach.[22] The Third Circuit held that, under governing Pennsylvania law, the ELR barred the negligence claims.

Noting the "roots" of the ELR doctrine in *Robins Dry Dock and Repair Co. v. Flint*, in which the U.S. Supreme Court explained that "economic advantage alone is too remote for recovery under a negligence theory,"[23] the court of appeals opined that issuers' sole remedy against the Card Network Players would have to be through Visa, based on the enforcement procedure set out in Visa's internal Operating Regulations:

> That provision expressly allows Visa to take specified remedial actions against Members who do not comply with the Operating Regulations, including levying fines and penalties. Enforcement actions can be appealed to Visa's Board of Directors, but the Board's decision is final. The Operating Regulations give Visa, and only Visa, the right to interpret and enforce the Operating Regulations, and only Visa can determine whether a violation of the Operating Regulations has occurred.[24]

The court of appeals, however, reversed the district court's grant of summary judgment to the defendants on the issuer's breach of contract claim, finding there to be a genuine issue of fact as to whether the issuer was an

---

[19] *In re TJX Companies Retail Sec. Breach Litig., 564 F.3d 489, 492 (1st Cir. 2009)*.

[20] *Id. at 498*.

[21] *Id. at 499*.

[22] *Sovereign Bank v. BJ's Wholesale Club, Inc., 533 F.3d 162 (3d Cir. 2008)*.

[23] *Id. at 176* (quoting *Robins Dry Dock and Repair Co. v. Flint, 275 U.S. 303 (1927)*).

[24] *Id. at 165*.

intended third-party beneficiary of the acquiring bank's "promise to Visa to ensure that BJ's complied with the provisions of the Member Agreement prohibiting Merchants from retaining Cardholder Information."[25]

More recently, in *Community Bank of Trenton v. Schnuck Markets, Inc.,* the U.S. Court of Appeals for the Seventh Circuit "decline[d] plaintiffs' invitation" to obtain "reimbursement for their losses above and beyond the remedies provided under the card network contracts," holding that: "Visa and Mastercard networks [already] provide a cost recovery process that allows issuing banks to seek reimbursement for at least some of these losses."[26]

As the court of appeals explained: "[t]he plaintiff banks are disappointed in the amounts the card networks' contractual reimbursement process provided. That type of tort claim is not permitted."[27] The Seventh Circuit further held that the issuer banks' third-party beneficiary claims failed as well, because the court found that "no express contract exists between Schnucks and its customers (beyond the basic exchange of products for payment), let alone one that specifically intends to include the plaintiff banks as third-party beneficiaries."[28]

Similarly, in *Selco Community v. Noodles*, the U.S. District Court for the District of Colorado dismissed the negligence claims brought by the issuer bank against the merchant for a credit card data breach.[29]

Citing to the ELR, the district court held that the plaintiff's "contractual remedies" were already spelled out in the Visa and Mastercard agreements, and that it made "no difference that [the merchant's] contractual duties arise from a web of interrelated agreements coordinated by Visa and Mastercard rather than bilateral contracts."[30]

The district court further opined that it "had no business sidestepping the agreements that sophisticated commercial entities [] voluntarily entered into to allocate the risk of payment card fraud."[31] An appeal was filed, but it was voluntarily dismissed prior to decision.

CONCLUSION

---

[25] *Id. at 172*.

[26] *Community Bank of Trenton v. Schnuck Markets, Inc., 887 F.3d 803, 809–811 (7th Cir. 2018)*.

[27] *Id. at 817*.

[28] *Id. at 821*.

[29] *SELCO Community Credit Union v. Noodles & Co., 267 F.Supp.3d 1288 (D. Colo. 2017)*.

[30] *Id. at 1296*.

[31] *Id. at 1297*.

The proverbial jury is still out on whether litigation can provide an effective means of redress for issuer banks faced with economic losses from merchant data breaches. For now, in all but the largest of cases, issuers are better off pursuing remedies through Visa's and Mastercard's internal cost recovery processes, and using their not-inconsiderable pull with those card networks to ensure that those procedures are meaningful and effective.

End of Document