Merchants Must Be Aware of Potentially Mishandled Credit Card Information

JASON WRIGHT AND KEVIN LYLES

Data security breaches are on the rise. A majority of states have enacted security breach notification laws that require businesses to notify customers when a security breach occurs. In this article, the authors caution merchants who accept credit card payments and store credit card information that, in addition to having notification obligations, they may also face liability to credit card issuers in the event of a data security breach.

As data security breaches become more common and the financial losses increase, lawsuits against the organizations who suffer such security breaches will also increase. Over the last few years, a majority of states enacted security breach notification laws, which generally require businesses to notify customers when a security breach occurs. The next evolution in this arena might be heightened liability. In particular, those businesses that accept credit card payments and store the credit card information face a specific form of potential liability. For the purposes of this article, we refer to these businesses as "merchants," which include the neighborhood market as well as the largest national retailer.

Merchants that suffer data security breaches could face liability from several different groups. Government agencies, such as state attorneys general or the Federal Trade Commission, may file suit against these mer-

Jason Wright is an associate in the New Attorney's Group in the Jones Day Los Angeles office. Kevin Lyles is a partner in the Columbus office and oversees the firm's Privacy & Data Security practice.

Published in the May 2009 issue of Privacy & Data Security Law Journal.

chants. These suits often result in settlements with fines and required security practices. Second, individual customers whose information is compromised by the security breach may sue, although these suits have been relatively unsuccessful. Most often they fail because the customers do not suffer any recognizable injuries — that is, the threat of potential illegal use of their information is not usually considered a recognizable injury.

Credit card issuers ("issuers"), however, may have more viable lawsuits because they suffer considerable damages. Cancelling the customers' accounts and issuing new credit cards can be quite costly. Issuers suffer additional damages covering fraudulent charges, for which the cardholder has limited liability. When sued by issuers, merchants may also find the basis of liability is their failure to comply with the PCI Data Security Standards ("PCI DSS"). The major payment card brands created the PCI DSS, which require members of the payment card system and merchants who accept credit card payments to take designated steps to ensure the security of credit card information. These lawsuits could become extremely costly for merchants if the credit card issuers are successful. Recent cases demonstrate at least two steps merchants should take to minimize liability: (1) become PCI DSS compliant; and (2) ensure their contracts preclude third-party liability and thereby preclude liability to the credit card issuers.

WHAT ARE THE PCI DATA SECURITY STANDARDS?

Over the last few years, the credit card industry has set the standard for the use and storage of credit card information. The five major payment card brands created the Payment Card Industry ("PCI") Security Standards Counsel to create consistent data security measures on a global basis. The Security Standards Counsel then developed the PCI DSS to protect cardholder data.[1] The requirements of the PCI DSS are divided into 12 categories and include requirements for security management and procedures, network architecture, software design, and other critical protective measures. The payment card brands then use the PCI DSS as the basis for their own compliance programs. Thus, merchants must examine the specific compliance program for each payment card network with which they participate.

The most important standard under the PCI DSS relates to authoriza-

Published in the May 2009 issue of Privacy & Data Security Law Journal.

tion information, which includes the full magnetic stripe data, card validation code, card validation value, and PIN block data. Under the PCI DSS, a merchant cannot store this information for any length of time; once an issuer authorizes the transaction, the authorization information cannot be retained. The belief is that once the transaction is authorized, there is no need for the authorization information.

In contrast to the authorization data, the merchant can store the primary account number, account holder name, and expiration date, so long as the information is properly protected. To accomplish that protection, the PCI DSS has six goals with 12 corresponding general requirements.[2] Each of the 12 requirements includes numerous specific directives.[3] For instance, the first requirement, "Install and maintain a firewall configuration to protect cardholder data," contains four subsections that are further broken into 17 requirements.

In addition, the PCI DSS includes assessment and reporting provisions with which merchants must also comply. Depending on how many transactions a merchant processes, it must either perform an annual onsite PCI Data Security Assessment or perform an annual Self-Assessment Questionnaire ("SAQ").[4] Nearly all merchants must also obtain a quarterly network vulnerability scan by an Approved Scan Vendor ("ASV").

These standards are relevant for two reasons. First, failure to comply can result in fines by the payment card brand. Second, and more importantly, credit card issuers have been pointing to a merchant's failure to comply with the PCI DSS as a basis to hold an acquiring bank liable for the injuries the issuers suffered after the data security breach. These cases are significant to merchants because liability for acquiring banks will swim upstream to the merchants. Indeed, issuers will probably continue to use the PCI DSS standards (reflected in the derivative payment card compliance programs) and breach-of-contract claims, and at least one more court recently allowed such a claim to survive a motion to dismiss.[5] In March 2009, issuers also filed suit against Heartland Payment Processors ("Heartland") and in part alleged that Heartland was liable for its security breach because it failed to comply with the PCI DSS.[6] Though Heartland is a payment processor who processes payments for merchants and acquiring banks, the lesson is clear, all parties concerned must vigilantly comply with the PCI DSS.

THE CONTRACTUAL RELATIONSHIPS OF THE PARTIES INVOLVED

One must first understand the contractual relationships involved to understand the potential liability. Merchants have no contractual relationship with the issuers or the payment card networks. Instead, the payment card networks generally involve a series of contractual relationships, beginning with the cardholder and ending with the merchant.

There are two types of members in the payment card networks. On one side are the issuers, who issue the credit cards to consumers. On the other side are the acquiring banks that process transactions on behalf of the merchants and recruit merchants to use the payment network. The issuers and acquiring banks have no contractual relationship; rather, they each have a contract with the payment card network. The acquiring banks then have contracts with the merchants. But the merchants are not members of the payment card networks and generally have no contractual relationship with the networks, or the issuers.[7]

Merchants may also contract with yet another third party, known as payment processors, who processes the credit card payments for the merchant. When these organizations suffer a data security breach, the liability may swim upstream to the merchants and acquiring banks as well. Indeed, the lawsuits arising from the Heartland Payment Processor's data security breach are just getting started and might be an example of how a payment processor's alleged liability also affects merchants and acquiring banks.

FAILURE TO ABIDE BY THE PCI DSS MAY GIVE RISE TO BREACH-OF-CONTRACT CLAIMS

In a recent battle where credit card issuers sought to avoid the cost of a security breach, the intricacy of these contractual relationships played a central role.[8] In *Sovereign Bank*, a merchant suffered a data security breach, and the credit card issuers filed suit against the merchant and the acquiring bank that had contracted with the merchant. Though the issuers' success was against the acquiring banks, this case could have drastic ramifications for the merchants because acquiring banks will inevitably seek indemnification from the merchants.

BJ's Wholesale Club ("BJ's") is a merchant who contracted with Fifth Third Bank ("Fifth Third") as its acquiring bank.[9] Fifth Third, in turn, is a member of the Visa network.[10] In early 2004, BJ's suffered a data security breach, and its customers' credit card information was compromised.[11] At least two issuers responded by filing suit against both Fifth Third and BJ's.[12] Except for the breach-of-contract claim against Fifth Third, all claims against BJ's and Fifth Third were dismissed.[13] The issuers filed breach-of-contract claims against BJ's in addition to Fifth Third, but the district court dismissed the contract claim against BJ's because BJ's agreement with Fifth Third expressly precluded third party beneficiaries.[14] After discovery regarding the breach-of-contract claim against Fifth Third, the district court granted summary judgment for Fifth Third.[15] The Court of Appeals for the Third Circuit reversed the grant of summary judgment in favor of Fifth Third but affirmed dismissal of the other claims.[16]

Sovereign Bank's Breach-of-Contract Claim Against Fifth Third

Though there were two consolidated appeals by issuers, the court of appeals first considered the claims made by Sovereign Bank ("Sovereign"). Sovereign first argued Fifth Third breached its Member Agreement with Visa because Fifth Third failed to ensure BJ's abided by the security requirements in the Operating Regulations, as the Member Agreement required Fifth Third to do (currently, the security requirements are based on the PCI DSS, but this case arose prior to release of the PCI DSS).[17] Sovereign next argued it was an intended third-party beneficiary of the agreement between Fifth Third and Visa; thus, Fifth Third was liable to Sovereign because of Fifth Third's breach of the Visa Member Agreement.[18]

Sovereign relied on the Restatement of Contracts Section 302 to prove it was an intended third party beneficiary. Section 302 provides: "Unless otherwise agreed between promisor and promisee, a beneficiary of a promise is an intended beneficiary if recognition of a right to performance in the beneficiary is appropriate to effectuate the intentions of the parties and…the circumstances indicate that the promisee intends to give the beneficiary the benefit…" of the promisor's performance.[19] To prevail, Sovereign needed to show (1) "recognition of a right to performance in Sovereign is appropriate to effectuate the intentions of both Visa and Fifth Third in entering their member agreement and (2) whether the circumstances indicate that Visa (the promisee) intended to give Sovereign the benefit of…" Fifth Third's performance.[20]

Fifth Third argued the issuers were not intended third-party beneficiaries. It relied on a Visa representative's testimony that the operating regulations were not intended to benefit any individual and were only intended to benefit the Visa system as a whole.[21]

Sovereign responded with a memorandum by Visa describing a new section of the operating regulations that would prohibit retention of magnetic-stripe data.[22] The memorandum stated: "[t]o protect the Visa system and *Issuers*…"[23] Sovereign argued the memorandum indicated Visa understood issuers would obtain direct benefits from "requiring members to ensure that magnetic-stripe data was not retained."[24] Sovereign also pointed to the Visa representative's testimony that the Visa operating regulations were intended to benefit the members of the Visa network and other stakeholders, such as merchants.[25] Since the issuers are members, Sovereign argued it was an intended beneficiary.

The court of appeals held Sovereign presented sufficient evidence to create a triable issue of fact regarding whether Sovereign was an intended third-party beneficiary.[26] The court also rejected the argument that by intending to benefit everyone with the security requirements, Visa did not specifically intend to benefit any individual.[27] Regarding the second issuer's breach-of-contract claim against Fifth Third, the court noted the second issuer relied on the same evidence and the same arguments as Sovereign; therefore, the court reversed the grant of summary judgment in favor of Fifth Third in that case as well.[28]

In a footnote, the court distinguished *In re TJX Co.*[29] In *In re TJX Co.*, the district court dismissed the issuers' third-party beneficiary claims because in a portion of the Visa operating regulations, Visa expressly intended to preclude third-party beneficiaries.[30] The court of appeals distinguished the cases and held that the section of the Visa operating regulations in *In re TJX Co.* was "in a later version of the Operating Regulations adopted after the events that occurred here."[31]

The facts of *In re TJX Co.* are quite similar to *Sovereign Bank*.[32] The merchant in *In re TJX Co.* also suffered a data security breach, and customers' information was stolen and used to make fraudulent charges.[33] As in *Sovereign Bank*, the credit card issuers in *In re TJX Co.* sued both the merchant and the acquiring bank for the costs of both the fraudulent charges and issuing new credit cards.[34] Though bound by different state law than *Sovereign Bank*, the *TJX* court also looked to the Restatement of Contracts to determine the availability of a third-party beneficiary claim.[35] But in *In re TJX Co.*, the district court dismissed the third-party beneficiary claims against both the merchant and the acquiring bank.[36] The plaintiffs were members of both the Mastercard and Visa networks, and the court examined both operating regulations.[37] First, the Mastercard operating regulations gave Mastercard the sole right to enforce the operating regulations, which precluded the issuers' suits as third-party beneficiaries.[38] The Visa operating regulations went further and expressly precluded any third-party beneficiary.[39] Thus, the court dismissed the contract claims against both the merchant and the acquiring bank.

It is difficult to say whether *Sovereign Bank* or *In re TJX Co.* demonstrates the future viability of breach-of-contract claims by credit card issuers. The potential liability of acquiring banks, and eventually the merchants, will turn on the payment card network's operating regulations and the extent to which it precludes third-party beneficiaries. *Sovereign Bank* also demonstrates that the contracts between acquiring banks and merchants can preclude a merchant's direct liability to credit card issuers as third-party beneficiaries.

To minimize liability, merchants must ensure their contracts with acquiring banks and any payment processors preclude third-party liability. At the very least, this prevents third-party beneficiary claims against the merchant. The merchant may also want to examine whether the agreement between the acquiring bank and the payment card brand precludes third-party beneficiary claims. This will minimize the chances the acquiring bank is liable to the credit card issuer and will also minimize the chance the acquiring bank seeks indemnification from the merchant.

FAILURE TO ABIDE BY PCI DSS MAY GIVE RISE TO STATUTORY CLAIMS

Merchants should be aware of another trend — making the PCI DSS a statutory requirement where the failure to comply gives rise to liability. In 2007, the Minnesota legislature passed a law based on the PCI DSS, and the law made merchants strictly liable to credit card issuers. The law prohibits merchants from retaining credit card authorization information for longer than 48 hours.[40] Though the PCI DSS prohibit storing this information for any length of time, the Minnesota law allows for a two-day window. A merchant that violates the statute and then suffers a data security breach will be liable to credit card issuers for the costs associated with replacing the credit cards and other "reasonable actions undertaken" either to protect the cardholders' information or to facilitate the continuation of services for the cardholder.[41]

Nearly a dozen other states considered similar laws, but none successfully passed a bill. California came the closest; however, in October 2008 Governor Schwarzenegger vetoed, for the second time, a bill similar to the Minnesota statute. A third bill has languished in the Senate Judiciary committee since June 2008. This third bill prohibited retention of authorization information for any period of time. If future cases or security breaches create a positive public perception of the Minnesota statute, states like California may find that these proposed bills will make it out of committee with no threat of a veto.

CONCLUSION

These cases and statutes demonstrate that merchants can take at least two steps to minimize liability. First, merchants should review their contracts and ensure they preclude third-party beneficiary claims. As *Sovereign Bank* demonstrates, merchants may even want to examine whether the payment card brand's membership agreement precludes third-party beneficiary claims and thereby limits the liability of the acquiring banks.

This in turn reduces the risk the acquiring bank will seek indemnification from the merchant. Second, and most important, merchants should ensure they are PCI DSS compliant. Even if third-party beneficiary claims are precluded, plaintiffs may still rely on the PCI DSS to establish a standard of care for other claims. Thus, a merchant who meets the PCI DSS requirement can minimize the risk of both breach-of-contract claims and other claims.

NOTES

[1] In addition to the PCI DSS, the PCI Security Standards Council also promulgates specific standards for PIN entry devices ("PED") and for payment application software ("PA-DSS"). The Council then publishes a list of approved PIN entry devices and payment applications that have satisfied the standards.

[2] PCI DSS Requirements and Security Assessment Procedures, *available at* https://www.pcisecuritystandards.org/security_standards/pci_dss_download.html. The 12 requirements are: (1) Install and maintain a firewall configuration to protect cardholder data; (2) Do not use vendor-supplied defaults for system passwords and other security parameters; (3) Protect stored data; (4) Encrypt transmission of cardholder data across open, public networks; (5) Use and regularly update antivirus software, (6) Develop and maintain secure systems and applications; (7) Restrict access to cardholder data by business need-to-know; (8) Assign a unique ID to each person with computer access; (9) Restrict physical access to cardholder data; (10) Track and monitor all access to network resources and cardholder data; (11) Regularly test security systems and processes; and (12) Maintain a policy that addresses information security.

[3] Note that the PCI Security Standards Counsel recently revised and updated the PCI DSS. Version 1.2 was released in October 2008, and PCI DSS compliance now means compliance with Version 1.2.

[4] Merchant Level and Compliance Requirements Defined, *available at* http://usa.visa.com/merchants/risk_management/cisp_merchants.html.

[5] *Cumis Ins. Soc'y v. Merrick Bank Corp.*, No. 07-cv-373-TUC-CKJ, 2008 WL 4277877 (Sep. 18, 2008).

[6] Jaikur Vijayan, *Banks, Credit Unions Begin to Sue Heartland Over Data Breach*, Computerworld, March 2, 2009, *available at* http://www.

computerworld.com/action/article.do?command=viewArticleBasic&articleId=9128841.

[7] The two less prominent payment card networks have a different system, though, where they are both the credit card issuers and the acquiring banks. Under their business models, the merchants have a contractual relationship with the payment card brand, which is also the credit card issuer. While these companies have not yet targeted merchants who suffer data security breaches, they will have much stronger claims than other credit card issuers because of their direct contractual relationship.

[8] *Sovereign Bank v. B.J.'s Wholesale Club*, 533 F.3d 162 (3rd Cir. 2008); *In re TJX Co.*, 524 F. Supp. 2d 83 (D. Mass. 2007).

[9] *Sovereign Bank*, 533 F.3d at 164.

[10] *Id*.

[11] *Id*. at 166.

[12] *Id*. at 167-68, 178.

[13] *Id*. at 167-68, 178.

[14] *Sovereign Bank v. BJ's Wholesale Club, Inc.*, 395 F. Supp. 2d 187, 192-93 (M.D. Penn. 2005).

[15] *Sovereign Bank*, 533 F.3d at 173-74, 183.

[16] *Id*.

[17] *Id*. at 166.

[18] *Id*. at 168.

[19] Restatement (Second) of Contracts § 302.

[20] Sovereign Bank, 533 F.3d at 168 (internal quotations omitted).

[21] *Id*. at 169.

[22] *Id*. at 169-70.

[23] *Id*. at 170.

[24] *Id*.

[25] *Id*. at 171.

[26] *Id*. at 173.

[27] *Id*.

[28] *Id*. at 179.

[29] *Id*. at 173 n.6.

[30] *Id*.

[31] *Id*.

[32] *In re TJX Co.*, 524 F. Supp. 2d at 86-87.

[33] *Id*.

[34] *Id*.

[35] *Id*. at 88.

[36] *Id*. at 90.

[37] *Id*. at 88-90.

[38] *Id*. at 89.

[39] *Id*.

[40] Minn. Stat. § 325E.64.

[41] *Id*.