

# Who is Minding the Legal Risk around PCI?

By David Navetta – ISSA member, Denver, USA chapter

**This article addresses some of the legal risk associated with PCI compliance and encourages organizations to equip themselves to address this risk when working toward compliance.**

When it comes to regulatory mandates of security such as those in GLB, HIPAA, SOX, the EU Data Protection Directive, and the FTC Act, there has always been a gray area between security and the practice of law. In fact, many security professionals find themselves in the midst of these regulatory compliance efforts oftentimes without the assistance of general counsel (or even an awareness by counsel that their involvement might be warranted). Under these circumstances, the obvious question is whether the organization is taking “legal risk” into account as security professionals make their decisions and take security-related actions to comply with these laws.

Ironically, the same holds true for the Payment Card Industry Data Security Standard (“PCI” or “PCI Standard”), which is not regulation. The main driver that has pushed PCI into the legal realm would be the lawsuits by consumers and banks that often are filed after a payment card security breach. For example, issuing banks have filed suits against merchants to recover their costs to reissue payment cards. These banks have alleged that these costs can amount to \$20-\$50 per card, multiplied by potentially thousands or millions of cards. It is in this context that an entity’s PCI-compliance efforts will be scrutinized under a different system and by a completely different audience: judges, juries, plaintiff lawyers, and regulators.

Yet, PCI compliance is often not viewed through a legal prism because legal counsel is not involved, and it is handled by IT professionals with no legal training or experience. The purpose of this article is to address some of the legal risk associated with PCI compliance and to encourage organizations to equip themselves to address this risk when working toward compliance.

## The link between PCI and the law

It is not unusual for a company suffering a payment card breach, especially a name brand company that is viewed as

having “deep pockets,” to be sued in multiple consumer class action lawsuits (see e.g., TJX, Hannaford, RBS Worldpay, and Heartland Payment Systems). In addition, that same company can expect either a lawsuit or behind-the-scenes legal maneuvering by issuing banks to recover their costs to reissue impacted payment cards. PCI compliance, and the manner by which PCI compliance is approached, is relevant in these lawsuits in several ways.

## Negligence

Negligence, the same theory or liability used by plaintiffs to sue for “slip and fall” or medical malpractice, can be used in a security context. To prevail in a negligence suit, a plaintiff must establish the following:

1. A duty to use ordinary care owed by the defendant
2. Breach of that duty
3. A proximate causal connection between the negligent conduct and the resulting injury
4. Resulting damage

In the PCI context, plaintiffs can allege negligence by arguing that a merchant handling payment card data has a duty to protect such data, and that the PCI Standard is evidence of what merchants must do to achieve “ordinary care” or “reasonable security.” If the merchant suffers a security breach exposing payment card data, the failure to comply with PCI would arguably amount to a breach of that duty.

In fact, in the lawsuit against TJX brought by issuing banks after its payment card breach, the banks were going down this road. The issuing banks retained an expert witness (former SVP for Security and Risk Management for MasterCard International) to opine on TJX’s PCI compliance efforts. The expert’s job was fairly simple because TJX’s own auditors had concluded that TJX only satisfied three of the 12 PCI requirements at the time of the breach.

Since TJX there have been several lawsuits filed against organizations that had been validated PCI-compliant at the time of the breach. It can be expected that plaintiffs and courts in these suits are going to finely scrutinize every decision, practice, and interpretation around the stated PCI validation. The plaintiffs' hope will be to discover that these merchants were not actually PCI-compliant despite the validation. In fact, as discussed below, they may get some help by the card brand's mandatory post-breach PCI assessment.

Actual PCI compliance, however, does not necessarily absolve an organization from liability in the negligence context. In fact, PCI, as an industry standard, should be viewed as the minimum or floor in terms of what a court will consider "reasonable security." The rationale for this was explained by Judge Learned Hand in the famous (for first year law students at least) *T.J. Hooper* case.<sup>1</sup>

In *T.J. Hooper*, the plaintiffs were shipping two barges full of cargo when the ships encountered a storm. The barges were accompanied by two tugboats owned by the defendants. Unfortunately the tugs were unable to safely pull the barges from the storm and the cargo they carried was lost. The plaintiffs asserted that the defendants were negligent because their tugboats were not equipped with effective radio sets capable of receiving warning of the storm.

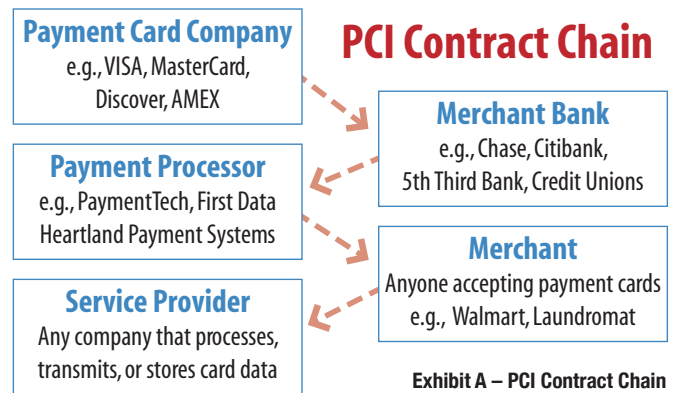
The defendants argued that they did not owe the plaintiffs a duty to carry such a radio because it was a new technology, and it was not a common practice in the tugboat industry to carry such radios. Judge Learned Hand disagreed:

Indeed in most cases reasonable prudence is in fact common prudence, but strictly it is never its measure. **A whole calling may have unduly lagged in the adoption of new and available devices....**Courts must in the end say what is required. There are precautions so imperative that even their universal disregard will not excuse their omission.

Translated to the PCI context, under the law, compliance with PCI is likely a necessity, but is not necessarily sufficient. Security professionals and organizations need to know that when determining which controls to implement to protect cardholder data, PCI compliance may not be enough in a court of law. There may be other actions to protect cardholder data, in addition to those specified in PCI, that satisfy "ordinary care" for purposes of a negligence action. In fact, under the law, as discussed below, the scope of a company's duty may actually vary depending on the particular circumstances and risk faced by that company.

### Contractual – issuing banks suing for breach of contract

In the first instance the duty to comply with PCI and payment card brand security programs arises from a chain of legal contracts (see Exhibit A). As such, one important measure of the liability associated with PCI compliance is dictated by the



scope of those contractual duties. The "merchant agreement" between a merchant and merchant bank (or payment processor working with a merchant bank) typically requires the merchant to comply with PCI as well as card brand security programs (e.g., Visa's CISP, Mastercard's SDP). The merchant will typically agree to indemnify and hold the merchant bank harmless for any fines, penalties, and liability arising out of the merchant's failure to comply with PCI and/or a merchant payment card security breach. These contractual obligations could lead to potential legal liability for breach of contract if an issuing bank incurs expenses to reissue payment cards.

In general, an entity can only sue for breach of contract if that entity is party to the contract and suing another party to the contract. Issuing banks typically do not have a direct contractual relationship with the merchants that suffer a security breach. However, the Federal appellate court in *Sovereign Bank v. B.J. Wholesale Club & Fifth Third Bank*, No. 06-3392/3405 (3rd Circuit, July 13, 2008) has allowed an issuing bank's breach of contract claim to continue against a merchant bank that sponsored a merchant. In short, the court agreed that the issuing bank could allege a breach of contract claim based on the contract between the merchant bank and Visa (see Exhibit B – Third Party Beneficiary Theory). If found liable under this theory, the merchant bank could then turn around and file suit against the non-PCI compliant merchant and demand that the merchant indemnify the merchant bank for any costs it is required to incur because of the merchant's security breach. Prior to this decision, issuing banks had a difficult time proceeding against merchant banks and merchants on any theory of liability.

### Statutory – plastic card protection laws

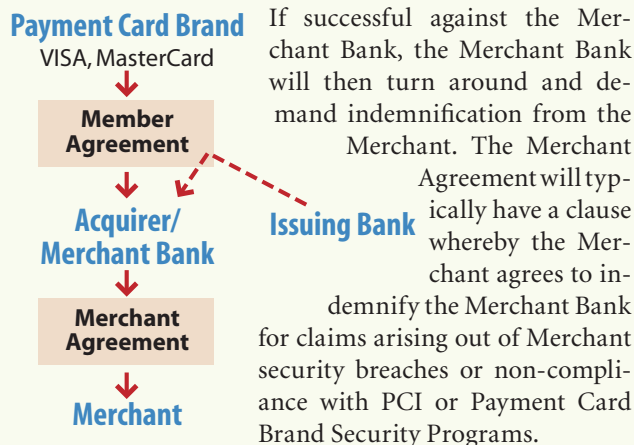
Several states have considered, and one state has actually passed, a "plastic card protection law." Minnesota's plastic card protection act essentially incorporates section 3.2 of PCI, which prohibits the storage of sensitive authentication data (security code data, PIN verification code numbers, or the full contents of any track of magnetic stripe data). Some of the bills that were not passed incorporated other sections of PCI directly into the law. Under the Minnesota law merchants holding sensitive authentication data for more than 48 hours that suffer a security breach must reimburse the issuing banks' reasonable costs to protect cardholder infor-

<sup>1</sup> *The T.J. Hooper* 60 F.2d 737 (2d Cir.), cert. denied, 287 U.S. 662 (1932).

### Third Party Beneficiary Theory

Under this theory of liability, despite the fact that Issuing Banks have no direct contractual relationship with the Merchant that suffered the payment card breach, they can effectively recover under a breach of contract theory.

As represented in the chart below, the Issuing Bank alleges that it is the intended third-party beneficiary of the Member Agreement between the Merchant Bank and Payment Card Brand. The Member Agreement will typically have security related terms, including terms that require the Merchant Bank to ensure that its Merchants are PCI compliant. It is the breach of this obligation that the Issuing Bank will use to try to recover its cost to reissue cards.



Note that it may also be possible for the Issuing Bank to sue the Merchant for breach of the Merchant Agreement under the same theory. The Issuing Bank would allege that it was the intended third-party beneficiary of the Merchant’s promise to comply with PCI and safeguard cardholder data as set forth in the Merchant Agreement.

The key to preventing this is strong contract language disclaiming all third-party beneficiaries. Merchants can make that happen in the Merchant Agreement, but do not have control over the terms of the relevant Member Agreement between the Merchant Bank and Payment Card Brand.

Exhibit B – Third Party Beneficiary Theory

mation and continue servicing cardholders, including reissuance costs. While the law was passed in Minnesota, it is not limited to Minnesota residents, and could arguably have a nationwide applicability for entities doing business in Minnesota and elsewhere in the United States. The Minnesota law (potentially others if they pass) provides a direct path to liability based in part on whether an entity was PCI-compliant.

### Legal risks faced by security professionals and their organizations

In light of the legal liability that could arise out of a failure to comply with PCI, organizations implementing PCI need

to be aware of potential legal pitfalls. The key question is whether security professionals working on PCI compliance understand how a judge, jury, plaintiff’s attorney or regulator will dissect and judge their PCI-related compliance activities. There are several areas where security practice and the law collide to create potential legal risk. If a lawyer is not working alongside a company’s security team, the failure to consider the potential legal pitfalls could come back to haunt an organization that suffers a payment card security breach.

### Resolving Ambiguities

One of the biggest challenges faced by organizations is resolving ambiguities in the PCI Standard as written and especially as applied to a particular organization or environment. Unfortunately, as PCI becomes a legal standard, the ambiguities arising out of the PCI Standard could increase the risk of legal liability. A natural consequence of these ambiguities is the need for security professionals (including qualified security assessors) to make “judgment calls.” A good example is the PCI concept of “compensating controls” which can allow an organization to avoid complying strictly to a particular PCI requirement if they believe, *in their judgment*, that existing controls address the same risk mitigated by the PCI requirement. Another example is the meaning of “proper due diligence” in PCI subsection 12.8.3. In fact, during various PCI-related meetings hundreds of ambiguities have been reported to exist (see Exhibit C at end of article for some more examples of potential ambiguities).

These judgment calls are going to be scrutinized under a microscope by a plaintiff’s attorney suing after a payment card security breach. The further an organization gets away from “strict” (e.g., “to the letter”) compliance with the particular PCI requirements, the more legal risk that organization will face if its PCI compliance status is challenged in court (see Exhibit D). Even if a security professional’s less than strict interpretation of a PCI requirement ultimately would meet the standard of care if put in front of a jury, the mere fact that there is a “deviation” from the strict wording of PCI gives a lawsuit legs and gives plaintiff attorneys litigation leverage, which in turn can induce a settlement to avoid a potentially disastrous jury award. The risk is further exacerbated by the typical fact scenario: organizations will essentially have to

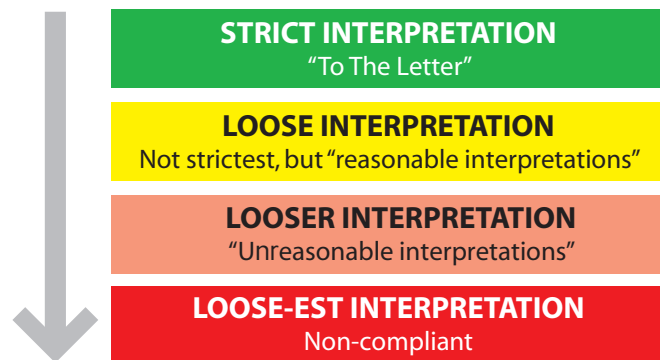


Exhibit D – Security Viewpoint v. Legal Viewpoint

prove to a jury that despite a security breach, their security was “reasonable.” That can be a difficult challenge and will be more daunting if the organization took a lot of interpretative liberties. In other words, being right on your judgment call at the end of the day will not necessarily eliminate legal risk, especially in the face of breach that has already occurred.

The problem is further complicated because there is no definitive way to resolve ambiguities under the PCI system. The PCI Council does provide some guidance and FAQs, and will sometimes give a straight answer to an email inquiry, but it is not clear to what extent PCI Council proclamations will have legally binding effect. In fact the PCI Council has specifically stated that some of its guidance documents are subordinate to the PCI Standard itself. In addition, resolving ambiguities may be difficult because multiple sources of interpretation exist: merchant banks, qualified security assessors (QSA), payment card brands, and the PCI Council. In some instances, for example, merchants have gone to their merchant banks (the parties with whom they contract) concerning an ambiguity and have received different answers from different banks. Unfortunately, unlike the accounting profession with the House of GAAP, there is no hierarchy of interpretations that indicates which interpretations trump other interpretations.

On the flip-side, some organizations focus narrowly on being “strictly compliant” with the letter of PCI, but fail to actually have controls in place to adequately reduce risk. The issue in this case is “depth of compliance.” Going back to the meaning of “proper due diligence” in PCI subsection 12.8.3, many QSAs will deem that requirement satisfied based solely on the word (or a document) from a service provider. Is this practice “deep enough” to actually address and mitigate the risk that is intended to be addressed by the control? Or should a merchant independently engage in some sort risk assessment and audit or verification of its service provider’s controls in order to achieve “proper due diligence?”

In fact, the concept of risk is one of the factors some courts take into account in determine whether a duty exists and whether it has been met for purposes of a negligence claim. Again, in another nautical-oriented lawsuit, Judge Learned Hand famously put forth the following legal concept:

Since there are occasions when every vessel will break from her moorings, and since, if she does, she becomes a menace to those about her; the owner’s duty, as in other similar situations, to provide against resulting injuries is a function of three variables: (1) The probability that she will break away; (2) the gravity of the resulting injury, if she does; (3) the burden of adequate precautions. Possibly it serves to bring this notion into relief to state it in algebraic terms: if the probability be called P; the injury, L; and the burden, B; liability depends upon whether B is less than L multiplied by P: i.e., whether  $B < PL$ .

This is a classic definition of risk incorporated and weaved into a legal framework around negligence. The idea of security controls matching to the risk posed is also represented

legally in laws like Gramm-Leach-Bliley, which describes its required information security program as follows:

*Information security program.* You shall develop, implement, and maintain a comprehensive information security program that is written in one or more readily accessible parts and contains administrative, technical, and physical safeguards **that are appropriate to your size and complexity, the nature and scope of your activities, and the sensitivity of any customer information at issue.**

What this implies (to be litigated of course) is that “surface” compliance with PCI may not be satisfactory in a court of law. In short, “proper” PCI compliance is likely to look different for a company like Heartland Payment Systems (100 million transactions a month; much risk) and your local laundromat (100 transactions a month; much less risk).

## Legally risky PCI practices

In addition to the challenge in resolving PCI ambiguities, certain approaches to PCI compliance and validation may pose legal risk to organizations. Again, any organization or security professional engaging in the practices described below should seek guidance as to how a judge, jury, or plaintiff’s attorney will scrutinize such behavior and PCI-compliance efforts in a security breach lawsuit.

### QSA shopping

Some companies, understandably, want to validate their PCI compliance as quickly and cheaply as possible. Rather than a security exercise, they may view validation as a means to ensure their continued ability to accept payment cards (the risk of losing that ability likely trumping their perceived risk of a security breach). With hundreds of qualified security assessors of varying sizes, sophistications, and skills, some companies will shop for the cheapest QSA that will validate their compliance in the least expensive and least painful way. To the extent the exercise focuses on the validation process and not security, and to the extent this process could potentially lead to mistakes or improper validation, an organization’s legal risk could increase.

### Rubber stamping

Another legally risky practice is “rubber stamping”: essentially failing to analyze actual security and simply treating PCI compliance like a facile checklist. In short, when QSA shopping occurs, rubber stamping is what can result. It can also occur for organizations doing self assessments, especially when the assessment is parceled out to overworked IT professionals who may lack the context to understand the impact of their actions and who may be under pressure to get PCI compliance done quickly and without much expense.

### Scoping

Some say that the first step in any journey is the most difficult. This can hold true in the PCI context when it comes to determining the scope of a PCI assessment. If an organi-

zation fails to properly identify its cardholder data environment, and conducts an assessment with respect to only a portion of such environment, its PCI compliance efforts may be for naught. Scoping can be difficult for companies that do not know exactly where cardholder data is being stored, processed, or transmitted on their systems. The legal risk posed in this instance is obvious: if a breach occurs with respect to part of a cardholder environment that did not have proper PCI controls in place, this fact will be used against the organization in court.

### Adverse admissions and attorney-client privilege

Unfortunately, not only must security professionals (and their general counsel) worry about how they achieve PCI compliance, in the legal context they must also be concerned about the paper trail and communications they leave in working toward compliance. What is being put in writing? Is it discoverable, e.g., will a plaintiff be able to get the documents in a lawsuit? How can the organization's communications about PCI compliance be used against it in a lawsuit? There are several instances where paper trail can hurt an organization in this context.

First, especially for companies just beginning PCI compliance or that have fallen out of compliance, it may not be unusual for emails and other documents going back in forth that essentially admit non-compliance. Second, in some cases, merchants or service providers will make promises (in writing) to acquiring banks or processors that they will become or work toward PCI compliance within a given time frame, for example six months. Last, if an organization suffers a payment card security breach, the payment card brands typically require a post-incident PCI audit. In each of these cases, the documents that are created and communications that occurred will normally be discoverable in a court of law (e.g., the plaintiff will be able to see copies and ask questions about them). This poses increased legal risk.

While it is inevitable that document trails will be created during the course of PCI compliance, it may be possible to shield some information from scrutiny. For example, the concept of attorney-client privilege or attorney work product doctrine may protect certain PCI-related conversations as long as legal counsel is involved and providing "legal advice"<sup>2</sup> or legal work product.

This is obviously true after a security incident has occurred and potential lawsuits loom, but less obvious is how attorney-client may potentially be utilized in working toward PCI compliance. To the extent that PCI impacts or is relevant to legal compliance, including for example being used as a yard marker to establish the standard of care in a negligence action or part of a legal contractual obligation, or where overlapping legal requirements may exist such as GLB, HIPAA, or SOX, some communications (between an organization's legal team

and security team) concerning PCI non-compliance may be protected. If general counsel (or outside counsel) utilizes the organizations internal security team<sup>3</sup> (or an outside team<sup>4</sup>) as an expert consultant to act as a translator of security issues for the purposes of providing legal advice, their communications, including some revealing non-compliance with PCI, may be shielded from court scrutiny.

In light of this, organizations may want to consider splitting their PCI compliance efforts into a remediation phase and an assessment phase. The remediation phase would involve a legal investigation coordinated by the organization's legal counsel with support from internal (or possibly external) security experts. The purpose of the remediation phase would be to analyze the legal impact of PCI compliance and to address and remedy areas of non-compliance. It may be possible, if set up properly, to cloak the remediation phase in attorney-client privilege. For example, communications concerning legal's opinions and advice on PCI ambiguities and decisions for resolving potential contractual non-compliance based on such ambiguities may be protected. If a breach were to occur, rather than a document trail evidencing the internal thinking and potential mistakes of an organization concerning PCI compliance, this information could be shielded from scrutiny by judges, juries, and plaintiff attorneys.

Once the remediation phase is finished, an independent assessment could take place to validate PCI compliance in an "assessment phase." Normally the activities and communications surrounding the assessment would be discoverable in a lawsuit. So if the assessor found and documented problems with PCI compliance, those would be used against the organization in court. Since those problems will have been fixed properly during the remediation phase, the assessor should essentially be providing a "clean opinion" without an adverse paper trail that could sink an organization.

Please be aware that the availability and effectiveness of attorney-client privilege in this context will depend entirely on the state of the law in the applicable jurisdiction and the actions of the organization and its legal counsel. It may not be available at all. For example, the privilege only applies when a client seeks "legal advice" and only if the attorney is acting pre-dominantly in a "legal capacity" (as opposed to a "business capacity"). As such, in the PCI context the engagement with the attorney must be seeking input concerning legal aspects of PCI. That advice may concern legal interpretation of contractual duties around PCI, or legal advice as to how PCI and ambiguities may be scrutinized in a court of law. Since

2 A party invoking the attorney-client privilege must show (1) a communication between client and counsel that (2) was intended to be and was in fact kept confidential, and (3) was made for the purpose of obtaining or providing legal advice. *United States v. Const. Prod. Research, Inc.*, 73 F.3d 464, 473 (2d Cir.1996).

3 The U.S. Supreme Court has held that the privilege protects communications by a corporate employee, regardless of position, when (1) the communications concern matters within the scope of the employee's corporate duties, and (2) the employee is aware that the information is being furnished to enable an attorney to provide legal advice to the corporation *Upjohn Co. v. United States*, 449 U.S. 383, 389 (1981). See <http://www.law.northwestern.edu/journals/njtip/v6/n2/2/#note12>.

4 For example, one court has ruled that the attorney-client privilege is not waived where the third-party consultant serves as a "translator" or "interpreter" of the client's communications with counsel. *United States v. Kovel*, 296 F.2d 918 (2d Cir. 1961) As the Second Circuit reasoned in *Kovel*, a case involving the use of an accountant, "accounting concepts are a foreign language to some lawyers," and the outside accountant may "interpret" the "client's story."

PCI is not a law like GLB, HIPAA, or SOX this argument may be more difficult to make (although in light of recent lawsuits, I believe it is fairly clear that PCI compliance has legal implications). As such, the privilege may not be available under the law, or may be lost if the engagement and communications are not handled properly. However, it is certain that if no attempt is made to ascertain and obtain attorney-client privilege, all of an organization's relevant adverse communications concerning PCI compliance will be discoverable in a court of law. In all, it will take some detailed legal analysis and careful planning to create an opportunity where attorney-client privilege might apply prior to any breach or litigation.

### PCI validation – false sense of security

Another key point that could increase the legal risk associated with PCI is the potentially false sense of security that can arise after being validated PCI-compliant. Validation does not necessarily equal compliance with PCI or “reasonable security” under the law. As discussed, a company may have made a mistake in their compliance efforts by misinterpreting a PCI ambiguity, failing to properly define the scope of a PCI engagement, or engaging in rubber stamping or QSA shopping. In addition, organizations must understand that PCI validation relates to compliance at a single point in time. Over the year between validation efforts, a company can become non-compliant with PCI. For example, if a PCI-compliant organization adds new system components to its network that store, process, or transmit cardholder data, those components could take the company out of compliance. In addition, to the extent that PCI requires particular security policies, if an organization has those policies in place but fails to actually follow them, they may not be PCI compliant. In fact, from a legal standpoint failing to follow your own policies can have very adverse consequences in a court of law.

Finally, confusion exists around the so-called PCI “safe harbor.” Some payment card brands have suggested to some degree that companies achieving PCI compliance may earn a “safe harbor” that offers some level of protection. However, the existence and scope of a “safe harbor,” especially from a legal perspective, is unclear. There does not appear to be any legal mechanism for an organization to achieve “safe harbor.” In other words, even if a merchant is PCI compliant there is no legal mechanism that would block a payment card brand, acquiring bank, or issuing bank from fining or penalizing the merchant, or preventing a lawsuit against the merchant, after a payment card security breach.

In fact, the description of the “safe harbor” on Visa’s website indicates that it is entirely at Visa’s option whether to refrain from imposing fines and penalties:

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.<sup>5</sup>

Previously, Visa’s website described its safe harbor as follows:

**Safe Harbor** – *Safe harbor provides members protection from Visa fines in the event its merchant or service provider experiences a data compromise. To attain safe harbor status:*

1. *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.*
2. *A member must demonstrate that prior to the compromise the merchant had already met the compliance validation requirements, demonstrating full compliance.*
3. *It is important to note that the submission of compliance validation documentation, in and of itself, does not provide the member safe harbor status. The entity must have adhered to all the requirements at the time of the compromise.<sup>6</sup>*

Until much more is learned about how alleged “safe harbors” work, and until service providers and merchants have a legal mechanism to actually enforce “safe harbor,” organizations should not assume they are protected. However, one possible option for merchants on this issue is to negotiate a “private safe harbor” in their merchant agreement with acquiring banks and processors. The goal would be to provide a contractually enforceable safe harbor that would block liability and fines and penalties coming from the merchant bank if the merchant was PCI compliant at the time of a breach.

### Conclusion

Despite its security-centric origins, PCI compliance is posing increased legal risk. For organizations with a strong risk management ethos the approach to PCI compliance will likely involve a legal perspective and risk analysis. That said, attorneys and security professionals now more than ever need to become aware of their respective worlds, communicate their concerns to each other, and translate those concerns into legal risk measurement and management.

There are several actions security professionals should consider to further this relationship and arm their organizations with the ability to identify and understand PCI-related legal risk:

- Draw your general and/or outside counsel into the PCI compliance process at the beginning
- Explore use of attorney-client privilege, and consider dividing PCI into two phases: (1) a remediation phase cloaked in attorney-client privilege, and (2) an assessment phase after all issues have been remediated (not protected by privilege)
- Reasonable security is the goal – not merely technical compliance with PCI

5 See [http://usa.visa.com/merchants/risk\\_management/cisp\\_overview.html](http://usa.visa.com/merchants/risk_management/cisp_overview.html) (last visited March 19, 2009). Note that this Visa webpage no longer even refers to “safe harbor.”

6 This was taken off of Visa’s website and can only be found at the Internet Archives: [http://web.archive.org/web/20070312081527/http://usa.visa.com/merchants/risk\\_management/cisp\\_overview.html#anchor\\_9](http://web.archive.org/web/20070312081527/http://usa.visa.com/merchants/risk_management/cisp_overview.html#anchor_9) (last visited March 19, 2009).

- Depth of compliance: do the controls in place mitigate the risk to an acceptable level?
- To reduce legal risk err on the side of caution for interpretations of PCI (stricter and to-the-word means less legal risk)
- Choose QSAs and internal assessors wisely – those that are not afraid to deliver bad news will be more likely to reduce legal risk

The key here is to at least expose this process to some legal scrutiny from an attorney that can understand how a judge, jury, or plaintiff's attorney may analyze the organization's PCI-compliance efforts. While in many cases the legal risk will not trump other concerns, and it may be burdensome for

the organization's security team to deal with their attorneys, an assessment of legal risk and implementing some legal risk mitigation techniques and tactics could save a company significantly if a breach occurs.

### About the Author

*David J. Navetta, Esq., CIPP, managing member InfoSecCompliance, LLC, is an attorney with over a decade of legal experience, including in the areas of contract drafting, litigation, insurance law and information security and privacy compliance. Mr. Navetta is now the vice-chair of the ABA's Information Security Committee and co-chair of the PCI Legal Risk and Liability Working Group. He can be reached at [djn@davidnavetta.com](mailto:djn@davidnavetta.com).*



#### Exhibit C – Examples of other PCI ambiguities

PCI Section	Description	Description of Ambiguity
n/a	"Store, transmit, process"	• Transmitting through an Internet browser
3.2	Do not store sensitive authentication data after authorization (even if encrypted)	• Pre-authorization (holding card open)
3.3	Masking PANs	• Meaning of "a legitimate business need" to see the full PAN
3.4	Encryption of Primary Account Number while stored	• "Strong cryptography" • Voice recording of PANs
3.5.2	Store cryptographic keys securely	• "Securely"
4	Encrypt transmission of cardholder data across open, public networks	• "Networks that are easily accessed by malicious individuals" (e.g., satellite) • "Open and public" OR "open or public"
11.3	Penetration testing	• Penetration testing beyond the cardholder data environment to networks/systems connected to cardholder data environment?

Many of the ambiguities surrounding PCI are contextual: the meaning/intent of PCI is unclear when applied to a certain fact scenario. Some, however, are inherent in the way PCI was drafted. The following is non-exclusive list of some examples of PCI ambiguities that have arisen (which were provided to the author from security assessors that work on PCI).