CHAPTER

Why is PCI Here?

3

INFORMATION IN THIS CHAPTER:

- What is PCI and Who Must Comply?
- PCI DSS in Depth
- Quick Overview of PCI Requirements
- PCI DSS and Risk
- Benefits of Compliance
- Case Study

Chances are if you picked up this book, you already know something about the Payment Card Industry Data Security Standard (PCI DSS); however, you might not have a full and clear picture of PCI DSS—both the standards and its regulatory regime—and why they are here. This chapter covers everything from the conception of the cardholder protection programs by the individual card brands to the founding of the PCI Security Standards Council (PCI SSC) and PCI DSS development. It also explains the reasons for PCI DSS's arrival that are critical in understanding how to implement PCI DSS controls in your organization. Many of the questions people ask about PCI DSS and many of the misconceptions and myths about PCI have their origins in the history of the program, so it only makes sense that we start at the beginning.

WHAT IS PCI AND WHO MUST COMPLY?

First, "PCI" is not a government regulation or a law.[1] As you know, when people say "PCI," they are actually referring to the PCI DSS Version 2.0 (at the time of this writing). However, to make things easy, we will continue to use the term *PCI* to identify the payment industry standard for card data security.

[1]PCI DSS or the elements of it have been adopted as actual law in at least two US states at the time of this writing. The State of Nevada explicitly called PCI DSS by reference and made it mandatory for some businesses operating in this state. The State of Minnesota has adopted select provisions of PCI DSS as a state law.

PCI Compliance. http://dx.doi.org/10.1016/B978-1-59-749948-4.00003-5

NOTE

PCI DSS applies to you if your organization accepts, processes, stores, and/or transmits member-branded card data. Member-branded card data is any card that is part of the Visa, MasterCard, American Express, Discover, and JCB payment schemes, including their subsidiaries. Should a new member be added to this list, their cards would also be included in the scope of PCI DSS compliance. Because of so-called "check" cards, you can expect that nearly every debit card will fall into the PCI DSS scope simply because they can be used as either a debit or member-branded credit card.

Unlike many other regulations, PCI DSS has a very simple and direct answer to the question "Who must comply?" Despite its apparent simplicity, many misunderstand the question to the point that they incorrectly name specific players as "in" or "out," which leads the authors to believe that many of such people have their own agenda. This always reminds us of a quote from Upton Sinclair, a noted American novelist, who said "It is difficult to get a man to understand something when his job depends on not understanding it" [1]. So, PCI's answer to "who must comply?" is any organization that accepts payment cards or stores, processes, or transmits credit or debit card data must comply with the PCI DSS.

It is very easy to understand the motivations for such broad applicability. It is pointless to protect card data only in a few select places; it needs to happen wherever and whenever said card data is present physically and electronically. You might be thinking, "why the data is present in so many places?" A recent MasterCard presentation at a payment security conference presented a curious statistic that there are more than 200,000 locations where payment card data is stored in large amounts. Visa believes that they work with over 32,000,000 acceptance locations, worldwide! Each of those could potentially be storing months or years of payment card data in places where criminals can steal it. Keep those statistics in mind as you read through the book to provide context on both the macro and micro scales. Without jumping too far ahead into our story, we'd say that in many cases, adjusting your business processes to not touch the card data directly will save you from a lot of security and compliance (and not just PCI DSS compliance!) challenges!

In this book, we are primarily concerned with merchants and service providers. Merchants are pretty easy to identify—they are the companies that accept credit cards in exchange for goods or services. The PCI official definition of a merchant [2] states: "a merchant is defined as any entity that accepts payment cards bearing the logos of any five members of PCI SSC (American Express, Discover, JCB, MasterCard, or Visa) as payment for goods and services." For example, a retail store that sells groceries for cash or credit cards is a merchant. An e-commerce site that sells electronic books is also a merchant.

However, when it comes to service providers, things get a bit trickier. PCI Council Glossary [3] states: "Business entity that is not a payment brand, directly involved in the processing, storage, or transmission of cardholder data. This also includes companies that provide services that control or could impact the security of cardholder

data. Examples include managed service providers that provide managed firewalls, IDS and other services as well as hosting providers and other entities. Entities such as telecommunications companies that only provide communication links without access to the application layer of the communication link are excluded." This definition is clunky and verbose. A better way to express service providers would be any entity that can affect the security of payment card information (excluding the same companies as the above definition does). If you have a provider that does something that can impact the security of cardholder data, they are a service provider and should be validated compliant with PCI DSS.

Sometimes a merchant can also be a service provider at the same time: "…a merchant that accepts payment cards as payment for goods and/or services can also be a service provider, if the services sold result in storing, processing, or transmitting cardholder data on behalf of other merchants or service providers [2]." A more esoteric business model could be when a company accepts credit cards as a payment for services it provides to other merchants who also accept credit cards. In this case, such an entity is both a merchant and a service provider. For example, if you provide hosted shopping cart and processing services to merchants and accept payment cards, you would be both.

Now that we have some baseline definitions described, we will describe the whole payment ecosystem for the purposes of PCI DSS.

Electronic Card Payment Ecosystem

Before we go into detail on PCI compliance, we'd like to paint a quick picture of an entire payment card "ecosystem" (see Figure 3.1).

Figure 3.1 shows all the entities in payment card "game":

- Cardholder, a person holding a credit or debit card.
- Merchant, who sells goods and services and accepts cards.
- Service provider (sometimes Merchant Service Provider (MSP) or Independent Sales Organization (ISO), who provides all or some of the payment services for the merchant.
- Payment processor, which is a particular example of an MSP.
- Acquiring bank, which connects to a card brand network for payment processing and also has a contract for payment services with a merchant.
- Issuing bank, which issues payment cards to consumers (who then become "card holders").

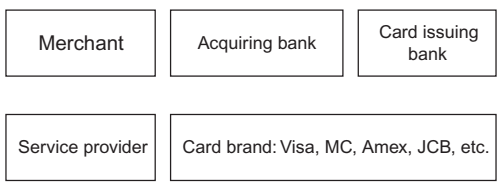


Figure 3.1 PCI Payment Ecosystem

- Card brand (also known as a payment brand or card scheme depending on regionalization), which is a particular payment "ecosystem" (called "association network") with its own processors, acquirers, and for the purposes of PCI DSS includes the member brands (Visa, MasterCard, American Express, Discover, and JCB).

The primary focus of PCI DSS requirements is on merchants and MSPs. This is understandable since this is exactly where most of the data is lost to malicious hackers. Whether TJX in 2005–2007 (45 or 90 million cards stolen, depending on the source) or Heartland Payment Systems in 2008–2009 (more than 100 million reported cards stolen [CITE THIS: http://voices.washingtonpost.com/securityfix/2009/01/payment_processor_breach_may_b.html]), merchants and service providers have let cards be stolen from them without incurring any of the re-issuing or replacement costs and without having a motivation to improve their security even to low levels prescribed by PCI DSS. While merchants were letting card data "run away," issuing banks were replacing them at their own cost and incurring other administrative and fraud costs as well. Thus, PCI DSS was born to restore the balance to the system by making sure that merchants and service providers took care of protecting the card data. The motivation for merchants to comply with PCI DSS comes in the form of fines, higher processing costs, and litigation risk.

Goal of PCI DSS

In light of what is mentioned above, PCI DSS is here to reduce the fraud risk of payment card transactions by motivating merchants and service providers to protect card data. Whether this goal is worthy, whether there are other secondary goals, or even whether this goal is being achieved by a current version of the data security standard is irrelevant. What matters to us is that PCI is aimed at reducing the fraud risk of transactions; and it seeks to accomplish that by making merchants and service providers pay attention to many key aspects of data security including network security, system security, application security, and security awareness and policy. Even more important, it encourages merchants to drop cardholder data entirely and conduct their business in a way that eliminates costly and risky data storage and on-site processing. A reduction of fraud is expected to be a natural result of such focus on security practices and technologies. One of the original PCI creators has also described PCI as the following: "the original intent was to design, implement, and manage a comprehensive, cost effective and reliable security effort" [4] and not a patchwork of security controls.

It is interesting to note that the "Ten Common Myths of PCI DSS" document from the PCI Council presents the six domains of PCI DSS as its goals [5]:

1. Build and maintain a secure network,
2. Protect cardholder data,
3. Maintain a vulnerability management program,
4. Implement strong access control measures,
5. Regularly monitor and test networks,
6. Maintain an information security policy.

While the above six domains can be seen as tactical goals while implementing PCI DSS, the strategic focus of PCI DSS is card data security, payment card risk reduction, and ultimately the reduction of fraud losses for merchants, banks, and card brands.

Overall, while motivating security improvements and reducing the risk of card fraud, PCI DSS serves an even higher goal of boosting consumer confidence in what is currently the predominant payment system—credit and debit cards. While we can debate whether paper, plastic, and metal money is truly on the way out, the volume of cashless transactions is still increasing annually though your percentage numbers will vary depending on how you slice the research. If anything—whether malicious hackers, insiders, or any other threat—can hinder it, our global economy will suffer losses. Thus, PCI DSS defends something even bigger than "bits and bytes" in computer systems, but the functioning of a major cog in the economic system itself.

Applicability of PCI DSS

Though the statements about accepting, processing, storing, and transmitting payment card data will probably sound tiresome by the time you are finished reading our book, remember that PCI DSS applies to all organizations that perform the above and there are no exceptions. Our Chapter 17, "PCI DSS Myths and Misconceptions" covers some of the common, industry-wide delusions and clarifies that the above PCI applicability is indeed the reality and not the myth.

The question of validating or proving PCI compliance is a bit different than the argument of PCI DSS applicability to organizations that deal with card data. The type of validation and requirements you must follow can differ for merchants and service providers, and by card brand and transaction volume.

First, there are different levels of merchants and service providers. Tables 3.1 and 3.2 show the breakdown.

Table 3.1 Merchant Levels

Merchant Level	Description
Level 1	Any merchant that has suffered a hack or an attack that resulted in an account data compromise (can vary based on payment brand), or any merchant deemed level 1 by any payment brand Any merchant that processes more than 6 million Visa, MasterCard, or Discover transactions annually 2.5 million American Express Card transactions or more per year, or any merchant that has had a data incident; or any merchant that American Express otherwise deems a level Merchants processing over 1 million JCB transactions annually, or compromised merchants (as RECOMMENDED), however, JCB doesn't have firm levels anymore. This is an approximation of level based on requirements from other payment brands.

Table 3.1 Merchant Levels

Merchant Level	Description
Level 2	Any merchant that processes between 1 and 6 million Visa or Discover transactions annually
	Any merchant with greater than 1 million but less than or equal to 6 million total combined MasterCard and Maestro transactions annually
	Any merchant that processes between 50,000 and 2.5 million American Express transactions annually
	Merchants processing less than 1 million JCB transactions annually
Level 3	Any merchant that processes between 20,000 and 1 million Visa or Discover card not present (e-commerce) transactions annually
	Any merchant with greater than 20,000 combined MasterCard and Maestro e-commerce transactions annually but less than or equal to 1 million total combined MasterCard and Maestro e-commerce transactions annually
	Any merchant that processes less than 50,000 American Express transactions annually
Level 4	All other Visa, MasterCard, and Discover merchants

Table 3.2 Service Provider Levels

Level	MasterCard	American Express	Visa Inc
Level 1	All third-party providers (TPPs), all data storage entities (DSEs) that store, transmit, or process greater than 300,000 total combined MasterCard and Maestro transactions annually	2.5 million American Express Card transactions or more per year; or any Service Provider that American Express otherwise deems a Level 1 Service Providers.	VisaNet processors or any service provider that stores, processes, or transmits over 300,000 transactions per year
Level 2	Includes all DSEs that store, transmit, or process less than 300,000 total combined MasterCard and Maestro transactions annually	50,000–2.5 million American Express Card transactions per year	Any service provider that stores, processes, or transmits less than 300,000 transactions per year
Level 3		Less than 50,000 American Express Card transactions per year	

As we mentioned above, these levels exist for determining compliance validation that is discussed in the next section. The levels are also sometimes used by the payment brands to determine which fines to impose upon the merchant for noncompliance.

NOTE

Visa Canada levels may differ. Visa Europe is also a separate organization that has different rules, especially as it relates to compliance around their Technology Innovation Program (TIP) and Chip & PIN (EMV) transactions. For more specific information, contact your acquiring bank to provide level and validation guidance.

PCI DSS IN DEPTH

In the next section, we take a detailed look at PCI DSS standard, its entire regulatory regime, deadlines, as well as related security vendor certification programs.

Compliance Deadlines

Now that we touched upon the compliance basics, it is time to face the painful fact: for the most part, all the PCI DSS compliance deadlines are *in the past* (See Table 3.3). This means that yesterday was the time to be compliant. There are additional dates for various other related requirements (such as card brand dates for Payment Application Data Security Standard [PA-DSS] compliance or specific programs like Visa's Technology Innovation Program [TIP]), but all core PCI DSS compliance dates have indeed passed. In some cases, you will find some dates that are in the future like MasterCard's new Levels 1 and 2 dates, but those are in the future simply because the criteria changed, thus merchants have a period of time to adjust their operations accordingly.

Some of you may recall receiving a letter that had a target compliance dates. Such letters today are rare since the dates for PCI DSS compliances have passed, but can happen when you change levels or when looking at non-US compliance efforts. These dates may or may not be aligned with the card brands' global published dates. This is because the card brands may not have a direct relationship with you and are working through your acquiring bank who sponsors you into the payment network.

Thus, barring unusual circumstances, the effective compliance deadlines have long passed. Various predecessor versions of the PCI 1.2 standard had unique dates associated with them, so if your compliance efforts have not been aligned to the card

Table 3.3 Original Compliance Dates for Merchants: All Passed

Level	American Express	MasterCard	Visa Inc
Level 1	October 31, 2006	June 30, 2005 or December 31, 2010 for merchants that are self-certified previously	June 30, 2004
Level 2	March 31, 2007	June 30, 2004	June 30, 2007
Level 3	N/A	June 30, 2005	June 30, 2005
Level 4	N/A	N/A	N/A

TIP

When in doubt, always follow the guidance of the legal professionals responsible for reviewing and advising on your contracts.

brand programs, you are way behind the curve and will not likely get any sympathy from your bank.

As far as additional dates by card brands, please refer to the following resources[2]:

- *Visa:* http://usa.visa.com/merchants/risk_management/cisp_key_dates.html. This page includes dates such as "US Level 1 Merchants Full PCI DSS Compliance Validation Deadline" (September 30, 2010) and "US Level 2 Merchants Full PCI DSS Compliance Validation Deadline" (December 12, 2010).
- *MasterCard:* www.mastercard.com/us/company/en/whatwedo/determine_merchant.html. This page includes recent change for merchant compliance validation for Levels 1 and 2 merchants with an associated deadline of June 2012 (only for on-site validation by an Internal Security Assessor [ISA]).
- *Discover:* www.discovernetwork.com/merchants/data-security/disc.html. This page contains no additional deadlines and simply refers to the PCI Council site. Merchant levels and reporting criteria are listed on subsequent pages after clicking links on the left.
- *American Express:* www209.americanexpress.com/merchant/singlevoice/dsw/FrontServlet?request_type=dsw&pg_nm=merchinfo&ln=en&frm=US. This page does not contain any additional deadlines, but validation requirements and merchant levels are different than other brands.
- *JCB:* partner.jcbcard.com/security/jcbprogram/index.html. Merchant levels here are not labeled in levels, but split into two thresholds and two different classes based on the types of payments you accept.

Compliance and Validation

As we mentioned before, depending on your company's merchant or service provider level, you will either need to go through an annual on-site PCI assessment by a Qualified Security Assessor (QSA) or Internal Security Assessor (ISA), or complete a Self-Assessment Questionnaire (SAQ) to validate compliance. In addition to this, you may have to present the results of the quarterly network perimeter scans to be performed by an approved scanning vendor (ASV).

If you are filling out a SAQ or doing other self-assessing under the ISA program, keep in mind that third parties may question your documentation a bit more simply because there is no third party validation. We recommend that you use a combination

[2]Please note that these URLs change frequently. Please go to pcicompliancebook.info for more up to date links if these do not work.

Table 3.4 PCI DSS Validation Requirements

Merchant or Service Provider Level	Visa USA		MasterCard	
Level 1	ASV scan	QSA on-site assessment	ASV scan	QSA on-site assessment
Level 2	ASV scan	SAQ self-assessment	ASV scan	QSA/ISA on-site assessment or assisted SAQ completion
Level 3	ASV scan	SAQ self-assessment	ASV scan	SAQ self-assessment
Level 4	ASV scan if requested by the acquirer	SAQ self-assessment	ASV scan if requested by the acquirer	SAQ self-assessment

of ISA and QSA (where an on-site assessment is required) resources to perform your annual assessment to be sure you get a thorough and fair result.

When submitting a SAQ, it will have to be physically signed by an officer of your company.[3] At the present time, there is no court precedent for officer liability as a result of false PCI DSS compliance attestation. However, industry speculation is that this person may be held accountable in a civil court, especially if he or she intentionally misrepresents information while certifying.

If you are planning on submitting a Report on Compliance (ROC) instead of the SAQ, you will need to follow the document template outlined in the PCI DSS Security Assessment Procedures document. This document is the same document that contains the PCI DSS requirements in their entirety and is available on the PCI Security Council's website. After the SAQ has been filled out or the ROC has been completed, it must be sent along with all the necessary evidence and validation documentation to the acquiring organization or processor. It depends on who requested the compliance validation in the first place.

It is a common misconception that the compliance requirements vary among the different levels. Both merchants and service providers must comply with the entire DSS, regardless of their level and validation requirements. What varies is the way and frequency you report compliance upstream. If you determine you are a Level 4 Merchant, don't interpret the "recommended" under validation requirements to mean PCI DSS compliance is optional. Visa Web site explains it like this: "In addition to adhering to the PCI DSS, compliance validation is required for all service providers [6]."

The validation mechanisms, as of the time of this writing, are given in Table 3.4.

Further, the scope of PCI DSS validation differs based on the exact way the organization interfaces with card data. Specifically, quoting from the PCI Council Web

[3]Electronic attestation of a full digital copy has also been considered acceptable.

NOTE

Discover and JCB handle merchant PCI compliance validation differently. Contact your acquirer for more information.

site, the circumstances that affect what sections of the SAQ the merchant should complete for validation are provided in Table 3.5.

So, to summarize, the exact scope of any one's PCI DSS validation depends on the following:

- Merchant or service provider status,
- Transaction volume,
- Card brand,
- The method of accepting cards and interacting with card data.

The specific validation requirements can change. For example, MasterCard recently announced that Level 2 merchants now need to be validated via an on-site assessment from a QSA or have the person performing the SAQ be a current ISA. Expect validation requirements to become stricter in the future from all payment brands.

Interestingly enough, companies can be merchants and service providers at the same time. If this is the case, the business should be described in detail in the

Table 3.5 SAQ Validation Types Based on Card Acceptance Methods

Card Processing	Self-Assessment Validation
Card-not-present (e-commerce or mail/telephone-order) merchants, all cardholder data functions outsourced. This would never apply to face-to-face merchants	SAQ type A, which is the smallest. It only includes parts of 2 out of 12 requirements, 13 questions
Imprint-only merchants with no electronic cardholder data storage, or standalone, dial-out terminal merchants with no electronic cardholder data storage	SAQ type B, which covers sections of 5 out of 12 requirements, 29 questions
Merchants using only web-based virtual terminals, no electronic cardholder data storage	SAQ type C-VT, which covers sections of 9 out of 12 requirements, omitting unique IDs (Req 8) logging (Req 10), and regular testing (Req 11)
Merchants with payment application systems connected to the Internet, no electronic cardholder data storage	SAQ type C, which covers sections of 11 out of 12 requirements; curiously, it does not include the logging requirement (Req 10)
All other merchants not included in descriptions for SAQ types A through C above, and all service providers defined by a payment brand as eligible to complete an SAQ	SAQ type D, which includes all the 12 requirements and a full set of questions

NOTE

Although American Express, Discover, and Visa allow Level 1 merchants to have their PCI compliance validated by the merchant's internal audit group, MasterCard does not explicitly allow this. To qualify for internal validation under MasterCard's new rules, the professional performing the assessment must be a current Internal Security Assessor (ISA). Check the PCI Council's website for more information on this program, including the steps required to join.

WARNING

Don't let yourself become complacent. If you are a Level 4 merchant across the board and are not required to do anything to validate your compliance with PCI DSS, remember, by accepting even one card per year, you must comply with PCI DSS. Many Level 4 merchants end up in big trouble when they realize they had to comply with PCI DSS regardless of their validation requirements. In addition, due to different validation levels across major card brands, their situation in regards to PCI compliance may be much worse. Don't let a breach put you out of business from fines and fees. Ensure you are complying with PCI DSS at all times for all levels.

assessment documentation and the compliance validated at the most stringent level. In other words, if a company is a Level 3 Visa merchant and a Level 1 Visa service provider, the compliance verification activities should adhere to the requirements for a Level 1 Visa service provider.

One notable PCI assessor, Walt Conway, relates the following educational story about merchant and provider validation:

> *"My favorite is when the vendor replies that they are compliant as a Level 3 (or 2 or whatever) merchant. That response is completely irrelevant and inexcusably misleading. That they are compliant as a merchant is meaningless to you when you use them as a service provider. They can self-assess as a merchant—they cannot as a Level 1 service provider. That extra step is meant to protect you. If you get that kind of reply, you are likely dealing with an over-eager and/or ill-informed sales rep…ask to talk to an adult [7]."*

History of PCI DSS

To better understand the PCI DSS role, motivation, and future, let's review its origins and history.

PCI DSS evolved from the efforts of payment brands battling fraud and counterfeiting. In the 1990s, the payment brands developed various standards to improve the security of sensitive information. In the case of Visa (formerly a regional association model), different regions came up with different standards because European countries and Canada were subject to different standards than the US. In June 2001, Visa launched the Cardholder Information Security Program (CISP, mostly pronounced

KISP). The CISP Security Audit Procedures document version 1.0 was the granddaddy of PCI DSS. These audit procedures went through several iterations and made it to version 2.4 in mid-2004. At this time, Visa was already collaborating with MasterCard on creating a single mechanism for merchants to go through. Their agreement was that merchants and service providers would undergo annual compliance validation according to Visa's CISP Security Audit Procedures and would follow MasterCard's rules for vulnerability scanning. Visa maintained the list of approved assessors and MasterCard maintained the list of ASVs.

This collaborative relationship had a number of problems. The lists of approved vendors was not well-maintained, and there was no clear way for security vendors to get added to the list for each particular card brand. To complicate things further, every card brand division did not endorse the program. Other brands such as Discover, American Express, and JCB were running their own programs as well, further clouding the compliance requirements and process. The merchants and service providers in many cases had to undergo several independent assessments by different "certified" assessors just to prove compliance to each brand, which was cost too much and yielded a low quality result. For that and many other reasons, the five major payment brands came together and created the PCI DSS 1.0, giving us the concept of PCI compliance.

Unfortunately, the issue of ownership still was not fully addressed, and just under two years later on September 7, 2006 we saw the founding of the PCI Security Standards Council and its website www.pcisecuritystandards.org. Comprised of American Express, Discover Financial Services, JCB, MasterCard Worldwide, and Visa International, the PCI Council (as it came to be known) maintains the ownership of the DSS, approved vendor lists, training programs, and interpretation responsibility for the requirements.

Even today, each card brand/region still maintains its own security program beyond PCI. These programs go beyond the data protection charter of PCI and include activities such as fraud prevention. The information on such programs can be found in Table 3.6. In certain cases, your PCI ROC may need to be submitted to a payment brand's program office separately if you have separate processing relationships with them.

PCI Council

The PCI Council or, fully, PCI Security Standards Council or PCI SSC, describes itself as "open global forum, launched in 2006, that is responsible for the development,

> **NOTE**
>
> Since our last edition, the Council has been busy adding to their sphere of influence. Forensic investigators are now qualified by the Council under the PCI Forensic Investigator (PFI) program, and the Payment Application Qualified Security Assessor (PA-QSA) program is in full swing listing approved assessors for the Payment Application Data Security Standard (PA-DSS).

Table 3.6 Brand Security Programs

Card Brand	Additional Program Information
American Express	Web site: https://www209.americanexpress.com/merchant/singlevoice/dsw/FrontServlet?request_type=dsw&pg_nm=home&ln=en&frm=US E-mail:American.Express.Data.Security@aexp.com
Discover	Web site: http://www.discovernetwork.com/merchants/data-security/index.html E-mail: askdatasecurity@discoverfinancial.com
JCB	Web site: http://partner.jcbcard.com/security/jcbprogram/index.html E-mail: riskmanagement@jcbati.com
MasterCard	Web site: http://www.mastercard.com/us/company/en/what-wedo/security_fraud_management.html E-mail: sdp@mastercard.com
Visa Inc.	Web site: www.visa.com/cisp E-mail: cisp@visa.com
Visa EU	Web site: http://www.visaeurope.com/en/businesses__retailers/payment_security.aspx
Visa Canada	Web site: www.visa.ca/ais

management, education, and awareness of the PCI Security Standards, including the Data Security Standard (PCI DSS), Payment Application Data Security Standard (PA-DSS), and PIN Transaction Security (PTS) requirements" [8].

The PCI Council charter provides oversight to the development of various PCI security standards (including PCI DSS, PA-DSS, and PTS) globally as well as maintaining the four vendor certifications programs for on-site assessments (QSA and PA-QSA), scanning companies (ASV), and forensic investigators (PFI). The PCI Council publishes the updated DSS, at the time of this writing at version 2.0, which is accepted by all brands and international regions; it also updates the supporting documents such as the "PCI Quick Reference Guide" and "Prioritized Approach for DSS 2.0" and a slew of supporting documents ranging from interpretation guidance to output from the various Special Interest Groups.

The lists of current PA-QSA, QSA, and ASV companies are located at the council Web site: https://www.pcisecuritystandards.org/approved_companies_providers/index.php. In addition, the Council also runs the Quality Assurance Program (QA Program) for QSAs, PA-QSAs, and ASVs, which are aimed at boosting the overall quality and maintaining the integrity of site assessments and vulnerability scans.

The PCI Council is technically an independent industry standards body, and its exact organizational chart is published on its Web site (https://www.pcisecuritystandards.org/organization_info/org_fact_sheet.php). Since our last writing, the Council staff has grown quite a bit, but it still remains a relatively small force of people managing the standards side of the PCI ecosystem.

The PCI ecosystem immediately felt the positive impact of the PCI Council. Merchants and service providers can now play a more active role in the compliance program and

TOOLS

At the time of this writing, PCI Council provides a few useful tools to help track PCI DSS compliance. These are explained in the following (all available here: https://www.pcisecuritystandards.org/security_standards/documents.php):

"Prioritized Approach for DSS 2.0" tracking spreadsheet allows for easy compliance program tracking and reporting, whether internal or to the card brands or acquirers.

The "SAQ Instructions and Guidelines" document is helpful for those validating PCI compliance via an SAQ. The PCI Council provides the fillable documents that can be used for tracking compliance at a small organization. All the SAQs can be obtained for free.

"Attestation of Compliance" forms are also provided by the PCI Council. These forms accompany the SAQ during self-assessment or the ROC after the on-site assessment.

the evolution of the standard, whereas the QSA, PA-QSAs, and ASVs find it much easier to train their personnel.

To summarize, the most important things to know about PCI Council are as follows:

- The Council maintains and updates the PCI DSS, PA-DSS, and PTS, as well as all of their related supporting documents.
- The Council does *not* deal with PCI validation process and, specifically, with enforcement via fines or other means. These responsibilities are retained by the payment brands.
- The Council also certifies and maintains the lists of security vendors as QSAs, PA-QSAs, and ASVs, as well as polices the vendors to maintain the integrity of PCI validation.

Let's look at QSAs, PA-QSAs, PFIs, and ASVs in more detail.

QSAs

The PCI Council administers the Qualified Security Assessor (QSA)[4] program in which members are allowed to conduct on-site DSS compliance assessments. These companies have gone through the application and qualification process, having had to show compliance with tough business, capability, and administrative requirements. QSAs must invest in personnel training and certification to build up a team of assessors, also called QSAs.

QSAs have to recertify annually via a computer-based training module. The exact qualification process and the requirements are outlined on PCI Council Web site; however, of particular interest are the insurance requirements. QSAs are required to carry high coverage policies, much higher than typical policies for the professional service firms, which becomes important later. A recent lawsuit ("Merrick Bank v. Savvis," see more details in [9]) presents an example risk that QSAs face. In this

[4]In the past, there was a different name for a company (QSAC or Qualified Security Assessor Company) and an individual professional employed by such company (QSA or Qualified Security Assessor).

NOTE

QSAs are only permitted to conduct on-site DSS assessments. They are not automatically granted the right to perform perimeter vulnerability scans, unless they also certify as an Approved Scan Vendor (ASV). Many companies today can be found on multiple lists (QSAs, PA-QSAs, PFIs, and ASVs) to be able to provide complete PCI validation services to merchants and service providers.

suit, a bank is suing the assessor who validated CardSystems, a victim of a massive card data breach, as PCI compliant. Please use Google to find out how the lawsuit progressed and who won; the results will not be known before the book goes to print.

Individuals wanting to become a QSA must first and foremost work for a QSA company or for a company in the process of applying to become a QSA. Then, they must attend official training administered by the PCI Council and pass a written test. They must also undergo annual requalification training to maintain their status. An individual may not be a QSA, unless he or she is presently employed by a QSA company; however, a QSA can carry the certification between QSA companies when changing jobs.

We cover the tips on working with your QSA in Chapter 11, "Don't Fear the Assessor." If there is one thing to remember when engaging a QSA, the QSA should be your partner. Treating your QSA like an auditor will only lead to a painful process whereby both parties end up frustrated and disillusioned.

PA-QSAs

Payment Application Qualified Security Assessors (PA-QSAs) assess payment applications as part of the Payment Application Data Security Standard (PA-DSS) program that used to be Visa's Payment Application Best Practices (PABP) program. Individuals wanting to assess applications under this standard must apply for a special designation called a PA-QSA and take additional training. You cannot be a PA-QSA

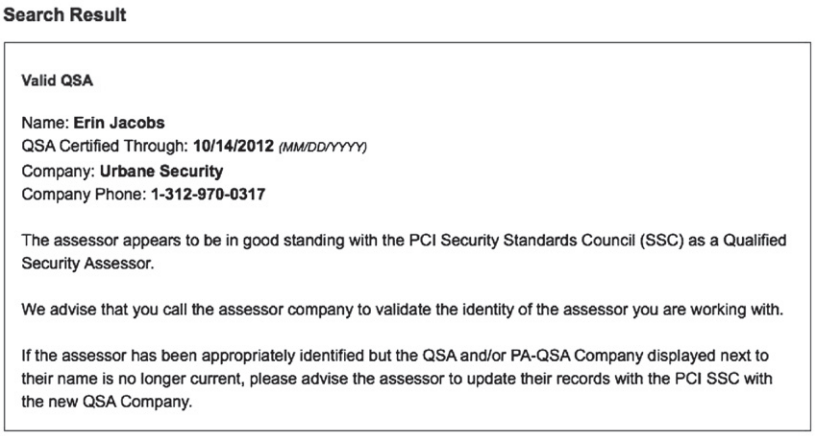
NOTE

The QSAs are approved to provide services in particular markets or subsets of markets: US, Asia Pacific, CEMEA (Central Europe, Middle East, and Africa), Latin America and the Caribbean, and Canada. The qualification to service a particular market depends on the QSA's capabilities, geographic footprint, and payment of appropriate fees.

TOOLS

Anybody can look up the individuals with current QSA certification by using QSA Employee Lookup at www.pcisecuritystandards.org/qsa_lookup/index.html.

See Figure 3.2 for an example.


Search Result

Valid QSA

Name: **Erin Jacobs**
QSA Certified Through: **10/14/2012** *(MM/DD/YYYY)*
Company: **Urbane Security**
Company Phone: **1-312-970-0317**

The assessor appears to be in good standing with the PCI Security Standards Council (SSC) as a Qualified Security Assessor.

We advise that you call the assessor company to validate the identity of the assessor you are working with.

If the assessor has been appropriately identified but the QSA and/or PA-QSA Company displayed next to their name is no longer current, please advise the assessor to update their records with the PCI SSC with the new QSA Company.

Figure 3.2 QSA Employee Lookup Tools

without first becoming a QSA, and just like in the QSA world, your company must be signed up as a PA-QSA company in order to perform PA-DSS assessments against payment applications. PA-DSS is outside the scope of this book, but you can read about it on the PCI Security Standards website.

Principal-Associate QSAs

This special case, not to be confused with the PA-QSA above, can allow certain individuals to perform functions as a QSAs under the agreement of another, larger QSA company. The use case for this special group of people is for new or small markets that may not be able to sustain a full QSA company, but need to have a local, trained consultants to perform an on-site assessment for a willing merchant or service provider. Branden used this concept at VeriSign when he needed local services in Australia but didn't have an official presence there after we exited the market as a business. Branden found a local Australian company that was willing to pay the reduced Principal-Associate QSA registration fees, so he hired them and they fell under VeriSign's global QSA designation.

PFIs

PCI Forensic Investigators (PFIs) combine all the individual payment brand programs around forensic investigations into one Council program like all the others you have read about. Like PA-QSAs, PFIs must be a QSA, and companies with the designation must also be QSAs in each region they want to do PFI work. There is no training requirement for PFIs, however they must have experience on their resume and should include copies of certificates from their forensic-related training courses for review.

Contrary to popular belief, even though the Council manages the PFI program, they do not get copies of the forensic reports to create that closed-loop feedback channel the industry is asking for as it relates to negligence by a QSA, PA-QSA, or ASV after a breach.

ASVs

As you know, PCI DSS validation also includes network vulnerability scanning by an ASV.

To become an ASV, companies must undergo a process similar to QSA qualification. In addition to a training class for each analyst to be trained and performing ASV related duties, ASVs must submit a scan report conducted against an outsourced test network perimeter. ASVs must certify at least two analysts before they can be approved. An organization can choose to become both a QSA and an ASV, or they could simply do one or the other.

ASVs are authorized to perform external vulnerability scans from the Internet, but PCI DSS also mandates internal vulnerability scans (performed from inside the company network), which can be performed by any qualified individual like an internal security team or consultant.

We cover all the tips on working with your ASV in Chapter 8, "Vulnerability Management."

QUICK OVERVIEW OF PCI REQUIREMENTS

Now it is time to briefly run through all 12 PCI DSS requirements, which we cover in detail in the rest of this book.

PCI DSS version 2.0 is comprised of six control objectives that contain one or more requirements:

- Build and maintain a secure network.
  - *Requirement 1*: Install and maintain a firewall configuration to protect cardholder data.
  - *Requirement 2:* Do not use vendor-supplied defaults for system passwords and other security parameters.
- Protect cardholder data.
  - *Requirement 3:* Protect stored cardholder data.
  - *Requirement 4:* Encrypt transmission of cardholder data across open, public networks.
- Maintain a vulnerability management program.
  - *Requirement 5:* Use and regularly update antivirus software.
  - *Requirement 6:* Develop and maintain secure systems and applications.
- Implement strong access control measures.
  - *Requirement 7:* Restrict access to cardholder data by business need to know.

  - *Requirement 8:* Assign a unique ID to each person with computer access.
  - *Requirement 9:* Restrict physical access to cardholder data.
- Regularly monitor and test networks.
  - *Requirement 10:* Track and monitor all access to network resources and cardholder data.
  - *Requirement 11:* Regularly test security systems and processes.
- Maintain an information security policy.
  - *Requirement 12:* Maintain a policy that addresses information security for all personnel.

The above-mentioned 12 requirements cover a vast spectrum of information technology (IT) areas as well as venture outside of IT in Requirement 12. Some requirements are very technical in nature (e.g. Requirement 1 calls for specific settings on the firewalls), and some are process and policy-oriented (e.g. Requirements 7 and 12) and even go into contract law (some of the subrequirements in Requirement 12 cover the interactions with MSPs.

The detailed coverage of controls makes things easier for both the companies that have to comply with the standards, the auditors (in case of Sarbanes–Oxley Act of 2002 [SOX] or other laws and standards), or the assessors (in case of PCI DSS). For example, when compared to SOX, companies do not have to invent (or pay for somebody to invent) the controls for them; they are already provided. This can also create challenges as more compliance initiatives become more prescriptive about their required controls, companies are forced to create a common control set and map them back to all of the individual compliance requirements.

What is interesting is that almost every time there is a discussion about PCI DSS, someone would claim that PCI is too prescriptive. In reality, PCI being prescriptive is the best thing since antivirus solutions invented automated updates (hopefully, you can detect humor here). PCI DSS prescriptive nature simply means that there is some specific guidance for people to follow and be more secure as a result (if they follow the spirit and not only the letter of PCI standards)! Sadly, in many cases, the merchants who have to comply with PCI DSS and who still think it is "too fuzzy" and "not specific enough" are the ones either fighting to comply in the first place, or looking for a simple compliance and security *to do* list or a task list; and no external document that guarantees that your organization will be secure can ever be created.

In particular, when people say "PCI is too prescriptive," they actually mean that it engenders "checklist mentality" and leads to following the letter of the mandate blindly without thinking about why it was put in place. For example, it says "use a firewall," so they deploy a shiny firewall with a basic "ALLOW ALL<->ALL" rule—an obvious exaggeration that clarifies the message here. Or, they have a firewall with a default password unchanged, or maybe slightly more secure by allowing all outbound and denying most inbound traffic. In addition, the proponents of "PCI is too prescriptive" tend to think that fuzzier guidance (and, especially, prescribing the desired end state *and* not the tools to be installed) will lead to people actually think about the best way to do it.

So, the choices to write security-motivated regulatory guidance are as follows:

1. Mandate the tools (e.g. "must use a firewall") and risk "checklist mentality," resulting in both insecurity and "false sense" of security.
2. Mandate the results (e.g. "must be secure") and risk people saying "yes, but I don't know how" and then not acting at all, again leading to insecurity and a wide interpretation of intent.

The author team is of the opinion that in today's reality #1 works better than over pill #2, but with some pause to think, for sure. Although the organizations with less mature security programs will benefit at least a bit from #1, organizations with more mature programs might be able to operate better under #2. However, data security today has to cover the less-enlightened organizations, which makes #1 choices—embodies by PCI DSS—the preferred one.

As a far as scope of PCI DSS within the organization is concerned, PCI compliance validation may affect more than what you consider the "cardholder environment." According to PCI DSS 2.0, the scope includes the cardholder data environment as well as anything connected to it. Chapter 4 will help you with the scoping problem including giving you some ideas on how to reduce its impact. If you do not have basic network segmentation controls in place, the scope of PCI compliance validation will cover your entire network. Think about it: if you cannot ensure that your cardholder data is confined to a particular area, then you cannot focus on this area alone, and you have to look everywhere.

For the benefit of consumers who may be more familiar with a brand name rather than a parent company (e.g. TJX is the corporate parent of TJ Maxx), PCI compliance validation should always follow the merchant ID. Any transaction processed under that merchant ID, regardless of origin, should fall under that company's PCI validation process.

You may discover that you are unable to always comply with the strict letter of PCI DSS while still striving for its spirit. For example, you may need to temporarily

NOTE

Just because a POS system is on the list of compliant payment applications (PA-DSS), it does not mean that your particular implementation is compliant. Also, it definitely does not mean that your entire organization is PCI compliant. Only applications configured and maintained according to their PA-DSS Implementation Guide will be able to operate in a compliant manner. You should work with the application vendor and with your QSA to verify this.

In order for the device to be added to the PA-DSS list, the payment application, online shopping cart, or POS vendor has to show and document the secure method for their application deployment. However, it is ultimately the merchant responsibility to follow the secure and compliant deployment guidance.

For merchants using an integrator or reseller, ensure they are deploying and managing your POS in a compliant manner. Most do not do this, and it forced the Council to create the Integrator/Reseller Task Force late in 2011 to address this problem.

store cardholder data unencrypted for troubleshooting purposes or to use a password of less than mandated minimum length on a legacy system. Another example may include recording certain call-center conversations for customer service purposes. Again, card brands understand that these recordings may contain cardholder data, so accommodations must be made accordingly to protect that data.

In many cases, compensating controls have to be used to achieve compliance when your company cannot exactly meet a given requirement. The important thing to remember about compensating controls is that they have to go beyond the requirements of PCI to provide the same or higher assurance of cardholder data protection. When compensating controls are used you must gather and supply additional documentation about the control. Please see Chapter 12, "The Art of Compensating Control" for detailed coverage of compensating controls.

Changes to PCI DSS

One of the key challenges for any security standard is to change fast enough to address the changes to the threat environment (and this changes literally every day since the criminal computer underground has to evolve to stay in business) and to change slow enough to still be considered a technical standard (and not simply advise to "do the right thing"). For prescriptive technical standards that directly call out security controls such as firewalls, network intrusion prevention, and vulnerability scanning, the challenge is even more extreme.

PCI DSS is sometimes criticized for being "constantly in flux" and for "not moving fast enough" at the same time, but by different people.

The PCI standards are governed by a process called the "Lifecycle Process for Changes to PCI DSS" [10]. Since our last edition, this was updated to change from a two year to a three year cycle. The document describes the following stages for each standard revision which kicked off in 2010 after the last release of PCI DSS:

1. Standards Published (October),
2. Standards Effective (January 1 following release),
3. Market Implementation (All year),
4. Feedback Begins (November),
5. Old Standards Retired (December 31, which is 15 months past Phase 1),
6. Feedback Review (April–August),
7. Draft Revisions (November–April),
8. Final Review (May–July).

The overall process takes three years and always includes extensive public commenting and review periods to incorporate the input from all stakeholders.

PCI DSS AND RISK

The relationship between PCI DSS and risk management isn't harmonious. PCI DSS's goal is to reduce the risk of card transactions and to build consumer confidence

in the payment card systems. On the other hand, many people point out that PCI DSS presents a list of controls with no regard to an organization's own risk assessment. Let's explore the relationship of PCI and risk a bit further.

First, a common question: can one claim that complying with PCI increases the merchant's overall business risk? When people ask that question they usually imply that PCI added the risk of loss via noncompliance fines and raised fees to the risk of direct losses due to card theft from a merchant's environment (such as reputation damage, cost of new security measures, and monitoring)? The answer is clearly a "no," since before PCI, most of the negative consequences of a card theft, even a massive one, were not falling upon the merchant shoulders but on others such as card-issuing banks. PCI, on the other hand, creates a powerful motivation for protecting the data on the merchant side.

Still, despite that reality about PCI, many CEOs or CFOs are asking the question, "Why would I need to spend money on PCI?" And, no, the answer is not "Because there are fines" (even though there are noncompliance penalties). The answer is that the list of negative consequences due to neglecting data security and PCI DSS is much longer than fines.

Your company's contract with the acquiring bank probably has a clause in it that any fines from the card brand will be "passed through" to you. With all compliance deadlines passed, the fines could start tomorrow. Visa maintains a global Compliance Acceleration Program that fines acquirers (which will pass on the costs to the merchant) between $5000 and $25,000 per merchant per month if their Level 1 or Level 2 merchants are not reported as compliant. In addition, fines of $10,000 per month may already be imposed today for storing prohibited data.

On top of that, if your organization is not compliant with PCI DSS when you are compromised, higher fines are imposed as well. And if you find yourself in that situation, you might just end up with more data, including that dreaded sensitive authentication data, compromised which drives fines up even further. However, believe it or not, if compromised, this will be the least of your concerns. Possible civil liabilities could dwarf the fines from the card brands in over-litigious societies that cultivate class-action lawsuits. Some estimates place the cost of compromise at $50–$250 per stolen account (note stolen, and not per one used for fraud, which will likely be a subset of the whole stolen card pool). Some companies that have been compromised have been forced to close their doors or sold to competition for nominal amount. Smaller merchants fall victim to this reality often, and companies in the business of protecting cardholder data don't last long after compromises.

Let's use The TJX Companies, which operates stores like TJ Maxx, Marshalls, and so on, as a case study. On January 17, 2007, TJX announced that they were compromised. Because they did not have robust monitoring capabilities such as those mandated by PCI, it took them a very long time to discover the compromise. The first breach actually occurred several years prior. TJX also announced that more than 90 million credit-card numbers were compromised. In addition to the fines, volatility in the stock price, and direct costs of dealing with the compromise, over 20 separate law suits were filed against TJX; some of which were converted to class-action status. At

the time of this publication, most if not all have been settled. This is good news for the rest of us because most of the outcomes are public record. It might take you some time, but with a good search engine and some time you could add up all of those losses into one big, fat scary number.

Whether you believe your company to be a target or not, the fact is that if cardholder data comes into contact with your network at some point *you are a target!* The resale value of cardholder data has plummeted dramatically in the last few years, but that doesn't mean that the size of the target on your back is smaller. You and your organization are simply someone's sheep to be fleeced, and your losses are their gains. Organized crime units profit from credit-card fraud, so your company is definitely on their list if you deal with card data. International, federal, and state law enforcement agencies are working hard to bring perpetrators to justice and shut down the infrastructure used to aid in credit-card-related crimes; however, thousands of forum sites, Internet chat channels, and news groups still exist, where the buyers can meet the sellers. Data breaches like the one at TJX are not the work of simple hackers looking for glory. Instead, well-run organizations from the Eastern European block [11] and selected Asian countries [12] sponsor such activity and earn a great living from various illegal hacking activities.

The Web site http://datalossdb.org maintains the history of the compromises and impacts in terms of lost card numbers and other records. Since 2005, over 1 billion personal records (a mix of cards, identities, etc.) have been compromised. This includes companies of all sizes and lines of business. If the industry does not get this trend under control, the US Congress will give it a try.

Finally, and few people actually know it, but PCI DSS does mandate a formal risk assessment, not just a list of controls to implement! Requirement 12.1.2 states that the information security policy must "include an annual process that identifies threats, and vulnerabilities, and results in a formal risk assessment." One of the best things you can do for your business is take this requirement very seriously, and expand it beyond the confines of cardholder data. Don't perform this to check an audit box, take it as an opportunity to get a broad look at how your business operates and the kind of risk it carries.

BENEFITS OF COMPLIANCE

While the inclusion of benefits is irrelevant— after all PCI DSS compliance is *mandatory* for the organizations that deal with payment cards—it is worthwhile to highlight the fact that PCI DSS has important benefits for the merchants, acquiring banks, issuing banks, as well as for the public at large.

If we are to mention one benefit, PCI DSS has motivated security improvements in businesses (especially retail) like nothing else before it. Many of us lived through the virus-infested 1980s, then worm-infested and spammy 1990s, and then through heavy data loss early 2000s without doing anything on security. PCI DSS moved the needle farther toward the "Secure" end for the laggards that fell victim to that reality.

CASE STUDY

Much of this book focuses on case studies where a company makes a mistake, or fails to do something that result in a breach. This case study is a nice change of pace where we examine someone doing something right!

The Case of the Developing Security Program

Yvette's Evangelical Emporium is a small chain of 50 stores supplying religious supplies to local churches and individuals. Yvette started her business in 1990 with a single store. Throughout the 1990s, she was able to open several new stores in neighboring counties and states, eventually building a 10 retail location business by 2000. In 2002, she took advantage of a depressed economy, and using some capital from investors and a significant trust that matured, she expanded her operation to 25 stores in three years and continued to expand over the next four years to double her size.

In 2005, Yvette realized that she needed to formalize her IT division and hired Erin, a progressive and security-minded IT executive, as her chief information officer. Erin presented a plan to standardize and build out her infrastructure so that future growth could be done in a cookie-cutter fashion; thus, saving millions in deployment and maintenance costs.

By 2006, they crossed the threshold from a Level 2 Visa merchant to a Level 1 Visa merchant and knew they would quickly need to put a solid PCI compliance program in place. Erin knew from her previous experience that small companies struggled with information security and made it a point to build in basic information security fundamentals into her IT operations, but they did not meet the baseline PCI DSS requirements and needed to be reworked.

Because of her new reporting levels for PCI, Yvette hired Steve to serve as the chief information security officer, reporting directly to her. Steve's task was to build an information security program that addressed PCI immediately, but would expand to be more applicable to information security such that future regulation would only require minor tweaks to the program.

Steve and Erin worked closely together to build a common set of controls to be rolled out to the entire company. Steve knew that PCI was a priority but considered everything he did in light of the ISO security framework (ISO17799 at the time). In some cases, he found that ISO far exceeded specific PCI requirements like in Business Continuity and Risk Assessments, and he found unique parts of PCI that were much more granular than ISO, like the treatment of sensitive authentication data (PCI Requirement 3.2). Steve's efforts ultimately paid off in spades as his information security program matured. Recent changes and additions to restrictions on healthcare data (which Yvette housed as part of an employee self-insurance program) and state data breach notification laws were already addressed by the program as it matured, and Yvette's cost associated with protecting data was much less than her competitors who only chased standards with immediate noncompliance repercussions.

NOTE

It is well-known that initial PCI DSS creators were well aware of ISO 17799 and other security standards. This awareness leads to the fact that if your organization has a solid security management program based on ISO IEC 27002 (a modern descendant of ISO/IEC 17799 and BS7799), your PCI effort will be relatively easy and you will gain both solid security and compliance as a result. It is also likely that compliance with other regulations will not be overly onerous. PCI is more granular, whereas ISO is more broad, but they are largely in sync!

The Case of the Confusing Validation Requirements

Garrett's Gas Guzzling Garage operates 800 car repair locations across the United States. Garrett's recently opened 20 locations in Mexico City to help maintain and upgrade the fuel efficiency of old cars. Garrett is considered a Level 1 merchant in the United States but set up a different entity in Mexico City, and processes and settles locally with Bancomer. Although Garrett authorizes and settles locally in Mexico City at his small regional headquarters, he shares the data with the US-based parent for backup and analysis purposes.

His business is booming in Mexico City, and that business quickly became a Level 2 merchant. According to MasterCard's new validation requirements, this would mean that Garrett must have a QSA perform an on-site assessment of compliance for both locations, or get someone internally trained under the Internal Security Assessor (ISA) program. He was already doing this in the United States based on his Level 1 status, but now faces additional costs for doing this locally in Mexico City.

"But wait," some of you are saying, "What about Visa's rules?" Certainly glad you asked that! According to Visa, if a smaller, wholly owned subsidiary shares infrastructure and data with a parent company considered a Level 1, then that smaller subsidiary should also be viewed as a Level 1 and perform the same level of validation.

Back to Garrett; even though the 20 Mexico locations process through Bancomer, the data is shared with the US headquarters for backup and analysis. According to Visa's rules, the Mexican entity is considered Level 1 based on its relationship with the parent, and a Level 1 assessment must be performed.

As always, when in doubt, ask your acquirer what is expected of you. Your mileage may vary when it comes to some of these intricate rules. Some acquiring institutions may still treat certain subsidiaries as lower levels depending on the circumstances.

SUMMARY

PCI refers to the PCI DSS established by the credit-card brands. Any company that stores, processes, or transmits cardholder data has to comply with this data protection standard. Effectively, all the target compliance dates have already passed, so if your company has not validated compliance, you are at risk of fines and other negative consequences of insecurity and noncompliance. The PCI is composed of 12

requirements that cover a wide array of business areas. All companies, regardless of their respective level, have to comply with the entire standard as written. If you end up filling out a self-assessment questionnaire, you are responsible for validating the subset that applies to you, but don't forget about the rest of the standard, *especially* if the nature of your business changes! The actual mechanism for compliance validation varies based on the company classification, driven by the individual card brand, transaction volume, exact method of accepting cards, etc. The cost of dealing with data breaches keeps rising, as does their number; noncompliance exacerbates the loss in case of a breach. Companies that do not take data security and compliance efforts seriously may soon find themselves out of business.

Now is the time to start the journey toward data security and compliance: get an endorsement from the company's senior management and business stakeholders, and start fulfilling your obligations and protecting the data.

REFERENCES

[1] Sinclair Jr UB. I, Candidate for governor: and how I got licked (1935), ISBN 0-520-08198-6; repr. University of California Press; 1994. p. 109.

[2] PCI Council Website, Article # 5410. <http://selfservice.talisma.com/article.aspx?article=5410&p=81> [accessed 31.08.09].

[3] PCI Council Glossary, Entry Service Provider. <http://selfservice.talisma.com/display/2n/index.aspx?c=58&cpc=MSdA03B2IfY15uvLEKtr40R5a5pV2lnCUb4i1Qj2q2g&cid=81&cat=&catURL=&r=0.73831444978714>; 2009 [accessed 17.07.09].

[4] Joel Weise, private communication, e-mail dated July 1, 2009.

[5] Ten Common Myths of PCI DSS. <http://www.pcisecuritystandards.org/pdfs/pciscc_ten_common_myths.pdf>; 2009 [accessed 17.07. 09].

[6] Visa Cardholder Information Security Program for Service Providers web page. <http://usa.visa.com/merchants/risk_management/cisp_service_providers.html>; 2009 [accessed 02.08.09].

[7] PCI and Your Third-Party Service Providers – First, the Bad News. <http://treasuryinstitutepcidss.blogspot.com/2009/07/pci-and-your-third-party-service.html>; 2009 [accessed 10.08.09].

[8] PCI Security Standards Council website. <www.pcisecuritystandards.org/>; 2011 [accessed 05.12.11].

[9] Merrick Bank v. Savvis Update: Savvis Files Motion to Dismiss. <http://infoseccompliance.com/2009/06/23/merrick-bank-v-savvis-update-savvis-files-motion-to-dismiss>; 2009 [accessed 17.07.09].

[10] Lifecycle Process for Changes to PCI DSS. <http://www.pcisecuritystandards.org/pdfs/OS_PCI_Lifecycle.pdf>; 2009 [accessed 17.07.09].

[11] Black Hat: Fighting Russian Cybercrime Mobsters. <www.informationweek.com/blog/main/archives/2009/07/black_hat_fight.html>; 2009 [accessed 11.08.09].

[12] Chinese Hackers Attack Web Site Over Uighur Film. <www.bloomberg.com/apps/news?pid=20601081>; 2009 [accessed 11.08.09].