Introduction: Why Another Article on PCI?

Security standards governing the credit card industry are not new. In fact, the first such program was introduced by Visa back in 2001. Over the years, a lot has been written about the topic. comForte first contributed to the discussion in this publication back in 2006, writing about Visa’s Cardholder Information Security Program (CISP). We also wrote about “The PCI Security Standard: Encryption Requirements in the NonStop World” in 2008, and in 2012, wrote how tokenization is “A New Approach to Fully Comply with PCI 3.4”. Most recently, we wrote about how the whole experience can turn into a “Nightmare on PCI Street” (Sept/Oct 2012)1.

While there is no shortage of articles focusing on credit card security standards, and how to comply with them, we are still seeing a fair amount of confusion when it comes to non-compliance. In this article, we will focus on thinking the unthinkable: What happens to organizations who are not PCI compliant? We also will discuss compensating controls for requirement 3.4 of the PCI DSS, and their future as we see it.

Refresher: Introduction to PCI

For quite a few years now, credit card brands have implemented security rules for safeguarding credit card information. Initially, the brands issued their own rules, but over time those standards were consolidated for all the major payment brands. Since 2006, the PCI Security Standards Council (PCI SSC) has been responsible for managing this program, which today features several standards and initiatives, including the PCI Data Security Standard (PCI DSS) and the Payment Application Data Security Standard (PA-DSS).

The PCI DSS has been developed to secure cardholder data throughout the card payment ecosystem, and so reduce the high costs associated with fraud. PCI DSS applies to all those organizations involved in payment card processing, including merchants, acquirers, issuers, processors.

PCI DSS represents a framework for developing a robust payment card data security process, offering strategies for preventing, detecting, and responding to security incidents. Consequently, these PCI standards represent a useful, comprehensive security framework.

The following diagram details the key stakeholders that are typically involved in the payment process:

Depending on the type of card used, the issuer of the card and the location where the card is used, the full payment transaction path may be simple or complex; also the path will not always involve all entities depicted above.
The table above illustrates a few potential examples. In all cases the card has been issued by Bank A:

<table>
<thead>
<tr>
<th>Color in Diagram</th>
<th>Card used in</th>
<th>Acquirer</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>ATM belonging to Bank A</td>
<td>Bank A (equal to Issuer)</td>
</tr>
<tr>
<td></td>
<td>ATM belonging to Bank B</td>
<td>Bank B</td>
</tr>
<tr>
<td></td>
<td>POS terminal issued by Bank A</td>
<td>Bank A (equal to Issuer)</td>
</tr>
<tr>
<td></td>
<td>POS terminal issued by Bank B</td>
<td>Bank B</td>
</tr>
</tbody>
</table>

Non-compliance of Merchants

The schedule of audits and deadlines vary depending on the merchant's number of annual card transactions. That said, today, merchants of any level need to be compliant. When the QSA does an assessment, it passes the final report to the acquiring bank. The bank then decides whether or not the merchant is compliant. It is the bank that issues the fine to a merchant if they find the organization non-compliant or not making the progress towards compliance that they expect.

Beyond the acquiring bank fining the merchant in case of non-compliance, the payment brands may choose to fine the acquiring bank. The acquiring bank can then assign this fine downstream, whether to intermediary processors or to the merchant. Beyond these fines, the acquiring bank may very well terminate their relationship with the non-compliant merchant or raise their service fees⁴—all of which can be catastrophic to a business.

It is important to note that all these implications may come into play simply because of a repeated failure to demonstrate improvements against the audit process. If a breach occurs, things get more serious. As the PCI site states, “Merchants that do not comply with PCI DSS may be subject to fines, card replacement costs, costly forensic audits, brand damage, etc., should a breach event occur.”⁵

Further, if a merchant suffers a breach in which account data is exposed, their level could be escalated. As a result, they would face more audit scrutiny, which leads to increased audit effort and costs, and potentially more security investments.

Merchants should be under no illusion: they are being targeted. In fact, in 2012, retailers were by far the most targeted organizations, making up 45% of the year’s breaches⁶. For example, early in 2012, Zappos.com, which is owned by Amazon, announced that details on 24 million customers were stolen. In October 2012, Barnes and Noble announced that POS devices at 63 of its stores

---

¹ All past editions of The Connection are available via the CONNECT website at http://www.connect-community.org. You can also contact the authors for the articles mentioned here.
² We left out entities such as payment processors and switches for brevity.
³ https://www.pcisecuritystandards.org/approved_companies_providers/vpa_agreement.php
⁴ As the acquiring bank generates revenue through the relationship with the merchant, there is an obvious conflict of interest here. The acquiring banks have to walk a fine line between properly enforcing the PCI regulations to protect themselves from risk and turning sour the business relationship with the merchant.
⁵ http://www.pcicomplianceguide.org/pcliqqs.php#23
⁶ http://www.foxbusiness.com/industries/2013/02/15/hackers-aim-arrows-at-retail-bulls-eye/
had been tampered with, enabling thieves to steal payment card details. Further, it’s not just the largest retailers being victimized. Late in 2011, it was discovered that, over the course of several years, the POS systems of hundreds of small merchants, including more than 150 Subway franchises, were compromised. These breaches reportedly led to over $3 million in fraudulent charges.

**Non-compliance of Issuers, Processors, and Acquirers**

The focus of PCI DSS audit oversight has historically been on merchants and—to a lesser degree—on payment processors and other service providers. In addition, acquiring banks must have their compliance with PCI DSS validated through audits. Historically, issuing banks have not been required to go through audits. However, adhering to PCI DSS and defending against breaches is still a critical mandate. Every financial institution that issues credit cards is a member of a card association, and so is contractually obligated to follow the rules set forth in the PCI DSS. Further, whether they undergo an audit or not, their compliance is especially critical because these organizations often manage large volumes of payment data, which means the potential damage associated with a breach can be far greater.

In addition, virtually every organization that manages cardholder data is also directly or indirectly affected by state or national privacy rules, which typically require public disclosure of breaches. For any bank, payment processor, or other entity in the payment ecosystem, these public disclosures of breaches can exact a very high cost, both in terms of tarnished reputations, out-of-pocket expenses, fines, and a range of other penalties.

**Impact of Non-compliance**

The bottom line is that PCI DSS exists for a very good reason: It provides a sound security framework that can help mitigate the risk of a data breach, which would otherwise severely hurt everyone within the ecosystem.

To illustrate, consider a case that happened last year. In March 2012, hackers stole account numbers of upwards of 1.5 million accounts from Global Payments, a large card processor. Visa promptly withdrew its seal of approval from the vendor, which can represent a fatal blow for an organization built around delivering secure card services. Further, the company’s share price took an immediate hit, and potential large-scale customer defections and legal actions may have also resulted. The total direct costs have been estimated to be about $94 million. The processor further estimated that about $60 million of these costs were associated with professional fees and other costs associated with such efforts and services as investigation, remediation, and identity protection.

The damage didn’t stop there. Many issuing banks were forced to reissue cards and research transactions to identify potential fraud. Consumers, even if not liable for fraudulent charges, still had to deal with the inconvenience of changing cards and having charges declined. The issuing banks are the ones that need to notify their customers of a breach, and suffer the tarnished brand associated with that kind of news, whether or not it was actually their systems that were compromised. Further, even if they push the charges off to downstream entities, their resources still need to be involved in all the effort associated with card reissuance and fraud mitigation.

Ultimately, if you’re not compliant, you’re nearly always more susceptible to a breach—and that can spell some very bad news for your organization. That’s why it’s important to take a more holistic approach, not just in complying with a mandate, but in applying security best practices. With that as a context, in the next section, we look at the topic of compensating controls surrounding a specific PCI DSS requirement.

**Compensating controls for PCI 3.4**

PCI DSS is comprised of 12 broad rules, with each containing many specific requirements. While many amount to basic, very common steps, such as restricting physical access to the data center, others are less straightforward. To be practical for the broad range of companies that are regulated, the PCI DSS introduced the concept of compensating controls, which can be employed if and only if there are specific technical or business challenges to adhering to a specific rule.

By establishing compensating controls, organizations are, in effect, demonstrating that, while the specific rule isn’t being addressed, that the rule’s ultimate objective is. It is important to note, however, that compensating controls need to be applied, documented, and audited on an annual basis, so, even if a compensating control is accepted by an auditor one year, that doesn’t mean it will continue to be.

Requirement 3.4 of the PCI DSS, which requires the encryption of data at rest, is a rule that has traditionally been problematic to comply with on HP NonStop systems (formerly known as Tandem systems). Payment applications running on NonStop provide a prominent example in this area. The BASE24 product suite from ACI is undoubtedly among the market leading applications for processing electronic payments from POS terminals and for handling ATM transactions. Given BASE24 applications process credit card transactions on the HP NonStop platform, they fall very much under PCI DSS (Note, that while we’re...

---

1. [http://www.huffingtonpost.com/2012/10/24/barnes-noble-credit-card-hacked-_n_2007585.html](http://www.huffingtonpost.com/2012/10/24/barnes-noble-credit-card-hacked-_n_2007585.html)
3. [http://online.wsj.com/article/SB10001424052702304375040457773100830975652936.html](http://online.wsj.com/article/SB10001424052702304375040457773100830975652936.html)
5. All copyrights acknowledged
focusing on BASE24 in this article, the statements on
compensating controls are valid for any application that
manages regulated data without providing data-at-rest encryption).

While the BASE24 and BASE24-eps products
by ACI are both PA-DSS compliant, that does not
mean a customer running these applications is fully
compliant with PCI DSS. Neither product supports
the encryption requirement specified in rule 3.4. The
BASE24 PA-DSS Implementation Guide states: “The
BASE24 product does not provide data level encryption
to protect cardholder data. To be PA-DSS compliant,
users must implement a disk level encryption solution
on their HP NonStop platform. Any implemented disk
level encryption solution must adhere to the following
PCI DSS requirements: Logical access to encrypted file
systems must be implemented via a mechanism that is
separate from the native operating systems mechanism
(for example, not using local account databases).”

How do organizations address this encryption
requirement? Until recently13, no commercial solution
matching this standard has been available for the HP NonStop
platform. Therefore, it is safe to assume most BASE24
customers have been relying on compensating controls, and
that those compensating controls were approved by auditors.

Conclusions as to the validity of compensating
controls will vary according to the judgment of the
auditor and the specifics of the environment. However,
it does appear compensating controls will not be as
likely to pass audits moving forward—particularly as
technically and financially feasible alternatives come
to market. Further, as outlined in the prior section,
if organizations can implement measures that more
effectively safeguard sensitive payment data, they are
well advised to do so—whether or not compensating
controls are accepted or not.

**Tokenization and the comForte SecurData/24 product**

For a long time, it was considered impossible to protect
sensitive data in applications without requiring massive
code changes. One particular issue was that the size of
encrypted data would be larger than the original, clear-
text data, which can potentially break many layers of
application code.

As described in a prior article in The Connection ,
comForte has combined the concepts of tokenization and
intercept technology; enabling full PCI 3.4 compliance for
applications, such as BASE24, that do not offer data-at-rest
encryption.

The solution is currently being installed at customer
sites and we will report on the lessons learned in future
articles. In the meantime, please contact the authors of
this article to learn more about the product.

---

**Conclusion**

Bruce Schneier, renowned security technologist and
author, has written that, if the information security
industry is ever to truly mature, it will be when insurance
models come into play15. Today, the only way a building
owner can get insurance is if they take such precautions
as installing fire detectors. In many respects, the PCI DSS
represents a form of this insurance model, as it provides
regulatory pressure that creates the financial incentives to
invest in security.

comForte strongly believes that properly securing
systems should be about as normal a part of ongoing
NonStop operations as providing a backup power supply.
If you or your organization’s management believes “we will
never get hacked”, you might want to reconsider: the well-
publicized breaches at Sony, RSA, and, most recently, the
New York Times vividly illustrate that the attacks being
waged are increasingly sophisticated—and very often
effective. Further, last year’s processor breach provides
ample evidence as to the high cost of a breach for those
associated with payment data. To avoid meeting the same
fate, it is incumbent to make not just compliance, but true
security, a priority.

**Disclaimer**

This article is based on comForte’s experience and
research regarding PCI DSS, including discussions with
customers, PCI QSAs, and members of the PCI Security
Standards Council. Statements made in this article about
fines in case of non-compliance are non-binding as
these are down to contractual arrangements between the
stakeholders. Similarly, whether or not compensating
controls are acceptable is at the discretion of the entity
deciding about compliance and/or fines.

---

13 To the best of our knowledge, ACI offers no product for data-at-rest encryption for either BASE24-classic or BASE24-eps. The Volume Level Encryption (VLE)
product from HP does not fulfill the separation of logical access criteria set forth in PCI.