The Bunker
Ultra Secure

7 ways to get fined for PCI DSS non-compliance

How to avoid communication pitfalls of PCI DSS v3.0 compliance

November 2014

The Bunker
Ultra Secure

Contents

Introduction

Historically, businesses that need to be in compliance with the PCI Security Standards Council have fallen foul of the rules of PCI DSS simply through a failure to understand the requirements correctly. There are a number of reasons for this. However, two of the key contributory factors are a lack of clarity and a questionable approach to enforcement.

A lack of clarity has led many to believe they are compliant when, they are in fact, not. There are perceptions that enforcement action has seemed arbitrary with a bottom up approach to penalties, which has unfairly targeted and penalised smaller merchants.

In the US these issues have been partially responsible for attracting a range of criticism. Some attack the technical specifications of PCI DSS, characterising the standards as little more than a minimal baseline for security. Others have been nothing short of scathing of the key stakeholders, the card companies. Legal cases have seen merchants challenge the PCI DSS Security Standards Reporting Council. Reporting these cases Wired.com said:

“The controversial system, imposed on merchants by credit card companies like Visa and MasterCard, has been called a “near scam” by a spokesman for the National Retail Federation and others who say it’s designed less to secure card data than to profit credit card companies while giving them executive powers of punishment through a mandated compliance system that has no oversight.”

Wherever you sit in the PCI ecosystem, such uncompromising words are far from re-assuring. In a decade that has exposed the role of compliance failure in widespread and systemic corporate fraud, the last thing the financial services industry needs is to be accused of operating a bogus compliance scheme.

Perhaps in response to such open and damaging opinions, PCI DSS v3.0 was announced in November 2013 with enforcement from January 2015. This promises to correct the problems of clarity and poor enforcement and signifies a new era of robust compliance activity.

With the January deadline for PCI DSS v3.0 compliance coming up fast, here we identify 7 ways to get fined for PCI DSS v3.0 non-compliance, and rather more importantly, explain how you can avoid them.

Ways to get fined

1. Follow the assumption that by definition MSPs and developers are all fully compliant

Many MSPs and developers are compliant with some of the standards. However, in many cases some comply with just two of the top level standards. Anecdotal research within the PCI data centre market suggests that only 7 in 10 are fully compliant. With 30% of MSPs and payment application developers either wilfully or mistakenly incorrectly claiming full compliance, the potential to outsource hosting to a non-compliant MSP or software developer is significant.

To avoid the threat of failing PCI DSS compliance, be 100% certain your PCI DSS hosting partner is 100% compliant The best way of making sure your Managed Service Provider is 100% PCI DSS v3.0 compliant is to refer to the Visa Merchant List. If an MSP is not on this list, then it simply isn't 100% compliant.

2. Work on the assumption that compliance risks and penalties are minimal

In many ways previous PCI DSS compliance enforcement policies seem to have been 'light touch'. Recent significant breaches at Sony, and Target, which exposed the card data of 40 million people, have led some to question the value of PCI DSS compliance. Moreover, some are of the view that it's cheaper to get fined than be compliant. However, with the scandals that have beset the financial services industry over recent years, such an approach has been consigned to history.

In the UK, fines for breaches of PCI DSS v3.0 and their consequences are up to £100 per card affected, and Visa is looking to increase its non-compliance fees. This means that any damage to your business is scalar – it depends on the extent of the failure. For a smaller or medium business the potential is for the penalty to render your business insolvent. Even if your business is able to survive the financial hit, there is also likely to be a short term impact on trade should the breach enter the public domain where it is likely to result in reputational damage.

Under PCI DSS v3.0 the era of 'light touch' regulation and slapped wrist penalties are over. The indications are that financial penalties are going to be stiffer. It's time for a new attitude to PCI DSS compliance. A good place to start is by identifying leading PCI DSS compliance organisations that have the ability to provide a one stop solution, whatever your requirement.

3. Thinking that you've outsourced and it's somebody else's problem

Even if you outsource to an MSP or a payment application software developer, compliance is still your responsibility. If you outsource to one that is non-compliant, as far as the PCI DSS Security Standards Council are concerned, you are accountable for failing to take measures to secure card data by observing compliance. This is one of the most common ways to fall foul of the regulations, and it's understandable given the lack of clarity and confusion that has surrounded the standards.

Ultimately, it is the responsibility of each business in the PCI ecosystem to take charge and control its PCI DSS v3.0 compliance status. Selecting a Managed Services Hosting Provider that has the credentials to support and demonstrate full compliance allows merchants and payment processors to eliminate non-compliance risks.

4. Believe you are currently PCI DSS v3.0 ready

Recent years have seen many organisations freeze or reduce IT budgets. Reducing budgets for environments that need to meet PCI DSS v3.0 compliance may turn out to be a false economy. Exposing 40 million cards under a breach of PCI DSS v3.0 could equate to a £400 million pound penalty, a sum that is likely to break anything other than the largest enterprises.

In cases where budgetary constraint has been unavoidable, those prioritising where best to invest sometimes face impossible challenges. It is little wonder that important elements sometimes get omitted or left until another spending round. One result is that your infrastructure may only be partially compliant to PCI DSS v3.0 standards.

In the event of non-compliance, especially one revealed through fraud, it is not just about the PCI DSS breach, the financial penalties and the reputational loss. It calls into question the effectiveness of executive control and governance right across the organisation.
The arrival of PCI DSS v3.0 gives the chance for the executive to open an honest dialogue with IT and infrastructure managers about readiness for PCI DSS v3.0. A good step forward is to seek the expertise of those that design, build and operate PCI DSS v3.0 compliant infrastructures.

5. Be under the impression that meeting the 12 top level requirements means you are compliant

Reasonably well known fact: There are 12 top level PCI DSS compliance requirements.

Not so well known fact: There are in excess of 200 sub-requirements.

On the face of it, the top level requirements of PCI DSS seem like standards to which any competently managed infrastructure should adhere. However, just because your IT systems are compliant with established standards for IT security and best practice at the time of assessment, this is no guarantee of continuing compliance under PCI DSS v3.0 standards. Continually meeting your obligations under PCI DSS Security Standards means compliance is an ongoing project that requires constant attention.

Smaller businesses should consider selecting a Managed Service Provider (MSP) that is guaranteed 100% PCI DSS compliant to host their payment systems. The best MSPs have evolved the management controls and technical proficiency to ensure continual compliance. Medium and larger businesses that elect to self-host payment systems need such expertise to ensure identification and remediation of any gaps. Compliance with the PCI DSS framework is an ongoing process.

6. Think you don't have to be compliant because you're not storing card data

There are many misconceptions that have grown up around PCI DSS compliance requirements. Some of them revolve around storage, processing and transmission of credit and debit card information.

The PCI DSS v3.0 standard is explicit in covering data at rest - that is stored on systems - or data in motion, information being transmitted or relayed across the payment processing network. Essentially, if your systems handle card data in any way, you need to achieve compliance with at least some of the requirements of the PCI DSS v3.0 standard.

A good way of determining your compliance requirement is to engage the services of an experienced PCI DSS v3.0 MSP that has the expertise to deploy compliant solutions. Gap analysis enables the accurate identification of compliance issues and provides remediation pathways.

7. Ignore PCI DSS compliance because you think it is too complicated

One of the key problems that results in relatively low levels of PCI DSS compliance is that many think it is too complex. Some form the impression that there is a need to unpick their infrastructure and put it back together at an expense that outweighs the benefit.

Compliance is often simpler than you think. The framework is relatively straightforward simple and prescriptive. Often, effectively executed IT best practice is all that is required to achieve compliance. Essentially, many that are in scope and need to achieve PCI DSS v3.0 compliance because of handling or storing card data, just need to find the right advice to help them take control.

If it all seems too complex or you are confused, a good option is to call in expert help to deal with the requirement for PCI DSS compliance. Selecting a hosting partner with systems purpose built for compliant hosting of PCI DSS v3.0 from the ground up reduces the attendant risks of breaching compliance.

Why select The Bunker as your PCI DSS Managed Service Provider

The Bunker is a centre of excellence for delivering PCI DSS v3.0 services and solutions. The core principle governing our PCI DSS v3.0 offer is that we provide solutions that are designed to keep in step with the growth of your business.

We achieved full compliance and have been delivering fully compliant services and solutions since 2010. The Bunker is one of only a handful of MSPs that are able to claim this with certainty and authority because of our presence on the Visa Merchants List.

There are many MSPs that are believed to be in compliance; however the truth is that only 4 UK MSPs are fully compliant with PCI DSS v3.0.

The key elements that underpin our PCI DSS v3.0 compliance offer are:

- Approved Managed Services Hosting Provider on the Visa Europe Merchant Agents List meeting all 12 requirements and sub-requirements in full
- Governance team of subject matter experts
- Full consultancy to deliver complete compliance solutions
- Customisable product suite tailored to individual requirements
- Independent QSA (Quality Standard Assessors) to sign off compliance
- Ongoing service and support to ensure continuing compliance

About The Bunker

The Bunker is a highly technical, service-lead business, delivering Ultra Secure mission critical Cloud solutions to mid-market companies.

We believe Information Security should enable businesses to be more competitive, manage risk, protect brand and allow innovation in a controlled manner and our mission is to help clients securely use technology to address business needs.

We combine unique physical environments with recognised excellence in digital security and Microsoft and Open Source technologies to offer high quality, responsive and Ultra Secure hosting and data centre services from within the UK.

Security is the essence of who we are and has evolved from the way our organisation and the individuals within it behave and think about security; it's the DNA of our organisation – our company culture.

Further reading and references

Visa Approved Merchants List

Search for: Managed Services Hosting Provider on the site below:

- https://www.visamerchantagentslist.com/

PCI DSS v3.0 Standards

https://www.pcisecuritystandards.org/documents/PCI_DSS_v3.pdf