

PCI DSS Compliance

Not my problem?

Survey Time

Does your organization deal with credit or debit card data?

Are you 100% sure about that?

Have you actually checked?

Negatory, no card data here!

Congratulations!

You can put your feet up and mock your less fortunate peers...



Yes... No ... Maybe? Don't ask me.

- ▶ If you don't know, find out as soon as possible
- ▶ If you acquirer asks, be prepared with *some* information
- ▶ If you play dumb, you risk getting fined

Affirmative, card data all over the place!

- ▶ Good luck

Who has given us this headache?

- ▶ *“The Payment Card Industry Data Security Standard (PCI DSS) is a collaborative effort to achieve a common set of security standards for use by entities that process, store or transmit payment card data. Mastercard and Visa were the main initiators of the standard but were soon joined by American Express, Diner’s Club, Discover Card and JCB.”*

Why?

- ▶ They care so very much about your security and the consumer's data

Why?

- ▶ ~~They care so very much about your security and the consumer's data.~~
- ▶ They were tired of paying for fraudulent card activity when it was the merchants that were being compromised

What card data can I store?

- ▶ Ideally, none of it!
- ▶ But if you really must...

	Data Element	Storage Permitted	Protection Required	PCI DSS Req. 3.4
Cardholder Data	Primary Account Number (PAN)	Yes	Yes	Yes
	Cardholder Name ¹	Yes	Yes ¹	No
	Service Code ¹	Yes	Yes ¹	No
	Expiration Date ¹	Yes	Yes ¹	No
Sensitive Authentication Data ²	Full Magnetic Stripe Data ³	No	N/A	N/A
	CAV2/CVC2/CVV2/CID	No	N/A	N/A
	PIN/PIN Block	No	N/A	N/A

Requirements

- ▶ 12 main requirements which can be paired down:
 - Building and maintaining of a secure Network [1 & 2]
 - Protection of cardholder data [3 & 4]
 - Maintenance of a vulnerability management program [5 & 6]
 - Implement strong access controls [7,8 & 9]
 - Regular monitoring and testing of networks [10 & 11]
 - Maintenance and an Information security policy [12]

- ▶ Do not let this deceive you, there is a lot more to it!

One size fits all?

- ▶ Not quite
- ▶ Going on the assumption that you are all merchants (as opposed to service providers) you may have fewer requirements...
- ▶ Enter the Self-Assessment Questionnaires:
 - SAQ A: No electronic storage, processing, or transmission of cardholder data
 - Some have called this the “Paypal SAQ” as the merchant will handle all data, including the shopping cart until the payment processing at which point it is forwarded to a third party.
 - Only paper reports/receipts
 - SAQ B: Imprint machines or stand-alone dial-out terminals only, no electronic cardholder data storage
 - SAQ C: Payment application connected to the Internet, no electronic cardholder data storage
 - Payment app on internet connected PC
 - Payment app connected to Internet to transmit cardholder data
 - SAQ D: All other merchants and all SAQ-Eligible service providers

Wait, what is a service provider?

- ▶ Not your business, hopefully
- ▶ *“Service Provider: Business entity that is not a payment card brand member or a merchant directly involved in the processing, storage, transmission, and switching or transaction data and cardholder information or both. This also includes companies that provide services to merchants, services providers or members 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”*
 - https://www.pcisecuritystandards.org/security_standards/glossary.shtml#s

Reality check

- ▶ It is a difficult standard – Oddly detailed in some areas and horribly vague in others
- ▶ There are no silver bullets to achieve compliance
 - Beware anyone who tells you their technology will make you fully compliant!
- ▶ ...
- ▶ But there are some *“shortcuts”*

What not to do

- ▶ Assume it is a quick job
 - We have come across many an organization that presumes that all they need to do is tick a few boxes, hire a QSA for a day to sign-off the ticked boxes and then relax
- ▶ Assume compliance = secure
 - The standard is not without its flaws
- ▶ Concern yourself with deadlines set by the council
 - There have been so many (utterly unfeasible) deadlines
- ▶ Shift the blame
 - You are responsible for your own compliance – Deal with it!

What not to do

- ▶ Expect miracles from your Qualified Security Assessor (QSA)
 - They can only work with the information that you give them
- ▶ Expect the standard to change significantly (in your favour)
 - The council is only releasing incremental updates and clarifications
- ▶ Introduce a technology and relax
 - Spend wisely, discuss with a QSA
- ▶ Get compliant and relax
 - Compliance is an on-going process.
 - Once you have all your policies and procedures in place, follow them!

What not to do

- ▶ Assume a compensating control is a permanent solution
 - Different QSAs, different opinion – The standard is interpretive
- ▶ Rely solely generic documentation
 - They will not always apply to your business!
- ▶ Use slow progress within your industry as an excuse
- ▶ Use new technologies as an excuse (VoIP, Cloud-computing, VLAN)

What to do

- ▶ **Identify your card data flow**
 - Conduct an exhaustive search to find areas where card data is stored, processed or transmitted
 - Document (and update) it!
- ▶ **De-scope**
 - Look at the possibility of outsourcing to a third-party – Almost always cheaper than full compliance
 - Question (ruthlessly) the need for handling card data in house
- ▶ **Treat compliance as an on-going process**
 - A QSA can sign-off your compliance one day, but if you don't follow the policies and procedures the next day, then you are no longer compliant!
- ▶ **Communicate with your acquirer**
 - Find out your compliance level
 - Update them with your progress

What to do

▶ Use public data and your peers

- There is a wealth of information out there to help you decipher the standard – Google it!
 - E.g. Navigating PCI DSS – https://www.pcisecuritystandards.org/pdfs/navigating_pci_dss_v1-1.pdf (Official)
 - E.g. PCI DSS FAQ – <http://pcidssfaq.org/forum/> (Unofficial)
- You are not alone in battling the standard – Ask for and share information

▶ Use the prioritized approach

- It can be difficult to judge exactly where to start, so make use of the council's milestone document:
- Acquirers will often encourage this approach as well

▶ Take responsibility for your compliance

- A QSA can help but ultimately you need to be able understand the standard to maintain compliance

▶ Get management on board

- Compliance can help with other accreditations
- Can the business afford to be fined or be prohibited from processing card data?

▶ Protect card data as you would expect another business to protect yours

So, what does a full audit involve?

- ▶ Questions (Lots and lots of them)
- ▶ Frustration
- ▶ Stress
- ▶ Time
- ▶ Money

So, what does a full audit involve?

- ▶ The full standard has approximately 250 “questions”
- ▶ A QSA has to fulfill various pieces of evidence within each of those questions
- ▶ A scoring matrix for a full report on compliance (ROC) consists of 966 points

V12 PCI DSS Requirement	Testing Procedure	Verified by Observation of system settings or configuration files	Verified by review of documentation	Verified by Interview	Verified by observation of process, action or state	Sampling Specified	Verified by network traffic monitoring	Points	N/A Points
1.3 Prohibit direct public access between the Internet and any system component in the cardholder data environment.	1.3 Examine firewall and router configurations, as detailed below, to determine that there is no direct access between the Internet and system components, including the choke router at the Internet, the DMZ router and firewall, the DMZ cardholder segment, the perimeter router, and the internal cardholder network segment.								
1.3.1 Implement a DMZ to limit inbound and outbound traffic to only protocols that are necessary for the cardholder data environment.	1.3.1 Verify that a DMZ is implemented to limit inbound traffic to only protocols that are necessary for the cardholder data environment.	1	1	1	1			4	0
	1.3.1 Verify that a DMZ is implemented to limit outbound traffic to only protocols that are necessary for the cardholder data environment.	1	1	1	1			4	0

Questions?