PCI COMPLIANCE

You've probably heard of the term "PCI compliance," but what does it actually mean?

This resource is being provided to give you some of the basics on PCI compliance: what it is and why it matters. Below are answers to some of the most common questions we receive on the subject. The bottom line is if you accept credit cards for payment at your place of business, you will have some PCI compliance obligations.

What is PCI?

Before we delve into "PCI," let's talk about data security; and, more specifically, about the security of credit card data.

Most of us have a credit card. We use it to pay for the things we like. While "laying down plastic" seems like a straight-forward, easy-to-understand concept, numerous parties are involved behind the scenes to complete even a single credit card transaction. It's a complex system. From the device manufacturers that build payment hardware to the banking institutions involved with the settlement of funds, from the major card brands (like Visa and Mastercard) that have set up vast networks of merchants to the payment processors that "operate the rails" along which credit card transactions are run, at any point along this continuum of interconnected parties, a cardholder could have his or her data stolen and used without permission.

The card brands understand that if people don't trust the system, they'll stop using credit cards as a form of payment. For credit cards to remain a viable payment method, cardholders must see them as useful, they must continue to see them as convenient, and, perhaps most importantly, they must see them as secure.

"PCI" is the payment industry's response to making credit card payments more secure for everyone. Being "PCI compliant" means taking steps to ensure that your "link" in the payments chain remains strong and secure. And, in so doing, you help mitigate the risk of a payments-related breach.

Practically speaking, PCI is a set of rules and regulations that apply to any business, of any size, that accepts credit card data. For merchants to be PCI compliant, they are expected to follow a specific set of safety protocols designed to protect both the business and the customers from fraudulent credit card activity.

What does PCI stand for?

It's actually "PCI-DSS" (often shortened to "PCI"), but it stands for Payment Card Industry Data Security Standard. "PCI compliance" means complying with the PCI data security standards. "PCI-DSS" and "the PCI standards" are the same thing.

Who created PCI-DSS?

PCI-DSS was created by the five largest credit companies – Visa, Mastercard, American Express, Discover and JCB International – to help in the fight against credit card fraud. PCI-DSS were rules promulgated by the Payment Card Industry Security Standards Council (PCI-SSC), which is the governing body and open forum responsible for developing, managing, educating and raising awareness of the relevant PCI standards.

Is PCI-DSS the law?

No. PCI-DSS isn't the law per se. There's been no federal or state legislative body that's stepped in to promulgate PCI rules or regulations. PCI-DSS exists as a matter of contract law as a creation of the five major credit card brands. When you, as the merchant, decide to accept payment with credit cards bearing the Visa, Mastercard, American Express, or Discover logo, contractually, per your agreement with those card brands or your payment facilitator, you've agreed to maintain the relevant PCI compliance standards.

Why does PCI exist?

PCI-DSS exists to help you, as a merchant, safely and securely store, process and handle sensitive customer data. Again, any business that accepts credit cards are subject to the PCI standards.

What PCI-DSS requirements do I need to follow?

It depends. Based on your annual transaction volumes, you would fall into one of four different compliance levels. Each level has its own set of requirements and obligations.

How are the four different merchant levels determined?

Merchant levels are tied to total Visa transactions run over a 12-month period. Transaction volume is based on the aggregate number of Visa transactions (inclusive of credit, debit and prepaid) run from a merchant's "DBA," or "doing business as." Visa defines merchant levels by the following criteria:

Level	Description
1	Any merchant, regardless of acceptance channel, processing over 6,000,000 Visa transactions per year.
2	Any merchant, regardless of acceptance channel, processing 1,000,000 to 6,000,000 Visa transactions per year.
3	Any merchant processing 20,000 to 1,000,000 Visa e-commerce transactions per year.
4	Any merchant processing fewer than 20,000 Visa e-commerce transactions per year, and all other merchants – regardless of acceptance channel – processing up to 1,000,000 Visa transactions per year.

Most Clubessential clients will be considered Level 4 merchants.

What does a small-to-medium sized business (Level 4 merchant) need to do in order to satisfy the PCI-DSS requirements?

Complete the following steps:

(1) Determine which Self-Assessment Questionnaire (SAQ) your business should use to validate compliance.

(2) Complete the SAQ according to its instructions.

(3) If applicable, complete and obtain evidence of a vulnerability scan with a PCI-SSC Approved Scanning Vendor (ASV). ***Note***: scanning does not apply to all merchants – it's only required for SAQ-A-EP; SAQ-B-IP; SAQ C; SAQ D-Merchant; and SAQ D-Service Provider.

(4) Complete the relevant Attestation of Compliance (AOC) in its entirety (found in the SAQ tool).

(5) Submit the SAQ, evidence of a passing scan (if applicable), and the AOC, along with any other requested documentation, to your acquirer.

How do I know which SAQ to use?

QUESTIONNAIRE	HOW DO YOU ACCEPT PAYMENT CARDS?
A	Card-not-present merchants (e-commerce or mail/telephone-order) that have fully outsourced all cardholder data functions to PCI DSS compliant third-party service providers, with no electronic storage, processing, or transmission of any cardholder data on the merchant's systems or premises. *Not applicable to face-to-face channels.*
A-EP	E-commerce merchants who outsource all payment processing to PCI DSS validated third parties, and who have a website(s) that doesn't directly receive cardholder data but that can impact the security of the payment transaction. No electronic storage, processing, or transmission of any cardholder data on the merchant's systems or premises. *Applicable only to e-commerce channels.*
B	Merchants using only: • Imprint machines with no electronic cardholder data storage; and/or • Standalone, dial-out terminals with no electronic cardholder data storage. *Not applicable to e-commerce channels.*
B-IP	Merchants using only standalone, PTS-approved payment terminals with an IP connection to the payment processor, with no electronic cardholder data storage. *Not applicable to e-commerce channels.*
C-VT	Merchants who manually enter a single transaction at a time via a keyboard into an Internet-based virtual terminal solution that is provided and hosted by a PCI DSS validated third-party service provider. No electronic cardholder data storage. *Not applicable to e-commerce channels.*
C	Merchants with payment application systems connected to the Internet, no electronic cardholder data storage. *Not applicable to e-commerce channels.*
P2PE-HW	Merchants using only hardware payment terminals that are included in and managed via a validated, PCI SSC-listed P2PE solution, with no electronic cardholder data storage. *Not applicable to e-commerce channels.*
D	For Merchants: All merchants not included in descriptions for the above types.
D	For Service Providers: All service providers defined by a payment card brand as eligible to complete a Self-Assessment Questionnaire.

Please note that Clubessential is unable to provide you with legal advice or the correct SAQ to use.

Where can I find more in-depth information on the SAQ process and PCI-DSS in general?

The Payment Card Industry Security Standards Council website includes some great resources, including SAQ instructions and guidelines (available here).

Where does Clubessential, LLC fall in the spectrum of parties providing a payment service?

Clubessential is a "payment facilitator," or "PayFac", and has attained a PA-DSS Level 1 Service provider status.

One common misconception is that Clubessential is a payment processor – it's not. Clubessential has partnered with Worldpay, Inc. ("Worldpay"), a third party, for its payment processing services. Although somewhat over-simplified, it's fair to think of Worldpay as the rail network upon which Clubessential's payments software runs.

As a payment facilitator, Clubessential has its own proprietary technology, CE Payments™, which enables seamless credit card processing through the Clubessential System. Clubessential is set up as the primary merchant account holder and you, our client, are set up under us as a sub-merchant.

From a PCI-DSS perspective, Clubessential has heightened compliance obligations over and above the typical merchant.

Can't I just piggy-back on Clubessential's compliance with its PCI obligations?

No. Because you accept credit card payments at the club level, you will be required to maintain some level of PCI compliance as a sub-merchant. Again, cardholder theft can occur at any point of weakness in the chain of credit card payments. This includes any point of weakness originating at the club level (for example, at the club house, golf shop or restaurant point-of-sale). There's no such thing as a "pass-through" on one's PCI compliance measures. While Clubessential's PCI compliance efforts benefit our entire client base, including you, individual sub-merchants must take appropriate steps of their own to do their part.

What if I don't actually store any credit card data at my business? Does PCI still apply?

Yes. If you accept credit or debit cards as a form of payment, and those credit or debit cards bear the logo of Visa, Mastercard, American Express, Discover, then the PCI standards will apply to you.

My club has multiple locations. Is each location required to validate PCI compliance?

If your multi-club locations all run credit card payments under the same sub-merchant tax ID number, then you may only be required to validate once annually for all locations.

What if I don't comply? What are the consequences?

The worst consequence of a failure to comply with PCI requirements is you suffer a data breach, cardholder data is lost, and your business suffers as a result. Separate and apart from monies that may have to be paid out in claims, a data breach could tarnish your reputation and keep new members away.

Putting aside the unfortunate possibility of a data breach, however, failing to comply with PCI standards creates potential liability for the other parties within the chain of payment services. For example, the card brands may, at their choosing, fine the acquiring bank – which is the bank linked to the primary merchant account – between $5,000 and $1,000,000 per month for PCI compliance violations. These banks will most likely pass along the fine until it eventually hits you at the merchant level. It's likely the bank would also terminate its business relationship with you, or Clubessential, or increase its transaction fees across the board to make up for its losses. Penalties are not widely discussed or publicized, but they can be extremely harmful to a business. It's definitely in your and everyone else's interest to comply with PCI-DSS.

What is Clubessential required to do to maintain PCI compliance?

As a payment facilitator, Clubessential is required to maintain heightened PCI compliance standards from typical merchants. Each year, we invest thousands of dollars in the security of our technology systems and are constantly refining our processes.

It's important to note that PCI compliance is one facet of a broader data security plan. Although Clubessential has made an intentional choice not to broadcast our security measures to potential bad actors, the company employs both on-line and off-line measures to protecting Client and End User Data. Those interested in learning more can review Clubessential's Privacy Policy or request a copy of our Data Security Whitepaper.

I have more questions about PCI compliance? Who at Clubessential should I contact?

Additional questions about PCI compliance can be directed to us at legal@clubessential.com.