The background is a blue gradient with a network of glowing lines and nodes. In the upper left, a cluster of icons is arranged in a circular pattern, including a cloud with an up/down arrow, a Wi-Fi symbol, a shopping cart, a globe, a play button, a laptop, an envelope, a classical building, a smartphone, a padlock, and a lightbulb. The main text is centered in the lower half of the image.

**Secure Payment and Processing
Solutions To Protect Your Business**
PAYMENT SERVICES ONBOARDING GUIDE

PAYMENT SERVICES ONBOARDING GUIDE

Thank you for choosing Clarien Bank as your Payment Services partner.

Clarien is committed to helping you navigate payment and processing safety and providing the support required to help you become compliant with the data security standards set by the Payment Card Industry.

Here's a quick look at the necessary steps to keep your business and customers' information safe with guidance from our partners at Clover.



Understanding PCI DSS

PCI DSS, or Payment Card Industry Data Security Standard (PCI DSS), represent the industry standard for security policies, technologies and ongoing processes that protect merchant payment systems from breaches or theft of cardholder data. Prior to 2004, every major card brand (Visa,

MasterCard, Discover, and American Express) had their own unique systems for protecting against fraud. These card brands eventually united to create an industry-wide standard for protection, now known as the PCI DSS.

The Clover Security Advantage

PCI compliance is assessed in two ways: Self-Assessment Questionnaires (SAQs) and audits. Generally, businesses are required to submit SAQs annually and are audited quarterly to ensure compliance.



In order to comply with PCI DSS, there are a number of requirements your business must satisfy. We have partnered with Clover to help our clients simplify the process.

As a new Clarien Payment Services client, you will automatically receive an email from Clover to help ensure that you have PCI compliance tools and

guidance.

The Clover Security team will advise on next steps required to set up your profile in order to determine the self-assessment questionnaires needed to help you across the finish line to PCI compliance.



Establishing and Maintaining PCI Compliance

GOAL 1: Build and maintain a secure network and systems.

- **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.

GOAL 2: Protect cardholder data.

- **Requirement 3:** Protect stored cardholder data.
- **Requirement 4:** Encrypt transmission of cardholder data across open, public networks.

GOAL 3: Maintain a vulnerability management program.

- **Requirement 5:** Protect all systems against malware and regularly update anti-virus software or programs.
- **Requirement 6:** Develop and maintain secure systems and applications.

GOAL 4: Implement strong access control measures.

- **Requirement 7:** Restrict access to cardholder data by business' need to know.
- **Requirement 8:** Identify and authenticate access to system components.
- **Requirement 9:** Restrict physical access to cardholder data.

GOAL 5: 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.

GOAL 6: Maintain an information security policy.

- [Requirement 12](#): Maintain a policy that addresses information security for all personnel.

Frequently Asked Questions

What must I do to maintain PCI compliance?

As a business owner, you must ensure that you meet the 12 Requirements outlined in the Requirements and Security Assessment Procedures. Please see the Establishing and Maintaining PCI Compliance section of this guide. You will be required to complete Self-Assessment Questionnaires (SAQs) or Audits for compliance validation. Clover will advise of the steps need for your specific requirements.

What does it cost to be PCI compliant?


Becoming (and remaining) PCI compliant carries a range of costs. What you can expect to pay depends on your merchant level, which is dependent on variables such as:

- The size, location, and nature of your organization
- The number of card-based transactions you process annually
- How you capture and process card-based payments (i.e., in-person or online)

There may be additional costs associated with employee training, which is voluntary for smaller organizations, but often required for larger ones. Upgrading magstripe POS terminals with more secure EMV-enabled readers also carries expenses. The same is true for eCommerce merchants that protect their visitors by adding Secure Sockets Layer (SSL) certificates to their sites. Of course, there are direct PCI compliance fees – normally calculated and charged by your payment processor.

These variables make it difficult to provide an exact “cost” for PCI compliance. However, smaller organizations can expect to pay \$300 to \$500 annually to become and remain compliant. By contrast, a multinational enterprise might need to spend \$70,000 to \$100,000 a year to remain in good standing.



A close-up photograph of a hand holding a credit card over a Clover POS terminal. The terminal is silver and black with a screen and a keypad. The background is blurred.

Now that I know the goals and requirements of PCI DSS, what should I do with that knowledge?

Your business will be regularly assessed against these security guidelines, so it's best to understand how it can impact your day-to-day tasks and responsibilities.

If you're using a point-of-sale device (POS) that's more than a few years old, chances are it's not protecting you against potential threats in adherence to current security standards.

One way to simplify your security is to start with a modern POS, specifically one that is PCI PTS (Payment Card Industry PIN Transaction Security) certified. Think of PTS certification like PCI compliance for payment terminals. POS providers like our partners at Clover provide payment terminals and can submit their machines for inspection and certification to make sure that a third party will not be able to access cardholder and PIN information.

How do I assess and report my business' PCI compliance?

PCI compliance is assessed in two ways:

- *Self-Assessment Questionnaires (SAQs) and;*
- *Audits*

Generally, businesses are required to submit SAQs annually and are audited quarterly to ensure compliance.

Answering a questionnaire once a year may not sound that complicated, but how your business is structured and the number of credit card transactions you process dictate which of the 8 different SAQs you will have to complete.

How does working with Clover simplify this process?

Self-Assessment Questionnaire questions are difficult and often time-consuming to address. If you choose to work with a Clover POS system, you get to bypass most of them.

The P2PE-certified hardware Clover builds includes multiple CPUs to protect data, even in the case of a virus being introduced to the system. Its high-level encryption protects customer information from the moment it is captured until it's through the payment gateway.

With this level of security built in, the PCI questionnaire merchants will have to complete is reduced to as few as five questions from 200 plus. Clover Security also offers add-ons, which allow you to access a team of people who will help you across the finish line to PCI compliance.

Is there anything else I will need to do to be compliant?

Yes, in addition to your annual SAQ, you'll also have to complete four system audits each year.

If you are PCI compliant, these electronic audits will be much easier.

If you use the services of Clover Security, you'll get automated reminders to schedule and complete these audits as well as a guided questionnaire to complete your SAQ. That means you can spend more time running your business, and less time worrying about how to protect your payment data.

What does it mean to be non-compliant?

There are many ways you can end up non-compliant. Here are just a few:

- Not filling out your annual SAQ (Self-Assessment Questionnaire)
- Filling out your annual SAQ incompletely and/or inaccurately
- Failing to complete quarterly network audits
- Not taking recommended steps provided by PCI compliance experts
- Sharing login information or usernames among employees
- Using default passwords for any of your networks or equipment
- Using a public WiFi for some of your transactions if you have a network issue, or are off-site
- Not using encryption services or firewall security protocols to protect card and personal data for your consumers.



We're Here For You

We take a concierge approach to service and we're here to help you get set up and compliant to keep your business safe and your client data protected.

Additional information and resources are available online at clarienbank.com/PCI-DSS.

For support, please speak with your Clarien Commercial Banking representative or call our Client Service Centre on [441-296-6969](tel:441-296-6969).



PERSONAL AND COMMERCIAL BANKING | WEALTH MANAGEMENT

clarienbank.com

Point House, 6 Front Street, Hamilton HM 11 | 441-296-6969

LISTENING. HELPING. BUILDING.

Clarien Bank Limited, through its wholly owned subsidiary companies, is licensed to conduct bank, investments, corporate service provider and trust business by the Bermuda Monetary Authority.