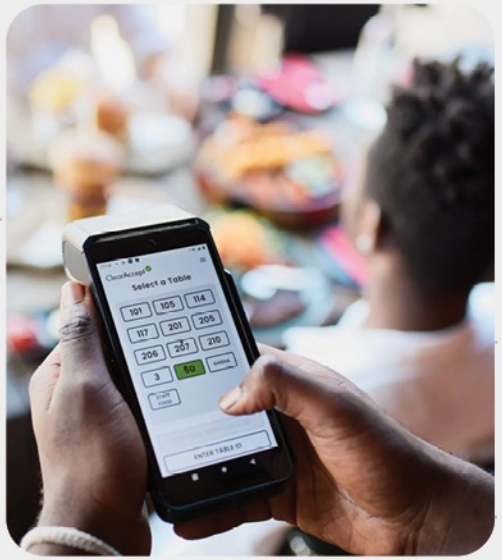
ClearAccept

PCI Basics for Face-to-Face Merchants



clearaccept.com

This presentation is applicable for merchants who interact directly with the card holder and their physical card.

We suggest reading the presentation
What is PCI? How does it apply to my business?
before proceeding with the details of this one.

Contents

ClearAccept

What does ‘face-to-face’ or ‘in person’ mean?

It excludes:

- Transactions done through a website or e-commerce shop “owned” by the merchant (even if it is provided by a third party) regardless of who enters the card number.
- Payments made through a mobile application on the card holder device.

It includes:

- The card holder presents either the physical card or their phone/watch/tablet where they keep their card in a mobile wallet.
- Payment is processed using a merchant-controlled device – for example, a payment terminal (stand alone, attached to a POS platform or a phone/tablet).
- This does include where the merchant takes payment by entering the card details directly into a web page provided by their payment service provider – a “virtual terminal” (more on that later).

ClearAccept

What do I have to do as a merchant?

If you are not compliant with PCI, you may be liable to penalties imposed by the card brands, and we may no longer be able to process payments on your behalf as you have not validated your security regarding payments.

- PCI DSS has several hundred requirements as it covers every possible activity that is in scope for assessment.
- For those requirements that apply to your business you need a 100% pass mark.
- The same standard applies to everyone, the individual requirements can be marked “Not applicable” if there are grounds to do so, but these must be justified.
- Larger entities (processing over 1 million transactions per year) may be required to have their annual assessment performed by an ISA or a QSA.
- Smaller entities may be able to self assess without needing an ISA or QSA.
- The annual assessment is a validation of compliance. However, you need to be compliant all the time.

ClearAccept

Which of the core principals of the standards apply to me?

For smaller merchants, the PCI Council has created a set of Self-Assessment Questionnaires (SAQs) which are targeted at specific business models.

See Requirements that apply to face-to-face payments below:

- **SAQ B:** Merchants using only imprint machines with no electronic cardholder data storage and/or standalone, dial-out terminals with no electronic cardholder data storage.
- **SAQ B-IP:** Merchants using only standalone, PTS-approved payment terminals with an IP connection to the payment processor, with no electronic cardholder data storage.
- **SAQ C-VT:** Merchants who manually enter single transactions 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.
- **SAQ C:** Merchants with payment application systems connected to the Internet, no electronic cardholder data storage.
- **SAQ 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.
- **SAQ SPoC:** Merchants using a commercial off-the-shelf mobile device (for example, a phone or tablet) with a secure card reader included on PCI SSC's list of validated SPoC Solutions. No access to clear-text account data and no electronic account data storage.

If none of these describe the exact situation, then the merchant must use SAQ D.

ClearAccept

More about the individual SAQs for face-to-face merchants

SAQ B.

If you meet the criteria to complete an SAQ B, then the below applies to your business:

CRITERIA FOR SAQ B:

- Merchants using only imprint machines with no electronic cardholder data storage and/or standalone, dial-out terminals with no electronic cardholder data storage.
- MUST be dial out – connected to telephone line and NOT the internet.
- NO storage of card data.

EXAMPLE OF REQUIREMENT FOR SAQ B:

- Monitoring and inspecting your payment terminals, training staff to perform inspections.

ClearAccept

More about the individual SAQs for face-to-face merchants

SAQ B-IP.

If you meet the criteria to complete an SAQ B-IP, then the below applies to your business:

CRITERIA FOR SAQ B-IP:

- Merchants using only standalone, PTS-approved payment terminals with an IP connection to the payment processor, with no electronic cardholder data storage.
- The payment terminals are connected through a network to the processor but are not connected to any other systems within the merchant environment and does not rely on any other device (e.g., computer, mobile phone, tablet, etc.) to connect to the payment processor.
- NO electronic card data storage.

EXAMPLES OF REQUIREMENT FOR SAQ B-IP:

- The payment terminals are PTS certified.
- Managing networks and systems securely.
- Monitoring and inspecting your payment terminals, training staff to perform inspections.
- Performing ASV Scans (certified vulnerability scans) on a quarterly basis on all internet facing IP addresses.

ClearAccept

More about the individual SAQs for face-to-face merchants

SAQ C-VT.

If you meet the criteria to complete an SAQ C-VT, then the below applies to your business:

CRITERIA FOR SAQ 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.
- Only a vendor provided payment page accessed by a browser is used.
- The PC used is not connected to any other systems.
- One transaction at a time – no file uploads or batch processing.
- NO other methods of taking payments exist.
- NO storage of card data.

EXAMPLES OF REQUIREMENT FOR SAQ C-VT:

- Managing networks and systems securely.
- Installing and maintaining anti-virus on all appropriate systems.

ClearAccept

More about the individual SAQs for face-to-face merchants

SAQ C.

If you meet the criteria to complete an SAQ C, then the below applies to your business:

CRITERIA FOR SAQ C:

- Merchants with payment application systems connected to the Internet, no electronic cardholder data storage.
- Single application running on a single PC or other device.
- Application does not store card data.
- Individual systems are stand alone, not connected to each other, locations are isolated.
- NO storage of card data.

EXAMPLES OF REQUIREMENT FOR SAQ C:

- Managing networks and systems securely.
- Using strong encryption.
- Installing and maintaining anti-virus on all appropriate systems.
- Developing software securely.
- Monitoring and inspect your payment terminals and train staff to perform inspections.
- Performing both internal and external vulnerability scans on a quarterly basis on all internet facing IP addresses and networks.
- Monitoring systems and log events with alerting in place.

ClearAccept

More about the individual SAQs for face-to-face merchants

SAQ PSPE-HW.

If you meet the criteria to complete an SAQ P2PE-HW, then the below applies to your business:

CRITERIA FOR SAQ 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.
- Only payment processing is done using a listed, certified, P2PE solution.
- The terminals, firmware and application versions match exactly the listing (Official P2PE listing).

EXAMPLES OF REQUIREMENT FOR P2PE-HW:

- Implementing all controls in the P2PE Implementation Manual (PIM) supplied by the vendor.
- Monitoring and inspecting your payment terminals, training staff to perform inspections.

ClearAccept

More about the individual SAQs for face-to-face merchants

SAQ SPoC.

If you meet the criteria to complete an SAQ SPoC, then the below applies to your business:

CRITERIA FOR SAQ SPoC:

- Merchants using a commercial off-the-shelf mobile device (for example, a phone or tablet) with a secure card reader included on PCI SSC's list of validated SPoC Solutions. No access to clear-text account data and no electronic account data storage.
- Only payment processing is done using a listed, certified, SPoC solution.
- The terminals, firmware and application versions match exactly the listing on the official PCI Council website.

EXAMPLE OF REQUIREMENT FOR SPoC:

- Monitoring and inspecting your payment terminals, training staff to perform inspections.

ClearAccept

More about the individual SAQs for face-to-face merchants

SAQ D.
If you don't meet the criteria to all other SAQs then SAQ D and the below applies to your business:

CRITERIA FOR SAQ D:

- Merchants that don't store account data electronically but that do not meet the criteria of another SAQ type.
- Merchants with a site that receives inbound transactions via electronic channels, processes them and then forwards the data to a payment processor.
- Merchants with multiple payment acceptance channels.
- Merchants with electronic storage of account data.
- No other SAQs eligible.

REQUIREMENT FOR SAQ D:

- SAQ D includes the majority of the requirements and may require the assistance of an internal or external resource to adequately assess.

What requirements are there?

The standard is structured in 12 sections, each covering a specific aspect of the requirements.

- The twelve sections of the standard below always stay the same, but each SAQ has its predetermined number of requirements.
- The individual requirements are the same no matter what reporting template is used, the Report on Compliance (“ROC”) used by larger merchants (processing over 6 million transactions per year) includes all of them, SAQ D contains most of them, SAQ P2PE contains very few.

CORE PRINCIPALS	SECTIONS OF THE STANDARD
Build and maintain a secure network and systems	1. Install and maintain network security controls. 2. Apply secure configuration to all system components.
Protect account data	3. Protect stored account data. 4. Protect cardholder data with strong cryptography during transmission over open, public networks.
Maintain a vulnerability management program	5. Protect all systems and networks from malicious software. 6. Develop and maintain secure systems and software.
Implement strong access control measures	7. Restrict access to system components and cardholder data by business Need to Know. 8. Identify users and authenticate access to system components. 9. Restrict physical access to cardholder data.
Regularly monitor and test networks	10. Log and monitor all access to system components and cardholder data. 11. Test security of systems and networks regularly.
Maintain an information security policy	12. Support information security with organizational policies and programs.

ClearAccept

What requirements are there? (cont)

1. SAQs simply require that the merchant indicates whether the requirement is in place or not.
2. The merchant “attests” that they are compliant through an AOC (“Attestation of Compliance”).
3. If you use a service provider to perform some of the functions in scope for the assessment, then you should obtain a copy of their AOC to prove they are compliant as you cannot claim to be compliant if they are not.
4. An AOC is valid for one year. You should complete (not start) your renewal assessment by the date the last one expires.
5. Some assessments require a vulnerability scans done by an ASV vendor that should be contracted by your company.
    - Passing scans must be obtained at least quarterly.
    - The final stage of an ASV scan is you “attesting” it – if you do not do this you have not completed the scan.

PCI is primarily intended to protect card data. You are strongly advised to implement similar security controls to protect your other business assets and systems.

ClearAccept

Where can I find more information?

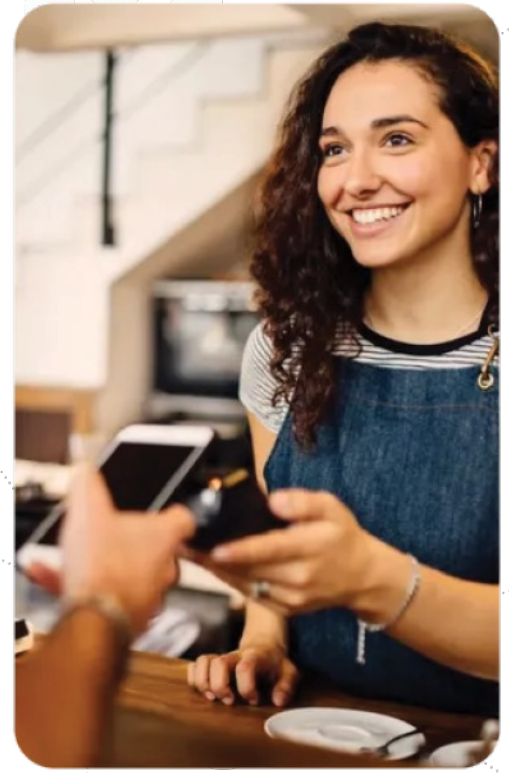
All the standards are maintained by the PCI Security Standards Council.

Official PCI Security Standards Council Site.

What you can find in the council website

- Downloadable copies of the guidance on SAQ types
- Actual SAQ's
- Frequently Asked Questions
- Guidance for Merchants
- Listings of vendors/products that have been certified under various PCI Standards: PTS, ASV, P2PE
- And more…

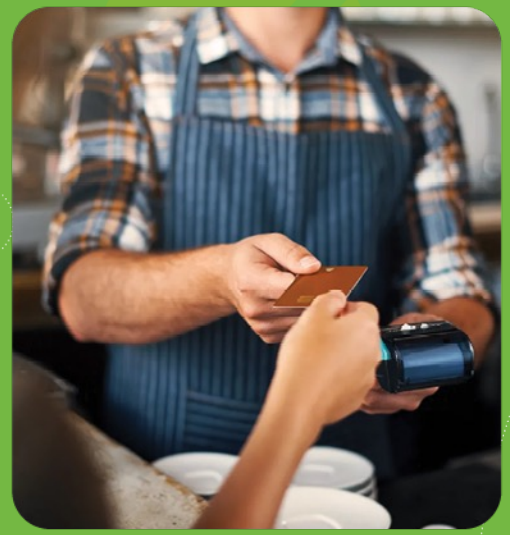
At ClearAccept we **ensure and support our merchants to be PCI DSS compliant** with the card schemes requirements and regulations.



PCI Security Standards Council

ClearAccept

Thank you



clearaccept.com