PCI Frequently Asked Questions

Understanding the SAQs for PCI DSS version 3

The PCI DSS self-assessment questionnaires (SAQs) are validation tools intended to assist merchants and service providers report the results of their PCI DSS self-assessment. The different SAQ types are shown in the table below to help you identify which SAQ best applies to your organization. Detailed descriptions for each SAQ are provided within the applicable SAQ.
Note: Entities should ensure they meet all the requirements for a particular SAQ before using the SAQ. Merchants are encouraged to contact their merchant bank (acquirer) or the applicable payment brand(s) to identify the appropriate SAQ based on their eligibility.

SAQ	Pages in Document	Description
A	19	Card-not-present merchants (e-commerce or mail/telephone-order) that have fully outsourced all cardholder data functions to PCI DSS validated 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	46	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	24	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	35	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		SAQ D for Merchants: All merchants not included in descriptions for the above SAQ types. SAQ D for Service Providers: All service providers defined by a payment brand as eligible to complete a SAQ.

Self-Assessment Questionnaire A and Attestation of Compliance (Card-not-present Merchants, All Cardholder Data Functions Fully Outsourced)
(19 Page Document)

Merchant Eligibility Criteria for SAQ A

SAQ A has been developed to address requirements applicable to merchants whose cardholder data functions are completely outsourced to validated third parties, where the merchant retains only paper reports or receipts with cardholder data.

SAQ A merchants may be either e-commerce or mail/telephone-order merchants (card-not-present), and do not store, process, or transmit any cardholder data in electronic format on their systems or premises.

SAQ A merchants confirm that, for this payment channel:

1. Your company accepts only card-not-present (e-commerce or mail/telephone-order) transactions;
2. All payment acceptance and processing are entirely outsourced to PCI DSS validated third-party service providers;
3. Your company has no direct control of the manner in which cardholder data is captured, processed, transmitted, or stored;
4. Your company does not electronically store, process, or transmit any cardholder data on your systems or premises, but relies entirely on a third party(s) to handle all these functions;
5. Your company has confirmed that all third party(s) handling acceptance, storage, processing, and/or transmission of cardholder data are PCI DSS compliant; **and**
6. Your company retains only paper reports or receipts with cardholder data, and these documents are not received electronically.

Additionally, for e-commerce channels:

- The entirety of all payment pages delivered to the consumer's browser originates directly from a third-party PCI DSS validated service provider(s).

This SAQ is not applicable to face-to-face channels.
This shortened version of the SAQ includes questions that apply to a specific type of small merchant environment, as defined in the above eligibility criteria. If there are PCI DSS requirements applicable to your environment that are not covered in this SAQ, it may be an indication that this SAQ is not suitable for your environment. Additionally, you must still comply with all applicable PCI DSS requirements in order to be PCI DSS compliant.

Self-Assessment Questionnaire A-EP and Attestation of Compliance (Partially Outsourced E-commerce Merchants Using a Third-Party Website for Payment Processing)

(46 Page Document)

Merchant Eligibility Criteria for SAQ A-EP

New SAQ to address requirements applicable to e-commerce merchants with a websites that do not themselves receive cardholder data but which do affect the security of the payment transaction and/or the integrity of the page that accepts the consumer's cardholder data.

SAQ A-EP has been developed to address requirements applicable to e-commerce merchants with a website(s) that does not itself receive cardholder data but which does affect the security of the payment transaction and/or the integrity of the page that accepts the consumer's cardholder data.

SAQ A-EP merchants are e-commerce merchants who partially outsource their e-commerce payment channel to PCI DSS validated third parties and do not electronically store, process, or transmit any cardholder data on their systems or premises.

SAQ A-EP merchants confirm that, for this payment channel:

1. Your company accepts only e-commerce transactions;
2. All processing of cardholder data is outsourced to a PCI DSS validated third-party payment processor;
3. Your e-commerce website does not receive cardholder data but controls how consumers, or their cardholder data, are redirected to a PCI DSS validated third-party payment processor;
4. Your e-commerce website is not connected to any other systems within your environment (this can be achieved via network segmentation to isolate the website from all other systems);
5. If merchant website is hosted by a third-party provider, the provider is validated to all applicable PCI DSS requirements (e.g., including PCI DSS Appendix A if the provider is a shared hosting provider);
6. All elements of payment pages that are delivered to the consumer's browser originate from either the merchant's website or a PCI DSS compliant service provider(s);
7. Your company does not electronically store, process, or transmit any cardholder data on your systems or premises, but relies entirely on a third party(s) to handle all these functions;
8. Your company has confirmed that all third party(s) handling storage, processing, and/or transmission of cardholder data are PCI DSS compliant; and
9. Your company retains only paper reports or receipts with cardholder data, and these documents are not received electronically.

This SAQ is applicable only to e-commerce channels.

This shortened version of the SAQ includes questions that apply to a specific type of small merchant environment, as defined in the above eligibility criteria. If there are PCI DSS requirements applicable to your environment that are not covered in this SAQ, it may be an indication that this SAQ is not suitable for your environment. Additionally, you must still comply with all applicable PCI DSS requirements in order to be PCI DSS compliant.

Self-Assessment Questionnaire B and Attestation of Compliance (Merchants with Only Imprint Machines or Only Standalone, Dial-out Terminals - No Electronic Cardholder Data Storage)

(24 Page Document)

Merchant Eligibility Criteria for SAQ B

SAQ B has been developed to address requirements applicable to merchants who process cardholder data only via imprint machines or standalone, dial-out terminals. SAQ B merchants may be either brick-and-mortar (card-present) or mail/telephone order (card-not-present) merchants, and do not store cardholder data on any computer system.

SAQ B merchants confirm that, for this payment channel:

1. Your company uses only an imprint machine and/or uses only standalone, dial-out terminals (connected via a phone line to your processor) to take your customers' payment card information;
2. The standalone, dial-out terminals are not connected to any other systems within your environment;
3. The standalone, dial-out terminals are not connected to the Internet;
4. Your company does not transmit cardholder data over a network (either an internal network or the Internet);
5. Your company retains only paper reports or paper copies of receipts with cardholder data, and these documents are not received electronically; and
6. Your company does not store cardholder data in electronic format.

This SAQ is not applicable to e-commerce channels.

This shortened version of the SAQ includes questions that apply to a specific type of small merchant environment, as defined in the above eligibility criteria. If there are PCI DSS requirements applicable to your environment that are not covered in this SAQ, it may be an indication that this SAQ is not suitable for your environment. Additionally, you must still comply with all applicable PCI DSS requirements in order to be PCI DSS compliant.

Self-Assessment Questionnaire B-IP and Attestation of Compliance (Merchants with Standalone, IP-Connected PTS Point-of-Interaction (POI) Terminals – No Electronic Cardholder Data Storage)

(35 Page Document)

Merchant Eligibility Criteria for SAQ B-IP

New SAQ to address requirements applicable to merchants who process cardholder data only via standalone, PTS-approved point-of-interaction devices with an IP connection to the payment processor.

SAQ B-IP has been developed to address requirements applicable to merchants who process cardholder data only via standalone, PTS-approved point-of-interaction (POI) devices with an IP connection to the payment processor.

SAQ B-IP merchants may be either brick-and-mortar (card-present) or mail/telephone-order (card-not-present) merchants, and do not store cardholder data on any computer system.

SAQ B-IP merchants confirm that, for this payment channel:

1. Your company uses only standalone, PTS-approved point-of-interaction (POI) devices (excludes SCRs) connected via IP to your payment processor to take your customers' payment card information;
2. The standalone IP-connected POI devices are validated to the PTS POI program as listed on the PCI SSC website (excludes SCRs);
3. The standalone IP-connected POI devices are not connected to any other systems within your environment (this can be achieved via network segmentation to isolate POI devices from other systems);
4. The only transmission of cardholder data is from the PTS-approved POI devices to the payment processor;
5. The POI device does not rely on any other device (e.g., computer, mobile phone, tablet, etc.) to connect to the payment processor;
6. Your company retains only paper reports or paper copies of receipts with cardholder data, and these documents are not received electronically; and
7. Your company does not store cardholder data in electronic format.

This SAQ is not applicable to e-commerce channels.

This shortened version of the SAQ includes questions that apply to a specific type of small merchant environment, as defined in the above eligibility criteria. If there are PCI DSS requirements applicable to your environment that are not covered in this SAQ, it may be an indication that this SAQ is not suitable for your environment.

Self-Assessment Questionnaire C and Attestation of Compliance (Merchants with Payment Application Systems Connected to the Internet - No Electronic Cardholder Data Storage)
(46 Page Document)

Merchant Eligibility Criteria for SAQ C
SAQ C has been developed to address requirements applicable to merchants whose payment application systems (for example, point-of-sale systems) are connected to the Internet (for example, via DSL, cable modem, etc.).

SAQ C merchants process cardholder data via a point-of-sale (POS) system or other payment application systems connected to the Internet, do not store cardholder data on any computer system, and may be either brick-and-mortar (card-present) or mail/telephone-order (card-not-present) merchants.

SAQ C merchants confirm that, for this payment channel:

1. Your company has a payment application system and an Internet connection on the same device and/or same local area network (LAN);
2. The payment application system/Internet device is not connected to any other systems within your environment (this can be achieved via network segmentation to isolate payment application system/Internet device from all other systems);
3. The physical location of the POS environment is not connected to other premises or locations, and any LAN is for a single location only;
4. Your company retains only paper reports or paper copies of receipts, and these documents are not received electronically; and
5. Your company does not store cardholder data in electronic format.

This SAQ is not applicable to e-commerce channels.

This shortened version of the SAQ includes questions that apply to a specific type of small merchant environment, as defined in the above eligibility criteria. If there are PCI DSS requirements applicable to your environment that are not covered in this SAQ, it may be an indication that this SAQ is not suitable for your environment. Additionally, you must still comply with all applicable PCI DSS requirements in order to be PCI DSS compliant.

Self-Assessment Questionnaire C-VT and Attestation of Compliance (Merchants with Web-Based Virtual Payment Terminals—No Electronic Cardholder Data Storage)
(32 Page Document)

Merchant Eligibility Criteria for SAQ C-VT
SAQ C-VT has been developed to address requirements applicable to merchants who process cardholder data only via isolated virtual payment terminals on a personal computer connected to the Internet.

A virtual payment terminal is web-browser-based access to an acquirer, processor, or third-party service provider website to authorize payment card transactions, where the merchant manually enters payment card data via a securely connected web browser. Unlike physical terminals, virtual payment terminals do not read data directly from a payment card. Because payment card transactions are entered manually, virtual payment terminals are typically used instead of physical terminals in merchant environments with low transaction volumes.

SAQ C-VT merchants process cardholder data only via a virtual payment terminal and do not store cardholder data on any computer system. These virtual terminals are connected to the Internet to access a third party that hosts the virtual terminal payment-processing function. This third party may be a processor, acquirer, or other third-party service provider who stores, processes, and/or transmits cardholder data to authorize and/or settle merchants' virtual terminal payment transactions.

This SAQ option is intended to apply only to merchants who manually enter a single transaction at a time via a keyboard into an Internet-based virtual terminal solution. SAQ C-VT merchants may be brick-and-mortar (card-present) or mail/telephone-order (card-not-present) merchants.

SAQ C-VT merchants confirm that, for this payment channel:

1. Your company's only payment processing is via a virtual payment terminal accessed by an Internet-connected web browser;
2. Your company's virtual payment terminal solution is provided and hosted by a PCI DSS validated third-party service provider;
3. Your company accesses the PCI DSS-compliant virtual payment terminal solution via a computer that is isolated in a single location, and is not connected to other locations or systems within your environment (this can be achieved via a firewall or network segmentation to isolate the computer from other systems);

4. Your company's computer does not have software installed that causes cardholder data to be stored (for example, there is no software for batch processing or store-and-forward);
5. Your company's computer does not have any attached hardware devices that are used to capture or store cardholder data (for example, there are no card readers attached);
6. Your company does not otherwise receive or transmit cardholder data electronically through any channels (for example, via an internal network or the Internet);
7. Your company retains only paper reports or paper copies of receipts, and these documents are not received electronically; and
8. Your company does not store cardholder data in electronic format.

This SAQ is not applicable to e-commerce channels.

This shortened version of the SAQ includes questions that apply to a specific type of small merchant environment, as defined in the above eligibility criteria. If there are PCI DSS requirements applicable to your environment that are not covered in this SAQ, it may be an indication that this SAQ is not suitable for your environment. Additionally, you must still comply with all applicable PCI DSS requirements in order to be PCI DSS compliant.

Self-Assessment Questionnaire D and Attestation of Compliance for Merchants (All other SAQ-Eligible Merchants)

(82 Page Document)

SAQ D for Merchants applies to SAQ-eligible merchants not meeting the criteria for any other SAQ type. Examples of merchant environments that would use SAQ D may include but are not limited to:

1. E-commerce merchants who accept cardholder data on their website.
2. Merchants with electronic storage of cardholder data
3. Merchants that don't store cardholder data electronically but that do not meet the criteria of another SAQ type
4. Merchants with environments that might meet the criteria of another SAQ type, but that have additional PCI DSS requirements applicable to their environment

While many organizations completing SAQ D will need to validate compliance with every PCI DSS requirement, some organizations with very specific business models may find that some requirements do not apply. See the guidance below for information about the exclusion of certain, specific requirements.

Self-Assessment Questionnaire P2PE-HW and Attestation of Compliance (Hardware Payment Terminals in a PCI-Listed P2PE Solution Only – No Electronic Cardholder Data Storage)

(26 Page Document)

Merchant Eligibility Criteria for SAQ P2PE-HW

SAQ P2PE-HW has been developed to address requirements applicable to merchants who process cardholder data only via hardware payment terminals included in a validated and PCI-listed Point-to-Point Encryption (P2PE) solution.

SAQ P2PE-HW merchants do not have access to clear-text cardholder data on any computer system and only enter account data via hardware payment terminals from a PCI SSC-approved P2PE solution. SAQ P2PE-HW merchants may be either brick-and-mortar (card-present) or mail/telephone-order (card-not-present) merchants. For example, a mail/telephone-order merchant could be eligible for SAQ P2PE if they receive cardholder data on paper or over a telephone, and key it directly and only into a validated
P2PE hardware device.

SAQ P2PE-HW merchants confirm that, for this payment channel:

1. Your company does not store, process, or transmit any cardholder data on any system or electronic media (for example, on computers, portable disks, or audio recordings) outside of the hardware payment terminal used as part of a validated PCI P2PE solution;
2. Your company has confirmed that the implemented PCI P2PE solution is listed on the PCI SSC's list of Validated Point-to-Point Encryption Solutions;
3. If your company stores cardholder data, such data is only in paper reports or copies of paper receipts and is not received electronically, and
4. Your company has implemented all controls in the P2PE Instruction Manual (PIM) provided by the P2PE Solution Provider.

This SAQ is not applicable to e-commerce channels.

This shortened version of the SAQ includes questions that apply to a specific type of small-merchant environment, as defined in the above eligibility criteria. If there are PCI DSS requirements applicable to your environment that are not covered in this SAQ, it may be an indication that this SAQ is not suitable for your environment.

PCI Frequently Asked Questions

(The following list contains FAQs asked by many of our CardConnect agents or merchants. For additional FAQs, please visit The PCI Security Standards Council at **https://www.pcisecuritystandards.org/faq**)

- **Q: What is PCI?**
- **A:** The Payment Card Industry Data Security Standard (PCI DSS) is a set of requirements designed to ensure that ALL companies that process, store or transmit credit card information maintain a secure environment. The PCI DSS body is administered and managed by the PCI SSC (www.pcisecuritystandards.org), an independent body that was created by the major payment card brands (Visa, MasterCard, American Express, Discover and JCB.).
- **Q: How does a merchange get educated about PCI?**
- **A:** Merchants getting started with PCI compliance, can find a wealth of information on the PCI Council website (https://www.pcisecuritystandards.org/merchants/index.php). For more information, a merchant can download the PCI Council's Getting Started Guide and Quick Reference Guide. To learn what a merchant's specific compliance requirements are, the PCI Council recommends the merchant to check directly with the card brands:
    - American Express
    - Discover Financial Services
    - JCB International
    - MasterCard Worldwide
    - Visa Inc.
    - Visa Europe
- **Q: To whom does PCI apply?**
- **A:** PCI applies to ANY organization or merchant (includes international merchants/organizations), regardless of size or number of transactions, that accepts, transmits or stores any cardholder data.
- **Q: How often is PCI DSS validation required?**
- **A:** Merchants must demonstrate compliance annually via a Self-Assessment Questionnaire (SAQ) or Report on Compliance (ROC). Validation requirements vary depending on the number of transactions processed annually and the payment card brand. Compliance requires establishing and maintaining a PCI program that incorporates appropriate business policies, procedures and technologies to ensure ongoing compliance through continuous protection of payment card data.
- **Q: What is the definition of 'merchant'?**
- **A:** PCI DSS defines a merchant as any entity that accepts payment cards bearing the logos of any of the five members of PCI SSC (American Express, Discover, JCB, MasterCard or Visa) as payment for goods and/or services. A merchant that accepts payment cards as payment for goods and/or services can also be a service provider, if the services sold result in storing, processing, or transmitting cardholder data on behalf of other merchants or service providers. For example, an ISP is a merchant that accepts payment cards for monthly billing, but also is a service provider if it hosts merchants as customers
- **Q: Who is Trustwave?**
- **A:** Trustwave is one of the most expert and renown qualified security assessors. They have been hired by CardConnect to help merchants, become officially PCI validated. They have an easy PCI survey that take a merchant through the process of validating PCI compliance, and they will report the merchant's compliance status directly to CardConnect once a merchant completes the survey. Trustwave will also give CardConnect up-to-date reports on the PCI status of CardConnect acquired merchants.
- **Q: What constitutes a Service Provider?**
- **A:** Any company that stores, processes, or transmits cardholder data on behalf of another entity is defined to be a Service Provider by the Payment Card Industry (PCI) guidelines. CardConnect is a gateway Service Provider.
- **Q: If a merchant is certified as PCI compliant, does it mean the merchant's data is secure?**
- No, as many high-profile data breach cases have shown, companies that are certified as PCI compliant can still suffer data breaches and financial losses. PCI compliance alone won't protect corporate data and systems from costly, time-consuming data breaches and advanced threats. PCI compliance should be viewed as the baseline, not the end goal, for any organization. Annual validation of compliance means nothing without continual efforts to maintain that compliant state. A well-defined security program can help organizations not only meet and maintain PCI compliance, but also address new and emerging threats as well as innovations such as mobile, virtualization and other technology. Only by designing, implementing and maintaining effective security controls to meet PCI requirements can organizations gain security alongside compliance.
- **Q: What is a payment gateway?**

- **A:** Payment Gateways connect a merchant to the bank or processor that is acting as the front-end connection to the Card Brands. They are called gateways because they take many inputs from a variety of different applications and route those inputs to the appropriate bank or processor. Gateways communicate with the bank or processor using dial-up connections, Web-based connections or privately held leased lines. CardConnect is a gateway.
- **Q: How is IP-based POS environment defined?**
- **A:** The point of sale (POS) environment refers to a transaction that takes place at a merchant location (i.e. retail store, restaurant, hotel, gas station, convenience store, etc.). An Internet protocol (IP) -based POS is when transactions are stored, processed, or transmitted on IP-based systems or systems communicating via TCP/IP.
- **Q: Does a merchant need to upgrade equipment, software or networks to become PCI DSS Compliant?**
- **A:** In order to become compliant, a merchant may be required to upgrade equipment or software that supports PCI compliance. A merchant may also need to address vulnerabilities within the internal networks. For more information, consult CardConnect to discuss PCI compliant solutions available and costs associated with software or equipment upgrades.
- **Q: What do merchants need to conside (as it relates to PCI compliance) regarding mobile devices and tablets used in a store environment?**
- **A:** A merchant needs to determine what the devices are going to be used for and whether or not they'll be used to process transactions or have any payment card data processed or stored within the device. Mobile devices being on the same network as systems that store, process or transmit payment card data bring these devices into PCI scope. Mobile devices that fall within PCI scope must be reviewed under the same PCI compliance standards.
- **Q: Can the full credit card number be printed on the consumer's copy of the receipt?**
- **A:** PCI DSS requirement 3.3 states "Mask PAN when displayed (the first six and last four digits are the maximum number of digits to be displayed)." While the requirement does not prohibit printing of the full card number or expiry date on receipts (either the merchant copy or the consumer copy), please note that PCI DSS does not override any other laws that legislate what can be printed on receipts (such as the U.S. Fair and Accurate Credit Transactions Act (FACTA) or any other applicable laws). This requirement does not apply to employees and other parties with a specific need to see the full PAN, nor does the requirement supersede stricter requirements in place for displays of cardholder data (for example, for point of sale (POS) receipts)." Any paper receipts stored by merchants must adhere to the PCI DSS, especially requirement 9 regarding physical security.
- **Q: Where can a merchant find the PCI Data Security Standards documentation (PCI DSS)?**
- **A:** The Standard can be found on the PCI SSC's Website: https://www.pcisecuritystandards.org/security_standards/pci_dss.shtml
- **Q: Does a merchant need vulnerability scanning to validate compliance?**
- **A:** If a merchant qualifies for a specific Self-Assessment Questionnaires (SAQs) or the merchant electronically stores cardholder data post authorization, then a quarterly scan by a PCI SSC Approved Scanning Vendor (ASV) is required to maintain compliance. If a merchant qualifies for any of the following SAQs under version 3.0 of the PCI DSS, the merchant is required to have a passing ASV scan:
    - SAQ A-EP
    - SAQ B-IP
    - SAQ C
    - SAQ D-Merchant
    - SAQ D-Service Provider
- **Q: What is a vulnerability scan?**
- **A:** A vulnerability scan checks a merchant or service provider's systems for security vulnerabilities. It is a tool that will conduct a non-intrusive scan to remotely review networks and Web applications based on the external-facing Internet protocol (IP) addresses provided by the merchant or service provider. The scan identifies vulnerabilities in operating systems, services and devices that could be used by hackers to target the company's private network. The scan does not require the merchant or service provider to install any software on their systems, and no denial-of-service attacks are generally performed.
- **Q: How often does a merchant have to have a vulnerability scan?**
- **A:** Once every 90 days. Merchants requiring a vulnerability scan are required to submit a passing scan. Merchants and service providers should submit compliance documentation (successful scan reports) according to the timetable determined by their acquirer. Scans must be conducted by a PCI SSC Approved Scanning Vendor (ASV) such as Security Metrics.
- **Q: Is a merchant obligated to be PCI compliant?**
- **A:** PCI is not a law. The PCI standards were created by the major card brands Visa, MasterCard, Discover, AMEX and JCB. At their acquirers'/service providers' discretion, merchants that do not comply with PCI DSS may be subject to fines, card replacement costs, costly forensic audits, brand damage, etc., should a breach event occur. With little upfront effort and cost to comply with PCI, a merchant greatly reduces the risk from facing extreme and unpleasant costly consequences.
- **Q: Do states have laws requiring data breach notifications to the affected parties?**

- **A:** As of June 2015, Forty-seven states, the District of Columbia, Guam, Puerto Rico and the Virgin Islands have enacted legislation requiring private or government entities to notify individuals of security breaches of information involving personally identifiable information. Security breach laws typically have provisions regarding who must comply with the law (e.g., businesses, data/ information brokers, government entities, etc.); definitions of "personal information" (e.g., name combined with SSN, driver's license or state ID, account numbers, etc.); what constitutes a breach (e.g., unauthorized acquisition of data); requirements for notice (e.g., timing or method of notice, who must be notified); and exemptions (e.g., for encrypted information).
- **Q: What does a small-to-medium size business need to do in order to satisfy the PCI DSS v3.0 requirements?**
- **A:** To satisfy the requirements of PCI, a merchant must complete the following steps:
    1. Determine which Self-Assessment Questionnaire (SAQ) your business should use to validate compliance. See the below to help select which SAQ is applicable.
    2. Complete the Self-Assessment Questionnaire according to the instructions it contains.
    3. Complete and obtain evidence of a passing vulnerability scan with a PCI SSC Approved Scanning Vendor (ASV). Note scanning does not apply to all merchants. It is 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 in its entirety as applicable.
    5. Submit the SAQ, evidence of a passing scan (if applicable), and the Attestation of Compliance, along with any other requested documentation, to your acquirer.

The PCI DSS self-assessment questionnaires (SAQs) are validation tools intended to assist merchants and service providers report the results of their PCI DSS self-assessment. The different SAQ types are shown in the table below to help you identify which SAQ best applies to your organization. Detailed descriptions for each SAQ are provided within the applicable SAQ.
Note: Entities should ensure they meet all the requirements for a particular SAQ before using the SAQ. Merchants are encouraged to contact their merchant bank (acquirer) or the applicable payment brand(s) to identify the appropriate SAQ based on their eligibility.

SAQ	Pages in Document	Description
A	19	Card-not-present merchants (e-commerce or mail/telephone-order) that have fully outsourced all cardholder data functions to PCI DSS validated 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	46	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	24	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	35	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		SAQ D for Merchants: All merchants not included in descriptions for the above SAQ types. SAQ D for Service Providers: All service providers defined by a payment brand as eligible to

		complete a SAQ.

- **Q: What are the requirements to be in compliance with the PCI Data Security Standard?**
- **A:** The PCI Data Security Standard is a multifaceted security standard that includes requirements for security management, policies, procedures, network architecture, software design and other critical protective measures. The PCI Data Security Standard is comprised of 12 general requirements designed to: Build and maintain a secure network; Protect cardholder data; Ensure the maintenance of vulnerability management programs; Implement strong access control measures; Regularly monitor and test networks; and Ensure the maintenance of information security policies.
- **Q: Which Self-assessment Questionnaire (SAQ) must be completed by a merchant?**
- **A:** The PCI DSS SAQ Instructions and Guidelines information (table posted within these FAQs) provides a summary of the different SAQs and the types of environments that each SAQ is intended for. Merchants should also consult with their acquirer (merchant bank) or payment brand to determine if they are eligible or required to submit an SAQ, and if so, which SAQ is appropriate for their environment. Merchant Account acquired via CardConnect automatically received notification of their respective SAQ that needs to be completed. Additional SAQs may apply depending on how the merchant is conducting business. For more information on the different SAQs available please visit the PCI Council website at https://www.pcisecuritystandards.org.
- **Q: How does CardConnect help minimize PCI scope within a merchant environment?**
- **A:** CardConnect provides card holder data tokenization. A token replaces the card holder data that a merchant needs to store when handling transactions. The token is used when submitting the transaction to the payment processor. Since the token is not card data, the merchant can store the token and reduce the PCI scope of the system storing the token. MOTO merchants cans further reduce their PCI scopy by making use of available CardConnect P2PE solutions. Merchants with Ecommerce sites can also reduce their website PCI scope by making use of the available CardConnect tokenization solutions (Ajax Tokenizer and hosted Tokenizer).
- **Q: Is storage of encrypted cardholder data considered "cardholder data" per the SAQ eligibility criteria?**
- **A:** Yes, encrypted cardholder data is considered cardholder data for the purposes of the SAQ eligibility criteria. Merchants must meet all the defined eligibility criteria for a particular SAQ in order to use that SAQ. The eligibility criteria for all SAQs, except SAQ D, include an attestation by the merchant that they do not store cardholder data in electronic format. As SAQ D is the only SAQ that includes PCI DSS requirements for protecting stored cardholder data, including encryption and key management requirements, SAQ D could apply to scenarios where only encrypted cardholder data is stored. Merchants should consult with their acquirer or CardConnect directly (as applicable) to determine which SAQ they should use.
- **Q: If a merchant only accepts credit cards over the phone, does PCI still applies to the merchant?**
- **A:** Yes. All businesses that store, process or transmit payment cardholder data must be PCI Compliant.
- **Q: Are debit card transactions in scope for PCI?**
- **A:** PCI In-scope cards include any debit, credit, and pre-paid cards branded with one of the five card association/brand logos that participate in the PCI SSC – American Express, Discover, JCB, MasterCard, and Visa International.
- **Q: Are merchants PCI compliant if they have an SSL certificate installed within their E-commerce site?**
- **A:** No. SSL certificates do not secure a Web server from malicious attacks or intrusions. SSL certificates provide the first tier of customer security and reassurance, but there are other steps to achieve PCI Compliance. An SSL Certificate provides 1) A secure connection between the customer's browser and the web server and 2) Validation that the Website operators are a legitimate, legally accountable organization
- **Q: What is defined as 'cardholder data'?**
- A: The PCI Security Standards Council defines 'cardholder data' as the full Primary Account Number (PAN) or the full PAN along with any of the following elements: 1) Cardholder name, 2) Expiration date, 3) Service code, and 4) Sensitive Authentication Data which includes full magnetic stripe data, CAV2, CVC2, CVV2, CID, PINs, PIN blocks.
- **Q: What are the penalties for failure to comply with PCI?**
- **A:** The payment brands may, at their discretion, fine an acquiring bank $5,000 to $100,000 per month for PCI compliance violations. The banks will most likely pass this fine on to their merchants. Furthermore, the bank will also most likely either terminate the relationship or increase transaction fees for a merchant in violation of PCI compliance. Penalties are not openly discussed nor widely publicized, but they can be catastrophic to a small business.
- **Q: If a business has multiple locations, is each location required to validate PCI Compliance?**
- **A:** If a business' locations process under the same Tax ID, that business is only required to validate once annually for all locations and submit quarterly passing network scans by an PCI SSC Approved Scanning Vendor (ASV), if applicable.
- **Q: Do organizations using third-party processors like CardConnect have to be PCI compliant?**

- **A:** Yes. Using CardConnect services does not exclude a company from PCI compliance. It may cut down on their risk exposure and consequently reduce the effort to validate compliance. However, it does not mean they can ignore PCI.
- **Q: Is a merchant website still in scope for PCI DSS if it meets all the criteria for SAQ A?**
- **A:** Yes. The merchant web server must be included in scope so the assessor can examine its configuration and verify the redirection mechanism used. Once verified, the applicable requirements will then need to be implemented (SAQ-AEP). If the merchant environment and web server redirection meet all criteria for SAQ A, then the minimum applicable requirements can be considered as those within that SAQ.
- **Q: Is VoIP in scope for PCI DSS?**
- **A:** PCI DSS requirements apply wherever account data is stored, processed, or transmitted. While PCI DSS does not explicitly reference the use of VoIP, VoIP traffic that contains cardholder data is in scope for applicable PCI DSS controls, in the same way that other IP network traffic containing cardholder data would be. Note that VoIP transmissions originating from an external source and sent to an entity's environment are not considered in scope for the entity's PCI DSS compliance, as an entity cannot control the method of inbound phone calls that their customers and other parties may make, including whether any account data sent over that transmission is being adequately protected by the caller. However, the entity does have control over transmissions, storage and processing of VoIP traffic within their own network, and any outbound transmissions that they instigate. Therefore, VoIP traffic containing account data that is stored, processed or transmitted internally over an entity's network, or transmitted externally by the entity, is in scope for applicable PCI DSS controls.
- **Q: Does PCI DSS apply to bank account data?**
- **A:** PCI DSS applies for the protection of cardholder data (PAN, cardholder name, service code and expiration date) and sensitive authentication data (full track data from the magnetic stripe or equivalent data on the chip, CAV2/CVC2/CVV2/CID, and PIN/PIN block), from a payment card using any payment brands (American Express, Discover, JCB, MasterCard, or Visa). Bank account data, such as branch identification numbers, bank account numbers, sort codes, routing numbers, etc., are not considered payment card data, and PCI DSS does not apply to this information. However, if a bank account number is also a PAN or contains the PAN, then PCI DSS applies.
- **Q: What data can a merchant store related to a credit Card and still meet PCI compliance?**
- **A:** A merchant can store a Card Holder name, token, address, zip code and expiry only. No CVV, clear text card data or encrypted track ought to be stored.
- **Q: Can card verification codes/values be stored for recurring transactions?**
- **A:** Card verification codes/values (the 3- or 4- digit number printed on a payment card) are considered sensitive authentication data, which in accordance with PCI DSS Requirement 3.2 must not be stored after authorization. Card verification codes/values are used for initial authorization in card-not-present transactions, and are not needed for recurring transactions. Merchants should contact their acquirer (merchant bank) or the payment brands directly, as applicable, for guidance on how to process recurring transactions without storing the prohibited data.
- **Q: Is CardConnect a PCI compliant Gateway Service Provider?**
- **A:** Yes. CardConnect is a PCI compliant Gateway. Every year, CardConnect engages in rigorous PCI DSS process to review and re-assess all data security measures. As a result of the process, a ROC (Report of Compliance) is generated. A yearly Attestation of Compliance (AOC) document is available upon request.
- **Q: Who is required to fill out a PCI SAQ document?**
- A: Any merchant handling credit card transactions is required to fill out a specificc PCI SAQ document based on the nature of the card holder data process in place. To determine which SAQ corresponds to a merchant, please visit our SAQ document summary section.

P2PE Frequently Asked Questions

- **Q:** What is P2PE?
- **A:** A point-to-point encryption (P2PE) solution cryptographically protects account data from the point where a merchant accepts the payment card to the secure point of decryption. By using P2PE, account data (cardholder data and sensitive authentication data) is unreadable until it reaches the secure decryption environment, which makes it less valuable if the data is stolen in a breach. Merchants using PCI-listed P2PE solutions also have fewer applicable PCI Data Security Standard (PCI DSS) requirements, which helps simplify compliance efforts. CardConnect offers P2PE solutions and is certified by the PCI Council as one of few companies qualified to offer P2PE. The CardConnect P2PE solution provides a terminal to device encryption/decryption process where the encrypted submited card data is fully protected from breach. To see the PCI Council CardConnect P2PE listing, click on the following link:https://www.pcisecuritystandards.org/approved_companies_providers/validated_p2pe_solutions.php
- **Q:** What are the benefits of P2PE?
- **A:** A P2PE solution:
    1. Makes account data unreadable by unauthorized parties and protects customer data and a company's reputation

2. “De-values” account data because it can’t be decrypted even if stolen
3. Simplifies compliance with PCI DSS requirements
4. The P2PE Self-Assessment Questionnaire includes only 26 PCI DSS requirements

- **Q: Who can use SAQ P2PE-HW?**
- **A:** SAQ P2PE-HW is intended for SAQ-eligible merchants, who process cardholder data only via approved payment terminals as part of a Council-listed P2PE solution. Merchants wishing to use SAQ P2PE-HW must confirm that they: 1) Are using a PCI P2PE solution that is listed on the PCI SSC’s List of Validated P2PE Solution 2) Do not store, process, or transmit any cardholder data on any system or electronic media (for example, on computers, portable disks, or audio recordings) outside of the payment terminal used as part of the P2PE solution 3) Do not store any cardholder data in electronic format. This includes verifying that there is no legacy storage of cardholder data from other payment devices or systems 4) Have implemented all controls in the P2PE Instruction Manual (PIM) provided by the P2PE Solution Provider.
- **Q: How does CardConnect remove an Independent Software Vendor application from PCI scope?**
- **A:** An Independent Software vendor who provides software solutions to merchants processing credit cards, can remove their respective application from PCI scope as long as their solution is integrated with the CardConnrect P2PE solution. With the CardConnect P2PE solution, a merchant application does not handle clear test credit card data. All card data transmission is secured end to end. The merchant application can store CardConnect tokens which are not credit card data. The merchant application can reuse a CardConnect token