A guide to PCI DSS compliance

If your business processes Visa, Mastercard and American Express debit or credit card transactions, you must have Payment Card Industry Data Security Standard (PCI DSS) compliance.

We understand that PCI DSS requirements can be confusing at first, so we've created this step-by-step guide to assist you.

Every business is different. Please contact Kiwibank to determine which PCI DSS compliance steps apply to you.

Look out for the **tips** in the blue boxes if you use any of our Fetch™ payment solutions.

Contents

Introduction - what is PCI DSS?

The Payment Card Industry Council developed the Payment Card Industry Data Security Standard (PCI DSS) in response to the growth of card fraud worldwide. The standards are global and mandated by the card schemes including Visa, MasterCard and American Express. It defines industry best practices for handling and protecting credit and scheme debit card details. The PCI DSS outlines minimum standards to ensure the protection of payment card information and provides you with a framework to manage risk and keep card details safe.

PCI DSS applies to all entities that process, transmit and/or store payment card information – this includes third parties.

Visit www.pcisecuritystandards.org for detailed information about your PCI obligations as a merchant and refer back to this website on a regular basis to ensure you always have the most up-to-date information.

Note: We've made sure that our Fetch™ payment solutions comply with the PCI DSS. However, you will still need to ensure that your processes meet the PCI DSS and that you are using your chosen Fetch products in accordance with your merchant terms and conditions.

As a merchant, you must ensure you are not storing cardholder information electronically.

You must also complete a Self-Assessment Questionnaire (SAQ) annually.

PCI DSS goals and requirements

The aim of the PCI DSS is to ensure businesses know how to follow good practice for processing, storing and transmitting card details.

The following table lists the 12 PCI DSS requirements for protecting cardholder data.

Goals	PCI DSS Requirements
Build and maintain a secure network	1. Install and maintain a firewall configuration to protect data
	2. Do not use vendor-supplied defaults for system passwords and other security parameters
Protect cardholder data	3. Protect stored data
	4. Encrypt transmission of cardholder data and sensitive information across public networks
Maintain a vulnerability management programme	5. Use and regularly update anti-virus software
	6. Develop and maintain secure systems and applications
Implement strong access control measures	7. Restrict access to data to a need-to-know basis
	8. Assign a unique ID to each person who has computer access
	9. Restrict physical access to cardholder data
Regularly monitor and test networks	10. Track and monitor all access to network resources and cardholder data
	11. Regularly test security systems and processes
Maintain an Information Security Policy	12. Maintain a policy that addresses information security for employees and contractors

Card information protected by PCI DSS

PCI DSS is designed to protect cardholder data and authentication data.

What information can and cannot be stored?

	Storage permitted	Protection required	Encryption required
Cardholder data			
Primary Account Number (PAN) *The 16 digit Card Number used by Visa and MasterCard*	Yes	Yes	Yes
Expiry date	Yes	Yes	No
Security code	Yes	Yes	No
Cardholder name	Yes	Yes	No
Authentication data			
Full magnetic stripe	No	n/a	n/a
Card Security Code (CSC) *Also known as Card Verification Value (CVV) for Visa and Card Validation Code (CVC) for MasterCard*	No	n/a	n/a
PIN	No	n/a	n/a

The six steps for PCI DSS compliance

You must validate your compliance annually with Kiwibank if your business is Level 1, 2 or 3 as defined in the table below, or, if you are a Level 4 merchant and Kiwibank has requested validation of your compliance.

The PCI DSS level you identify for your business will determine the PCI tools that are required to be completed, as outline in the table below. If you are unsure of your processing volumes, please contact Kiwibank for assistance.

Levels	Level Threshold	Assessment Requirements	SAQ
Level 1	More than 6 million card transactions per annum (any type of transaction)	On-site review by Qualified Security Assessor (QSA) annually *and* Network vulnerability scans by an ASV quarterly (if applicable) *and*	QSA determination
Level 2	More than 1 million but <6 million transactions per annum (any type of transaction)	On-site review by QSA or self-assessment by a qualified Internal Security Assessor (ISA) annually *and* Network vulnerability scans by an ASV quarterly (if applicable)	QSA/ISA determination
Level 3	More than 20,000 but < 1 million e-commerce transactions per annum	SAQ annually *and* Network vulnerability scans by an ASV quarterly (if applicable)	Self-Assessment
Level 4	All other merchants that are not Levels 1 – 3. i.e. under current standards, any merchant processing less than 20,000 e-commerce transactions and less than 1 million transactions in total	SAQ annually *and* Network vulnerability scans by an ASV quarterly	Self-Assessment
Service Providers	*any* Third Party Processor (TPP) *or* Data Storage Entity (DSE)	On-site review by QSA or annually *and*	D – Service Providers DESV if required

Step 1: Select the correct self-assessment questionnaire (SAQ)

Step 2: Complete the SAQ

Step 3: Remediate any issues identified in the self-assessment questionnaire

Step 4: Network vulnerability scan

Step 5: Complete Attestation of Compliance (AOC)

Step 6: Maintain PCI DSS compliance - annual revalidation is required

Step 1: Select the correct self-assessment questionnaire (SAQ)

The PCI DSS Self-Assessment Questionnaire (SAQ) is a validation tool that helps merchants and service providers to self-evaluate their compliance with the PCI DSS. There are specific Self-Assessment Questionnaires designed to meet merchant and service providers processes.

The SAQ consists of two parts:

1. **Questions** about the PCI DSS requirements for service providers and merchants.
2. **Attestation of Compliance** (AOC): The AOC is your self-certification to show you are eligible to perform and have actually performed a PCI DSS self-assessment.

Which SAQ applies to you?

You only need to complete one SAQ regardless of the number of card payment solutions you use. You should select the most detailed SAQ that applies to your payment solution/s. For example, if you have one of the Fetch™ payment solutions and an integrated EFTPOS terminal, you only need to complete SAQ D.

	← less detailed / more detailed →			
Payment solution	**SAQ A**	**SAQ C-VT**	**SAQ B/B-IP**	**SAQ D**
Fetch™ recurring card payments	✓			
Fetch™ invoice payments	✓			
Fetch™ web payments	✓			
Fetch™ mobile payments		✓		
Fetch™ virtual terminal		✓		
EFTPOS credit card only			✓	
Card not present + Card present				✓
Kiwibank QuickPay™			✓	

What are the five SAQs?

SAQ	Description
A	**SAQ A merchants** do not store cardholder data in electronic format and do not process or transmit any cardholder data on their systems or premises. This option does not apply to merchants with a face-to-face Point of Sale (POS) environment. Use **SAQ A** if you are subscribed to Fetch™ recurring card payments, Fetch web payments and/or Fetch invoice payments. Completion of SAQ A and the associated Attestation of Compliance (AOC) confirms that the business: • Handles only card-not-present (i.e. ecommerce or mail/telephone-order) transactions • Does not store, process, or transmit any cardholder data on your systems or premises, but relies entirely on third party service provider(s) (e.g. Fetch payment solutions) to handle all these functions • Has confirmed that any third party handling storage, processing, and/or transmission of cardholder data is PCI DSS compliant • Retains only paper reports or receipts with cardholder data, and these documents are not received electronically*; and • Does not store any cardholder data in electronic format. * A note for merchants who use **Fetch™ recurring card payments:** Please encourage customers to return the authority form to you on paper. If for any reason, your customer returns the authority form by email, it is important to delete the email securely and permanently from your system after printing the form for secure storage. Store the authority form securely in a locked cabinet after you have entered the details on the Fetch system.
B	**SAQ B merchants** process cardholder data only via imprint machines or standalone, dial-out terminals. They 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. This SAQ is not applicable to e-commerce channels.

SAQ	Description
	Completion of SAQ B and the associated Attestation of Compliance (AOC) confirms that: • The business uses only imprint machines and/or uses only standalone, dial-out terminals (connected via a phone line to your processor) to take customers' payment card information • The standalone, dial-out terminals are not connected to any other systems within the business's environment • The standalone, dial-out terminals are not connected to the internet • The business does not transmit cardholder data over a network (either an internal network or the internet) • The business retains only paper reports or paper copies of receipts with cardholder data, and these documents are not received electronically; and • The business does not store cardholder data in electronic format.
B-IP	**SAQ B-IP merchants** process cardholder data only via standalone, PIN Transaction Security (PTS)-approved point-of-interaction (POI) devices with an IP connection to the payment processor. They 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. This SAQ is not applicable to e-commerce channels. Completion of SAQ B-IP and the associated Attestation of Compliance (AOC) confirms that: • The business 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 • The standalone IP-connected POI devices are validated to the PTS POI program as listed on the PCI SSC website (excludes SCRs) • 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 system) • The only transmission of cardholder data is from the PTS-approved POI devices to the payment processor • The POI device does not rely on any other device (e.g., computer, mobile phone, tablet, etc.) to connect to the payment processor • Any cardholder data the business retains is on paper (for example, printed reported or receipts) and these documents are not received electronically; and • The business does not store cardholder data in electronic format

SAQ	Description
C-VT	**SAQ C-VT merchants** process cardholder data via web based virtual payment terminals with no electronic cardholder data storage. 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 does not apply to ecommerce merchants. Use **SAQ C-VT** if you use Fetch™ mobile payments and/or Fetch virtual terminal. Completion of SAQ C-VT and the associated Attestation of Compliance (AOC), confirms that: • The business's only payment processing is done via a virtual terminal accessed by an internet-connected web browser • The business's virtual terminal solution is provided and hosted by a PCI DSS validated third-party service provider • The business accesses the PCI DSS compliant virtual 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) • The business'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); • The business'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); • The business does not otherwise receive or transmit cardholder data electronically through any channels (for example, via an internal network or the internet) • The business retains only paper reports or paper copies of receipts; and • The business does not store cardholder data in electronic format.
D	**SAQ D** applies to all other merchants not included above. It also applies to all service providers defined by a payment brand as being eligible to complete an SAQ.

You can download the SAQ that applies to you here including instructions and guidelines to assist in completing the SAQ.

Step 2: Complete the SAQ

It is useful to sit down with the relevant people to agree who will be responsible for answering which section of the questionnaire.

It's important to answer the SAQ accurately. If in doubt, proceed on the side of caution and assume non-compliance until you have clarification. Remember to detail any compensating controls or provide information on any requirements which you have answered as 'not applicable'.

Handy tips:

- Follow the instruction pages at the start of the applicable SAQ document.
- Answer 'yes' if you are meeting the PCI DSS requirement and 'no' if you are not meeting the requirement or if you're not sure about the answer. If a requirement doesn't apply to your business, answer 'n/a' in the 'special' column. Use Appendix C at the end of the SAQ to explain why the requirement does not apply.
- If you can't answer some questions, you can contact us at merchantservices@kiwibank.co.nz. If there are a lot of requirements you are unsure about, it may be helpful to contact a qualified security assessor (QSA). Here's a list of qualified security assessors.
- If you can't meet a PCI DSS requirement because of a legitimate technical or documented business constraint, you may need to use a compensating control – see below.
- Email the completed SAQ to Kiwibank at merchantservices@kiwibank.co.nz, when requested by Kiwibank

Compensating controls

You can use compensating controls to meet a PCI DSS requirement when technology or business constraints won't allow you to otherwise meet the requirement. A compensating control must meet the intent of the PCI DSS requirement. There is more information about compensating controls in the back of each SAQ document.

You are unlikely to need compensating controls if you are processing card payments using Fetch™.

Step 3: Remediate all issues identified in the self-assessment questionnaire

When you've completed your SAQ, you will need to remediate any non-compliant requirements or implement compensating controls.

Remediation

Remediation timeframes differ from business to business. The time required depends on initial compliance status and the complexity of the cardholder environment.

Compliance

You will need to keep us updated on your compliance progress by completing the 'Action Plan for Non-Compliant Status' when you submit your AOC to merchantservices@kiwibank.co.nz
You will also need to provide us with quarterly updates.

Handy tips:

- It's helpful to structure your remediation into similar phases of work to maximise opportunities and reduce effort.
- A risk-based approach will ensure you focus your efforts on the requirements that will help reduce your business risk profile.
- The prioritised approach tool will help ensure you are remediating areas of your business that could be more at risk of an account data compromise or security breach.
- In some cases, it may be easier to outsource certain parts of your business to a PCI DSS compliant provider to help reduce the scope of remediation required.

Step 4: Network vulnerability scan

Do you need a network vulnerability scan?

If your business collects, processes, transmits and/or stores credit card information using a computer, you need a vulnerability scan.

> **Good news!** This doesn't apply to you if you use Fetch™ recurring card payments, Fetch web payments and/or Fetch invoice payments solutions because the Fetch system takes care of the vulnerability scan for you.

The vulnerability scan checks your IP connection/s (internet connection) and identifies common security weaknesses that a hacker attempting to access your system could find.

Step 5: Complete the Attestation of Compliance (AOC)

When you've completed the SAQ and any remediation, you will need to complete the AOC.

The AOC is located at the front of the SAQ document and you must complete it in full.

If you're not able to immediately remedy any issues identified in the SAQ, you must complete Part 4 of the SAQ 'Action Plan for Non-Compliant Status'.

Email the completed AOC to Kiwibank at merchantservices@kiwibank.co.nz .

Step 6: Maintain PCI DSS compliance

PCI DSS requires annual Attestation of Compliance. We recommend including these requirements in your regular business auditing process to help ensure your business remains compliant. You'll also need to ensure that a business owner is appointed to validate that your business remains compliant. Annual compliance validation is your business's responsibility. Please remember to diary note when you will need to provide your documentation to Kiwibank.

Your annual self-assessment, network scan results (if applicable) and AOC can be emailed to merchantservices@kiwibank.co.nz. Please include your merchant name and number in the subject header.

Here's a quick summary of the annual process:

1. Every year, successfully complete the applicable SAQ
2. Email the SAQ to Kiwibank at merchantservices@kiwibank.co.nz , when requested.

Help whenever you need it

If you ever need any assistance, you can contact us at merchantservices@kiwibank.co.nz or phone 0800 233 824.

PCI DSS compliance FAQs

Do I need to comply with PCI DSS if I use Fetch™ payment solutions?

No single payment solution addresses all 12 requirements of PCI DSS. The PCI DSS applies to all organisations that process, transmit and/or store payment card information. We've made the Fetch products compliant with the standard. As a merchant accepting payments, it is imperative to ensure that your end to end processes comply with the PCI DSS.

Do I need to worry about my providers being PCI DSS compliant too?

You must ensure that your providers' applications and card payment terminals comply with the PCI DSS standard and do not store your customers' sensitive cardholder data. You should request annual proof of compliance from providers by requesting their AOC. You are also encouraged to ensure that this is part of your contracts with such providers.

Who is the best person in my business to take care of PCI DSS?

Compliance with the PCI DSS is an on-going process of assessment, remediation and reporting. It is a business issue that is best addressed by a multi-disciplinary team. The risks of compromise are financial and reputational, so they affect the whole organisation.

I have only a few card transactions. Do I need to comply with PCI DSS?

PCI DSS compliance is required for any business that accepts credit or debit cards – even if the quantity of transactions is just one.

We've completed the correct SAQ. Are we PCI DSS compliant now?

SAQs represent a snapshot of the particular moment in time. After that moment a single system change can make your business non-compliant. Security of cardholder data requires non-stop assessment and remediation to ensure that the likelihood of a breach is kept as low as possible. Implementing PCI DSS should be part of a sound, basic enterprise security strategy, which requires making this activity part of your on-going business plan and budget.