

SAFERPAYMENTS PROGRAM

Sysnet.air user guide – Merchant Role

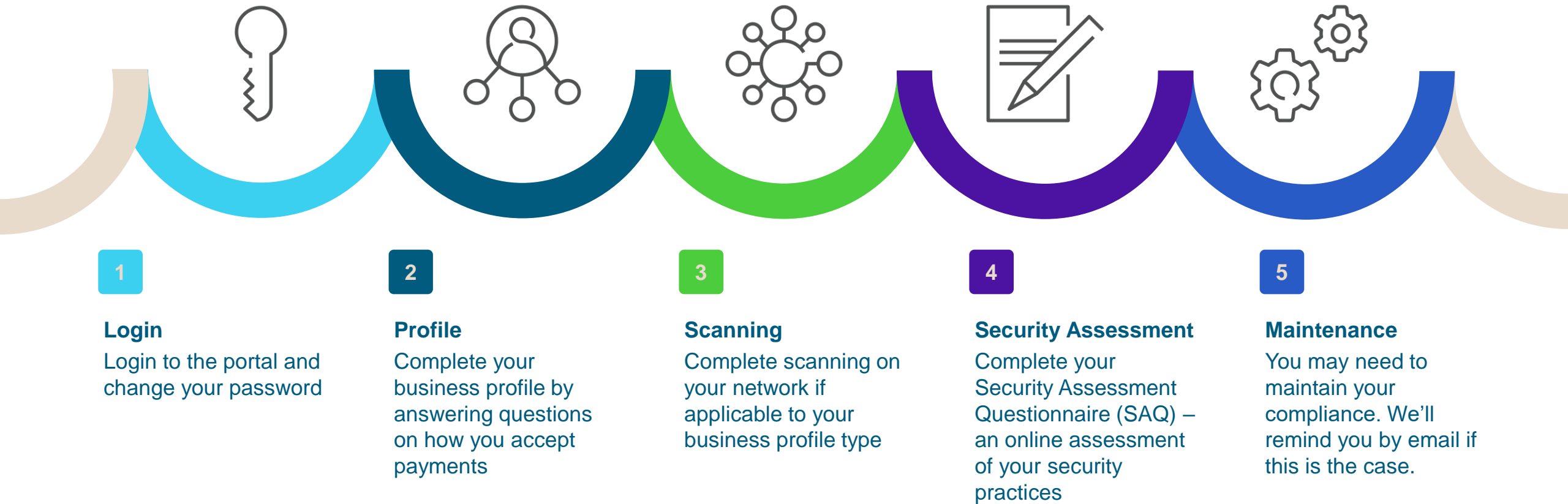
Table of contents

▪ What's included?	3
▪ The process	4
▪ Welcome to the program	5
▪ Login	6
▪ First time user?	7
▪ Your profile	8
– How you accept payments	9
– Information Security Policy	10
– Payment summary	11
▪ Your dashboard	12
▪ Scanning	16
– Finding your IP address	19
▪ Security Assessment Questionnaire (SAQ)	20
▪ You're done for now	27
▪ Maintaining your compliance	28
▪ Upload an existing certificate	30

What's included?

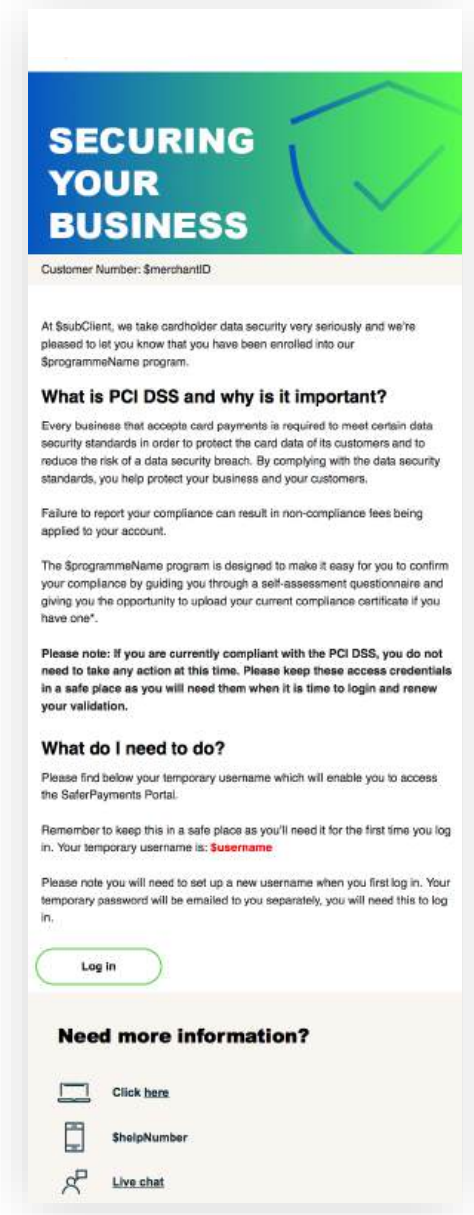
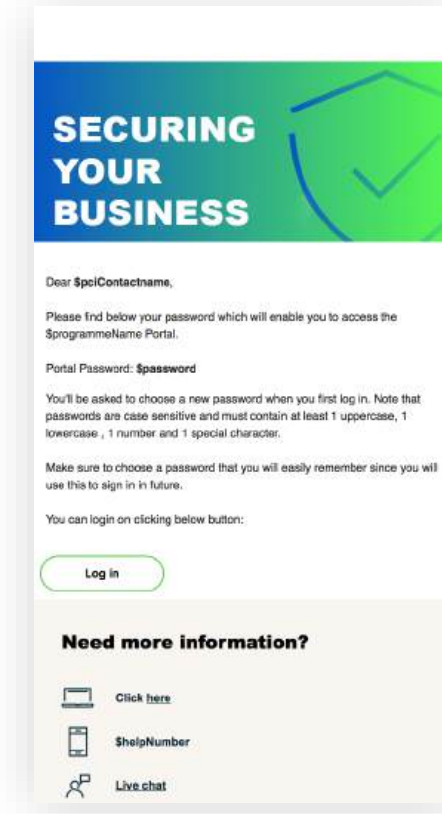
- **Report your PCI DSS Compliance**
 - Streamlined and simplified journey
 - Download your Information Security Policy template
- **Maintain your compliance throughout the year**
 - Login to complete regular scanning and maintenance tasks
- **Receive email alerts and reminders so you always stay up to date**
- **Rich online, chat and phone support available if you get stuck**

The process



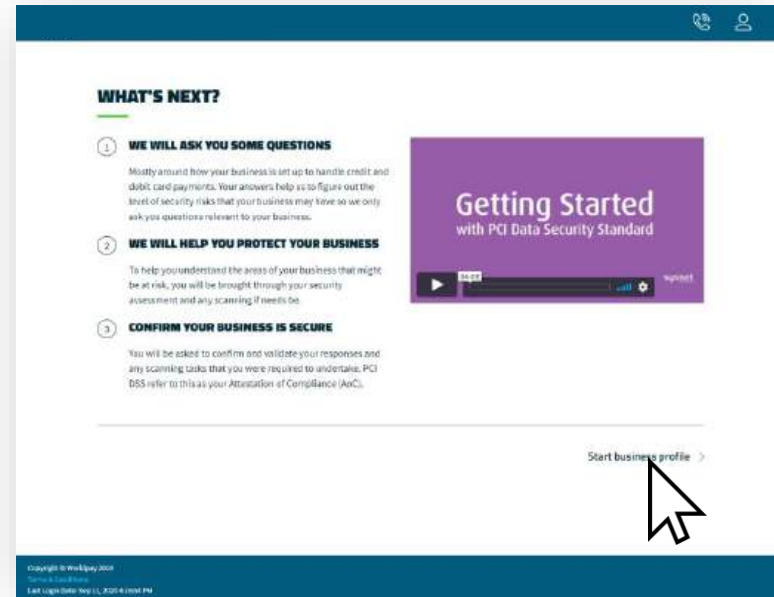
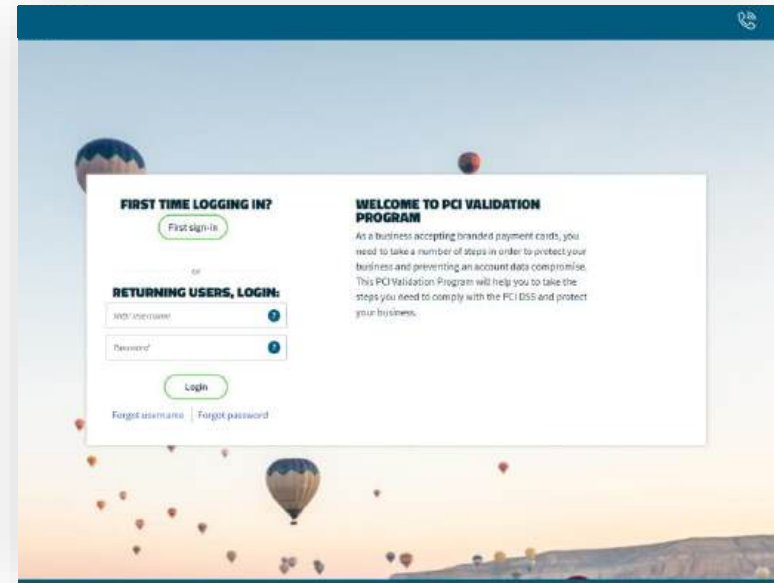
Welcome to the program

- When you have been loaded to the program, you will receive two emails.
 - The first email will be your username
 - The second will be your password
- When you receive these two emails you can use this information to login.
- Click the login link in the email to be brought to your portal.



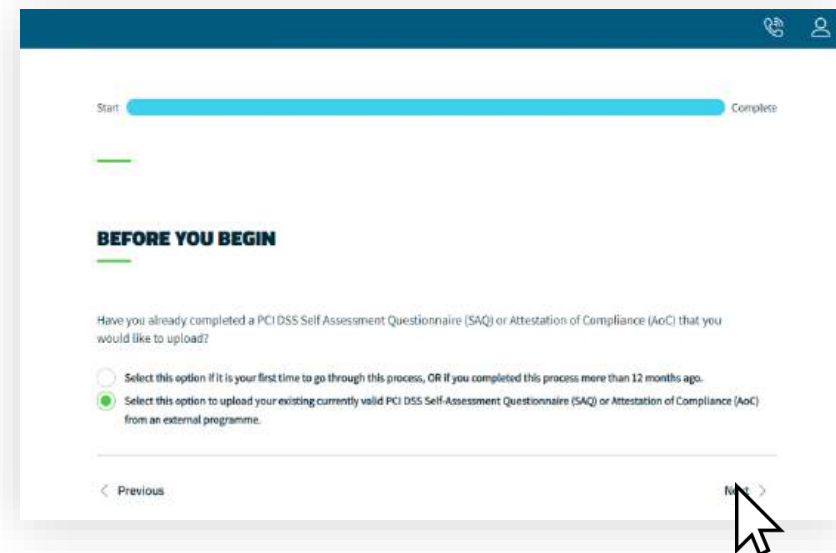
Login

- Upon first logging in to the portal, use the username and password provided in your emails and click **'First sign-in'**.
- You will then be prompted to update your password. Your password will need to meet the minimum-security criteria outlined on the screen.
- Once you have completed this, you will be brought to an information page that gives you an overview of what you need to do and an information video.
- Click **'Start Business Profile'** to begin.



First time use?

- The first screen you will encounter is a question as to whether you have completed this already.
- In some cases, you may have already completed your PCI compliance with an assessment company. If this is the case, select the option and click next.
- If you have previously reported your compliance with one of our partners or a previous portal, your compliance status will have been migrated to our new portal. Meaning you will not be required to complete your profile.

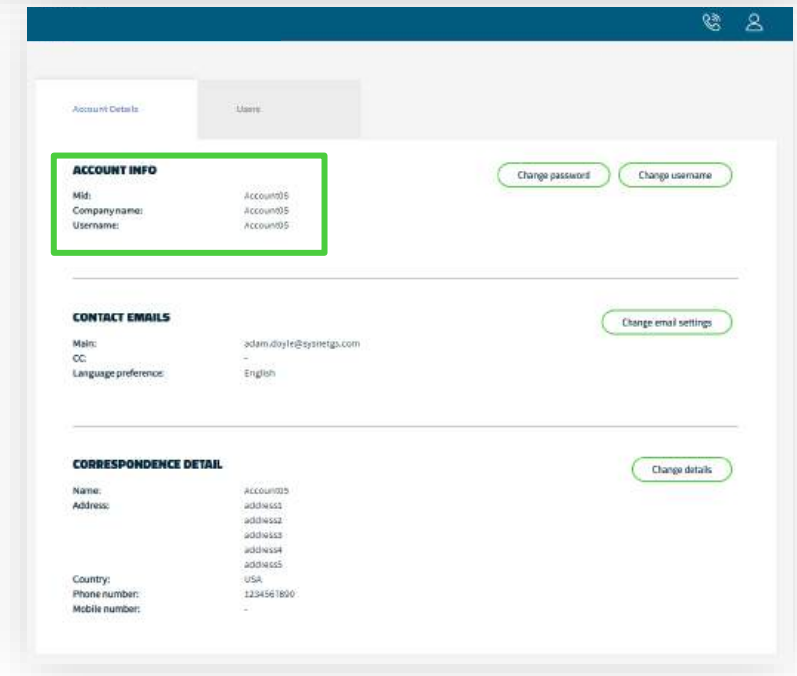
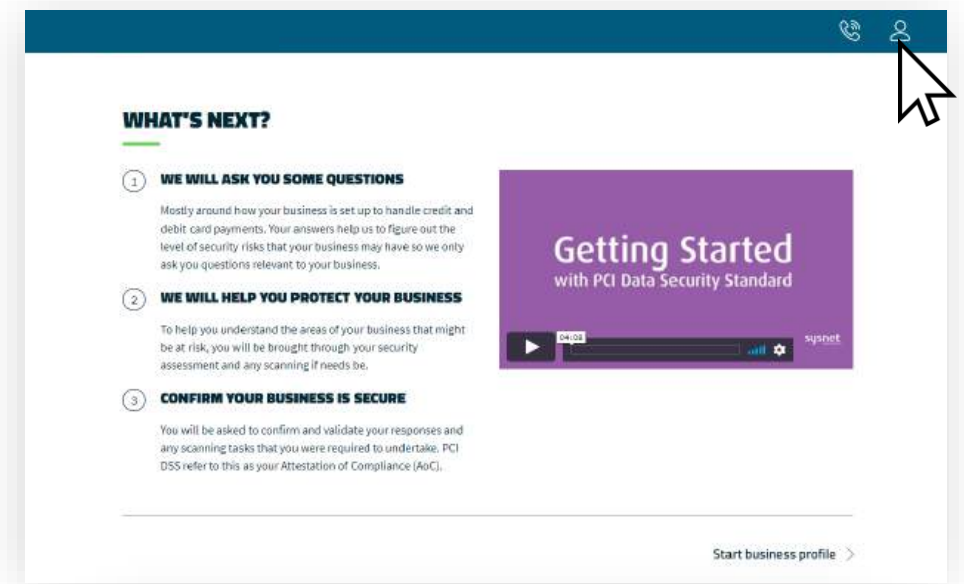


If you do not already have a valid certificate and need to complete your compliance online, select the first option on this screen and continue to page 9 of this guide.

If you already have a valid certificate, select the second option and proceed to page 31 of this guide for instructions on uploading your existing Attestation of Compliance (AoC).

Primary Merchant ID

- You may be asked, or you may need to locate your **“Primary Merchant ID”**
- This can be found by accessing the account menu via the profile icon
- Select the profile icon from the top right of your screen and select **“Account”**
- Your Primary Merchant ID can be found under the **“Account Info”** box on the following screen



How you accept payments

YOUR PROFILE

Profile – How you accept payments

- You will be guided through some questions asking how you accept payments in your business.
- You will be asked questions about the technology you use as well as methods by which you may transfer or store data.
- Select the options that apply to your company and click through via the “**Next**” button. You can select more than one option in many cases.
- If you are unsure about any of the options or need further clarification, more information is available by clicking: ?

The image displays two sequential screenshots of a payment terminal setup wizard interface.

Top Screenshot: HOW YOU ACCEPT CARD PAYMENTS

This screen features a progress bar at the top, labeled 'Start' on the left and 'Complete' on the right. Below the title, a sub-header reads: 'Please select all of the methods that you use to accept card payments in your business.' There are six options, each with a checkbox and an icon:

- ☐ I use a standalone counter-top or portable Point of Sale (POS) payment terminal
- ☐ I use a browser-based Virtual Terminal
- ☐ I use a mobile (smartphone, tablet etc) device to accept face-to-face payments
- ☐ I use an integrated/electronic Point of Sale (POS/wPOS) system (a POS computer system running a payment application that includes an attached or integrated card reader device)
- ☐ I use a payment application that allows my company's employees to manually input card data transactions for processing using a computer (This is not a Virtual Terminal)
- ☐ I use a manual imprint machine and/or paper sales vouchers

At the bottom, there are 'Previous' and 'Next' navigation buttons. A mouse cursor is pointing at the 'Next' button.

Bottom Screenshot: HOW YOUR PAYMENT TERMINAL IS CONNECTED

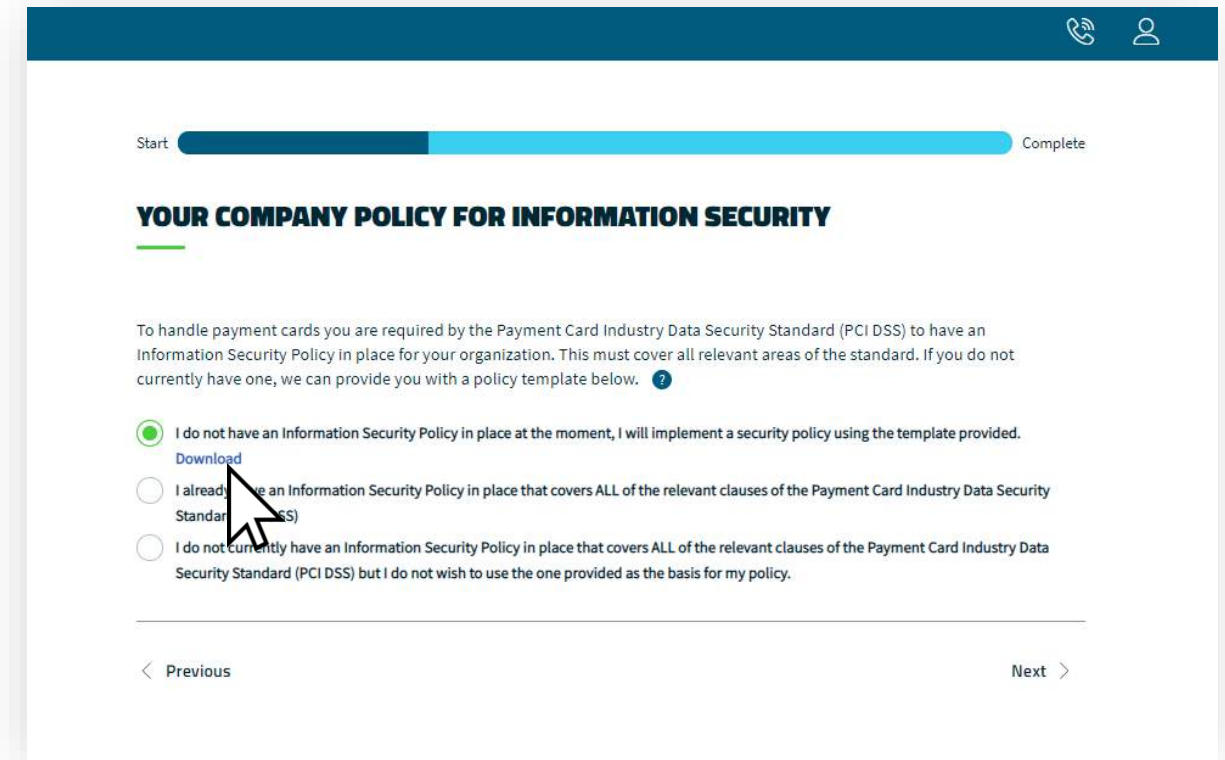
This screen also has a progress bar and a title. A sub-header reads: 'If your terminal is connected by a cable, it is important to determine if this is from a telephone line or through a data cable (Internet), and select the relevant option below.' There are three options, each with a checkbox and an icon:

- ☐ The phone line
- ☐ Mobile network using a SIM card
- ☒ The Internet (e.g. via a Broadband Router)

At the bottom, there are 'Previous' and 'Next' navigation buttons.

Profile – Information Security Policy

- **It's mandatory to apply an Information Security Policy**
 - This is a document that sets out the procedures you need to follow to handle information securely
- **You will be asked if you have a policy in your business. If you don't, you can download a sample template by clicking 'Download'**
- **To correctly implement your policy, you must:**
 - Tailor the sample template to suit your business
 - Ask all staff and third parties who come in contact with your data to read, sign and date it
 - Keep it on your business' premises and keep it up to date if/when your processes change



The screenshot shows a web form titled "YOUR COMPANY POLICY FOR INFORMATION SECURITY". At the top, there is a progress bar from "Start" to "Complete". Below the title, a paragraph explains the PCI DSS requirement for an Information Security Policy. Three radio button options are listed: the first is selected and has a "Download" link; the second is "I already have an Information Security Policy in place that covers ALL of the relevant clauses of the Payment Card Industry Data Security Standard (PCI DSS)"; the third is "I do not currently have an Information Security Policy in place that covers ALL of the relevant clauses of the Payment Card Industry Data Security Standard (PCI DSS) but I do not wish to use the one provided as the basis for my policy." Navigation buttons for "Previous" and "Next" are at the bottom.

Start Complete

YOUR COMPANY POLICY FOR INFORMATION SECURITY

To handle payment cards you are required by the Payment Card Industry Data Security Standard (PCI DSS) to have an Information Security Policy in place for your organization. This must cover all relevant areas of the standard. If you do not currently have one, we can provide you with a policy template below. ?

☒ I do not have an Information Security Policy in place at the moment, I will implement a security policy using the template provided.
[Download](#)

☐ I already have an Information Security Policy in place that covers ALL of the relevant clauses of the Payment Card Industry Data Security Standard (PCI DSS)

☐ I do not currently have an Information Security Policy in place that covers ALL of the relevant clauses of the Payment Card Industry Data Security Standard (PCI DSS) but I do not wish to use the one provided as the basis for my policy.

[< Previous](#) [Next >](#)

Profile – Payment Summary

- You will be asked to provide a summary of your payment acceptance processes.
- You will be asked to:
 - List your business premises and provide a summary of the locations where you accept payments
 - Explain how your business handles cardholder data
 - Provide a high-level description of how you accept payments
- Please provide as much information as possible. If you are stuck, help is available by clicking: ?

The screenshot shows a web interface for a 'Payment Summary' form. At the top, there is a progress bar with 'Start' on the left and 'Complete' on the right. Below the progress bar, the title 'A SUMMARY OF HOW AND WHERE YOU HANDLE CARD PAYMENTS' is displayed in bold. A sub-header reads: 'Please provide the information requested below. This will form part of your Attestation of Compliance.' The first question is: 'List your business premises type(s) and a summary of locations that are relevant to your PCI DSS assessment (eg, retail outlets, corporate offices, data centres, call centres etc.)'. It has a text input field and a character count '0 / 4000'. The second question is: 'How and in what capacity does your business store, process and/or transmit cardholder data?'. It also has a text input field and a character count '0 / 4000'. A mouse cursor is pointing at a question mark icon next to this question. The third question is: 'Provide a high level description of your overall business environment, applicable to your PCI DSS assessment. For example describe the type of equipment you use for card processing, storage and transmission; such as POS devices any databases and web servers, include a description as to how they connect both externally and any internal connections.' It has a text input field and a character count '0 / 4000'. At the bottom, there are 'Previous' and 'Next' navigation buttons.

Profile complete

YOUR DASHBOARD

Your dashboard

See next page for a visual explanation

- **Now that you have answered your profile questions, you will be presented with your dashboard.**
 - From here you can complete your security assessment as well as any other tasks that are assigned to you following your questions (e.g. scanning).
 - Your security assessment will be based on the profile type assigned to you.
 - You can read more information on how this works via the **‘More Info’** button on the **‘Your business profile’** widget.
- **If the scanning widget appears, you must complete a scan by selecting **‘Manage’** from this widget.**
- **If you do not require a scan, or have completed one, you can begin your security assessment by clicking **‘Manage’** on the relevant widget.**

Your dashboard

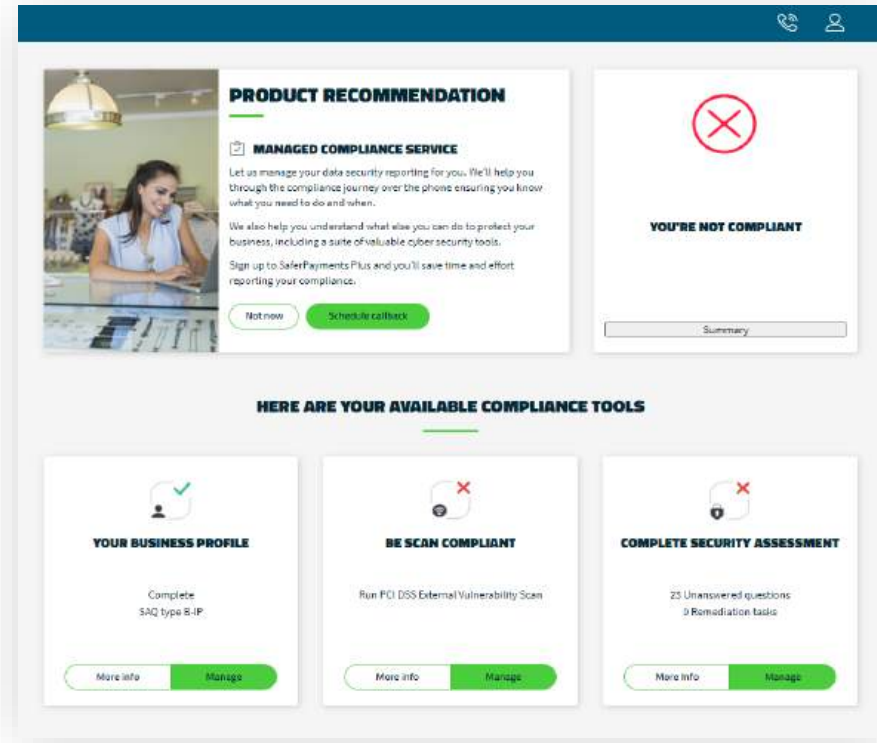
If you have previously reported your compliance with one of our partners or a previous portal, your compliance status will have been migrated to our new portal and your compliance status will be visible on this screen.

1

You will have been assigned a business profile type, based on the answers you provided in your questions. You can read more on what this means by clicking **'More Info'**

2

If applicable, you can conduct your scanning from here. Click **'Manage'** on the scan widget to begin.



3

Your compliance status is listed in the top right. You will not yet be compliant as you won't have completed your scanning (if applicable) or Security Assessment yet

4

When you have completed your scanning (if applicable) you can proceed to your security assessment by clicking **'Manage'**

Next steps

Scanning

If applicable to you, you will need to run a scan on your network. Proceed to page 17 for instructions.

Security Assessment

If don't have to do a scan, you can proceed to your security assessment on page 21.

Profile

Scanning

Security
Assessment

Compliance

Proceed to page 17

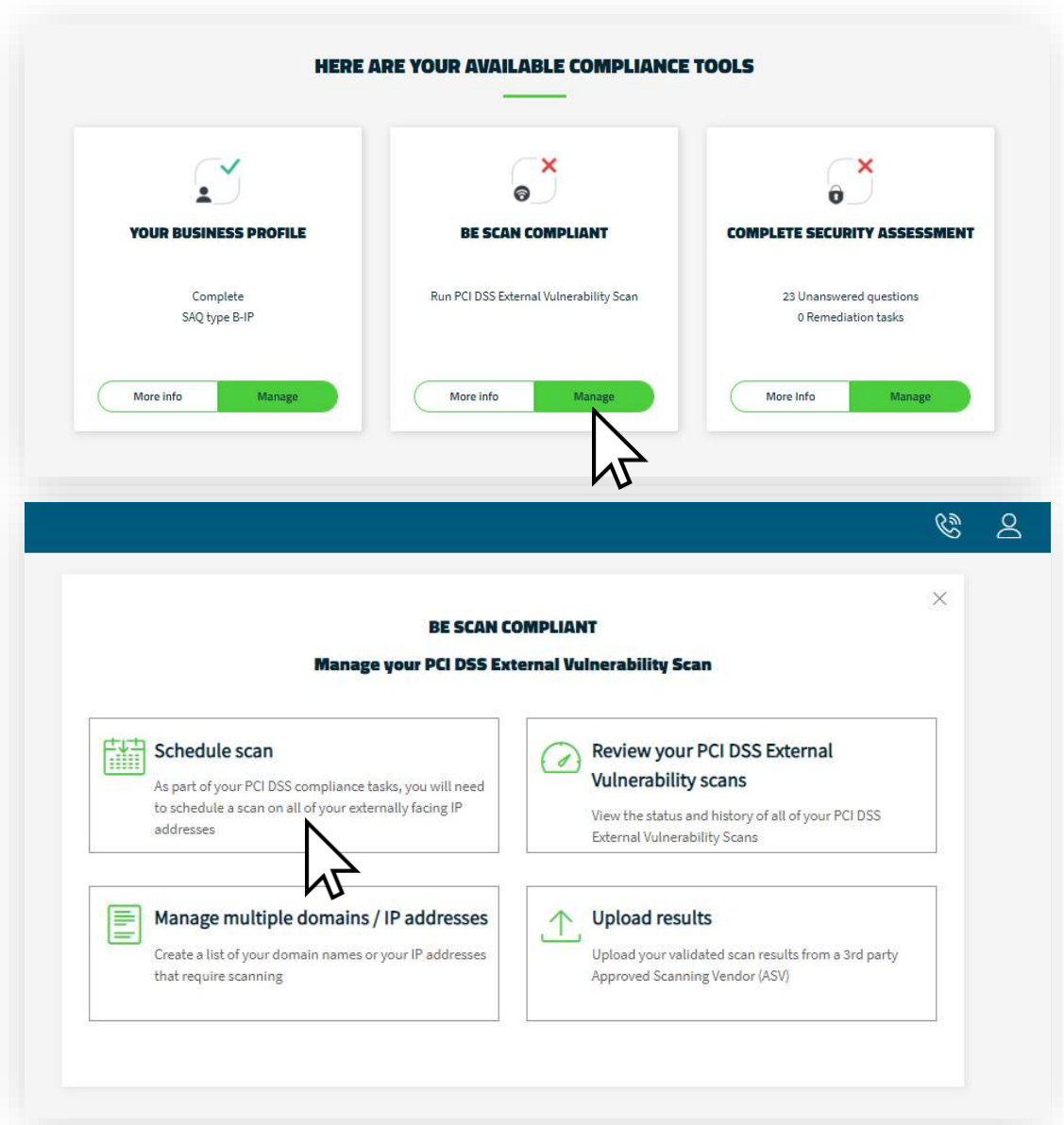
Proceed to page 21

External Vulnerability

SCANNING

Scanning

- From your dashboard, select **'Manage'** on the **'Be scan compliant'** widget.
- On the next page, select **'Schedule scan'**.



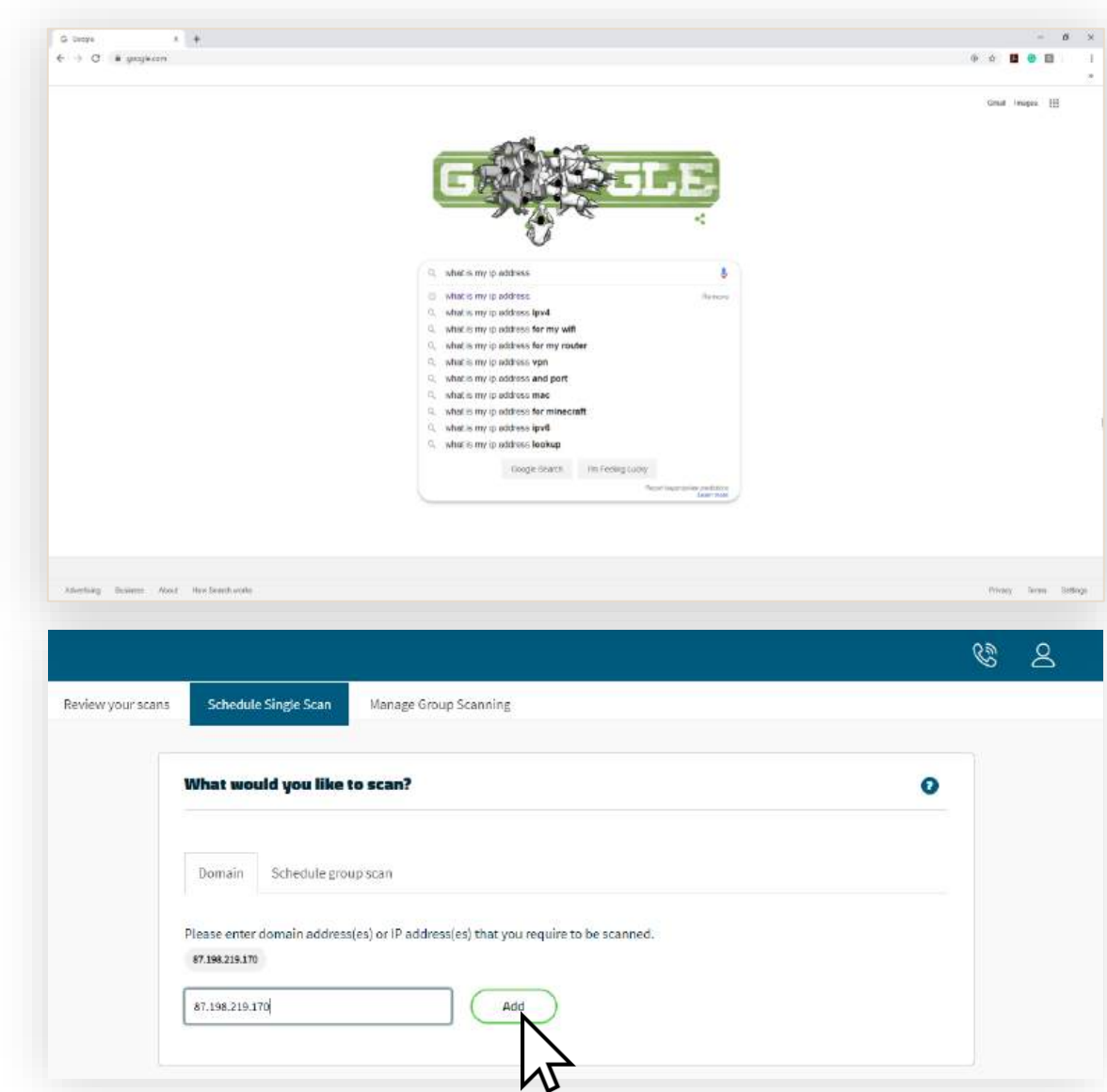
Scanning

- On the next screen you will need to input some details as follows:
 - **The IP address.** This must be the same IP address as used by your card payment machine. More information on locating your IP Address is available on the next page.
 - **Scan date.** It will default to the current date and time. You can change this if necessary.
 - Confirmation of whether you use a **load balancer**
- Once complete, select **'Schedule Scan'**
 - The scan will then run and can take up to 48 hours. You will receive an email when the scan is complete.
 - You will be notified if remediation action is needed via your dashboard.
 - If you scan fails, you will need to complete the recommended remediation and then rerun the scan until a passing grade is achieved

The screenshot displays the 'Schedule Single Scan' interface. At the top, there are three tabs: 'Review your scans', 'Schedule Single Scan' (which is active), and 'Manage Group Scanning'. The main content area includes several sections: 1. 'Scan date' with a text input field and a date/time picker showing 'Sep 14, 2020' and '09:43'. 2. 'Load Balancer?' with a question 'Do you use Load Balancers as a part of your in-scope PCI Infrastructure?' and radio buttons for 'Yes' and 'No' (where 'No' is selected). 3. 'Sysnet access' with explanatory text about granting access to IP addresses and a list of IP addresses: '64.39.96.0/20', '64.39.108.0/24', and '124.28.121.0/24'. 4. A 'WEBSITE DISCLAIMER NOTICE' section with a scrollable text area containing terms and conditions. At the bottom, there is a checkbox for 'I confirm that our domain and IP addresses will grant access to the IP address(es) stated above' and a green 'Schedule Scan' button with a mouse cursor pointing at it.

Finding your IP Address

- To conduct a scan, you will need to provide us with your IP address. This is a series of numbers and dots that is your address on the internet. This helps to ensure the scan runs on the correct network.
- To find your IP address:
 - Connect a laptop, desktop or mobile device to the **same Wi-Fi network** that your card payment machine is connected to
 - Open your preferred search engine or browser and search *“What is my IP address”*
 - You can find your address from the search results
 - **Please note**, it is the IPV4 address that is required, not the IPV6



SAQ

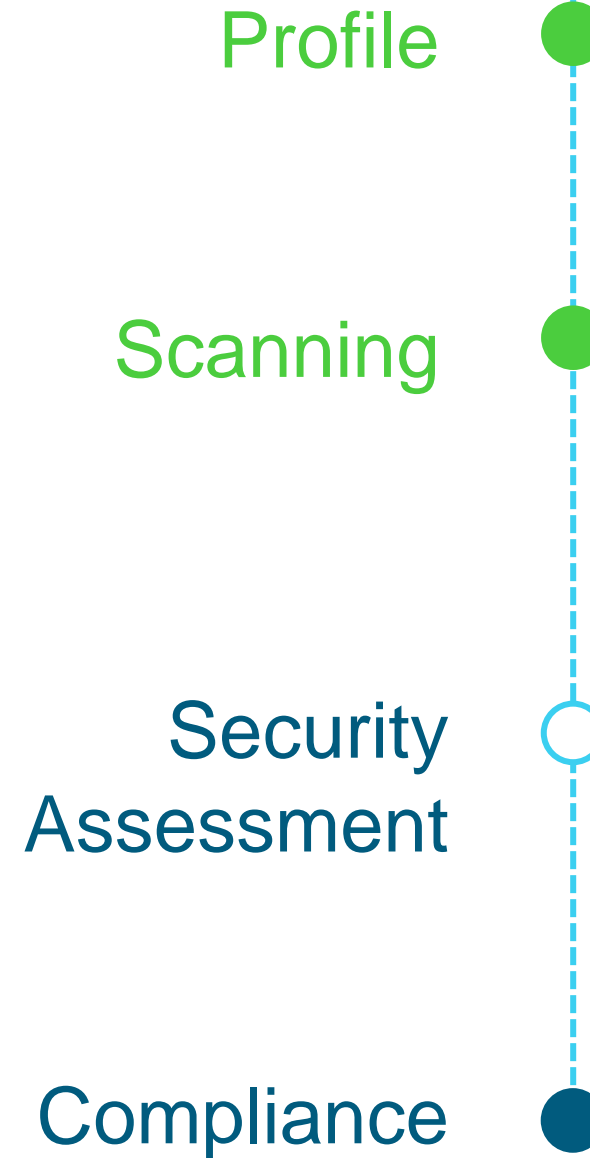
SECURITY ASSESSMENT QUESTIONNAIRE

Next steps

Security Assessment Questionnaire (SAQ)

Your security assessment is an assessment of how you deal with information in your business. Its length and complexity depends on the results of your business profile.

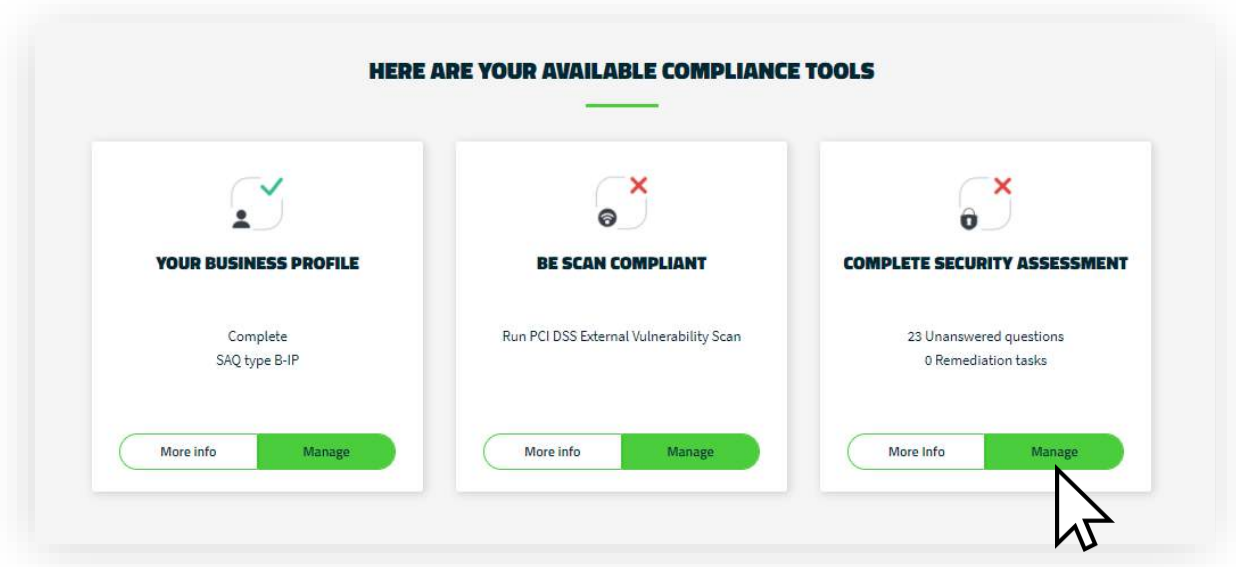
The system will prepopulate any questions that don't apply to you. So you only have to answer those that really matter.



Proceed to next page

Security Assessment Questionnaire (SAQ)

- From your dashboard, select '**Manage**' on the '**Complete security assessment**' widget.
- You will see on your dashboard how many questions you must answer.
 - The amount of questions you must answer depends on the business profile assigned to you and is based on your level of risk.



Security Assessment Questionnaire (SAQ)

1

You will be guided through the questions you need to answer to complete your Security Assessment

2

More information is available via the grey box underneath to help you understand the question

The screenshot shows the SAQ interface with a dark blue header containing a help icon and a user profile icon. Below the header, there's a filter section with a dropdown menu set to 'Only unanswered questions' and a toggle for 'Show Help Text' which is turned on. A note states: 'Please note, some answered questions may remain shown in order to provide appropriate context status'. The main content area is titled 'BUILD AND MAINTAIN A SECURE NETWORK AND SYSTEMS' with a green progress bar. The question is '1.1.2(a) Is there a current network diagram that documents all connections between the cardholder data environment and other networks, including any wireless networks?'. At the bottom of the question are three buttons: 'N/A', 'No', and 'Yes'. To the right of the question is a sidebar with a 'Sections' tab and a 'Milestones' tab. The 'Sections' list includes: 8 Build and Maintain a Secure Network and Systems, 9 Protect Cardholder Data, 1 Maintain a Vulnerability Management Program, 2 Implement Strong Access Control Measures, 3 Regularly Monitor and Test Networks, a checked item 'Maintain an Information Security Policy', and an unchecked item 'Confirm your compliance'. At the bottom of the main content area is an 'INFORMATION' box titled 'PCI COUNCIL GUIDELINES' which explains the importance of network diagrams for PCI DSS compliance.

Show me: Only unanswered questions Show Help Text: ☒

Please note, some answered questions may remain shown in order to provide appropriate context status

BUILD AND MAINTAIN A SECURE NETWORK AND SYSTEMS

Install and maintain a firewall configuration to protect cardholder data

1.1.2(a)

Is there a current network diagram that documents all connections between the cardholder data environment and other networks, including any wireless networks?

N/A No Yes

INFORMATION
PCI COUNCIL GUIDELINES

Network diagrams describe how networks are configured, and identify the location of all network devices.

Without current network diagrams, devices could be overlooked and be unknowingly left out of the security controls implemented for PCI DSS and thus be vulnerable to compromise.

PCI AUDIT PROCEDURES

Sections **Milestones**

- 8 Build and Maintain a Secure Network and Systems
- 9 Protect Cardholder Data
- 1 Maintain a Vulnerability Management Program
- 2 Implement Strong Access Control Measures
- 3 Regularly Monitor and Test Networks
- ✓ Maintain an Information Security Policy
- ✗ Confirm your compliance

3

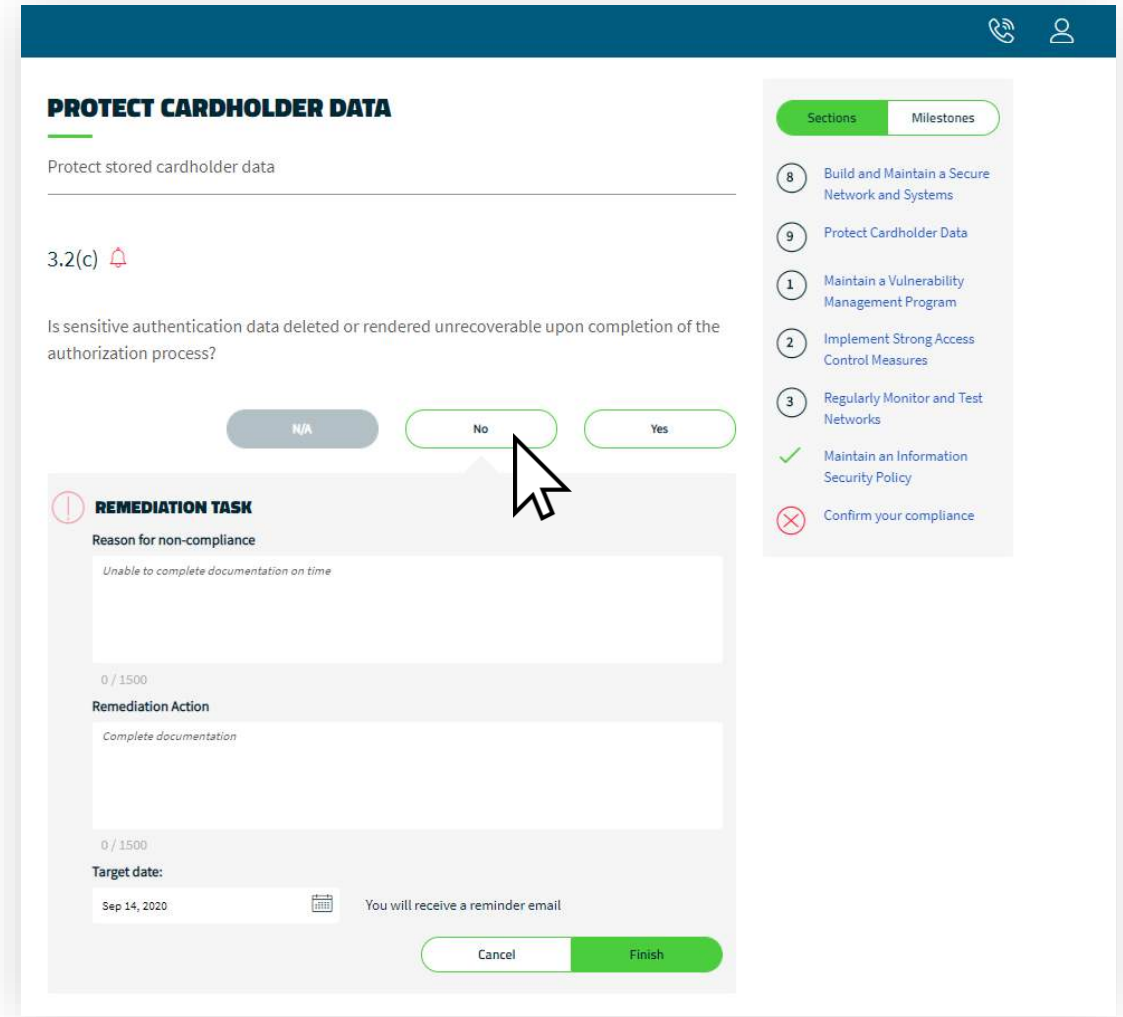
The box on the top right shows your progress through the questionnaire. Many of the questions will have been prepopulated for you based on your answers in the profile section. This greatly streamlines the process.

4

Work your way through the questionnaire by answering "Yes", "No" or "N/A" to the questions

Security Assessment Questionnaire (SAQ)

- If an answer you provide is against best practice or what is correct, you may need to further explain your answer or assign yourself a remediation task.
 - You must then fill out your reasons for non-compliance, the remediation action you intend to take and can then set a reminder to yourself to follow up.
- You can continue with your assessment questions. However, until these tasks are completed correctly you may not be able to complete your assessment.



The screenshot displays the 'PROTECT CARDHOLDER DATA' section of the SAQ. The main question is '3.2(c) Is sensitive authentication data deleted or rendered unrecoverable upon completion of the authorization process?'. Three buttons are visible: 'N/A', 'No', and 'Yes'. A mouse cursor is pointing at the 'No' button. Below the question, a 'REMEDIATION TASK' modal is open, showing a text area for 'Reason for non-compliance' with the placeholder text 'Unable to complete documentation on time', a text area for 'Remediation Action' with the placeholder text 'Complete documentation', and a 'Target date' field set to 'Sep 14, 2020'. At the bottom of the modal are 'Cancel' and 'Finish' buttons. On the right side, a sidebar shows a list of sections and milestones, with 'Protect Cardholder Data' highlighted.

PROTECT CARDHOLDER DATA

Protect stored cardholder data

3.2(c) Is sensitive authentication data deleted or rendered unrecoverable upon completion of the authorization process?

N/A No Yes

REMEDIATION TASK

Reason for non-compliance

Unable to complete documentation on time

0 / 1500

Remediation Action

Complete documentation

0 / 1500

Target date:

Sep 14, 2020 You will receive a reminder email

Cancel Finish

Sections Milestones

- 8 Build and Maintain a Secure Network and Systems
- 9 Protect Cardholder Data
- 1 Maintain a Vulnerability Management Program
- 2 Implement Strong Access Control Measures
- 3 Regularly Monitor and Test Networks
- ✓ Maintain an Information Security Policy
- ✗ Confirm your compliance

Security Assessment Questionnaire (SAQ)

- Once you have answered all your questions correctly, you will need to *attest to your compliance*. This simply means to confirm the information you have provided is correct.
- You can review all the answers you provided to the questions here.
- Once happy, select '**Confirm your Attestation**' at the bottom of the screen.

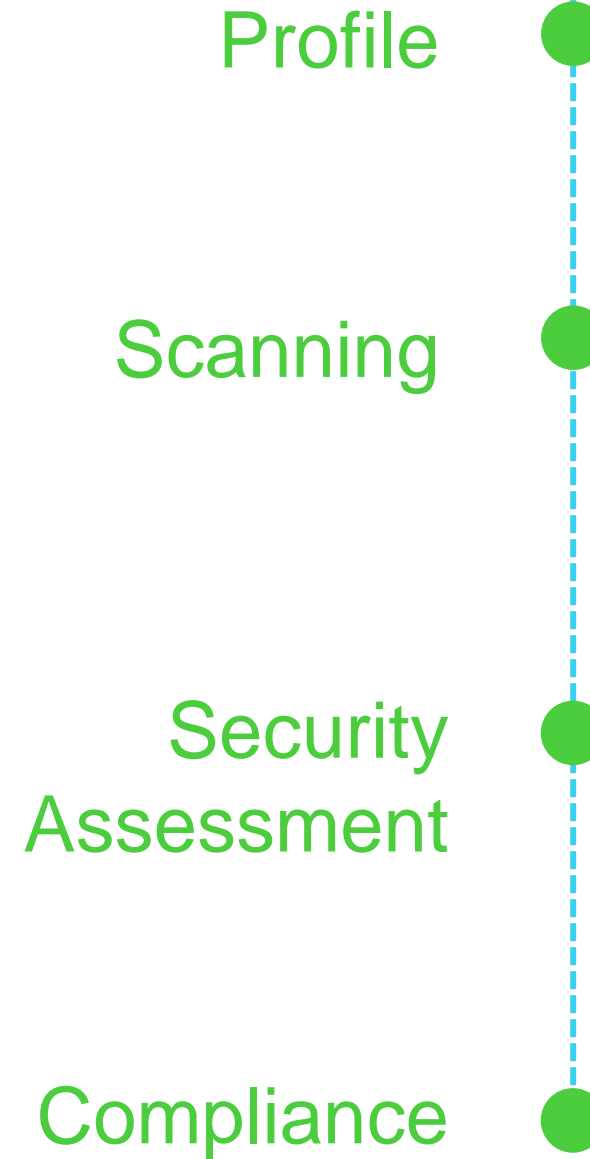
The screenshot shows the 'CONFIRM YOUR COMPLIANCE' section of the Security Assessment Questionnaire (SAQ) interface. The header is blue with a phone icon and a user profile icon. Below the header, the title 'CONFIRM YOUR COMPLIANCE' is in bold. A sub-header reads: 'Please review the form below and ensure all sections are correct and complete'. The main content area lists several sections, each with a green checkmark icon and a right-pointing arrow: 'Your organisation information details', 'Type of business', 'Description of environment', 'Eligibility to complete SAQ B', and 'Acknowledgement of status and attestation'. Below these is a section with a red 'X' icon and a downward arrow, labeled 'Attestation'. To the right of the main content is a sidebar with two tabs: 'Sections' (active) and 'Milestones'. Under 'Sections', there are four items: 'Protect Cardholder Data' (green checkmark), 'Implement Strong Access Control Measures' (green checkmark), 'Maintain an Information Security Policy' (green checkmark), and 'Confirm your compliance' (red 'X'). At the bottom of the main content area is a section titled 'INFORMATION FOR SUBMISSION.' with a checkmark icon. It contains two paragraphs of text: 'Based on the results noted in the SAQ B dated Sep 14, 2020, the signatories identified in Parts 1.1, assert(s) the following compliance status for the entity identified in Part 2 of this document as of Sep 14, 2020:' and 'Compliant: All sections of the PCI DSS SAQ are complete, all questions answered affirmatively, resulting in an overall COMPLIANT rating; thereby AccountDS has demonstrated full compliance with the PCI DSS.' At the bottom right of the screen is a green button labeled 'Confirm your Attestation' with a checkmark icon. A mouse cursor is pointing at the button.

Next steps

You've validated your compliance.

Your validation must be renewed annually. Your renewal date will be shown on your dashboard.

We will email you to remind you when it's time to revalidate.

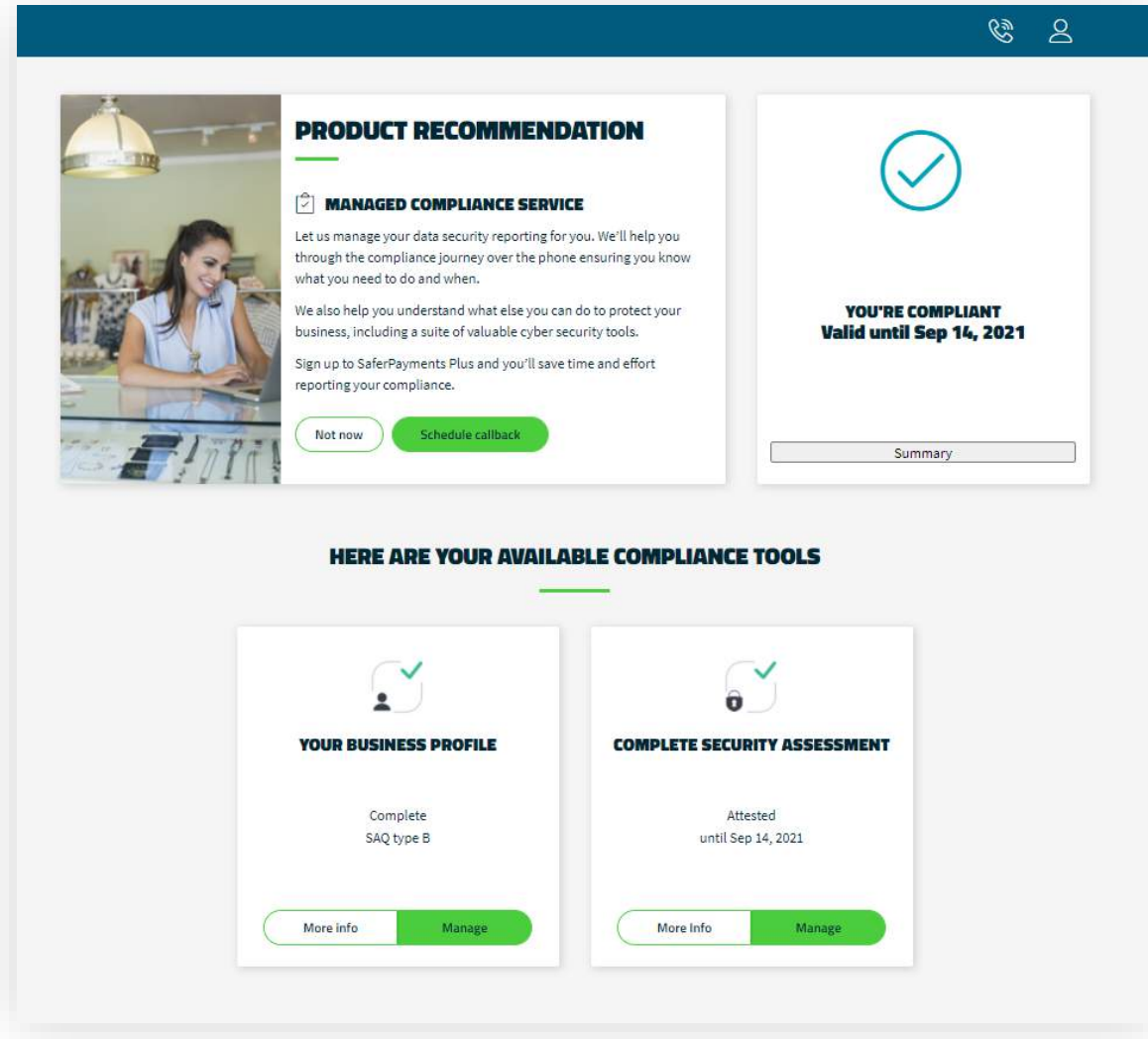


Proceed to put your feet up

You're done for now

1

Your dashboard should have green ticks across the board



2

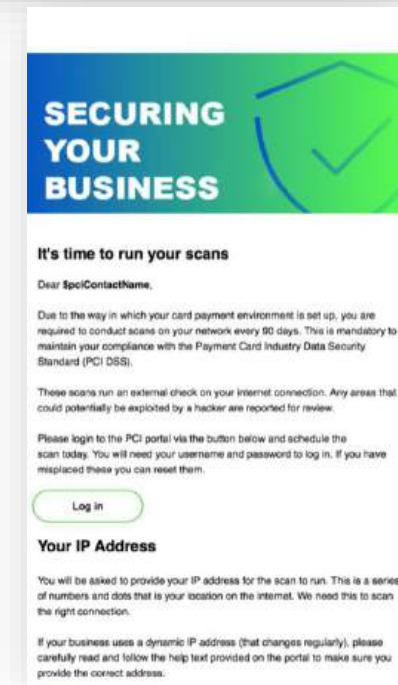
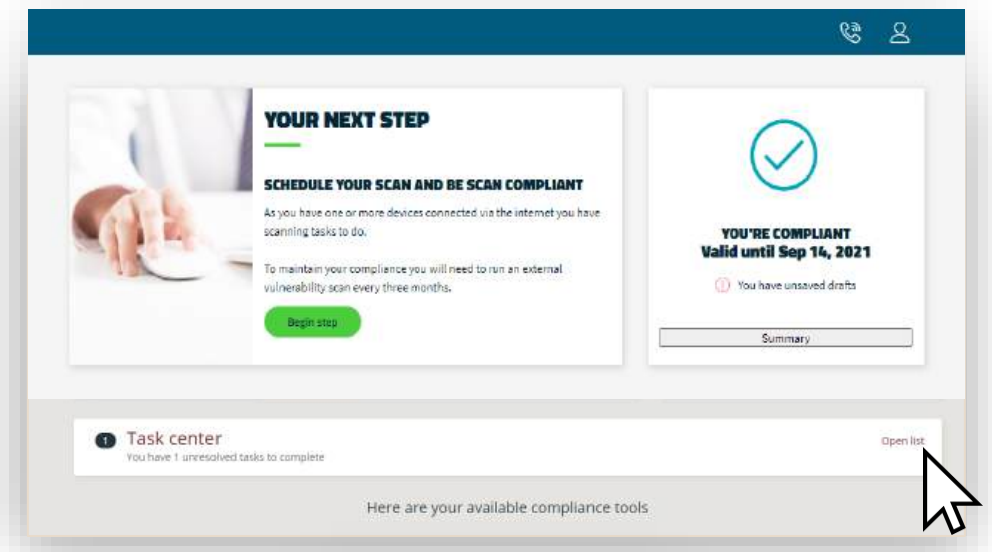
Your revalidation date is displayed in the top right corner

Throughout the year

MAINTAINING COMPLIANCE

Maintaining your compliance

- It's important to maintain your compliance throughout the year by:
 - Making sure you do all of the things you said you did in your assessment
 - Applying your Information Security Policy and keeping it up to date
- Depending on your business profile, you may have to conduct tasks, such as scanning throughout the year. You'll need to perform these tasks on the portal.
- You'll receive emails to remind you, if applicable.
- If you receive an email, login to your portal. What you need to do will be outlined on your dashboard under '**Task Center**'.



Already have a valid Attestation of Compliance?

UPLOADING AN EXISTING ATTESTATION

Uploading existing Attestation of Compliance

- If you select that you have an existing attestation of compliance, you will then be asked two questions:
 - The PCI Compliance assessment type of your business. You can find this on your existing certificate.
 - You'll also need to confirm if you use a third party to store or process card payments.
- You'll then arrive at your dashboard. The main widget will instruct you to confirm your compliance.
 - Select **'Begin Step'** to start.

The screenshot displays a web interface for PCI compliance. At the top, a progress bar shows 'Start' and 'Complete' points. Below it, the section 'YOUR CURRENT VALID PCI COMPLIANCE TYPE' asks the user to select an assessment type from a list of radio buttons: Self Assessment Questionnaire (SAQ) A, SAQ P2PE, SAQ B, SAQ C-VT, SAQ B-IP, SAQ A-EP, SAQ C, and SAQ D. Navigation links for 'Previous' and 'Next' are at the bottom of this section.

The main dashboard area is titled 'YOUR NEXT STEP' and contains a 'CONFIRM YOU'RE COMPLIANT' section. This section includes a message: 'You have indicated that you are compliant. Please upload your currently valid Attestation of Compliance.' and a green 'Begin Step' button, which is being pointed to by a mouse cursor. To the right of this is a 'YOU'RE NOT COMPLIANT' section with a red 'X' icon and a 'Summary' button.

Below these sections is a heading 'HERE ARE YOUR AVAILABLE COMPLIANCE TOOLS'. It features two main widgets: 'YOUR BUSINESS PROFILE' and 'ATTESTATION'. The 'YOUR BUSINESS PROFILE' widget shows 'Complete SAQ type B' and has 'More info' and 'Manage' buttons. The 'ATTESTATION' widget shows 'No documents uploaded' and has 'Attest' and 'View history' buttons.

Uploading existing Attestation of Compliance

- On the following page you will need to complete two steps
 - Upload your existing documents.
 - You will need to upload your Attestation of Compliance (AoC) that proves you are currently compliant. This is the certificate your third-party company should have provided you when you achieved compliance.
 - Confirm the details, acknowledge your status and attest to your compliance.

Instructions on the following pages.

ATTESTATION OF COMPLIANCE

ATTESTATION REQUIREMENTS
In order to proceed to attestation, you are required to upload at least one Attestation of Compliance document.

Please **Select** or **Upload** documents.

Eligibility to complete SAQ B

Merchant certifies eligibility to complete this shortened version of the Self-Assessment Questionnaire because:

- ✓ Merchant uses only an imprint machine to imprint customers' payment card information and does not transmit cardholder data either over a phone; and/or
- ✓ Merchant uses only standalone, dial-out terminals (connected via a phone line to your processor); and the standalone, dial-out terminals are not connected to the Internet or any other systems within the merchant environment;
- ✓ Merchant does not transmit cardholder data over a network (either an internal network or the Internet);
- ✓ Merchant does not store cardholder data in electronic format; and
- ✓ If Merchant does store cardholder data, such data is only paper reports or copies of paper receipts and is not received electronically

Attestation details:

Assessment type: B
Validation effective date:
PCI DSS Version:

Acknowledgement of status and attestation

- ☐ PCI DSS Self-Assessment Questionnaire SAQ B, Version 3.2.1 has been completed according to the instructions therein.
- ☐ All information within the above-referenced SAQ and in this attestation fairly represents the results of my assessment in all material respects.
- ☐ I have confirmed with my payment application vendor that my payment system does not store sensitive authentication data after authorization.
- ☐ I have read the PCI DSS and I recognize that I must maintain PCI DSS compliance, as applicable to my environment, at all times.
- ☐ If my environment changes, I recognize I must reassess my environment and implement any additional PCI DSS requirements that apply.
- ☐ No evidence of full track data, CAV2, CVC2, CID, or CVV2 data, or PIN data storage after transaction authorization was found on ANY system reviewed during the assessment.

Attest

Uploading existing Attestation of Compliance

The image shows a three-step process for uploading an existing Attestation of Compliance document. Step 1, 'ATTESTATION REQUIREMENTS', informs the user that at least one document must be uploaded and provides 'Select' and 'Upload' buttons. Step 2, 'PLEASE SELECT A FILE TO UPLOAD', shows a file selection interface with a 'Select File' button and a mouse cursor. Step 3, 'SELECTED 1/5 FILES TO UPLOAD', displays a detailed form for the selected file '1. DONEBEFORE1.PNG'. This form includes fields for 'Document Type' (Attestation Of Compliance), 'Document Date' (Sep 11, 2020), and a text area for 'Additional information'. At the bottom, there are dropdown menus for 'PCI DSS Version' (3.2.1), 'Status' (Compliant), and 'Completion' (Completed), followed by an 'Upload' button and a mouse cursor.

1 ATTESTATION REQUIREMENTS
In order to proceed to attestation, you are required to upload at least one Attestation of Compliance document

Please **Select** or **Upload** documents

2 PLEASE SELECT A FILE TO UPLOAD
*Accepted file types: pdf, jpg, doc, docx, rtf, png, xlsx. File size limit: 100 MB

3 SELECTED 1/5 FILES TO UPLOAD
*Accepted file types: pdf, jpg, doc, docx, rtf, png, xlsx. File size limit: 100 MB

1. DONEBEFORE1.PNG

Document Type: Attestation Of Compliance
Document Date: Sep 11, 2020

Additional information
Enter your text here

0 / 1500

PCI DSS Version: 3.2.1
Status: Compliant
Completion: Completed

Upload

■ Upload your documents

- Select **Upload**
- Select the necessary document(s) from your files
- Provide details of the document you are uploading and select **Upload**

Uploading existing Attestation of Compliance

- **Select from your uploaded documents to attach to the attestation**
 - Click **Select** from the main screen.
 - From the list of uploaded documents, select the ones you wish to attach to this attestation. Click **Add**.
 - The documents you wish to include will now appear on the main screen.

1

ATTESTATION REQUIREMENTS

In order to proceed to attestation, you are required to upload at least one Attestation of Compliance document

Please **Select** or **Upload** documents

2

<input type="checkbox"/>	Document Name	Document Type	Date uploaded	Document Date	Verification status
<input checked="" type="checkbox"/>	Example SAQ Document.pdf	Attestation Of Compliance	Sep 11, 2020	Sep 11, 2020	Not reviewed

Items: 1 / 1

Cancel **Add**

3

ATTESTATION OF COMPLIANCE

ATTESTATION REQUIREMENTS

In order to proceed to attestation, you are required to upload at least one Attestation of Compliance document

Please **Select** or **Upload** documents

FILES TO BE INCLUDED IN ATTESTATION FORM:

Document Name	Document Type	Date uploaded	Document Date	
Example SAQ Document.pdf	Attestation Of Compliance	Sep 11, 2020	Sep 11, 2020	X

Items: 1 / 1

Uploading existing Attestation of Compliance

- **Confirm details of your attestation, including:**
 - Assessment type.
 - Validation effective date.
 - The version of the PCI DSS to which you are compliant with.
- **Confirm by checking the boxes, that you acknowledge a number of conditions in relation to your status and attestation.**
- **Click ‘*Attest*’ to finish. Your validation is now complete.**
- **See page 29 for details on *Maintaining your Compliance***

The screenshot shows the 'Eligibility to complete SAQ B' section of the PCI DSS Self-Assessment Questionnaire. It includes a list of conditions that the merchant certifies eligibility to complete. Below this, there are three numbered steps: 1. Attestation details, 2. Acknowledgement of status and attestation, and 3. Attest. Step 1 includes fields for Assessment type (B), Validation effective date, and PCI DSS Version. Step 2 includes a list of conditions that the merchant acknowledges, each with a checkbox. Step 3 is a green button labeled 'Attest'.

Eligibility to complete SAQ B

Merchant certifies eligibility to complete this shortened version of the Self-Assessment Questionnaire because:

- ✓ Merchant uses only an imprint machine to imprint customers' payment card information and does not transmit cardholder data either over a phone; and/or
- ✓ Merchant uses only standalone, dial-out terminals (connected via a phone line to your processor); and the standalone, dial-out terminals are not connected to the Internet or any other systems within the merchant environment;
- ✓ Merchant does not transmit cardholder data over a network (either an internal network or the Internet);
- ✓ Merchant does not store cardholder data in electronic format; and
- ✓ If Merchant does store cardholder data, such data is only paper reports or copies of paper receipts and is not received electronically

1 Attestation details:

Assessment type: B
Validation effective date:
PCI DSS Version:

2 Acknowledgement of status and attestation

- ☐ PCI DSS Self-Assessment Questionnaire SAQ B, Version 3.2.1 has been completed according to the instructions therein.
- ☐ All information within the above-referenced SAQ and in this attestation fairly represents the results of my assessment in all material respects.
- ☐ I have confirmed with my payment application vendor that my payment system does not store sensitive authentication data after authorisation.
- ☐ I have read the PCI DSS and I recognize that I must maintain PCI DSS compliance, as applicable to my environment, at all times.
- ☐ If my environment changes, I recognize I must reassess my environment and implement any additional PCI DSS requirements that apply.
- ☐ No evidence of full track data, CAV2, CVC2, CID, or CWV2 data, or PIN data storage after transaction authorization was found on ANY system reviewed during the assessment.

3 Attest

SAFERPAYMENTS PROGRAM