



# PCI OVERVIEW

---

Your Guide To PCI Compliance



# 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
- Uploading An Existing Certificate ..... 30

# What's Included?

- **Report your PCI DSS Compliance**

- Streamlined and simplified journey
- Download your information Security Policy Template

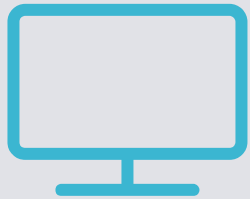
- **Maintain your compliance throughout the year**

- 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



1

## Login

Login to the portal and change your password



2

## Profile

Complete your business profile by answering questions on how you accept payments



3

## Scanning

Complete scanning on your network if applicable to your business profile type



4

## Security Assessment

Complete your Security Assessment Questionnaire (SAQ) - an online assessment of your security practices



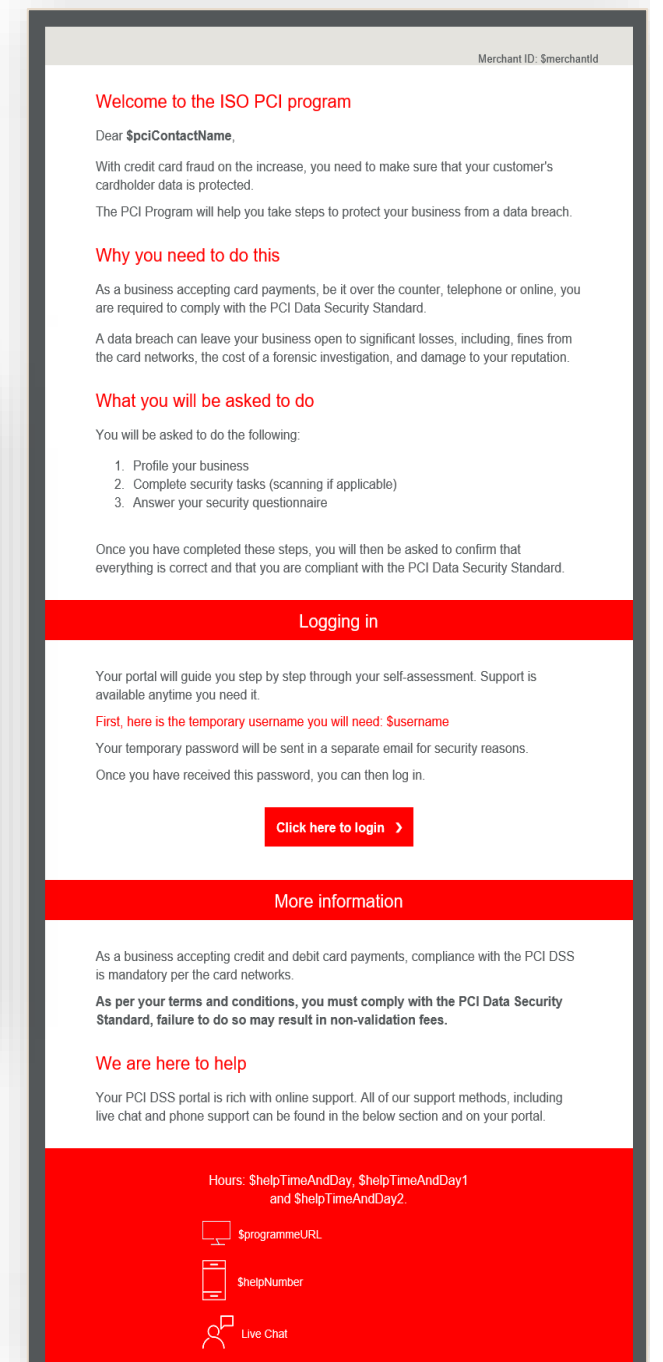
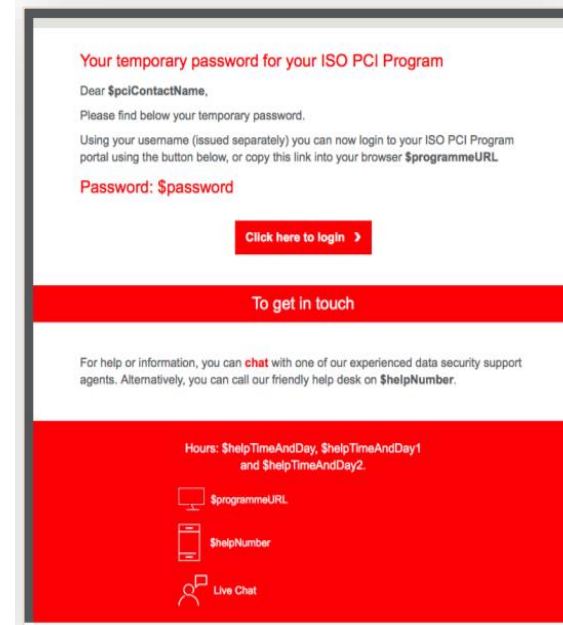
5

## Maintenance

You may need to maintain your compliance. We'll remind you by email if this is the case

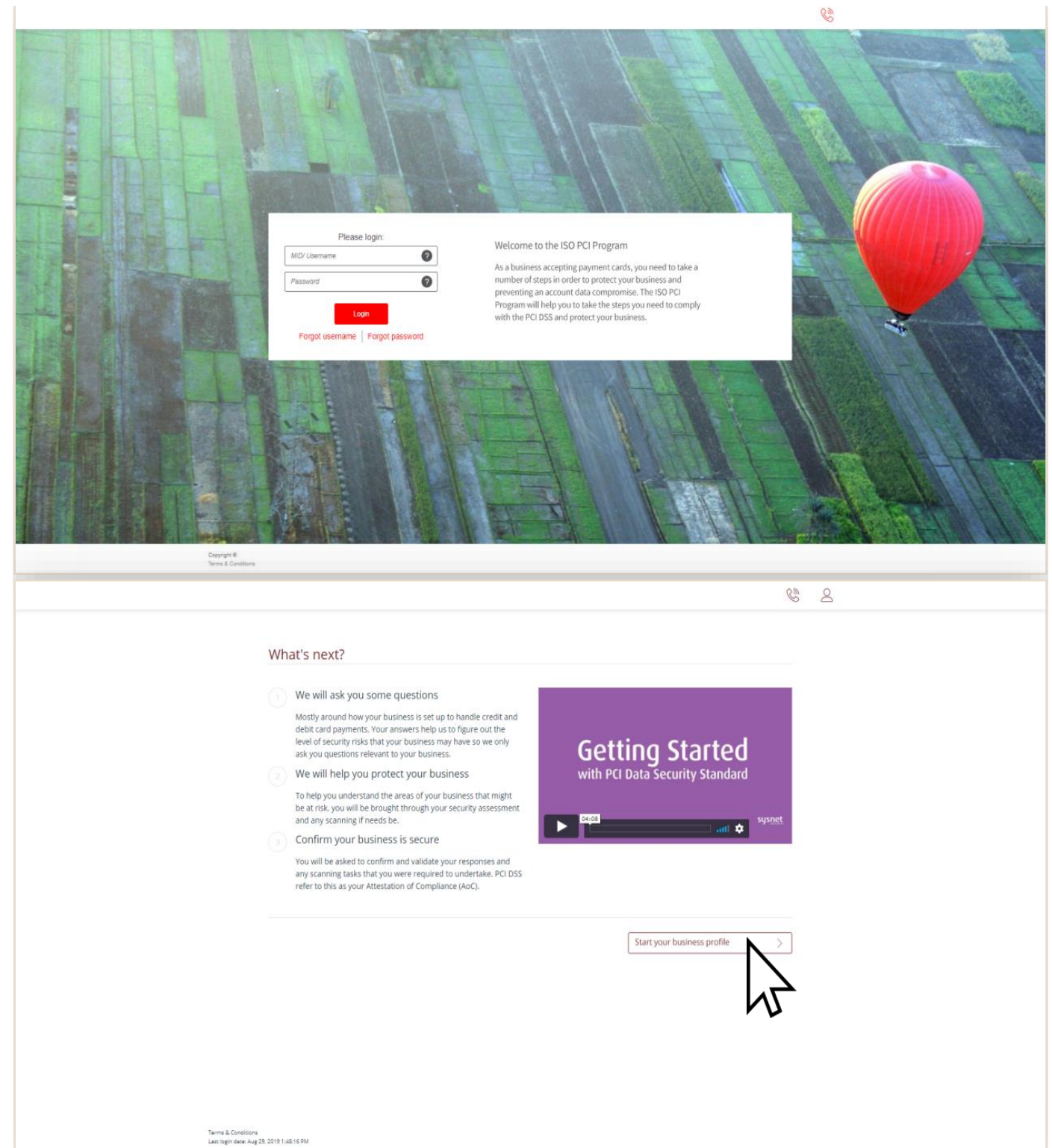
# Welcome To The Program

- **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

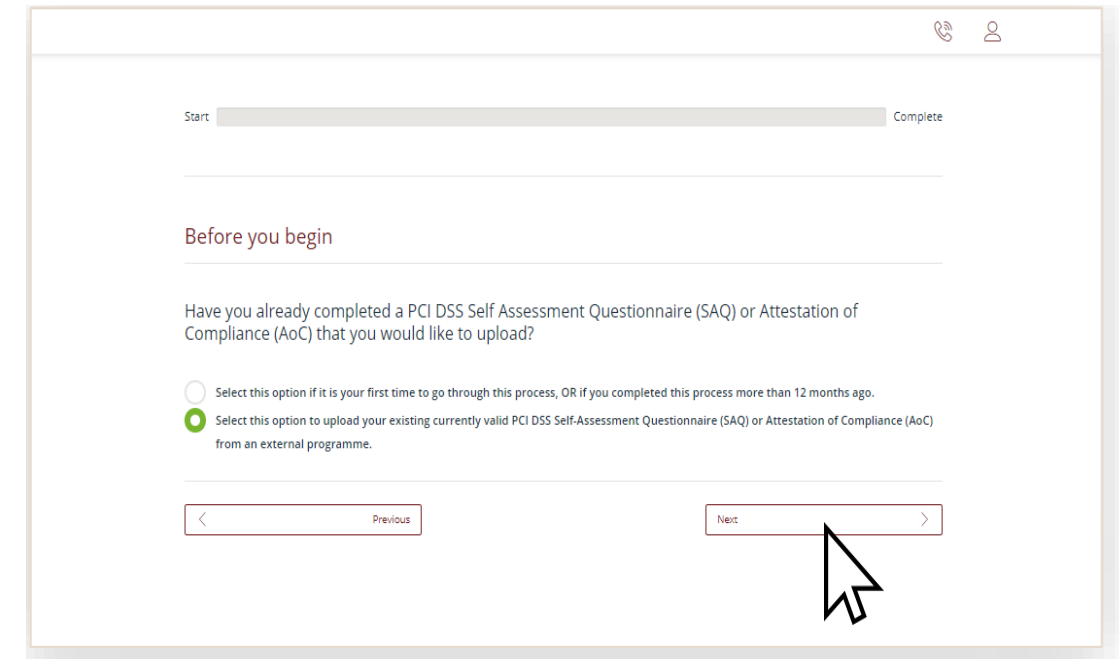
- Upon first logging in to the portal, use the username and password provided in your emails and click **'Login'**.
- You will then be prompted to update your password. Your password will need to meet the minimum-security criteria outlined on the screen
- Once you have completed this, you will be brought 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 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 8 of this guide.



The screenshot shows a web interface for PCI compliance setup. At the top, there is a progress bar from 'Start' to 'Complete'. Below this, the heading 'Before you begin' is followed by the question: 'Have you already completed a PCI DSS Self Assessment Questionnaire (SAQ) or Attestation of Compliance (AoC) that you would like to upload?'. There are two radio button options: the first is unselected and says 'Select this option if it is your first time to go through this process, OR if you completed this process more than 12 months ago.'; the second is selected (indicated by a green dot) and says 'Select this option to upload your existing currently valid PCI DSS Self-Assessment Questionnaire (SAQ) or Attestation of Compliance (AoC) from an external programme.' At the bottom, there are 'Previous' and 'Next' buttons. A mouse cursor is pointing at the 'Next' button.

If you already have a valid certificate, select the second option and proceed to page 30 of this guide for instructions on uploading your existing Attestation of Compliance (AoC)


How you accept payments

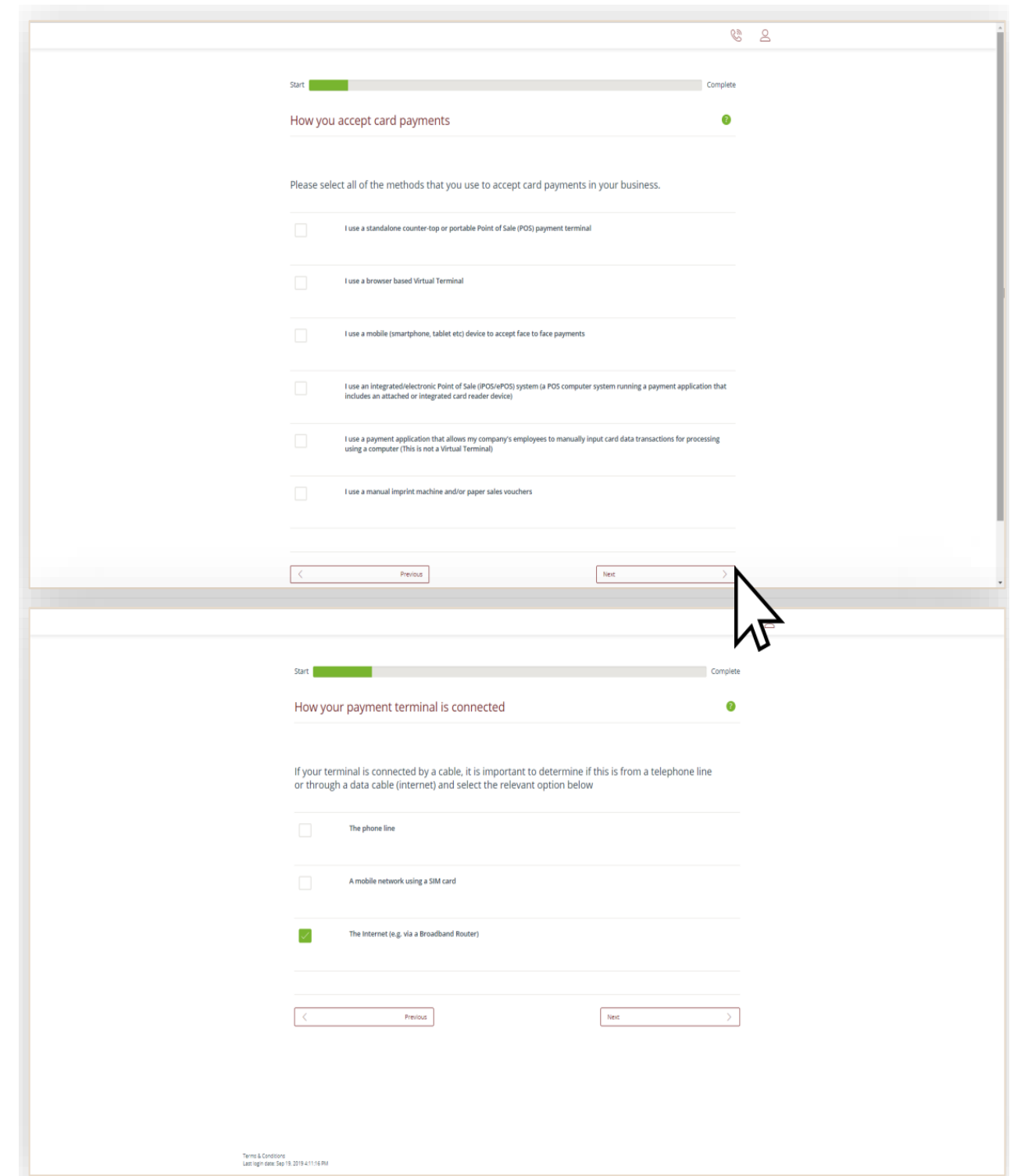
---

# 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 shows two screenshots of a web form titled 'Profile - How You Accept Payments'. The top screenshot is the 'How you accept card payments' step, which includes a progress bar at the top and a list of six payment methods with checkboxes. The bottom screenshot is the 'How your payment terminal is connected' step, which includes a progress bar and three connection options, with the third option selected. A mouse cursor is pointing at the 'Next' button in the top screenshot.

**How you accept card payments**

Please select all of the methods that you use to accept card payments in your business.

- ☐ 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/ePOS) 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

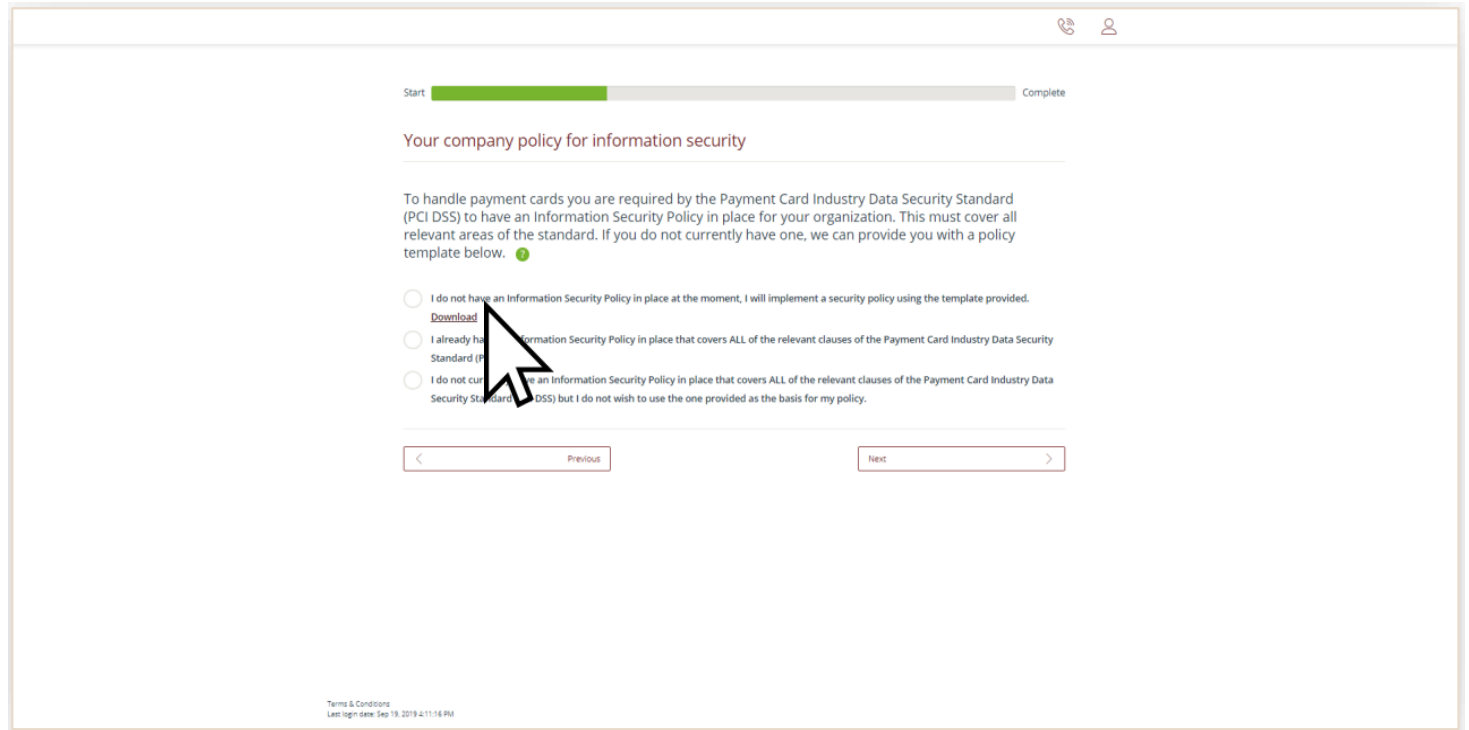
**How your payment terminal is connected**

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

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

# Profile - Information Security Policy

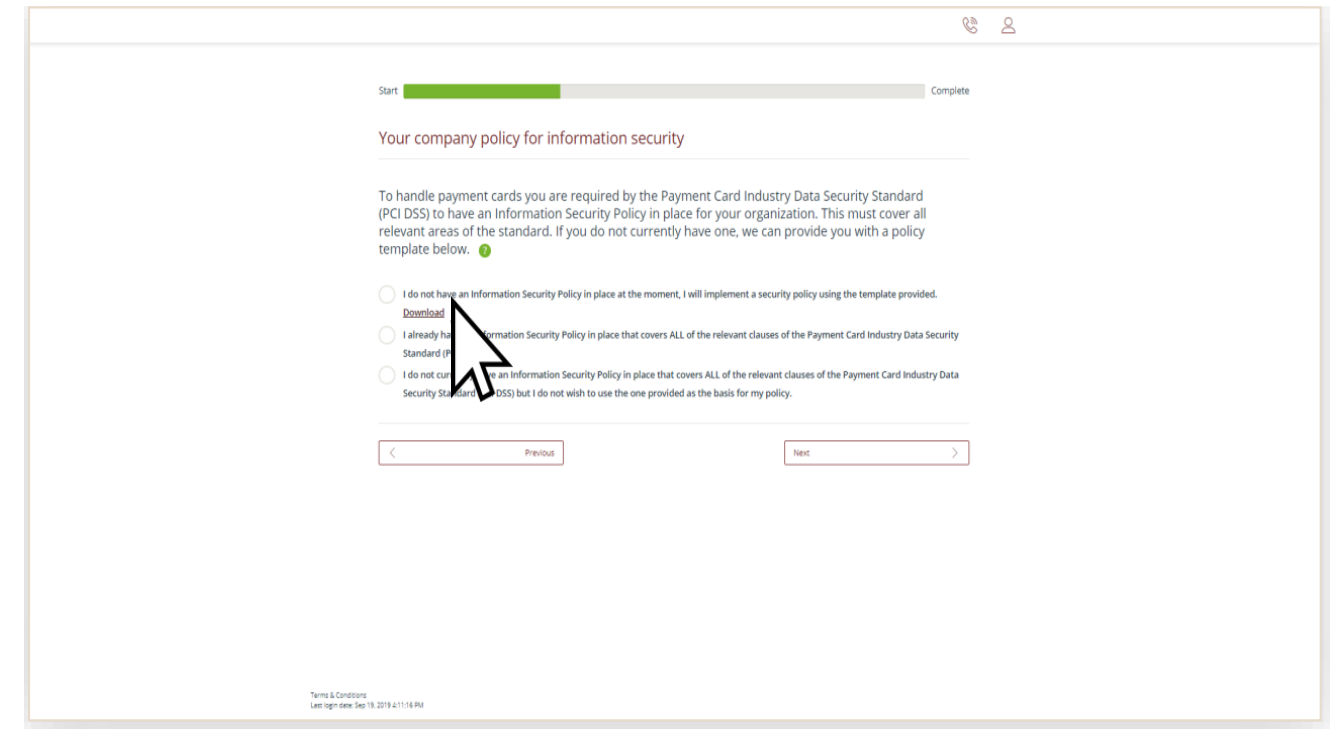
- **It's mandatory to apply an Information Security Policy**
  - This is a document that sets out the procedures you need to follow to handle information securely
- **You will be asked if you have a policy in your business. If you don't, you can download a sample template by clicking 'Download'.**
- **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". The form text explains that PCI DSS requires an Information Security Policy and offers a template download. Three radio button options are listed: "I do not have an Information Security Policy in place at the moment, I will implement a security policy using the template provided." (with a "Download" link), "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)", and "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, along with a small "Terms & Conditions" link and a "Last login date" timestamp.

# Profile - Information Security Policy

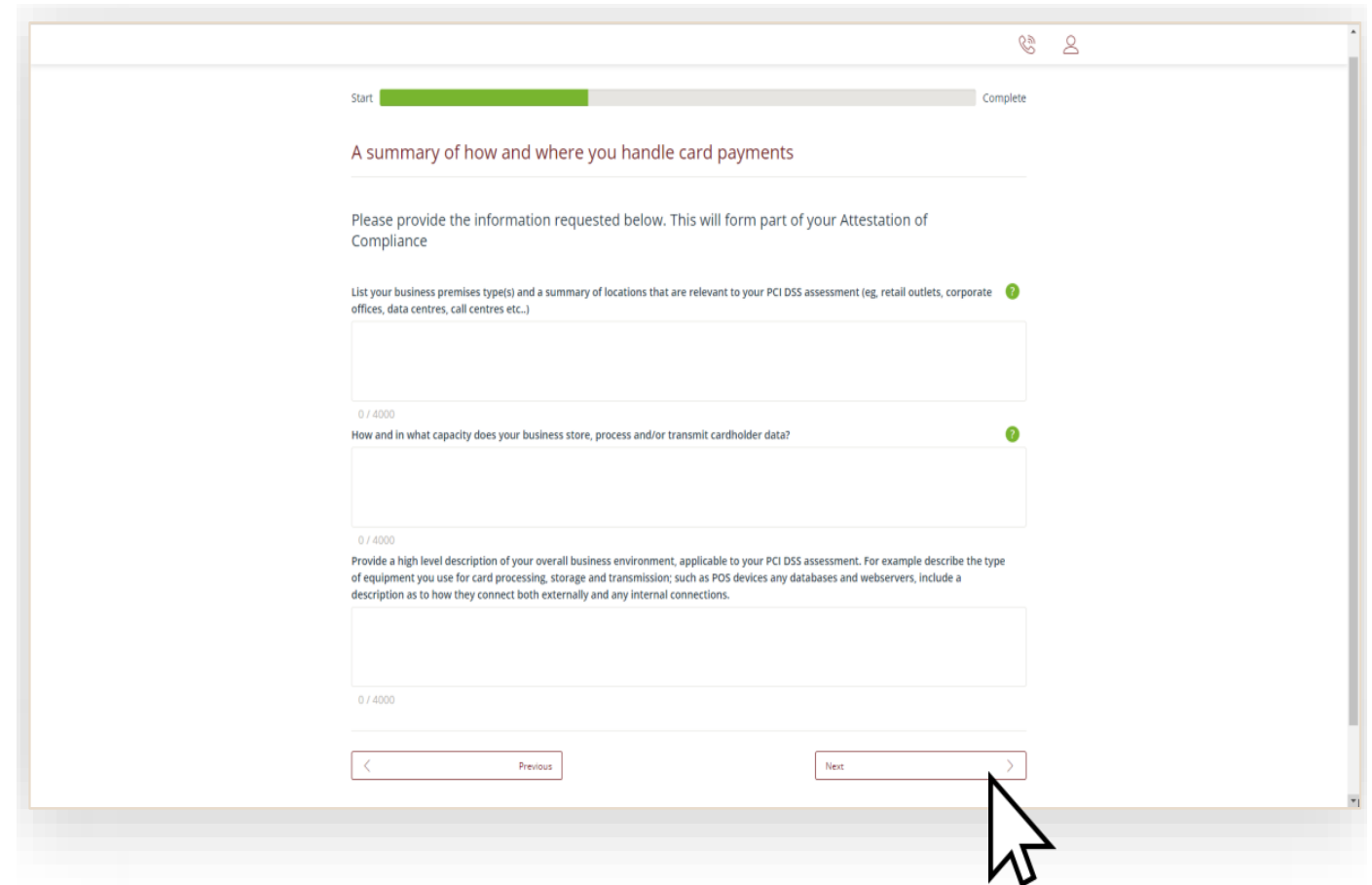
- **You will be asked to provide a summary of your payment acceptance processes.**
  - This is a document that sets out the procedures you need to follow to handle information securely
- **You will be asked if you have a policy in your business. If you don't, you can download a sample template by clicking '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 that PCI DSS requires an Information Security Policy. Three radio button options are listed: 1) "I do not have an Information Security Policy in place at the moment, I will implement a security policy using the template provided." with a "Download" link; 2) "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)"; and 3) "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." At the bottom are "Previous" and "Next" buttons. A mouse cursor is pointing at the "Download" link. Small text at the bottom left reads "Terms & Conditions Last updated: Sep 18, 2019 4:11:16 PM".

# Profile - Payment Summary

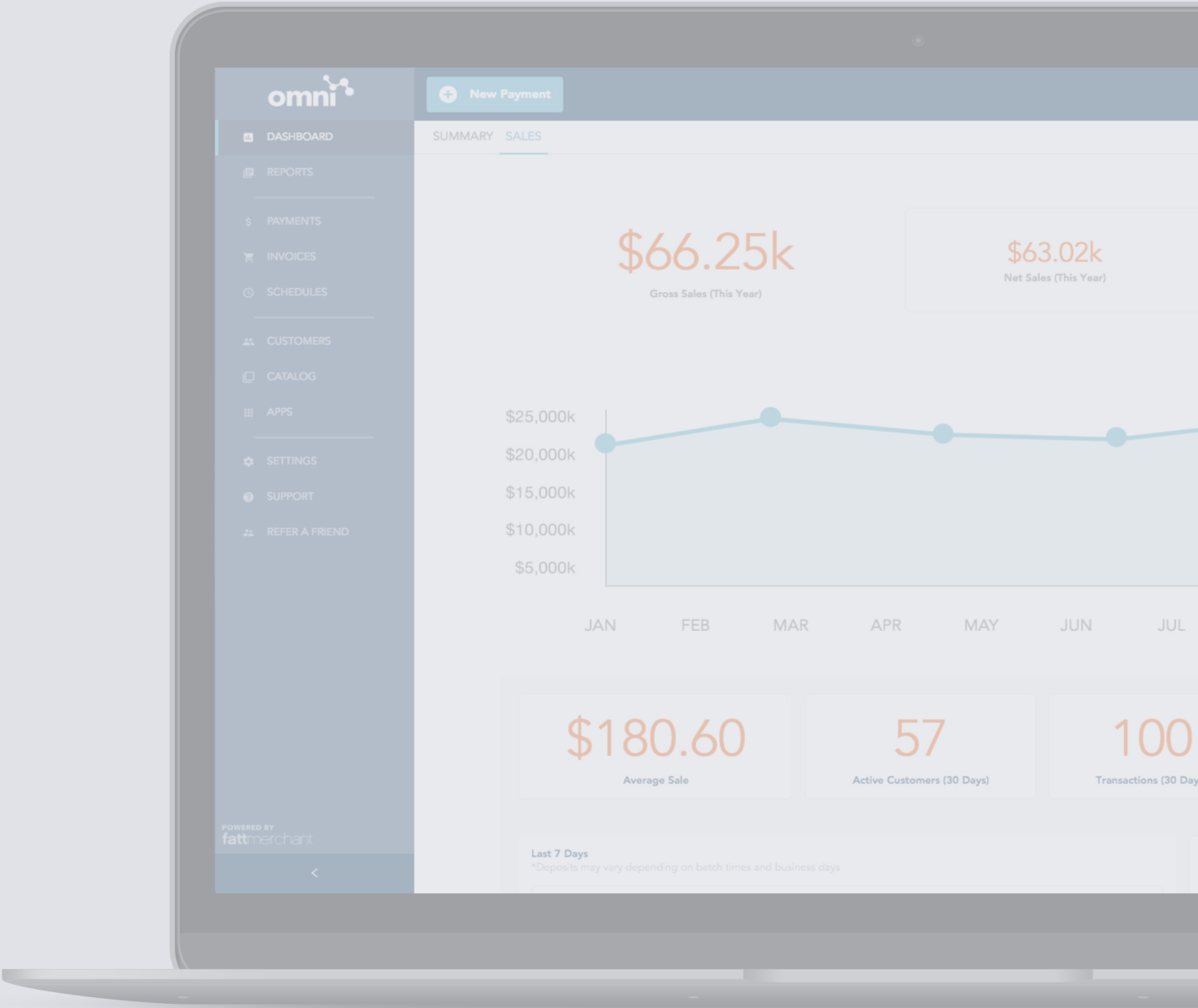
- **You will be asked to provide a summary of your payment acceptance processes**
- **You will be asked to:**
  - List your business premises and provide a summary of the locations where you accept payments.
  - Explain how your business handles cardholder data
  - Provide a high-level description of 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 browser window displaying a 'Payment Summary' form. At the top, there is a progress bar with 'Start' on the left and 'Complete' on the right, with a green bar indicating progress. The form title is 'A summary of how and where you handle card payments'. Below the title, a instruction reads: 'Please provide the information requested below. This will form part of your Attestation of Compliance'. The form contains three text input fields, each with a green question mark icon to its right. The first field is labeled '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.)'. The second field is labeled 'How and in what capacity does your business store, process and/or transmit cardholder data?'. The third field is labeled '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.' At the bottom of the form, there are 'Previous' and 'Next' buttons. A mouse cursor is pointing at the 'Next' button.

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.**

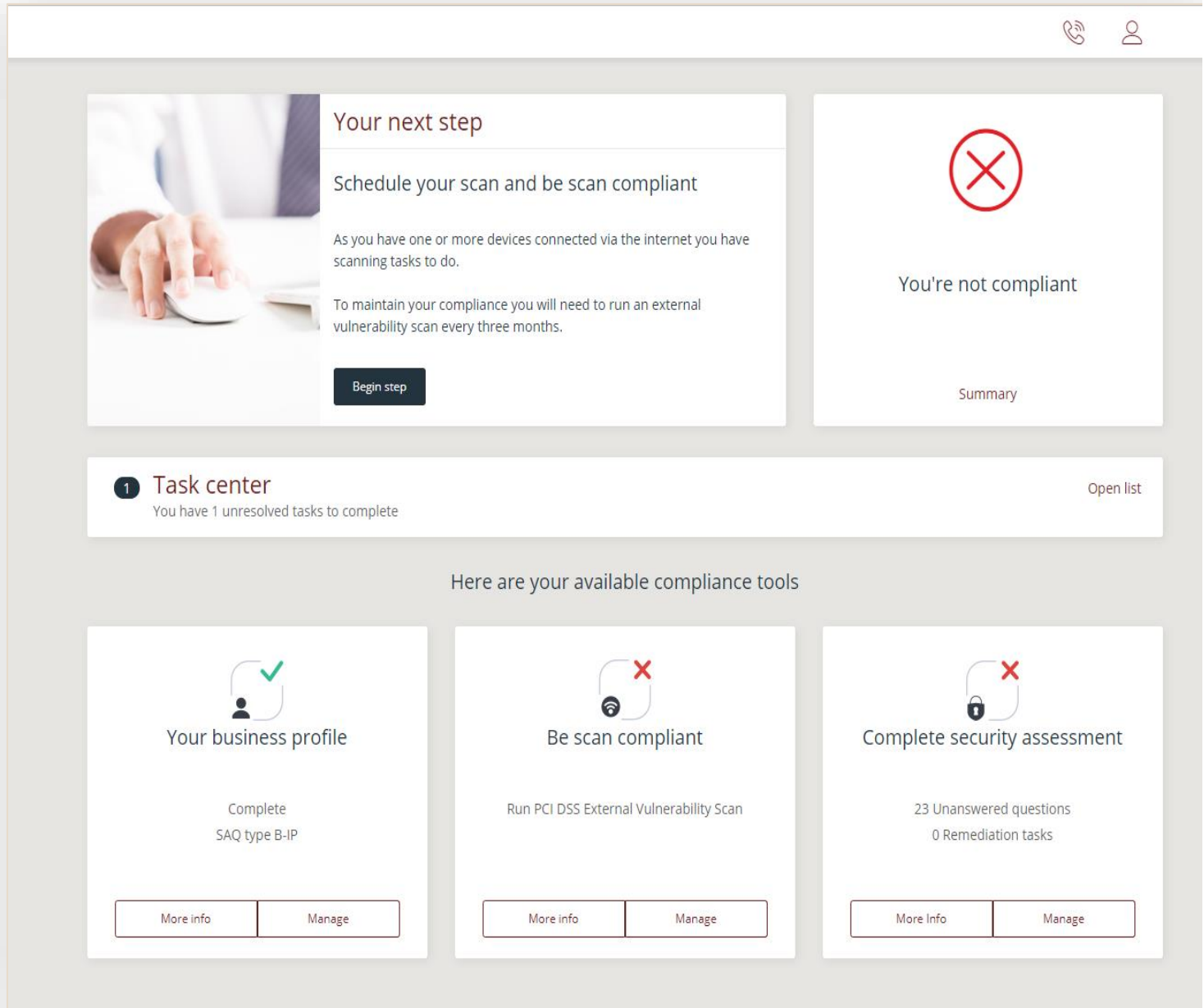
# Your Dashboard

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'

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'

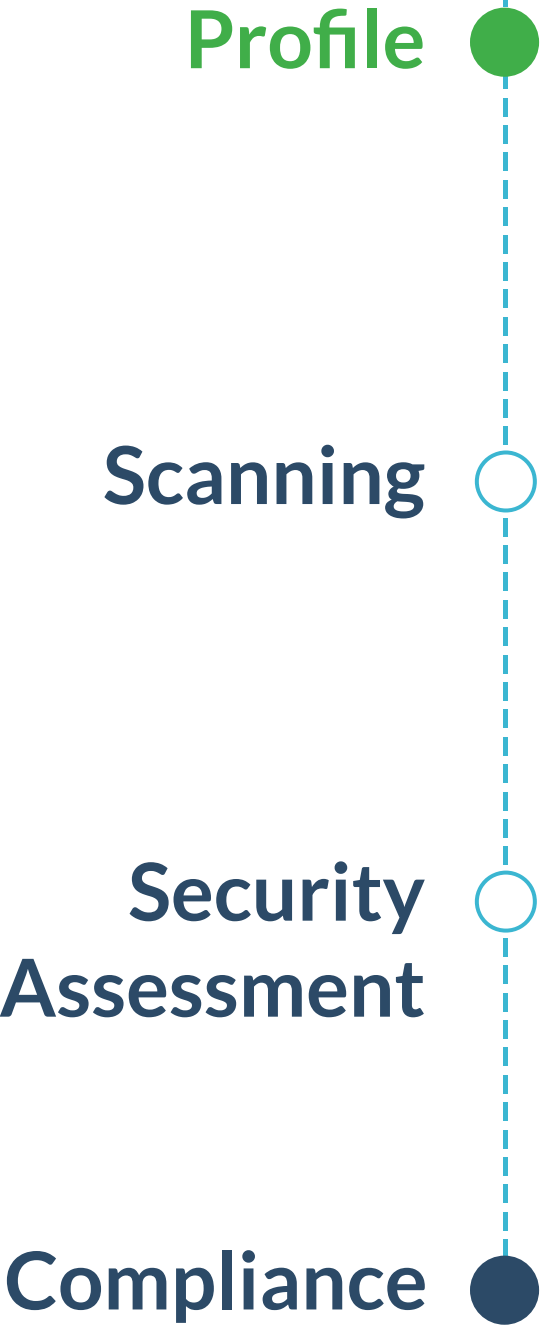
# Next Steps

## Scanning

If applicable to you, you will need to run a scan on your network. Proceed to page 15 for instructions.

## Security Assessment

If don't have to do a scan, you can proceed to your security assessment on page 18.



Proceed To Page 15

Proceed To Page 18

**External Vulnerability**

---

# SCANNING

# Scanning

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

The screenshot displays the Fattmerchant dashboard interface. At the top, a 'Task center' notification indicates one unresolved task. Below this, a section titled 'Here are your available compliance tools' features three widgets: 'Your business profile' (marked complete), 'Be scan compliant' (marked incomplete), and 'Complete security assessment' (marked incomplete). A mouse cursor points to the 'Manage' button on the 'Be scan compliant' widget. Below the dashboard, a modal window titled 'Be scan compliant' is open, showing options to 'Schedule scan', 'Review your PCI DSS External Vulnerability scans', 'Manage multiple domains / IP addresses', and 'Upload results'. A mouse cursor points to the 'Schedule scan' option.

**Task center**  
You have 1 unresolved tasks to complete [Open list](#)

Here are your available compliance tools

Your business profile

Complete  
SAQ type B-IP

[More info](#) [Manage](#)

Be scan compliant

Run PCI DSS External Vulnerability Scan

[More info](#) [Manage](#)

Complete security assessment

23 Unanswered questions  
0 Remediation tasks

[More Info](#) [Manage](#)

**Be scan compliant** [×](#)

Manage your PCI DSS External Vulnerability Scan

**Schedule scan**  
As part of your PCI DSS compliance tasks, you will need to schedule a scan on all of your externally facing IP addresses

**Review your PCI DSS External Vulnerability scans**  
View the status and history of all of your PCI DSS External Vulnerability Scans

**Manage multiple domains / IP addresses**  
Create a list of your domain names or your IP addresses that require scanning

**Upload results**  
Upload your validated scan results from a 3rd party Approved Scanning Vendor (ASV)

# 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
- 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

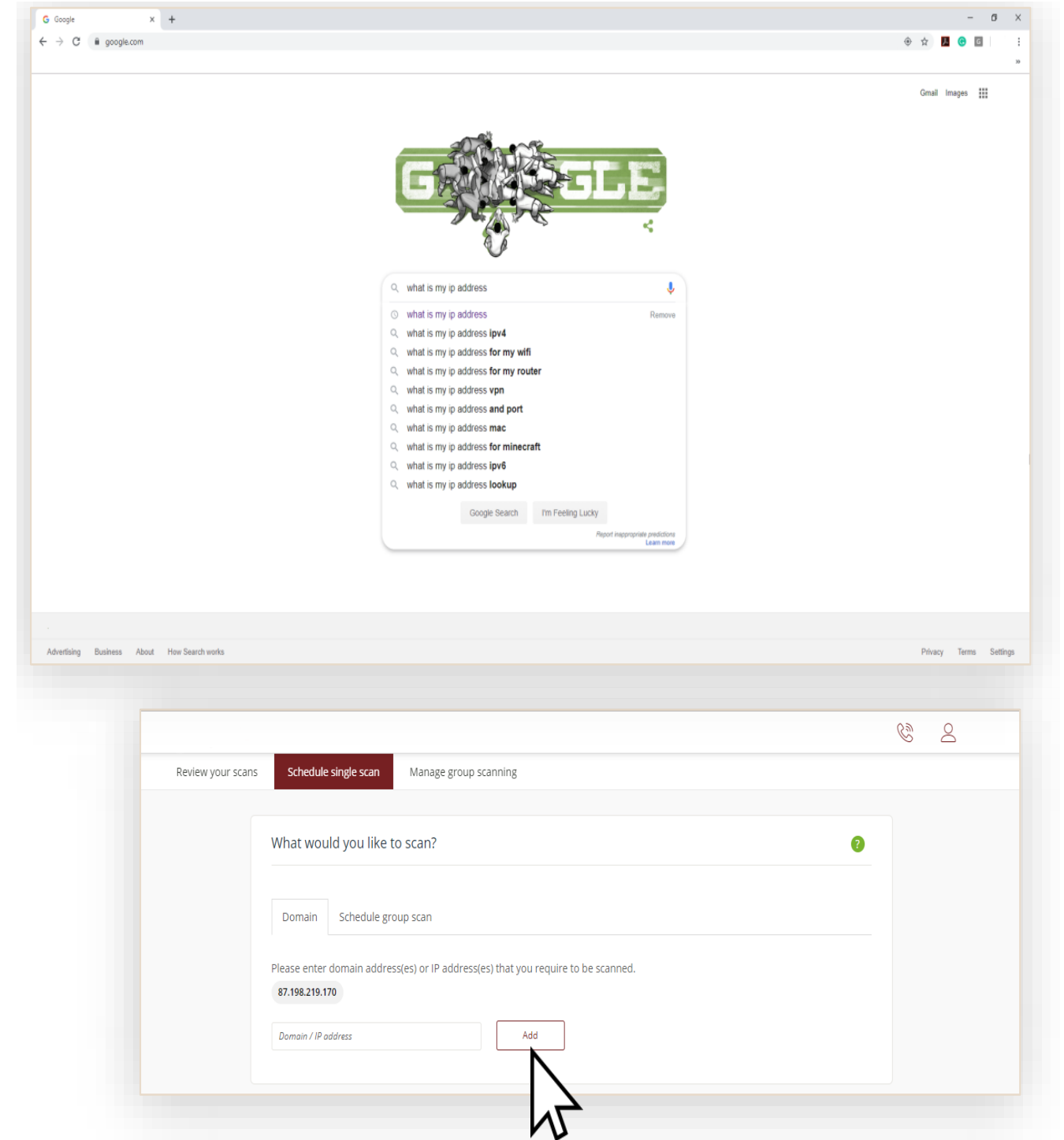
The screenshot displays the 'Schedule single scan' form within a web application. The top navigation bar includes 'Review your scans', 'Schedule single scan' (active), and 'Manage group scanning'. The form is divided into several sections:

- What would you like to scan?**: Includes a 'Domain' tab and a 'Schedule group scan' button. Below, it prompts for domain or IP addresses, with '87.198.219.170' entered in the 'Domain / IP address' field. An 'Add' button is present.
- Scan date**: Prompts for a preferred time and date. The date is set to 'Sep 19, 2019' and the time to '10:17'.
- Load Balancer?**: Asks 'Do you use Load Balancers as a part of your in-scope PCI Infrastructure?'. The 'No' option is selected.
- Sysnet access**: Explains that Sysnet requires access to specific IP addresses (64.39.96.0/20, 91.209.196.32/28, 178.255.82.64/27, 199.66.200.32/28) to complete a scan. It includes a 'Website disclaimer notice' section with a scrollable text area containing terms of use and a 'Warranties and Liability' section. A checkbox at the bottom confirms that the domain and IP addresses will grant access.

A 'Schedule Scan' button is located at the bottom of the form.

# 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
  - 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

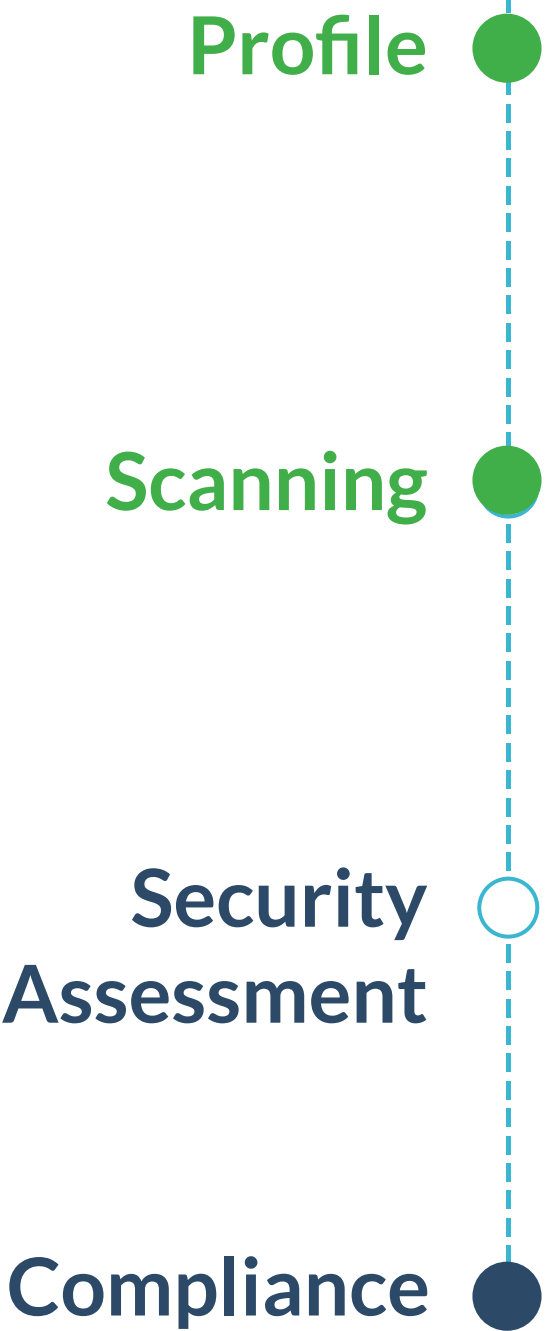


# Next Steps

## Security Assessment Questionnaire (SAQ)

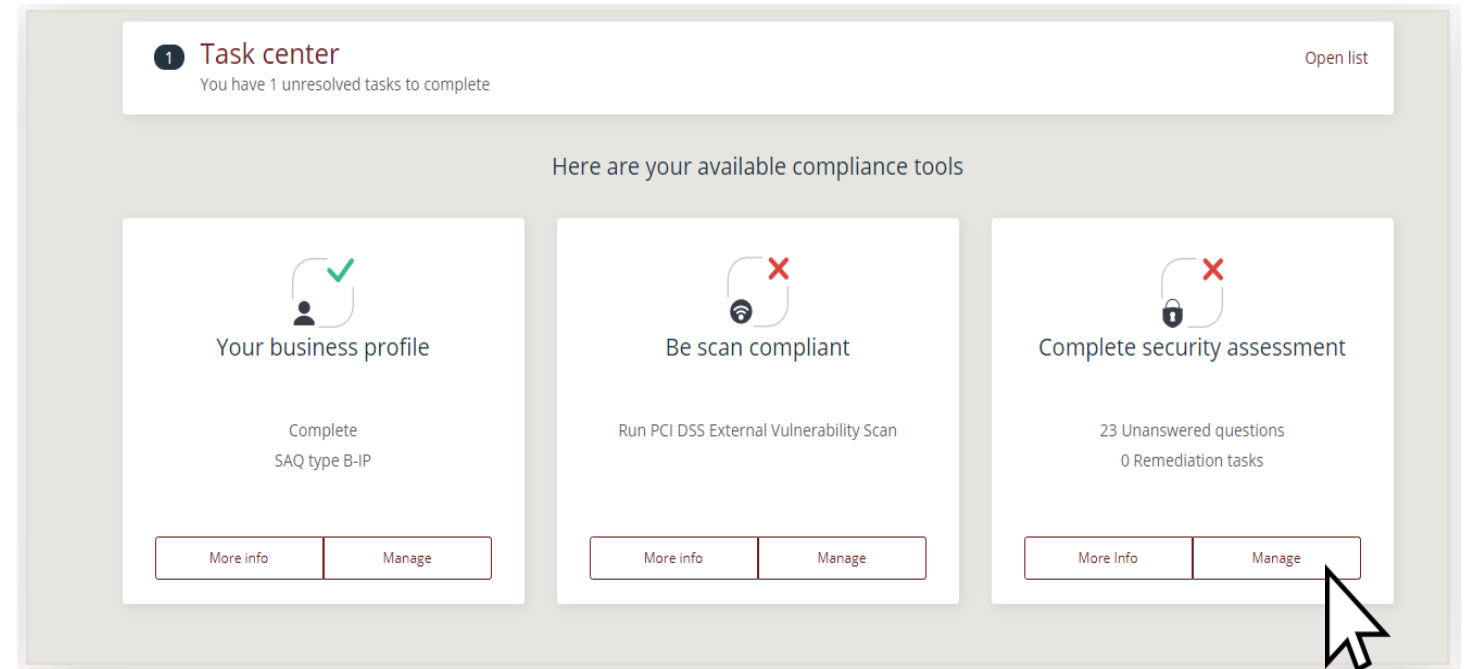
Your security assessment is an assessment of how you deal with information in your business. Its length and complexity depends on the results of your business profile.

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



# 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

Show me: Only unanswered questions Show Help Text: ☐

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

Sections

Milestones

5

Protect Cardholder Data

✓

Implement Strong Access Control Measures

✓

Maintain an Information Security Policy

✗

Confirm your compliance

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

Information

PCI Council Guidelines

Entities that issue payment cards or that perform or support issuing services will often create and control sensitive authentication data as part of the issuing function. It is allowable for companies that perform, facilitate, or support issuing services to store sensitive authentication data ONLY IF they have a legitimate business need to store such data.

It should be noted that all PCI DSS requirements apply to issuers, and the only exception for issuers and issuer processors is that sensitive authentication data may be retained if there is a legitimate reason to do so. A legitimate reason is one that is necessary for the performance of the function being provided for the issuer and not one of convenience. Any such data must be stored securely and in accordance with all PCI DSS and specific payment brand requirements.

PCI Audit Procedures

For all other entities, if sensitive authentication data is received, review policies and procedures, and examine system configurations to verify the data is not retained after authorization.

3

The box on the top right shows your progress through the questionnaire. Many of the questions will have been pre-populated 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 to 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 heading is 'Protect Cardholder Data' with the subtext 'Protect stored cardholder data'. Below this, the requirement '3.2(c)' is listed, followed by the question: 'Is sensitive authentication data deleted or rendered unrecoverable upon completion of the authorization process?'. Three buttons are visible: 'N/A' (grey), 'No' (red), and 'Yes' (green). A mouse cursor is pointing at the 'No' button. Below the buttons, a 'Remediation task' modal is open, containing a 'Reason for non-compliance' text area with the placeholder 'Unable to complete documentation on time', a 'Remediation Action' text area with the placeholder 'Complete documentation', and a 'Target date' field set to 'Sep 19, 2019'. At the bottom of the modal are 'Cancel' and 'Finish' buttons. On the right side, a sidebar shows a list of sections and milestones. The 'Protect Cardholder Data' section is highlighted with a green circle and the number 5. Other items in the list include 'Implement Strong Access Control Measures' (green checkmark), 'Maintain an Information Security Policy' (green checkmark), and 'Confirm your compliance' (red X).

# Security Assessment Questionnaire (SAQ)

- Once you have answered all your questions correctly, you will be 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.

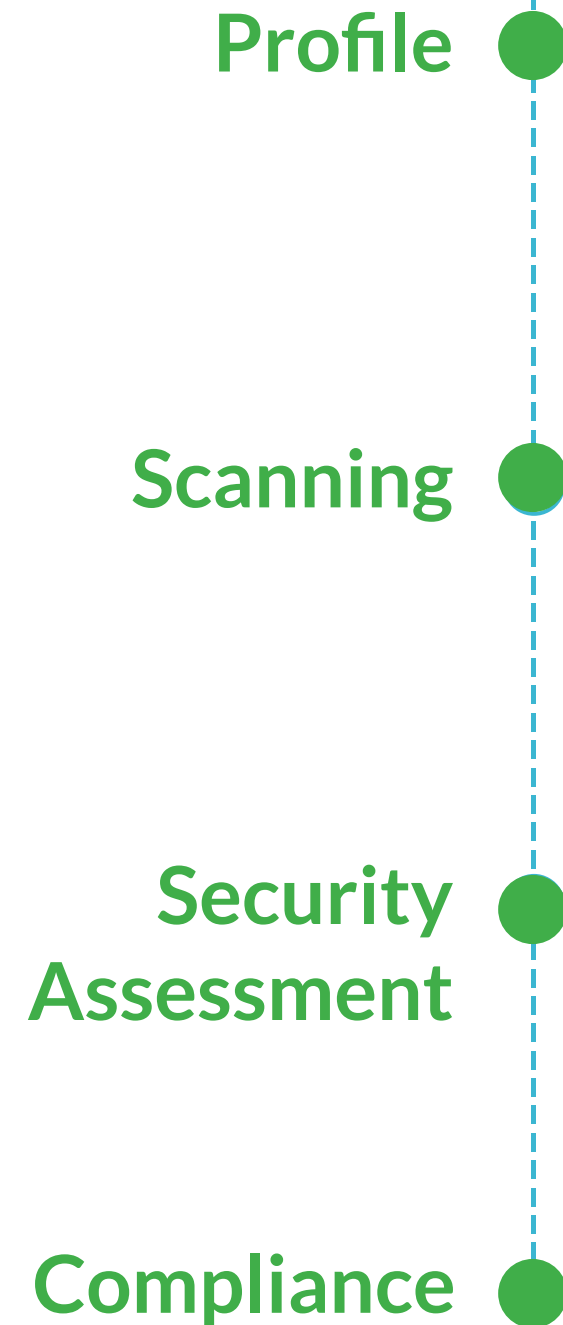
The screenshot displays the 'Confirm your compliance' section of the SAQ interface. The main heading is 'Confirm your compliance' with a sub instruction: 'Please review the form below and ensure all sections are correct and complete'. A list of sections follows, each with a status icon and a chevron: 'Your organization information details' (green checkmark, up), 'Type of business' (green checkmark, up), 'Description of environment' (green checkmark, up), 'Eligibility to complete SAQ B' (green checkmark, up), 'Acknowledgement of status and attestation' (green checkmark, up), and 'Attestation' (red X, down). To the right, a 'Milestones' sidebar shows 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). Below the sections, a grey box titled 'Information for Submission.' contains a summary: 'Based on the results noted in the SAQ B dated Sep 19, 2019, 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 19, 2019: Compliant: All sections of the PCI DSS SAQ are complete, all questions answered affirmatively, resulting in an overall COMPLIANT rating; thereby Unbranded01 has demonstrated full compliance with the PCI DSS.' At the bottom right, a dark button labeled 'Confirm your Attestation' with a green checkmark icon is being clicked by a mouse cursor.

# 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.

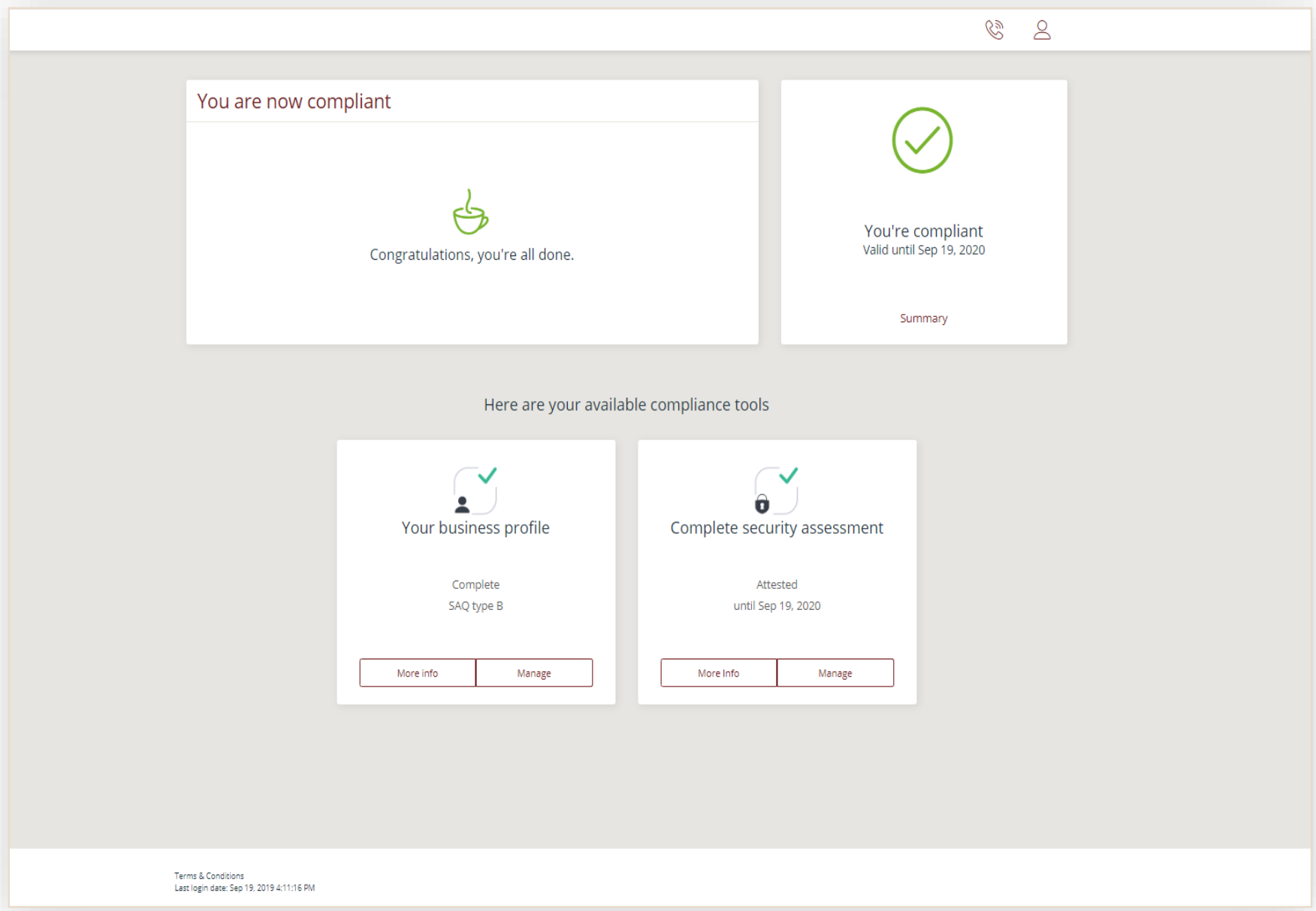


You're All Set!

# 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

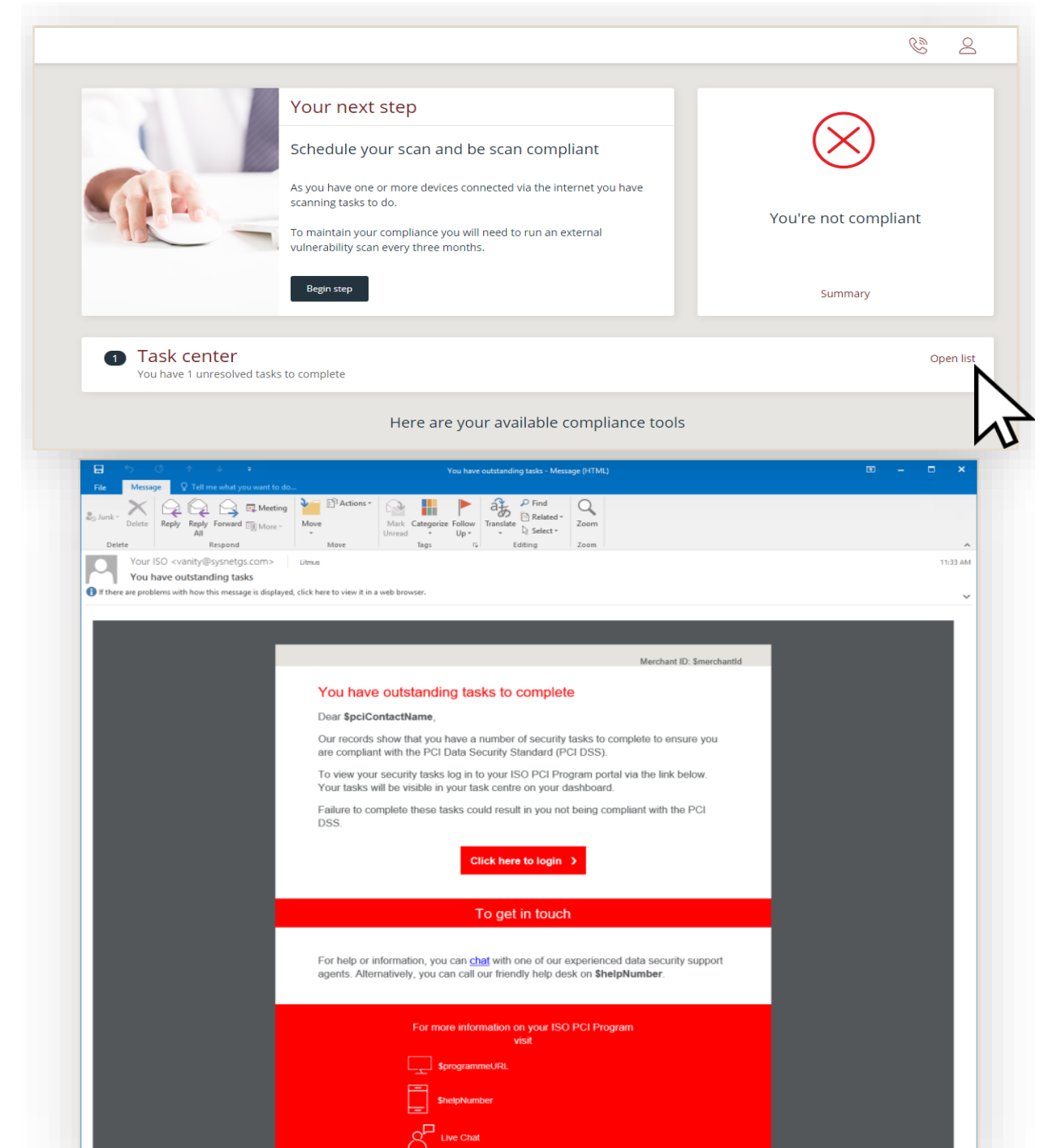
---

# 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 the Fattmerchant dashboard interface. At the top, a progress bar indicates the status from 'Start' to 'Complete'. Below this, a section titled 'Your current valid PCI compliance type' prompts the user to select an assessment type from a list of radio buttons. The options include Self Assessment Questionnaire (SAQ) A, P2PE, B, C-VT, B-IP, A-EP, C, and D. The 'SAQ B' option is currently selected. Navigation buttons for 'Previous' and 'Next' are located at the bottom of this section.

The main dashboard area features a 'Your next step' widget with the heading 'Confirm you're compliant'. It contains the instruction: 'You have indicated that you are compliant. Please upload your currently valid Attestation of Compliance.' A 'Begin step.' button is visible, with a mouse cursor hovering over it. To the right of this widget is a 'You're not compliant' section with a red 'X' icon and a 'Summary' link.

Below these widgets, a section titled 'Here are your available compliance tools' contains two main cards. The 'Your business profile' card shows 'Complete' status for 'SAQ type B' and includes 'More info' and 'Manage' buttons. The 'Attestation' card shows 'No documents uploaded' and includes '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

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

Please  or  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:

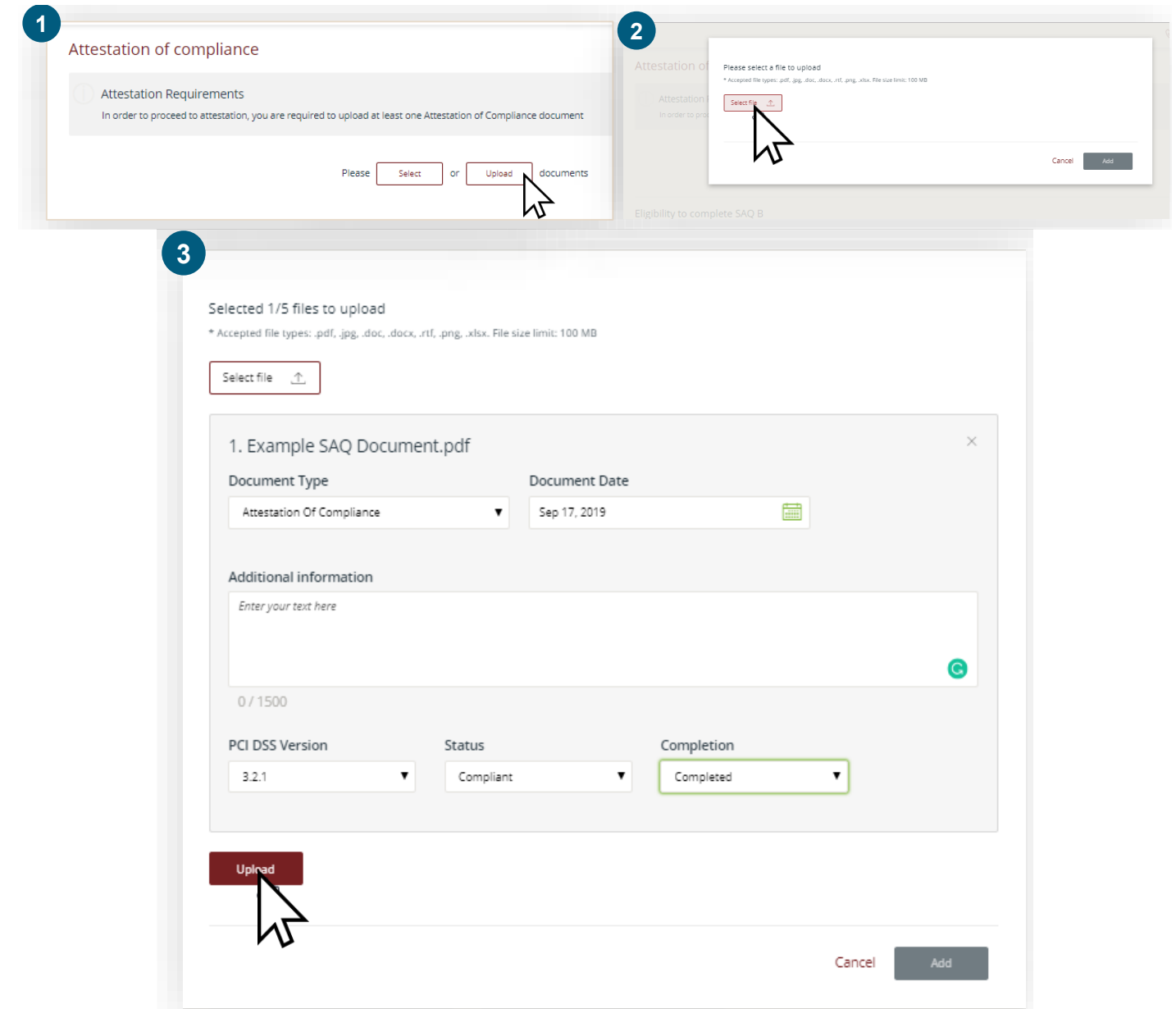
Acknowledgement of status and attestation

- ☐ 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 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 CVV2 data, or PIN data storage after transaction authorization was found on ANY system reviewed during the assessment.

# Uploading Existing Attestation Of Compliance

- **Upload Your Documents**

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



**1 Attestation of compliance**

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

Please  or  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. Example SAQ Document.pdf**

Document Type:  Document Date:

Additional information

0 / 1500

PCI DSS Version:  Status:  Completion:

# Uploading Existing Attestation Of Compliance

- **Select from your uploaded documents to attach to the attestation**

- Click  from the main screen.

- From the list of uploaded documents, select the ones you wish to attach to this attestation.



Click 

- The documents you wish to include will now appear on the main screen.

1

Attestation of compliance


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

Please  or  documents

2

	Document Name	Document Type	Date uploaded	Document Date	Verification status
<input checked="" type="checkbox"/>	Example SAQ Document.pdf	Attestation Of Compliance	Nov 1, 2020	Sep 17, 2019	Not reviewed
<input type="checkbox"/>	Example SAQ Document.pdf	Attestation Of Compliance	Nov 1, 2020	Sep 17, 2019	Not reviewed



Items: 2 / 2

Cancel 

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  or  documents

Files to be included in attestation form:

Document Name	Document Type	Date uploaded	Document Date	
Example SAQ Document.pdf	Attestation Of Compliance	Nov 1, 2020	Sep 17, 2019	×
Example SAQ Document.pdf	Scan	Nov 1, 2020	Sep 3, 2019	×

Items: 2 / 2

# 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**

### 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:

1

Assessment type  
B

Validation effective date

PCI DSS Version

### Acknowledgement of status and attestation

2

☐ 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 CVV2 data, or PIN data storage after transaction authorization was found on ANY system reviewed during the assessment.

3

Attest

