

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



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

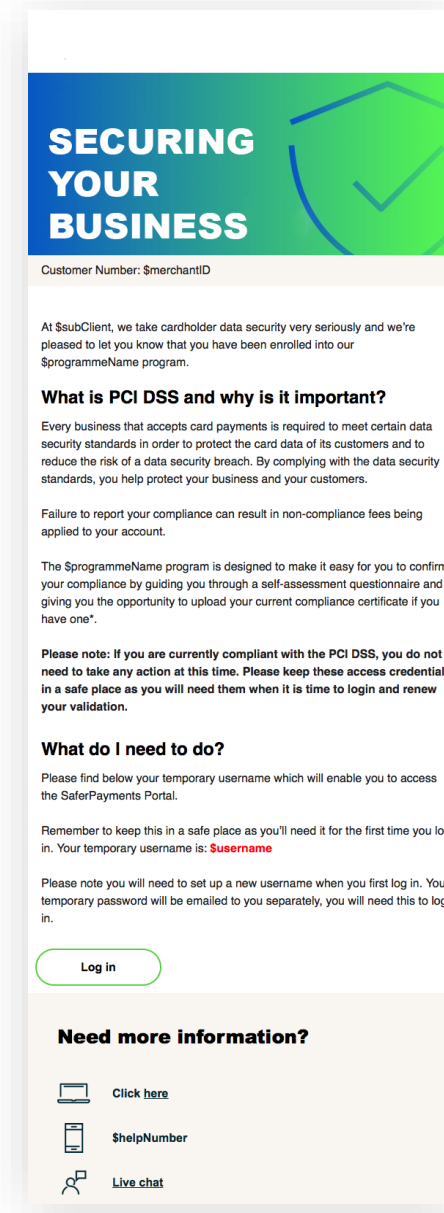
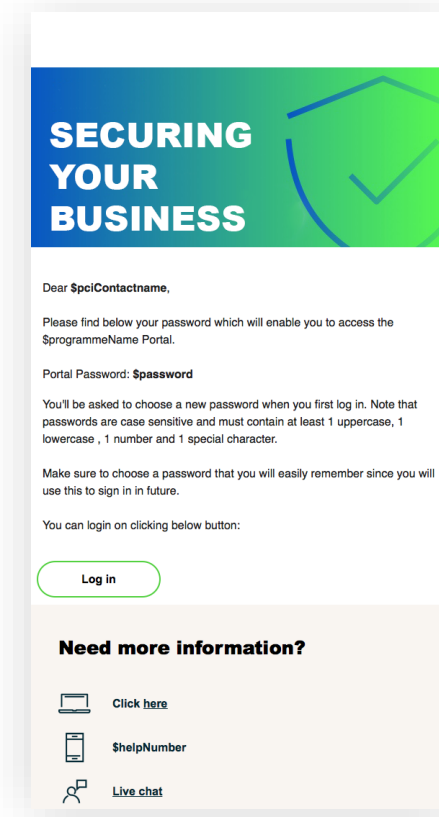
5

Maintenance

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

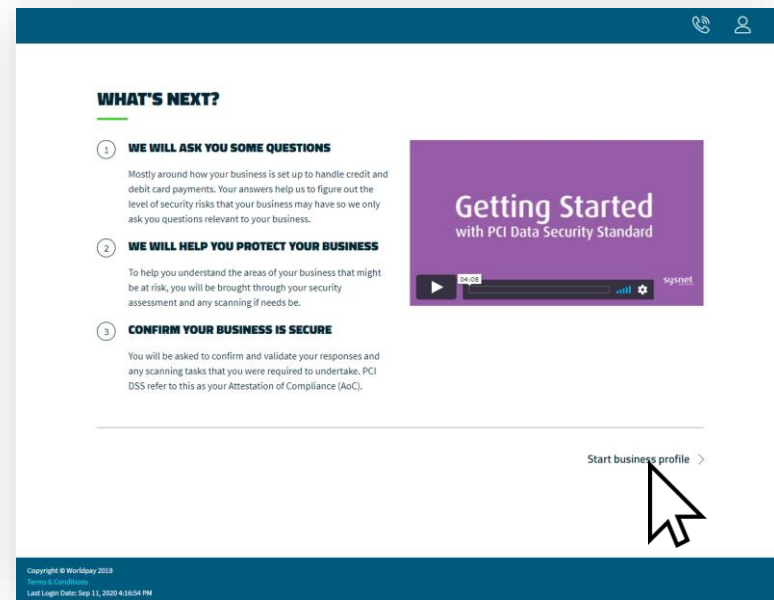
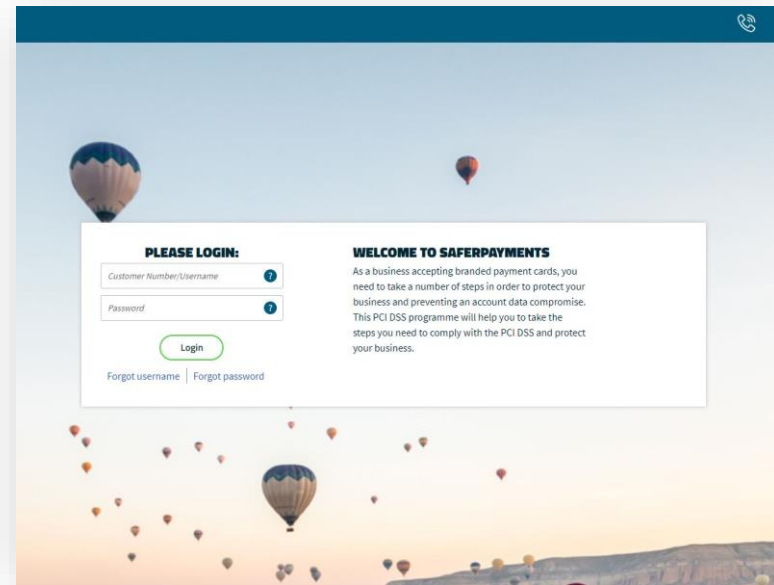
Welcome to the program

- 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 **'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 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.

Start Complete

BEFORE YOU BEGIN

Have you already completed a PCI DSS Self Assessment Questionnaire (SAQ) or Attestation of Compliance (AoC) that you would like to upload?

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.

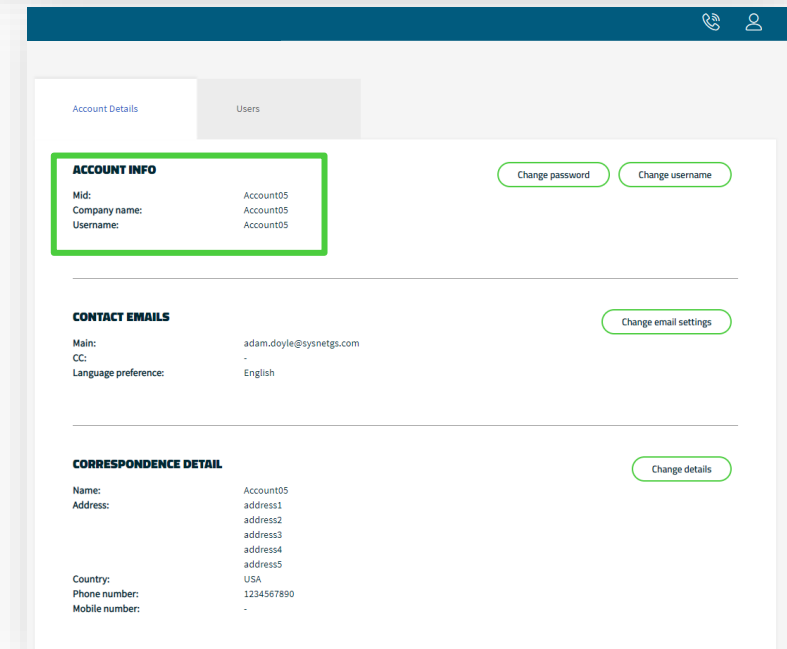
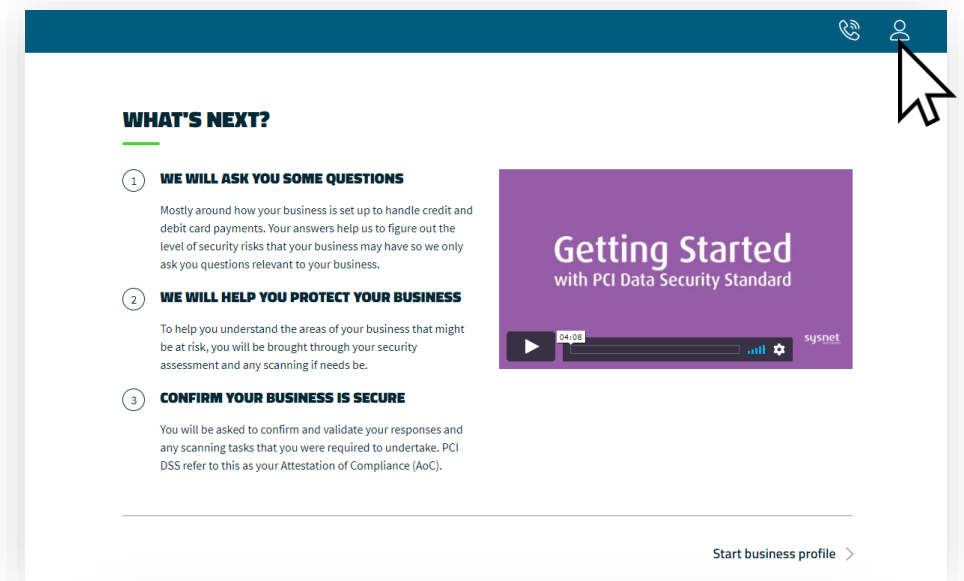
Select this option to upload your existing currently valid PCI DSS Self-Assessment Questionnaire (SAQ) or Attestation of Compliance (AoC) from an external programme.

< Previous Next >

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

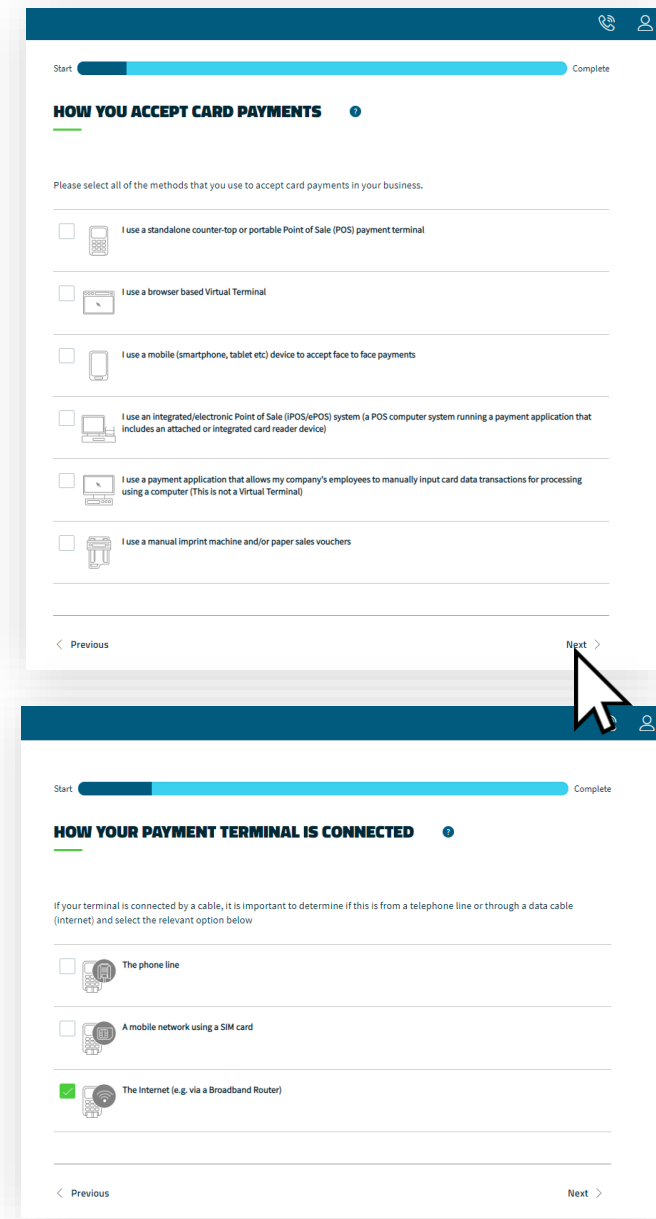


How you accept payments

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 shows two screenshots of the Worldpay profile setup interface. The top screenshot is titled "HOW YOU ACCEPT CARD PAYMENTS" and contains a progress bar at the top with "Start" on the left and "Complete" on the right. Below the title, there is a question: "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: 1. "I use a standalone counter-top or portable Point of Sale (POS) payment terminal" (checkbox unchecked, icon of a POS terminal); 2. "I use a browser based Virtual Terminal" (checkbox unchecked, icon of a browser window); 3. "I use a mobile (smartphone, tablet etc) device to accept face to face payments" (checkbox unchecked, icon of a smartphone); 4. "I use an integrated/electronic Point of Sale (ePOS) system (a POS computer system running a payment application that includes an attached or integrated card reader device)" (checkbox unchecked, icon of a computer monitor with a card reader); 5. "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)" (checkbox unchecked, icon of a computer monitor); 6. "I use a manual imprint machine and/or paper sales vouchers" (checkbox unchecked, icon of a manual imprint machine). At the bottom of the form, there are "Previous" and "Next" navigation buttons. A mouse cursor is pointing at the "Next" button. The bottom screenshot is titled "HOW YOUR PAYMENT TERMINAL IS CONNECTED" and also has a progress bar. It contains a question: "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: 1. "The phone line" (checkbox unchecked, icon of a telephone handset); 2. "A mobile network using a SIM card" (checkbox unchecked, icon of a SIM card); 3. "The Internet (e.g. via a Broadband Router)" (checkbox checked, icon of a broadband router). At the bottom of the form, 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 interface for setting an information security policy. At the top, there is a dark blue header with a user profile icon and a notification bell. Below the header is a progress bar starting at 'Start' and ending at 'Complete'. The main heading is 'YOUR COMPANY POLICY FOR INFORMATION SECURITY'. The text explains that PCI DSS requires an information security policy and offers a template. There are three radio button options: 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.

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 form with a dark blue header containing a refresh icon and a user profile icon. Below the header is a progress bar with 'Start' on the left and 'Complete' on the right. The main heading is 'A SUMMARY OF HOW AND WHERE YOU HANDLE CARD PAYMENTS' in bold, underlined text. Below this is a sub-heading: '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 '0 / 4000' character count and a question mark icon. The first field is for business premises and locations. The second field is for cardholder data handling, with a mouse cursor hovering over its question mark icon. The third field is for a high-level business environment description. 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

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.

The dashboard features a dark blue header with a hand icon and a user profile icon. Below the header, there are three main sections:

- PRODUCT RECOMMENDATION**: A card with a photo of a woman on the left. The text reads: **MANAGED COMPLIANCE SERVICE**. "Let us manage your data security reporting for you. We'll help you through the compliance journey over the phone ensuring you know what you need to do and when." "We also help you understand what else you can do to protect your business, including a suite of valuable cyber security tools." "Sign up to SaferPayments Plus and you'll save time and effort reporting your compliance." At the bottom are two buttons: "Not now" and "Schedule callback".
- YOU'RE NOT COMPLIANT**: A card with a red 'X' icon and a "Summary" button at the bottom.
- HERE ARE YOUR AVAILABLE COMPLIANCE TOOLS**: A section with three tool cards:
 - YOUR BUSINESS PROFILE**: Shows a green checkmark icon. Text: "Complete SAQ type B-IP". Buttons: "More info" and "Manage".
 - BE SCAN COMPLIANT**: Shows a red 'X' icon with a lock. Text: "Run PCI DSS External Vulnerability Scan". Buttons: "More info" and "Manage".
 - COMPLETE SECURITY ASSESSMENT**: Shows a red 'X' icon with a lock. Text: "23 Unanswered questions" and "0 Remediation tasks". Buttons: "More Info" and "Manage".

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



Proceed to page 17

Security Assessment



Proceed to page 21

Compliance



External Vulnerability

SCANNING

Scanning

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

The image shows a two-step process in a software dashboard. The top part is a dashboard titled "HERE ARE YOUR AVAILABLE COMPLIANCE TOOLS" with three widgets: "YOUR BUSINESS PROFILE" (Complete SAQ type B-IP), "BE SCAN COMPLIANT" (Run PCI DSS External Vulnerability Scan), and "COMPLETE SECURITY ASSESSMENT" (23 Unanswered questions, 0 Remediation tasks). A mouse cursor points to the "Manage" button on the "BE SCAN COMPLIANT" widget. The bottom part is a detailed view of the "BE SCAN COMPLIANT" widget, titled "Manage your PCI DSS External Vulnerability Scan". It contains four action cards: "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), and "Upload results" (Upload your validated scan results from a 3rd party Approved Scanning Vendor (ASV)). A mouse cursor points to the "Schedule scan" card.

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 shows a web interface for scheduling a scan. At the top, there are three tabs: "Review your scans", "Schedule Single Scan" (which is active), and "Manage Group Scanning".

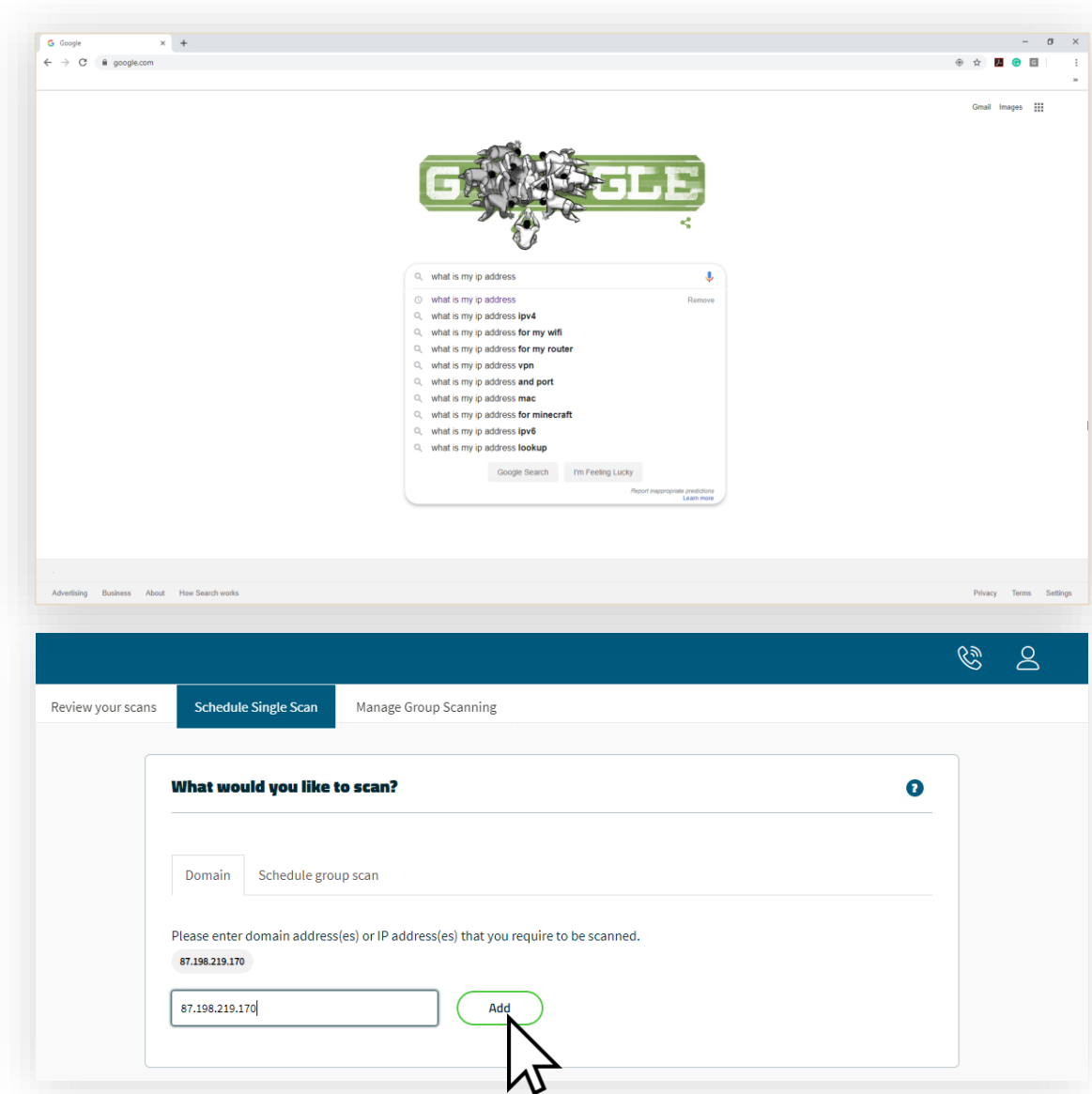
The main content area is divided into several sections:

- Scan date:** A section with a heading and a sub-heading "Please enter a preferred time and date for the scan to occur." Below this is a date and time picker. The date is set to "Sat 14, 2020" and the time is "09 : 45".
- Load Balancer?:** A section with a heading and a sub-heading "Do you use Load Balancers as a part of your in-scope PCI Infrastructure?". There are two radio buttons: "Yes" (unselected) and "No" (selected).
- Synet access:** A section with a heading and a sub-heading "In order to run the scan, we need you to grant access to the IP addresses listed below." It contains several paragraphs of text explaining the need for access and providing instructions for users with firewalls or dynamic IP addresses. Below this text are three IP addresses listed: "64.39.96.0/20", "64.39.108.0/24", and "134.39.121.0/24".
- WEBSITE DISCLAIMER NOTICE:** A section with a heading and a sub-heading "Granting Sysnet access". It contains several paragraphs of text explaining the terms of the disclaimer notice and the user's responsibility. Below this text is a checkbox labeled "I confirm that our domain and IP addresses will grant access to the IP address(es) stated above".

At the bottom of the form, there is a green button labeled "Schedule Scan" with a white mouse cursor pointing to 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.

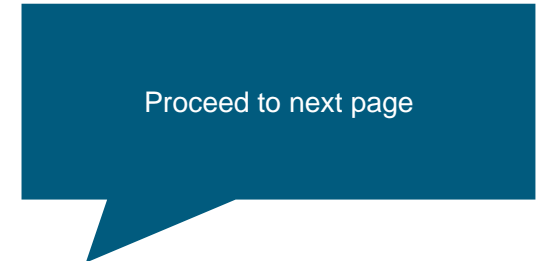
The system will prepopulate any questions that don't apply to you. So you only have to answer those that really matter.

Profile

Scanning

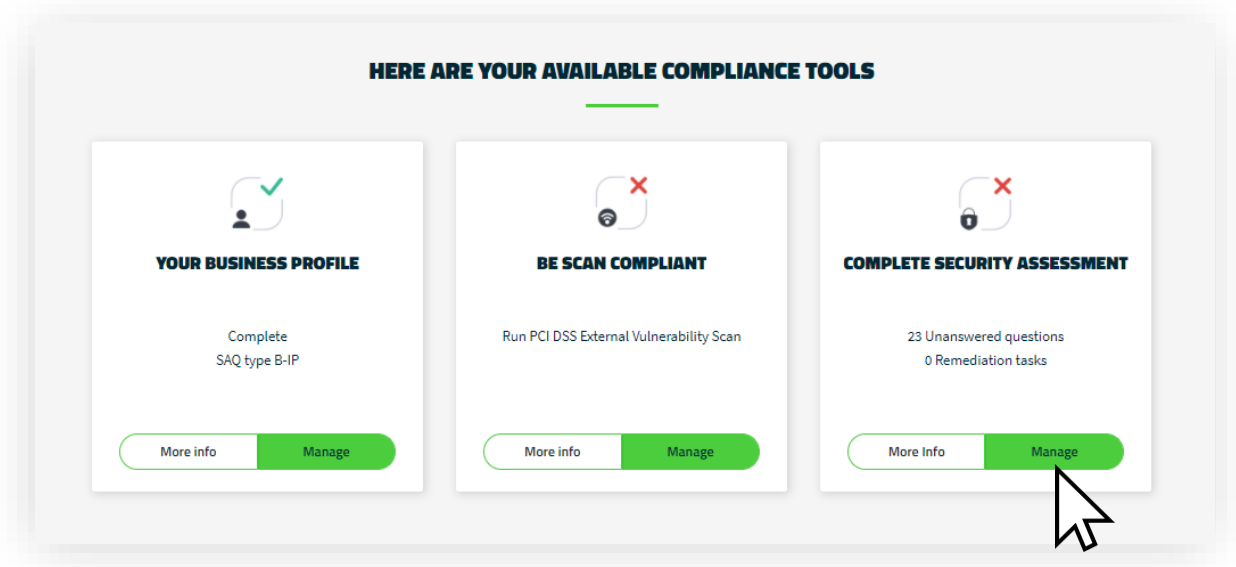
Security
Assessment

Compliance



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

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 question is: '3.2(c) Is sensitive authentication data deleted or rendered unrecoverable upon completion of the authorization process?'. The 'No' button is selected, and a mouse cursor is pointing at it. Below the question, a 'REMIEDIATION TASK' box is visible, containing the following fields:

- Reason for non-compliance:** 'Unable to complete documentation on time' (0 / 1500 characters)
- Remediation Action:** 'Complete documentation' (0 / 1500 characters)
- Target date:** 'Sep 14, 2020' (with a calendar icon) and a note: 'You will receive a reminder email'

At the bottom of the remediation task box are 'Cancel' and 'Finish' buttons. On the right side of the interface, a sidebar shows a list of milestones, with 'Protect Cardholder Data' (9) highlighted. Other milestones include 'Build and Maintain a Secure Network and Systems' (8), 'Maintain a Vulnerability Management Program' (1), 'Implement Strong Access Control Measures' (2), 'Regularly Monitor and Test Networks' (3), 'Maintain an Information Security Policy' (checked), and 'Confirm your compliance' (unchecked).

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 displays the 'CONFIRM YOUR COMPLIANCE' section of a web application. The header is dark blue with a white user icon and a refresh 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 is a list of sections, each with a green checkmark and an upward arrow, indicating completion. The sections are: 'Your organization information details', 'Type of business', 'Description of environment', 'Eligibility to complete SAQ B', and 'Acknowledgement of status and attestation'. The 'Attestation' section is currently expanded and shows a red 'X' icon, indicating it is not yet completed. To the right of the sections is a 'Milestones' sidebar with a green 'Sections' tab and a white 'Milestones' tab. The milestones list includes: '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 is a section titled 'INFORMATION FOR SUBMISSION.' with a checkmark icon. It contains 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: Compliant: All sections of the PCI DSS SAQ are complete, all questions answered affirmatively, resulting in an overall COMPLIANT rating; thereby Account05 has demonstrated full compliance with the PCI DSS.' At the bottom right, there is a green button labeled 'Confirm your Attestation' with a white checkmark icon, and a mouse cursor is pointing at it.

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

The screenshot displays a user dashboard with a dark blue header containing a phone icon and a user profile icon. The main content area is divided into several sections:

- PRODUCT RECOMMENDATION**: A section with a green underline. It features a photo of a woman on the left and text on the right. The text includes a checkmark icon and the heading **MANAGED COMPLIANCE SERVICE**. Below this, it states: "Let us manage your data security reporting for you. We'll help you through the compliance journey over the phone ensuring you know what you need to do and when." It continues: "We also help you understand what else you can do to protect your business, including a suite of valuable cyber security tools." and "Sign up to SaferPayments Plus and you'll save time and effort reporting your compliance." At the bottom of this section are two buttons: "Not now" and "Schedule callback".
- YOU'RE COMPLIANT**: A white card with a large green checkmark icon at the top. Below the icon, it says "Valid until Sep 14, 2021". At the bottom of the card is a "Summary" button.
- HERE ARE YOUR AVAILABLE COMPLIANCE TOOLS**: A section with a green underline. It contains two cards:
 - YOUR BUSINESS PROFILE**: Features a checkmark icon with a person silhouette. It says "Complete SAQ type B". At the bottom are "More info" and "Manage" buttons.
 - COMPLETE SECURITY ASSESSMENT**: Features a checkmark icon with a padlock silhouette. It says "Attested until Sep 14, 2021". At the bottom are "More Info" and "Manage" buttons.

2

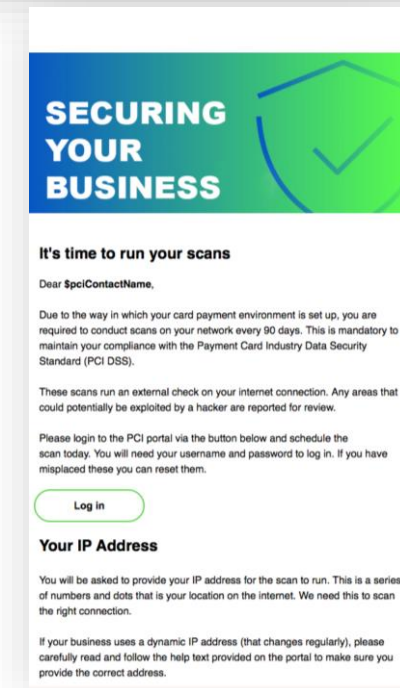
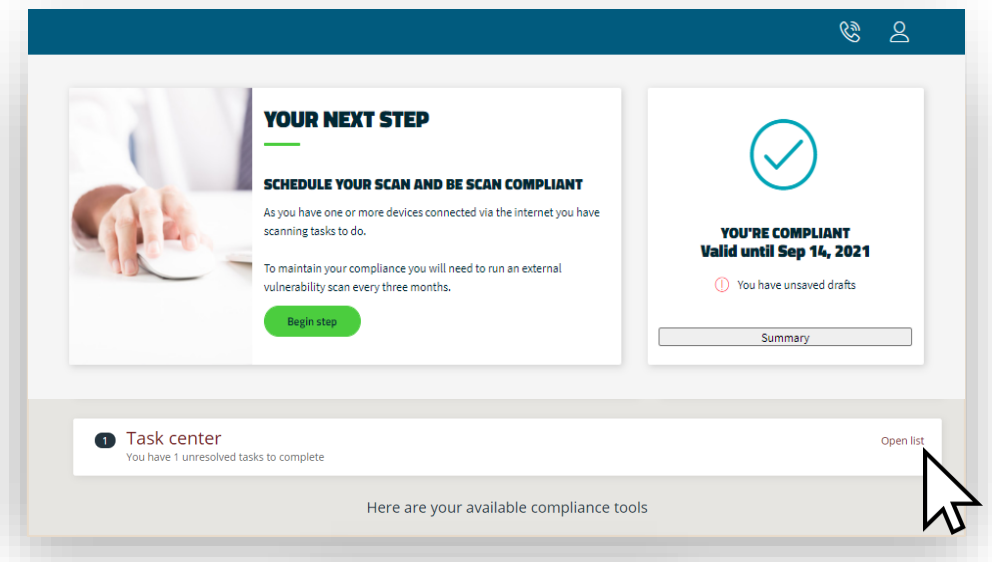
Your revalidation date is displayed in the top right corner

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.

Start Complete

YOUR CURRENT VALID PCI COMPLIANCE TYPE

Please select the PCI Compliance assessment type that you are currently valid for from the selection below.

- Self Assessment Questionnaire (SAQ) A
- Self Assessment Questionnaire (SAQ) P2PE
- Self Assessment Questionnaire (SAQ) B
- Self Assessment Questionnaire (SAQ) C-VT
- Self Assessment Questionnaire (SAQ) B-IP
- Self Assessment Questionnaire (SAQ) A-EP
- Self Assessment Questionnaire (SAQ) C
- Self Assessment Questionnaire (SAQ) D

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

YOUR NEXT STEP

CONFIRM YOU'RE COMPLIANT

You have indicated that you are compliant. Please upload your currently valid Attestation of Compliance.

[Begin step](#)

YOU'RE NOT COMPLIANT

[Summary](#)

HERE ARE YOUR AVAILABLE COMPLIANCE TOOLS

YOUR BUSINESS PROFILE

Complete
SAQ type B

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

ATTESTATION

No documents uploaded

[Attest](#) [View History](#)

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:

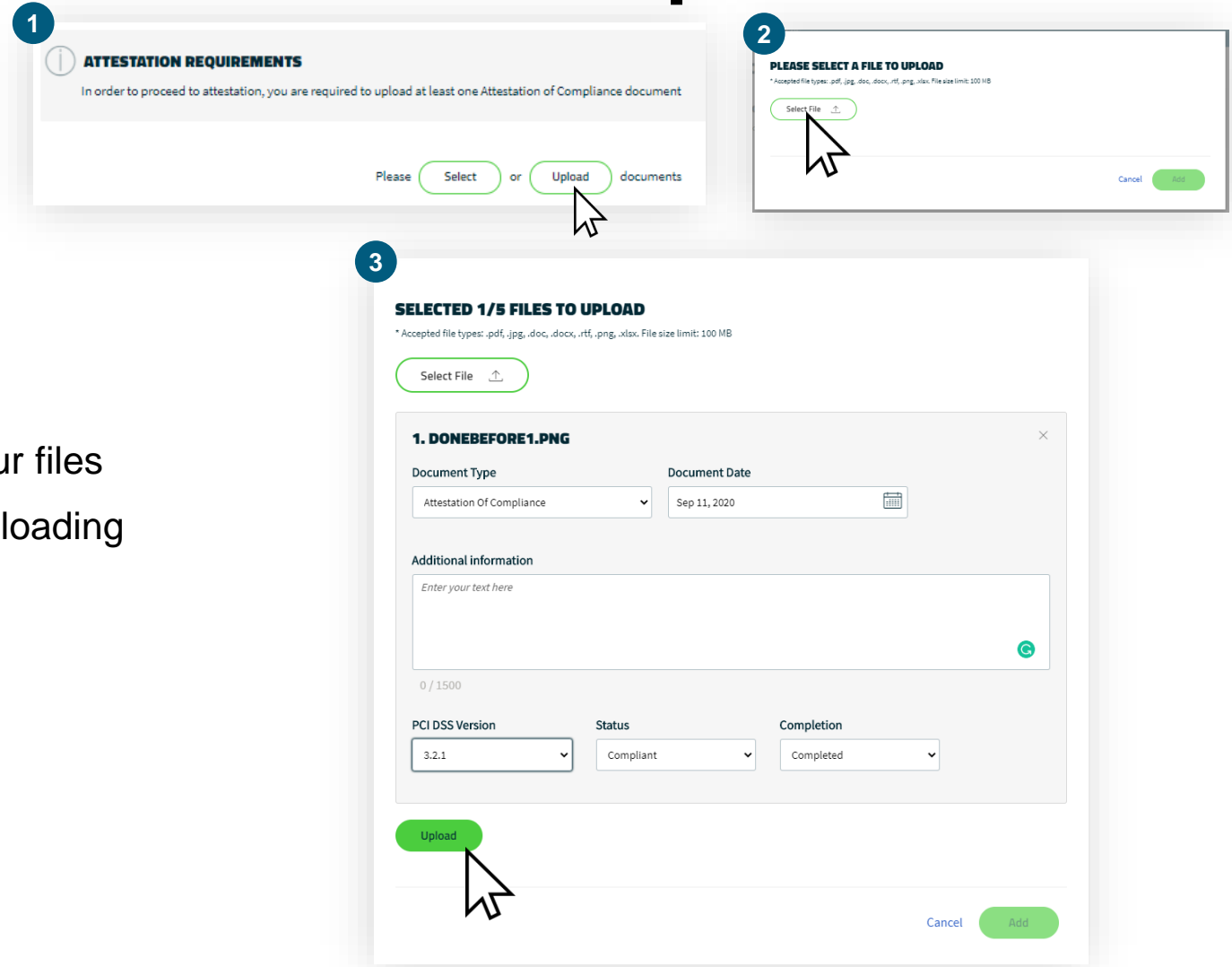
Assessment type: B Validation effective date: PCI DSS Version:

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



■ 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.

The screenshot illustrates the process of selecting an existing document for attestation. It is divided into three numbered steps:

- 1 ATTESTATION REQUIREMENTS**: A message states, "In order to proceed to attestation, you are required to upload at least one Attestation of Compliance document". Below this, the text "Please **Select** or **Upload** documents" is shown, with a mouse cursor pointing to the **Select** button.
- 2**: A table lists uploaded documents. The first row is selected with a green checkmark.

	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

Below the table, the text "Items: 1 / 1" is visible. A **Add** button is highlighted with a mouse cursor.
- 3 ATTESTATION OF COMPLIANCE**: A message states, "In order to proceed to attestation, you are required to upload at least one Attestation of Compliance document". Below this, the text "Please **Select** or **Upload** documents" is shown. A red box highlights a section titled "FILES TO BE INCLUDED IN ATTESTATION FORM:" which contains a table with the selected document:

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

Below this table, the text "Items: 1 / 1" is visible.

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

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

worldpay
from FIS