globalpayments

# PCI Portal

## Sysnet.air user guide – Merchant Role

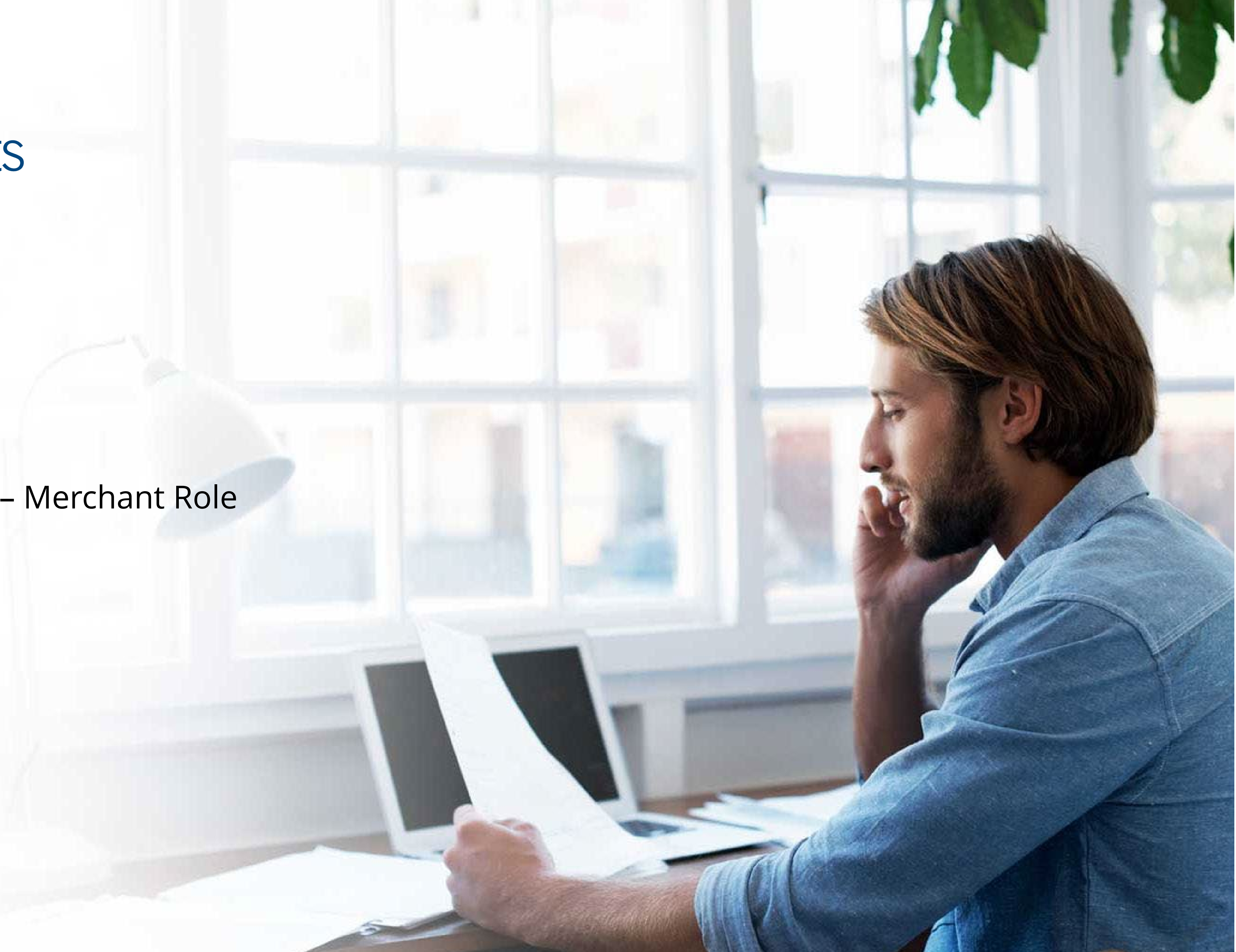


Table of contents

# 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

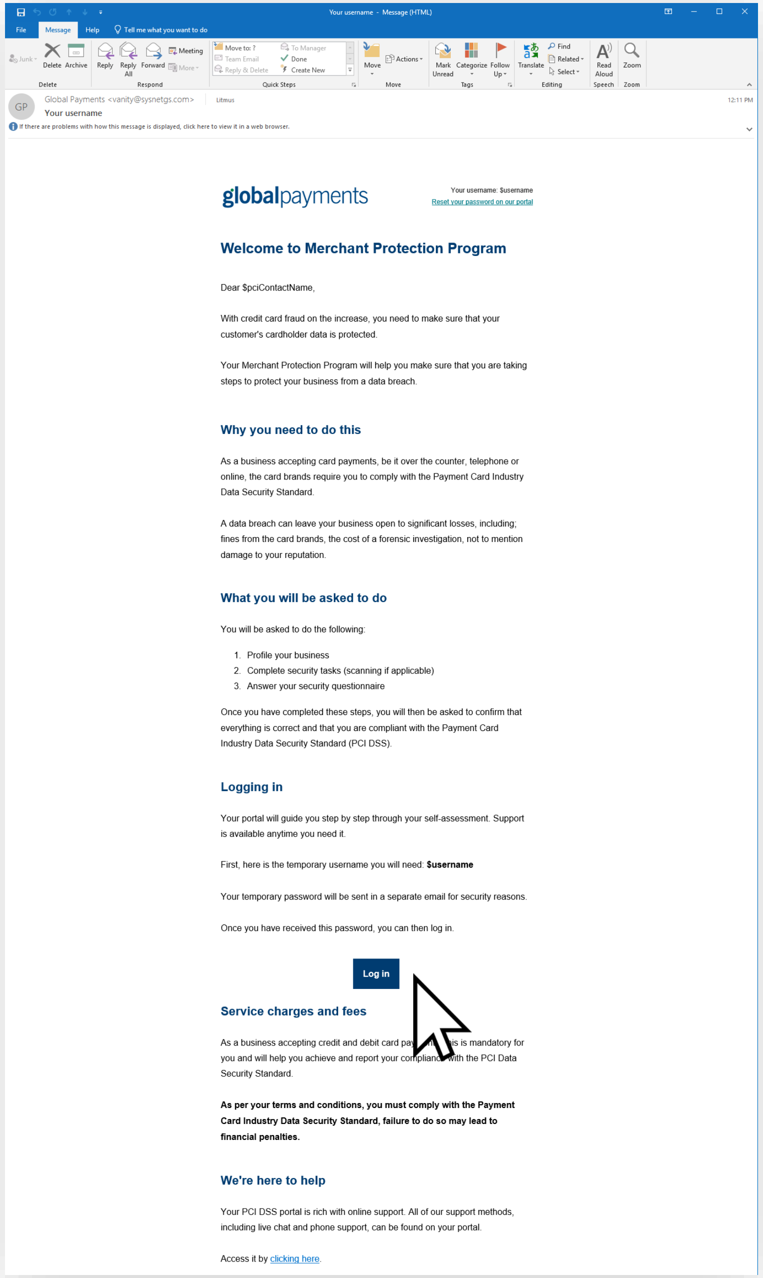
### Maintenance

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.



Global Payments <vanity@sysnetgs.com> Litmus 12:11 PM

Your username

If there are problems with how this message is displayed, click here to view it in a web browser.

globalpayments

Your username: $username

Reset your password on our portal

## Welcome to Merchant Protection Program

Dear $pciContactName,

With credit card fraud on the increase, you need to make sure that your customer's cardholder data is protected.

Your Merchant Protection Program will help you make sure that you are taking steps to protect your business from a data breach.

### Why you need to do this

As a business accepting card payments, be it over the counter, telephone or online, the card brands require you to comply with the Payment Card Industry Data Security Standard.

A data breach can leave your business open to significant losses, including; fines from the card brands, the cost of a forensic investigation, not to mention damage to your reputation.

### What you will be asked to do

You will be asked to do the following:

1. Profile your business
2. Complete security tasks (scanning if applicable)
3. Answer your security questionnaire

Once you have completed these steps, you will then be asked to confirm that everything is correct and that you are compliant with the Payment Card Industry Data Security Standard (PCI DSS).

### Logging in

Your portal will guide you step by step through your self-assessment. Support is available anytime you need it.

First, here is the temporary username you will need: **$username**

Your temporary password will be sent in a separate email for security reasons.

Once you have received this password, you can then log in.

### Service charges and fees

As a business accepting credit and debit card payments, this is mandatory for you and will help you achieve and report your compliance with the PCI Data Security Standard.

**As per your terms and conditions, you must comply with the Payment Card Industry Data Security Standard, failure to do so may lead to financial penalties.**

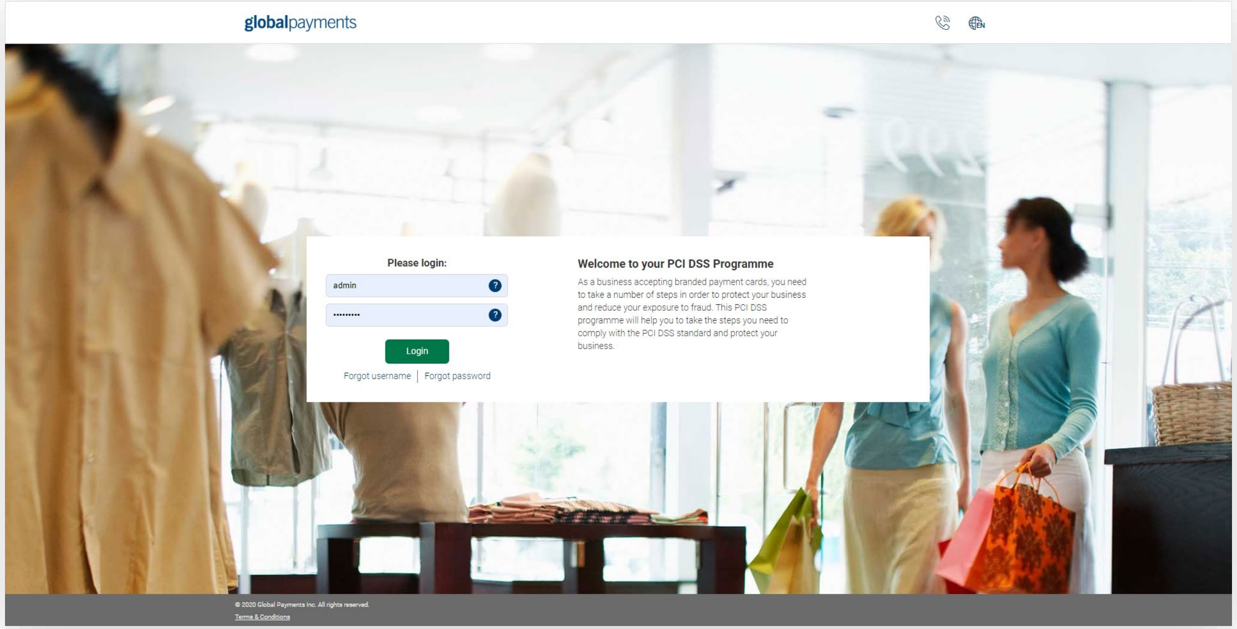
### We're here to help

Your PCI DSS portal is rich with online support. All of our support methods, including live chat and phone support, can be found on your portal.

Access it by clicking here.

# 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



globalpayments

Please login:

admin

••••••••••

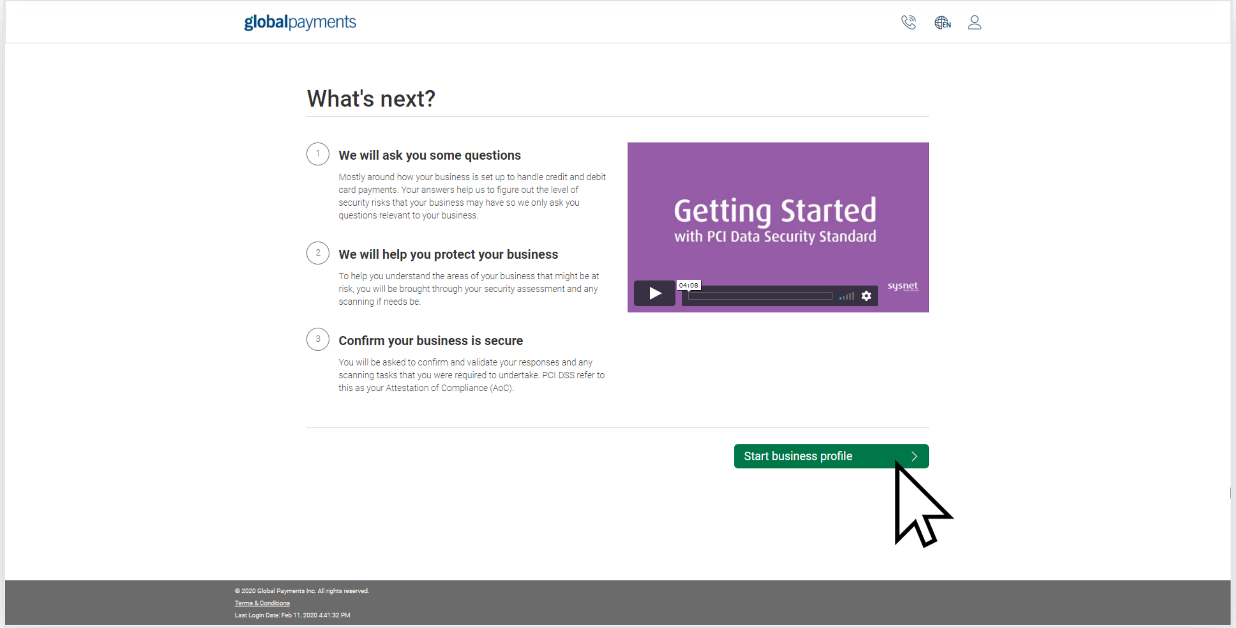
Login

Forgot username | Forgot password

Welcome to your PCI DSS Programme

As a business accepting branded payment cards, you need to take a number of steps in order to protect your business and reduce your exposure to fraud. This PCI DSS programme will help you to take the steps you need to comply with the PCI DSS standard and protect your business.

Terms & Conditions



globalpayments

What's next?

1. We will ask you some questions

   Mostly around how your business is set up to handle credit and debit card payments. Your answers help us to figure out the level of security risks that your business may have so we only ask you questions relevant to your business.

2. We will help you protect your business

   To help you understand the areas of your business that might be at risk, you will be brought through your security assessment and any scanning if needs be.

3. Confirm your business is secure

   You will be asked to confirm and validate your responses and any scanning tasks that you were required to undertake. PCI DSS refer to this as your Attestation of Compliance (AoC).

Start business profile >

Terms & Conditions

Last Login Date: Feb 11, 2020 4:41:32 PM

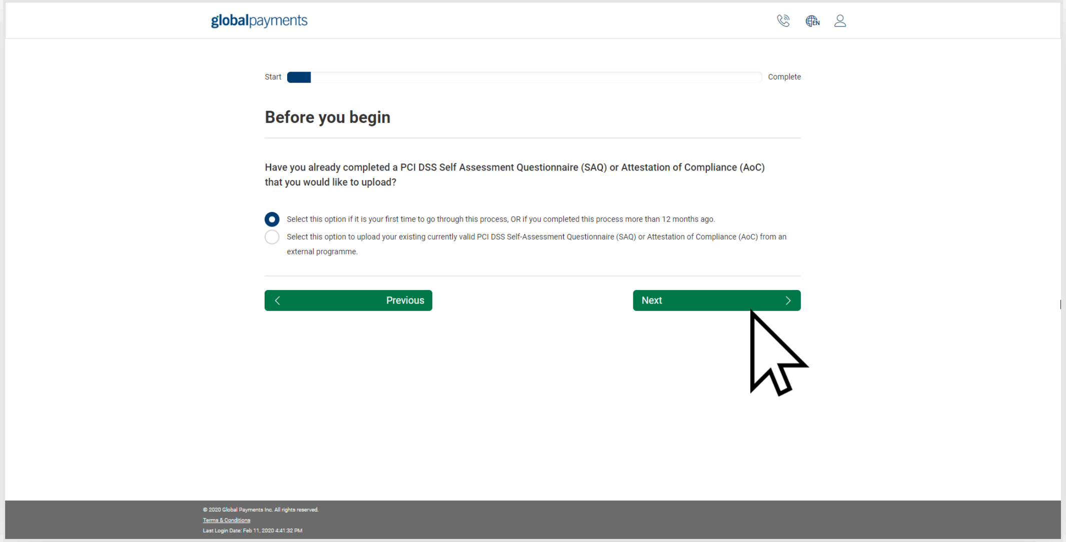
# First time use?

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.**

**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).**



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.

© 2020 Global Payments Inc. All rights reserved.
Terms & Conditions
Last Login Date: Feb 11, 2020 4:41:32 PM

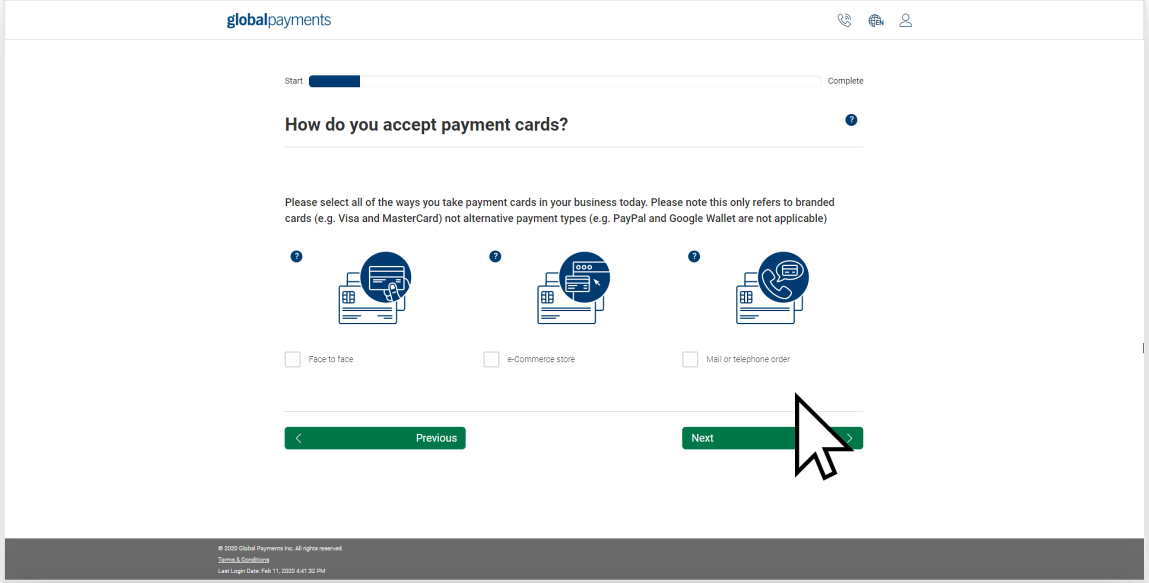
globalpayments

# Your Profile

How you accept payments

# 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 help icon.



How do you accept payment cards?

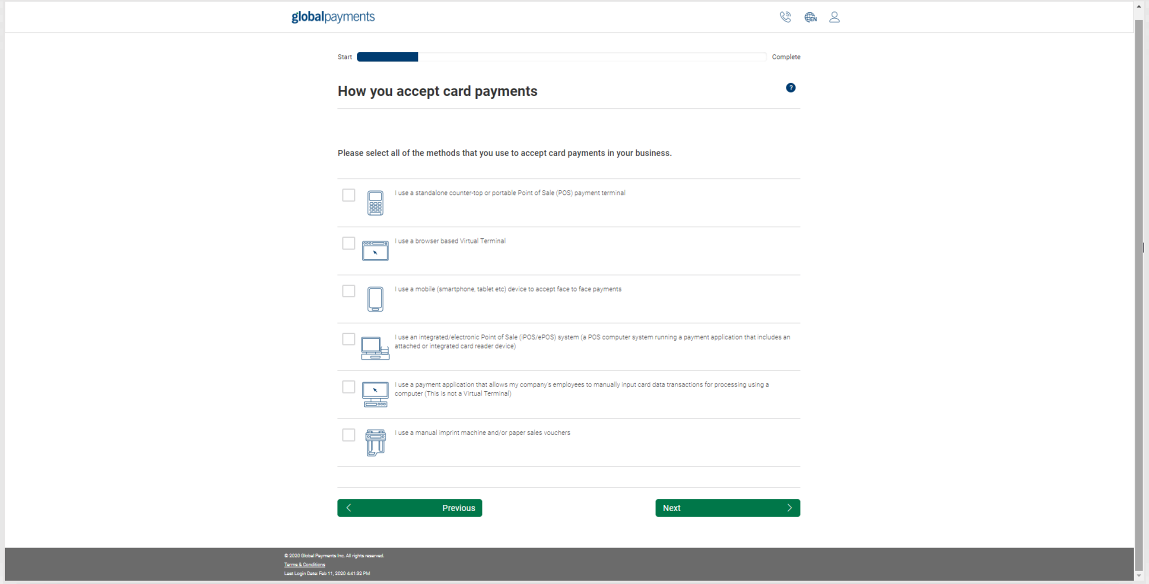
Please select all of the ways you take payment cards in your business today. Please note this only refers to branded cards (e.g. Visa and MasterCard) not alternative payment types (e.g. PayPal and Google Wallet are not applicable)

□ Face to face

□ e-Commerce store

□ Mail or telephone order

© 2020 Global Payments Inc. All rights reserved.
Terms & Conditions
Last Login Date: Feb 11, 2020 4:41:32 PM



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 (iPOS/ePOS) system (a POS computer system running a payment application that includes an attached or integrated card reader device)

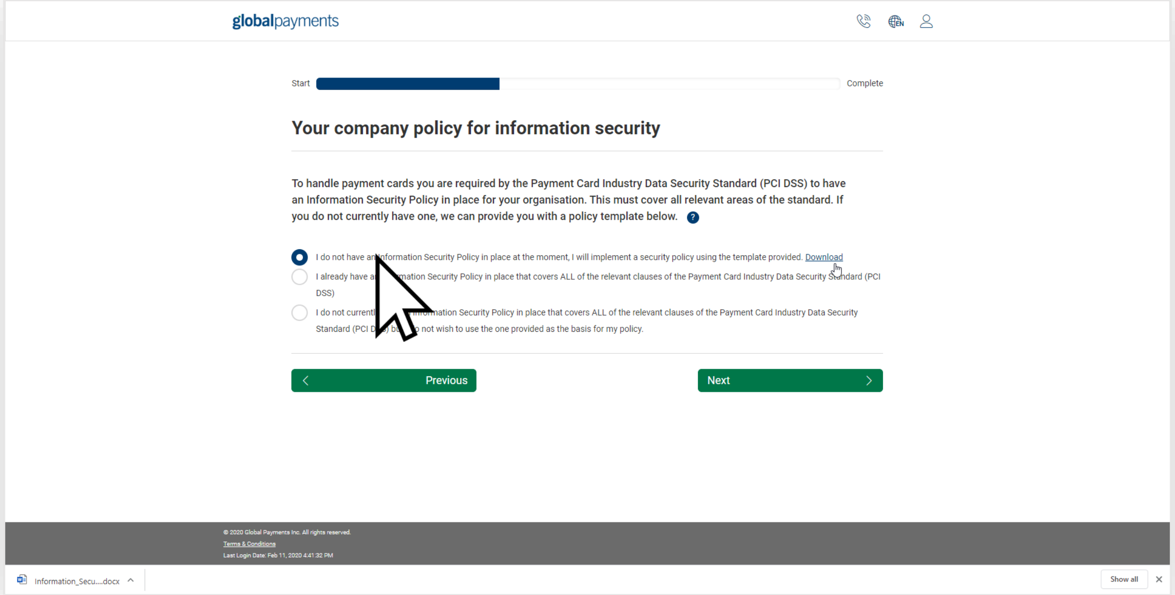
□ I use a payment application that allows my company's employees to manually input card data transactions for processing using a computer (This is not a Virtual Terminal)

□ I use a manual imprint machine and/or paper sales vouchers

© 2020 Global Payments Inc. All rights reserved.
Terms & Conditions
Last Login Date: Feb 11, 2020 4:41:32 PM

# 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



## 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 organisation. 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 [illegible]nformation Security Policy in place at the moment, I will implement a security policy using the template provided. Download

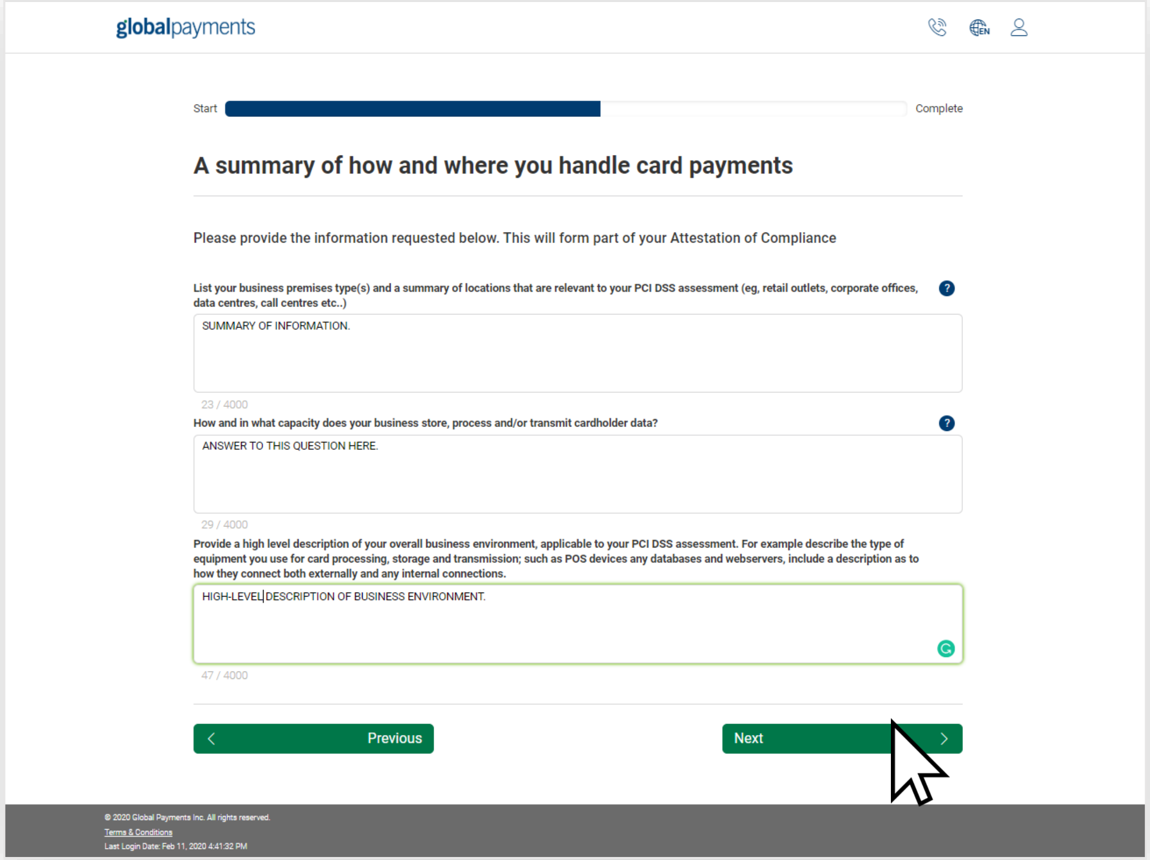
○ I already have a[illegible]mation Security Policy in place that covers ALL of the relevant clauses of the Payment Card Industry Data Security Standard (PCI DSS)

○ I do not currentl[illegible]mation Security Policy in place that covers ALL of the relevant clauses of the Payment Card Industry Data Security Standard (PCI D[illegible]) bu[illegible]o not wish to use the one provided as the basis for my policy.

© 2020 Global Payments Inc. All rights reserved.
Terms & Conditions
Last Login Date: Feb 11, 2020 4:41:32 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 help icon.



## A summary of how and where you handle card payments

Please provide the information requested below. This will form part of your Attestation of Compliance

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..) ?

SUMMARY OF INFORMATION.

23 / 4000

How and in what capacity does your business store, process and/or transmit cardholder data? ?

ANSWER TO THIS QUESTION HERE.

29 / 4000

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 webservers, include a description as to how they connect both externally and any internal connections.

HIGH-LEVEL DESCRIPTION OF BUSINESS ENVIRONMENT.

47 / 4000

© 2020 Global Payments Inc. All rights reserved.
Terms & Conditions
Last Login Date: Feb 11, 2020 4:41:32 PM

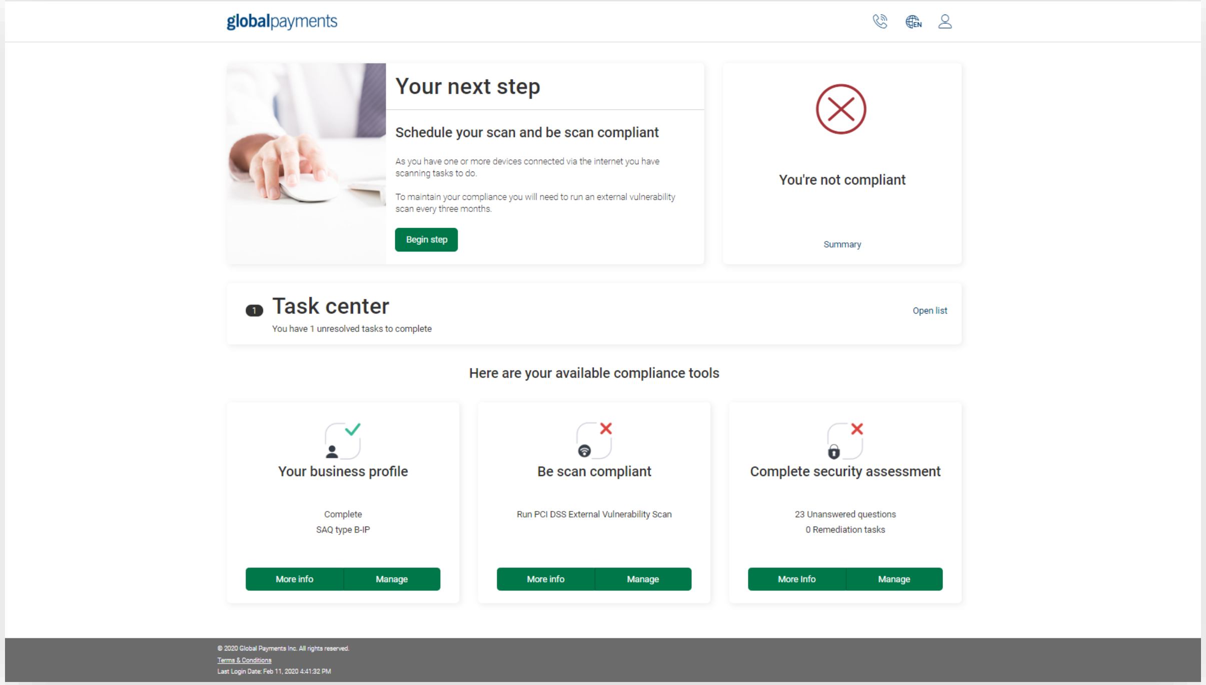
globalpayments

# Your dashboard

Profile complete

# Your dashboard

- 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 next step

Schedule your scan and be scan compliant

As you have one or more devices connected via the internet you have scanning tasks to do.

To maintain your compliance you will need to run an external vulnerability scan every three months.

You're not compliant

Task center

You have 1 unresolved tasks to complete

Here are your available compliance tools

Your business profile

Complete
SAQ type B-IP

Be scan compliant

Run PCI DSS External Vulnerability Scan

Complete security assessment

23 Unanswered questions
0 Remediation tasks

© 2020 Global Payments Inc. All rights reserved.
Terms & Conditions
Last Login Date: Feb 11, 2020 4:41:32 PM

See next page for a visual explanation

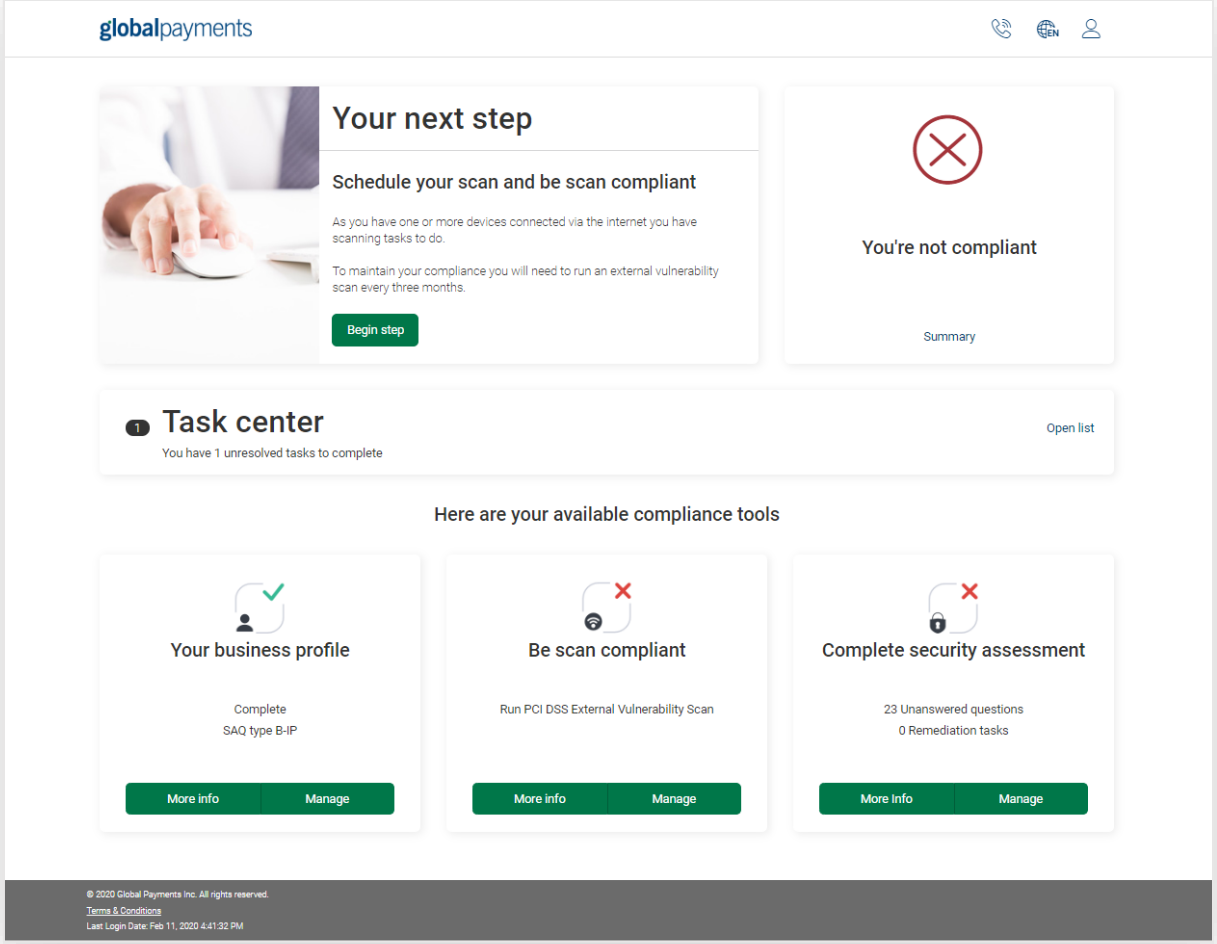
# Your dashboard

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.



## Your next step

**Schedule your scan and be scan compliant**

As you have one or more devices connected via the internet you have scanning tasks to do.

To maintain your compliance you will need to run an external vulnerability scan every three months.

You're not compliant

## Task center

You have 1 unresolved tasks to complete

Here are your available compliance tools

**Your business profile**

Complete
SAQ type B-IP

**Be scan compliant**

Run PCI DSS External Vulnerability Scan

**Complete security assessment**

23 Unanswered questions
0 Remediation tasks

Terms & Conditions

Last Login Date: Feb 11, 2020 4:41:32 PM

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'

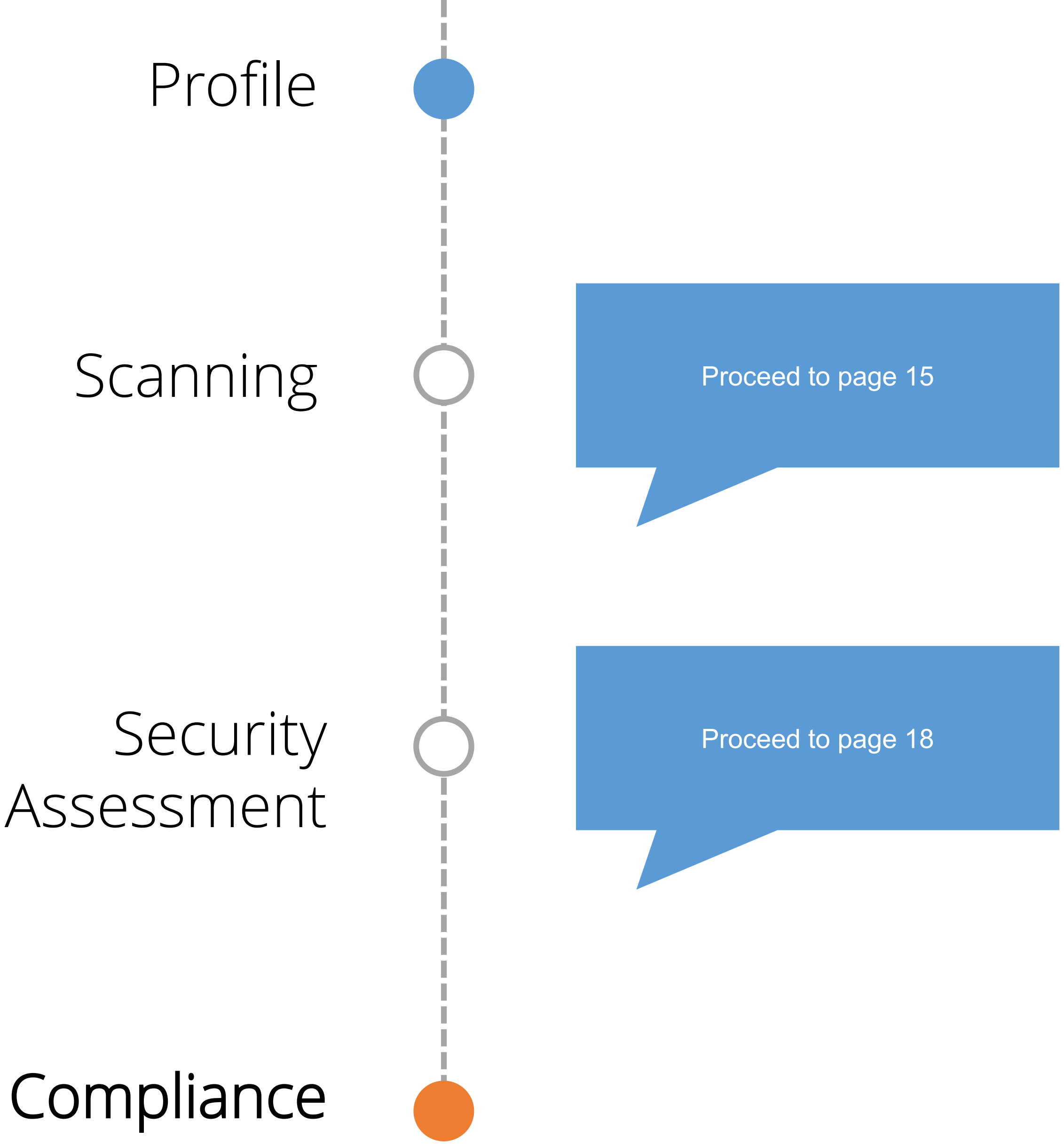
Next steps

## 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.



globalpayments

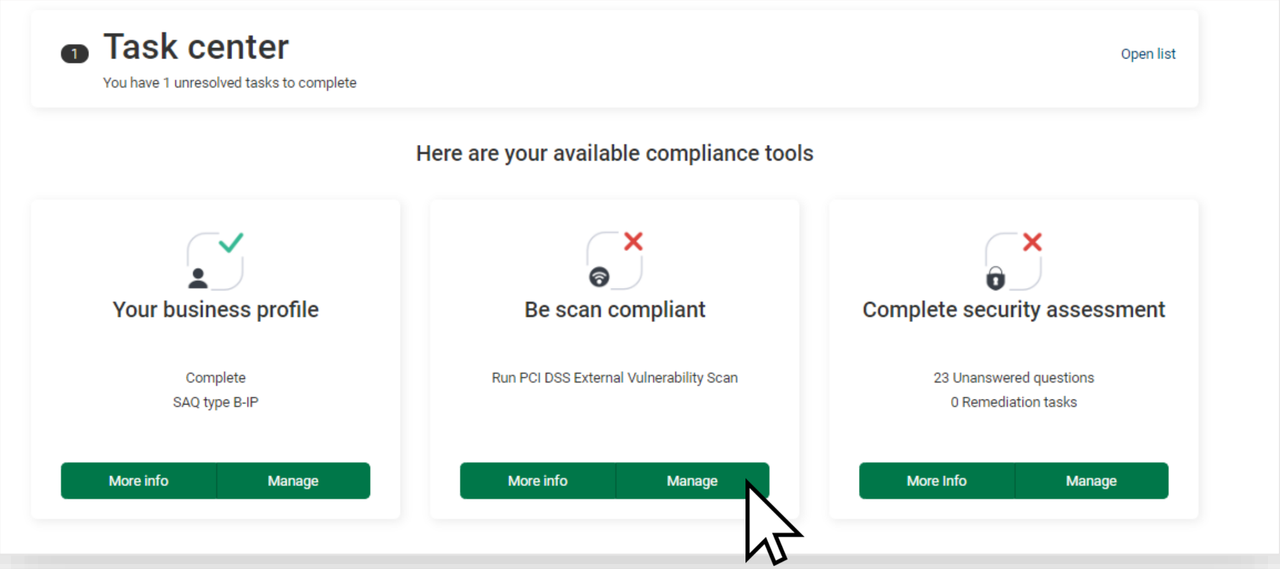
## External Vulnerability

Scanning

# Scanning

- From your dashboard, select ‘Manage’ on the ‘Be scan compliant’ widget.

- On the next page, select ‘Schedule scan’.



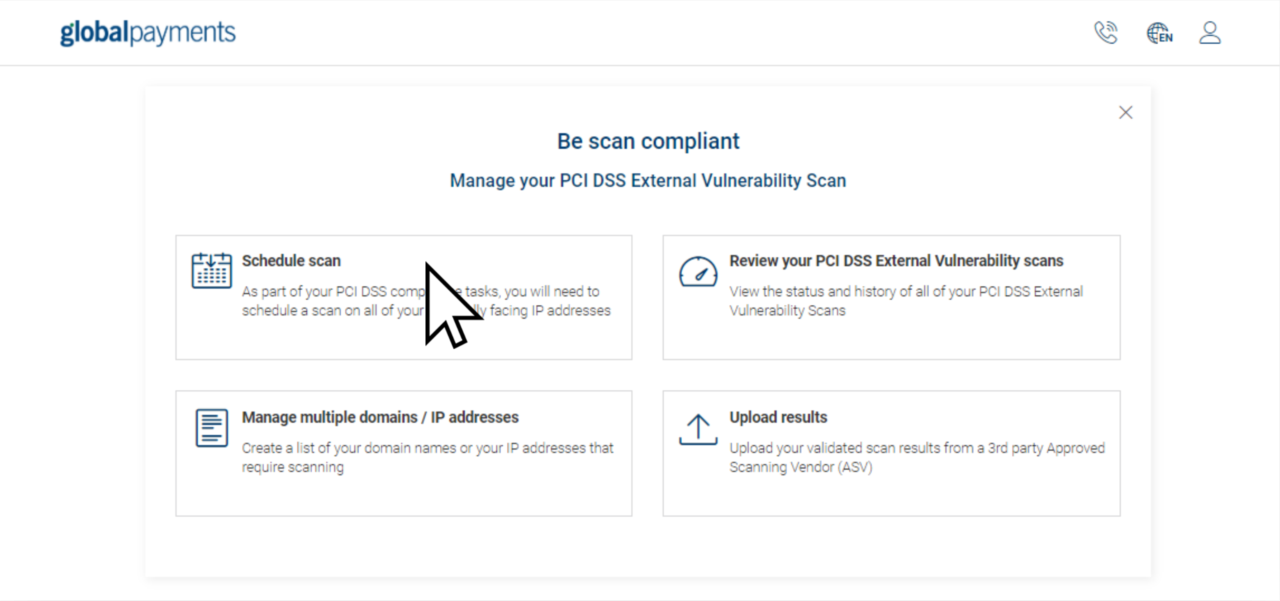
1 Task center

You have 1 unresolved tasks to complete

Open list

Here are your available compliance tools

| Your business profile | Be scan compliant | Complete security assessment |
|---|---|---|
| Complete<br>SAQ type B-IP | Run PCI DSS External Vulnerability Scan | 23 Unanswered questions<br>0 Remediation tasks |
| More info · Manage | More info · Manage | More Info · Manage |



Be scan compliant

Manage your PCI DSS External Vulnerability Scan

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

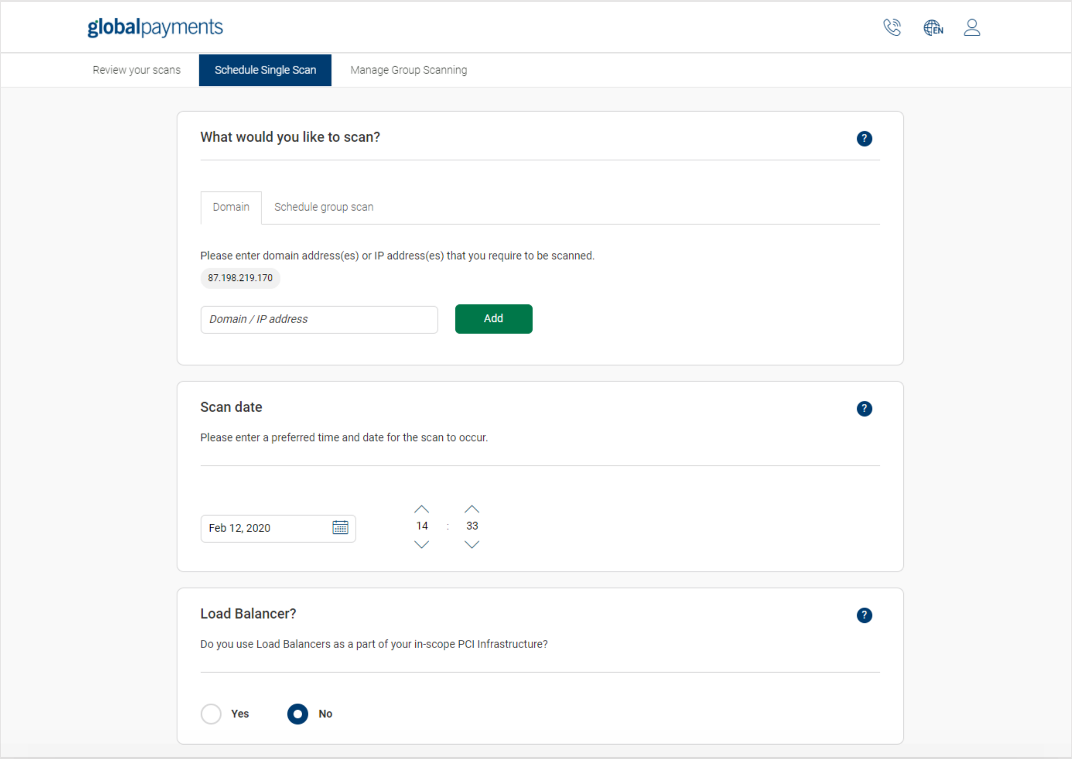
**Review your PCI DSS External Vulnerability scans**
View the status and history of all of your PCI DSS External Vulnerability Scans

**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



What would you like to scan?

Please enter domain address(es) or IP address(es) that you require to be scanned.

87.198.219.170

Scan date

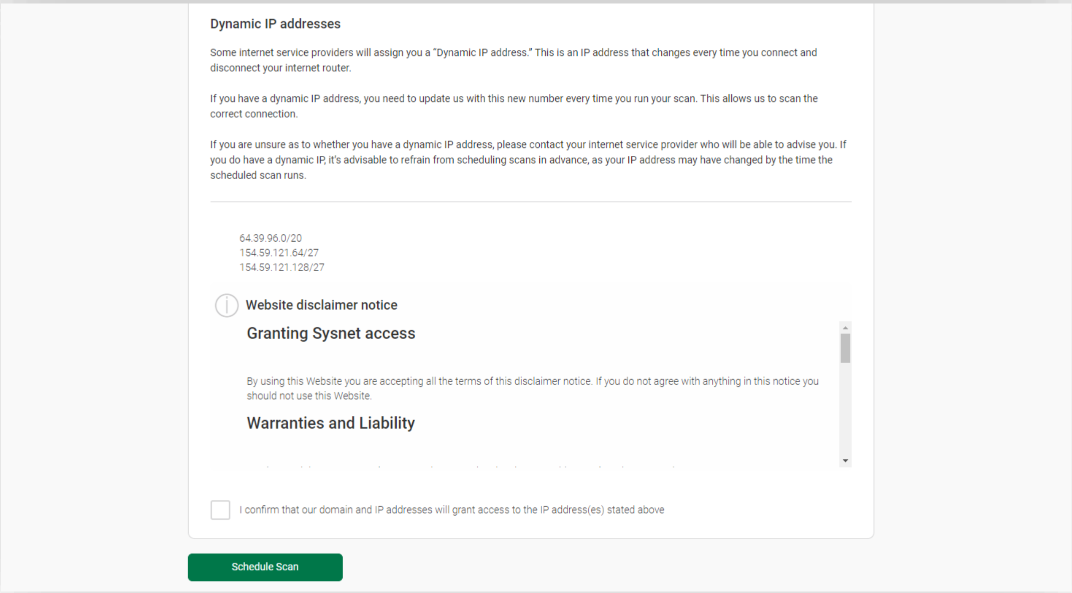
Please enter a preferred time and date for the scan to occur.

Feb 12, 2020 14 : 33

Load Balancer?

Do you use Load Balancers as a part of your in-scope PCI Infrastructure?

○ Yes ● No



Dynamic IP addresses

Some internet service providers will assign you a "Dynamic IP address." This is an IP address that changes every time you connect and disconnect your internet router.

If you have a dynamic IP address, you need to update us with this new number every time you run your scan. This allows us to scan the correct connection.

If you are unsure as to whether you have a dynamic IP address, please contact your internet service provider who will be able to advise you. If you do have a dynamic IP, it's advisable to refrain from scheduling scans in advance, as your IP address may have changed by the time the scheduled scan runs.

64.39.96.0/20
154.59.121.64/27
154.59.121.128/27

Website disclaimer notice

Granting Sysnet access

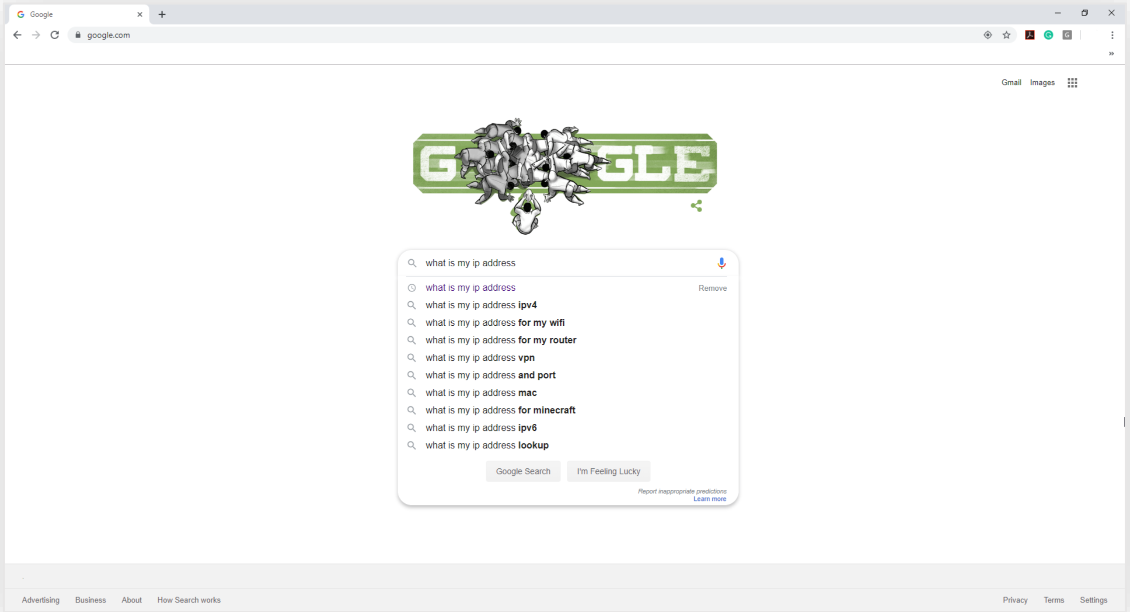
By using this Website you are accepting all the terms of this disclaimer notice. If you do not agree with anything in this notice you should not use this Website.

Warranties and Liability

□ I confirm that our domain and IP addresses will grant access to the IP address(es) stated above

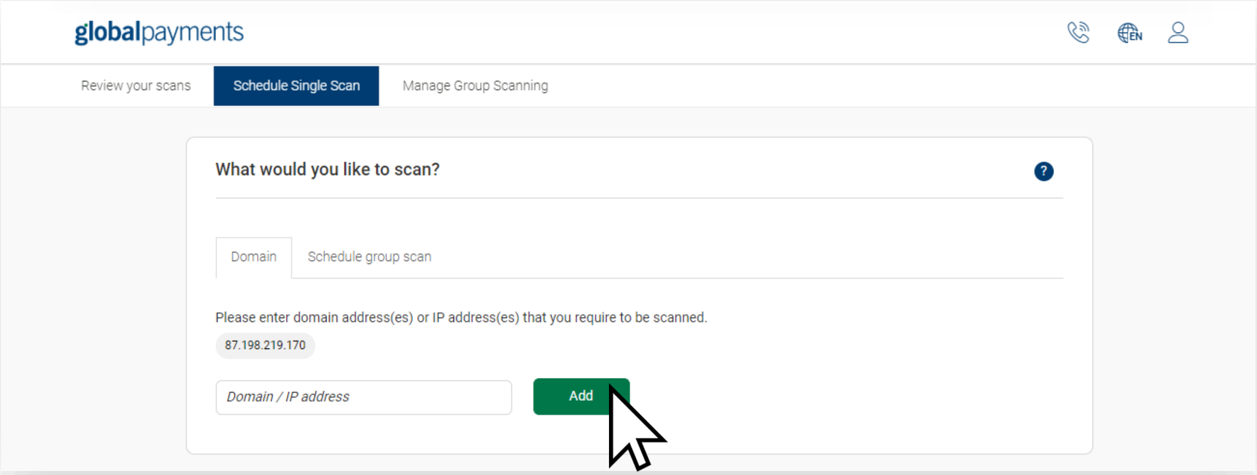
# Finding your IP Address

- **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



what is my ip address

Google
google.com
Gmail
Images
what is my ip address
Remove
what is my ip address ipv4
what is my ip address for my wifi
what is my ip address for my router
what is my ip address vpn
what is my ip address and port
what is my ip address mac
what is my ip address for minecraft
what is my ip address ipv6
what is my ip address lookup
Google Search
I'm Feeling Lucky
Report inappropriate predictions
Learn more
Advertising
Business
About
How Search works
Privacy
Terms
Settings



What would you like to scan?

Please enter domain address(es) or IP address(es) that you require to be scanned.

87.198.219.170

globalpayments

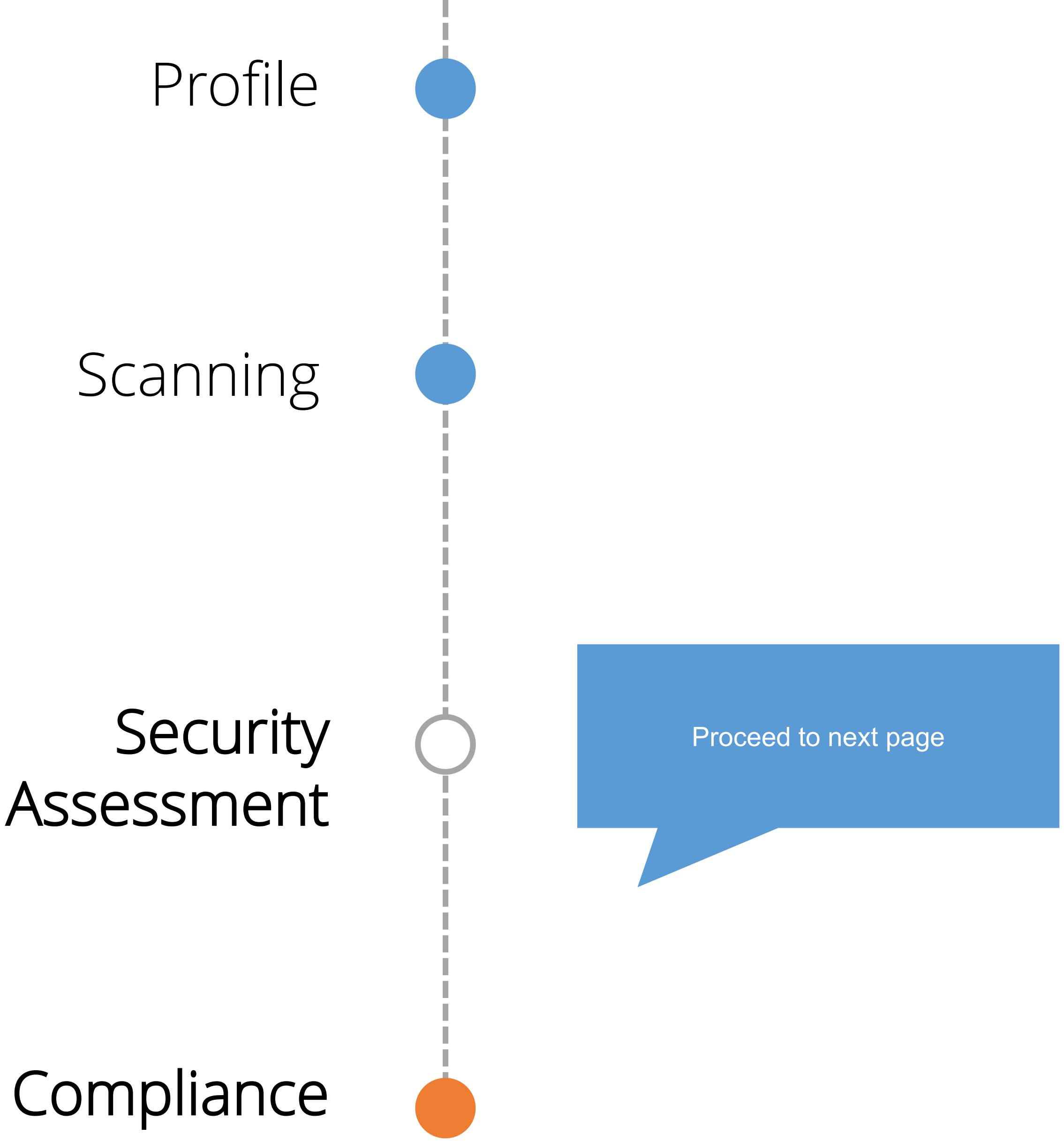
# Security assessment questionnaire

SAQ

# 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

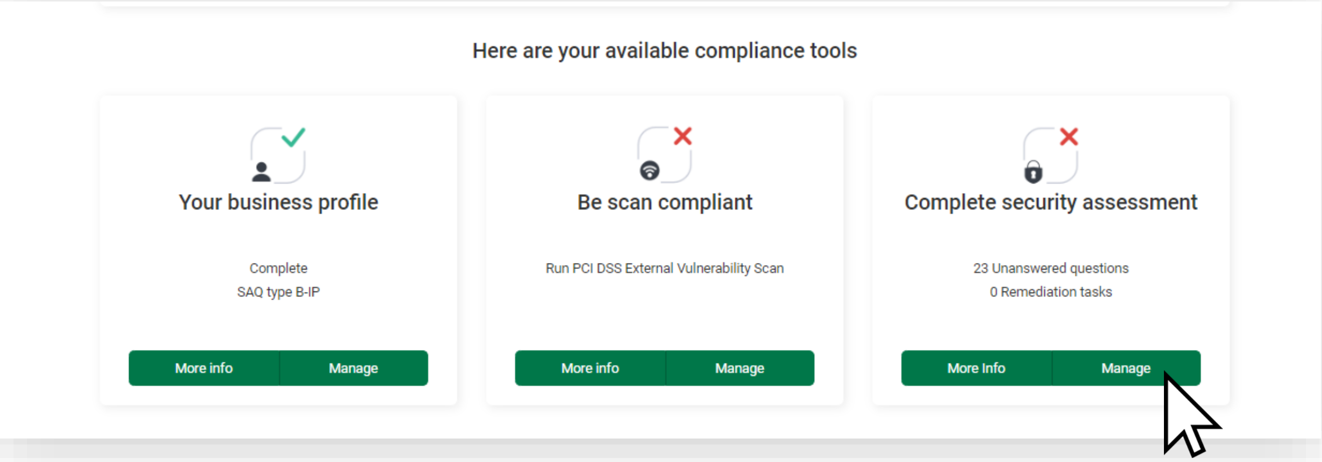
Compliance

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.



Here are your available compliance tools

Your business profile

Complete
SAQ type B-IP

Be scan compliant

Run PCI DSS External Vulnerability Scan

Complete security assessment

23 Unanswered questions
0 Remediation tasks

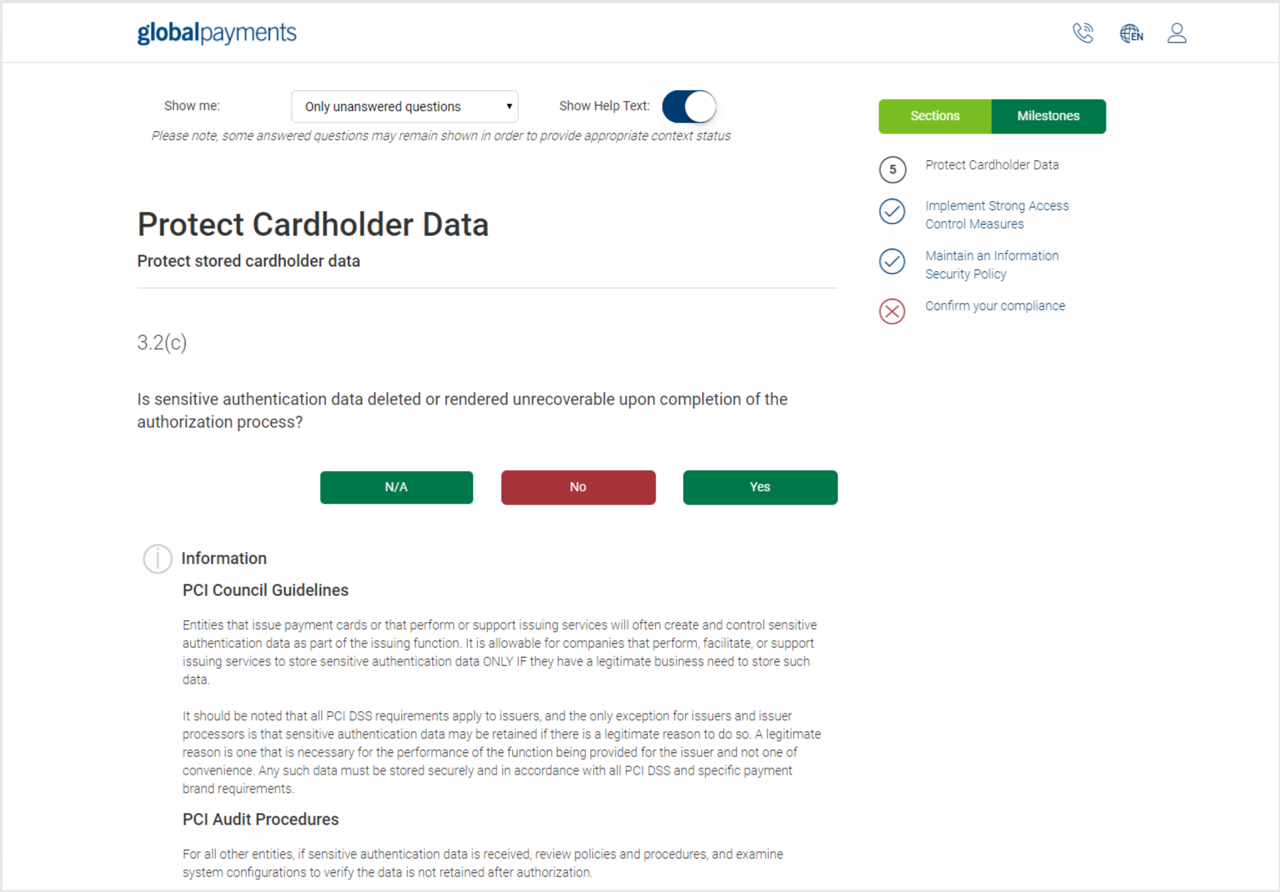
# Security Assessment Questionnaire (SAQ)

1

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

2

More information is available via the 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*

- 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?

**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

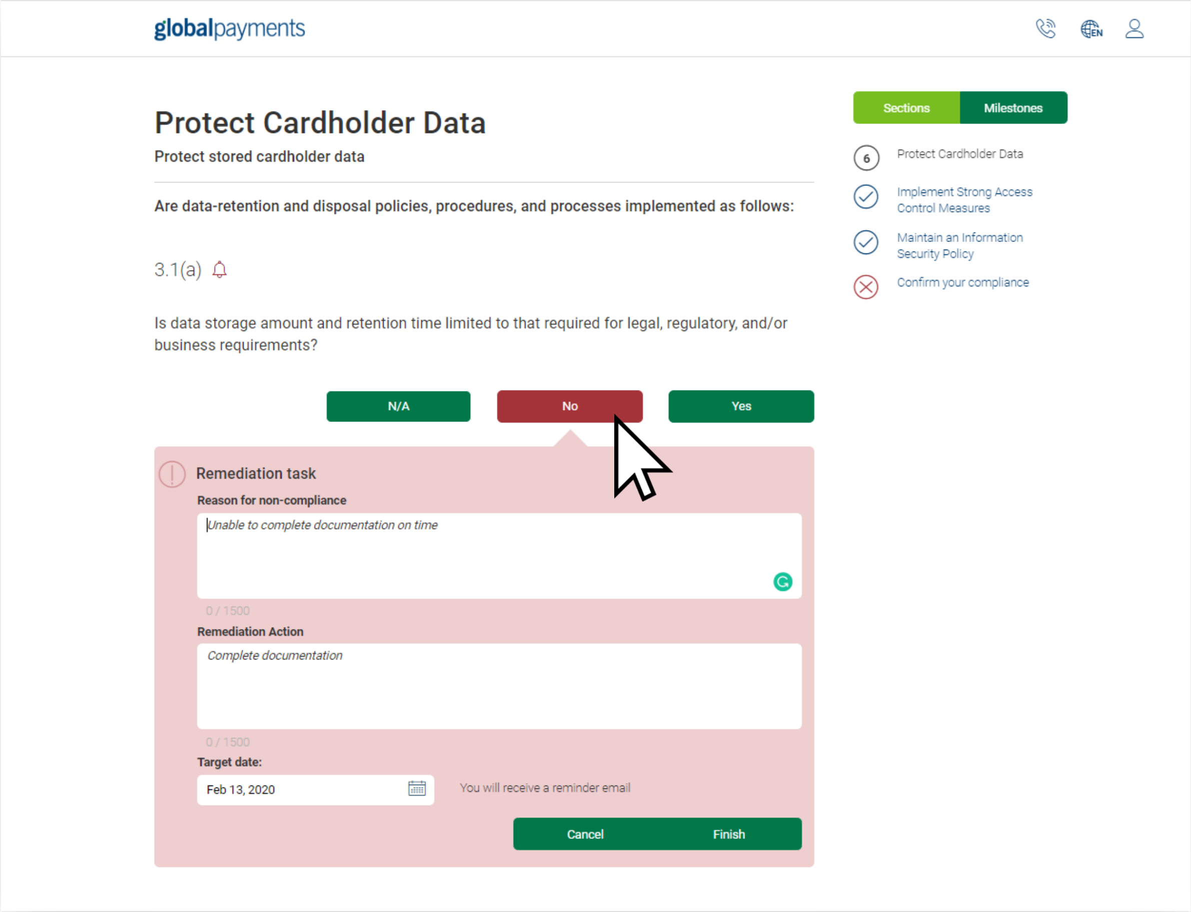
The box on the top right shows your progress through the questionnaire. Many of the questions will have been prepopulated for you based on your answers in the profile section. This greatly streamlines the process.

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.


globalpayments
Sections
Milestones
6 Protect Cardholder Data
Implement Strong Access Control Measures
Maintain an Information Security Policy
Confirm your compliance
N/A
No
Yes
Cancel
Finish

Protect Cardholder Data

Protect stored cardholder data

Are data-retention and disposal policies, procedures, and processes implemented as follows:

3.1(a)

Is data storage amount and retention time limited to that required for legal, regulatory, and/or business requirements?

Remediation task

Reason for non-compliance

*Unable to complete documentation on time*

0 / 1500

Remediation Action

*Complete documentation*

0 / 1500

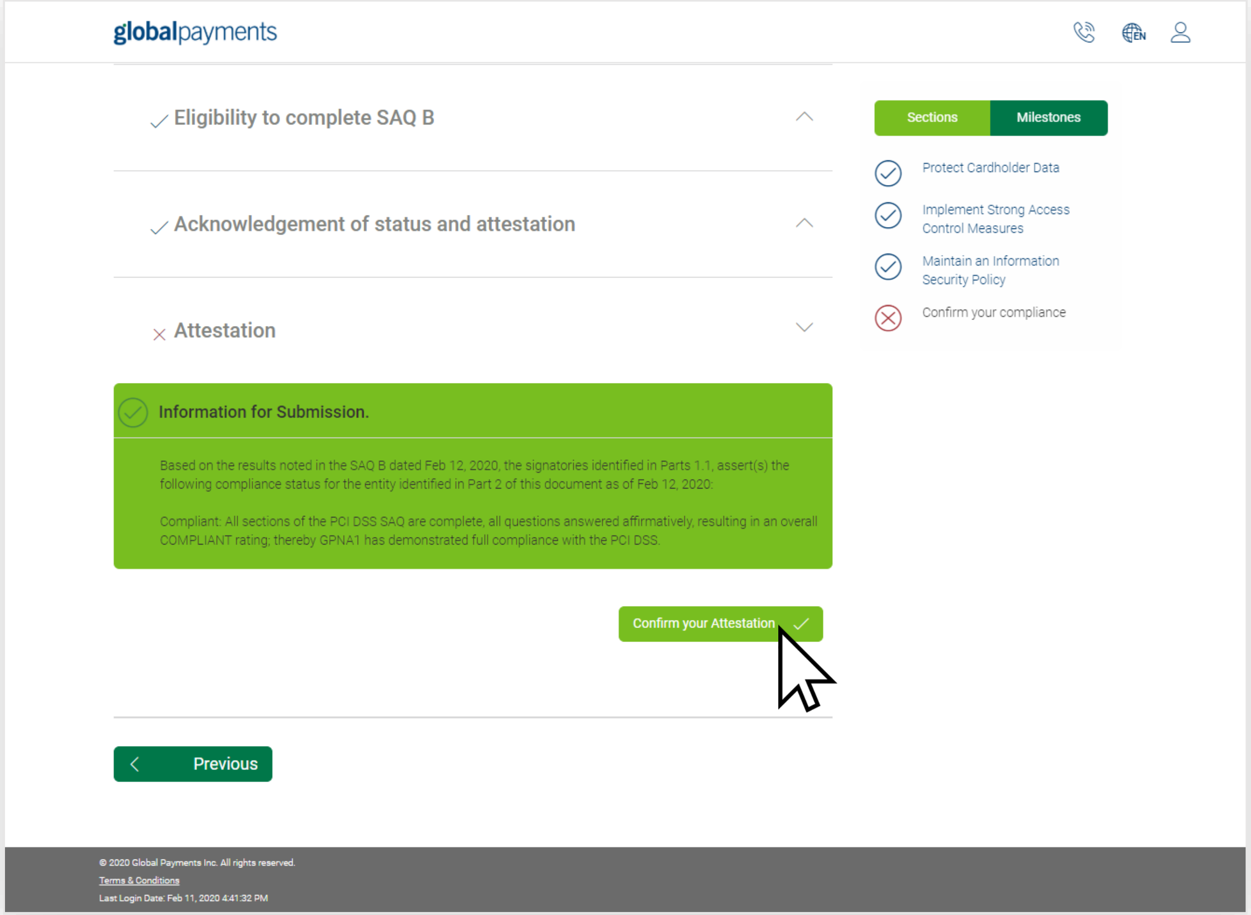
Target date:

Feb 13, 2020

You will receive a reminder email

# 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.


globalpayments
✓ Eligibility to complete SAQ B
✓ Acknowledgement of status and attestation
× Attestation
Sections
Milestones
Protect Cardholder Data
Implement Strong Access Control Measures
Maintain an Information Security Policy
Confirm your compliance
Confirm your Attestation ✓
Previous

Information for Submission.

Based on the results noted in the SAQ B dated Feb 12, 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 Feb 12, 2020:

Compliant: All sections of the PCI DSS SAQ are complete, all questions answered affirmatively, resulting in an overall COMPLIANT rating; thereby GPNA1 has demonstrated full compliance with the PCI DSS.

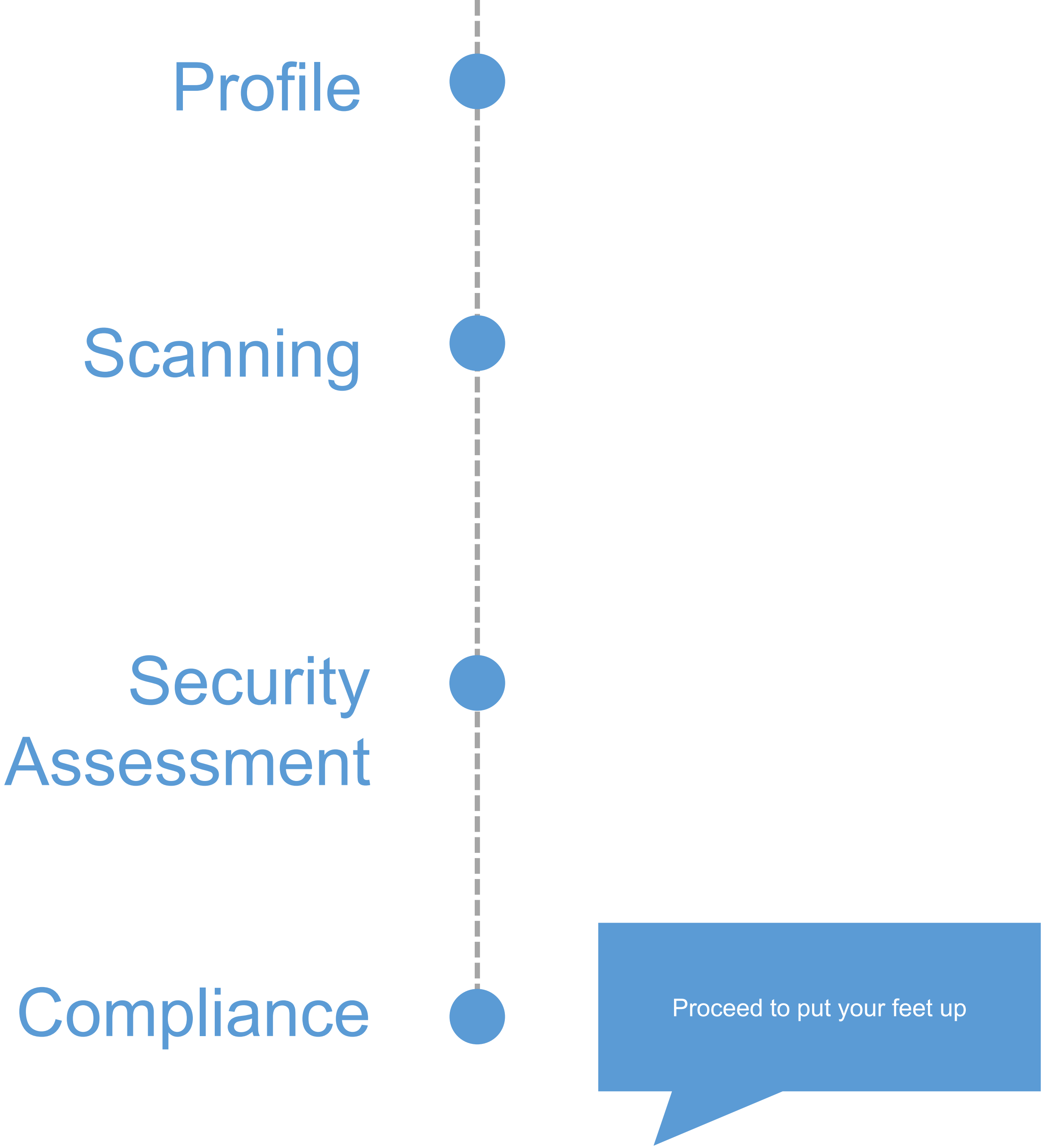
© 2020 Global Payments Inc. All rights reserved.
Terms & Conditions
Last Login Date: Feb 11, 2020 4:41:32 PM

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.



Profile

Scanning

Security Assessment

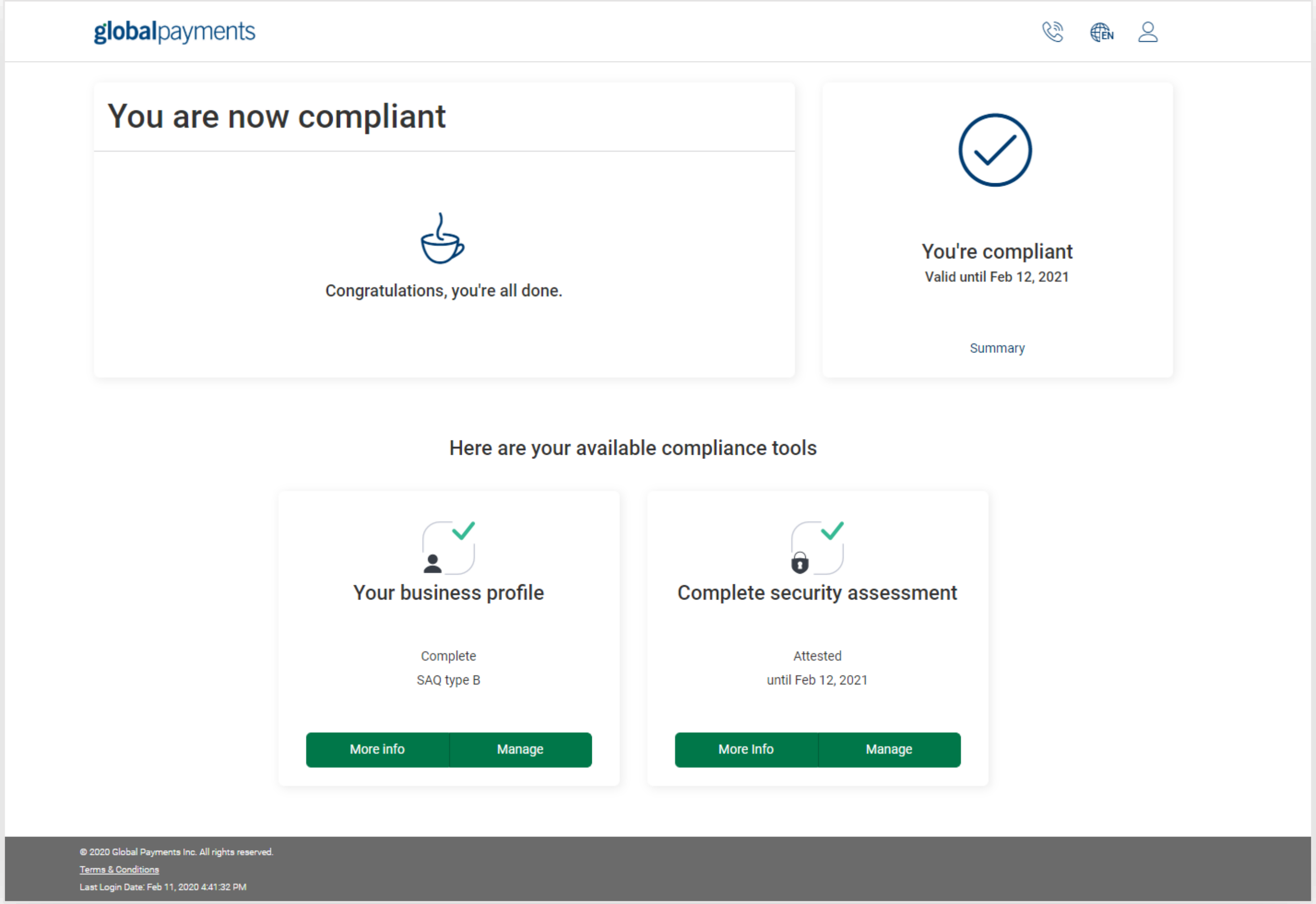
Compliance

Proceed to put your feet up

# You're done for now

1

Your dashboard should have green ticks across the board



## You are now compliant

Congratulations, you're all done.

You're compliant
Valid until Feb 12, 2021

Summary

Here are your available compliance tools

Your business profile

Complete
SAQ type B

Complete security assessment

Attested
until Feb 12, 2021

Terms & Conditions
Last Login Date: Feb 11, 2020 4:41:32 PM

2

Your revalidation date is displayed in the top right corner

globalpayments

# Maintaining compliance

Throughout the year

# Maintaining your compliance

**It's important to maintain your compliance throughout the year by:**

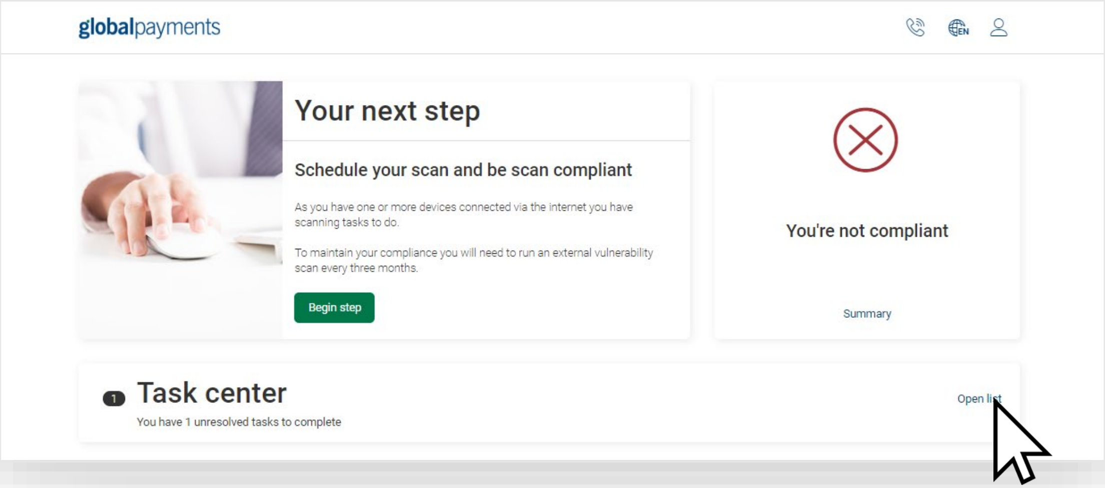
- Making sure you do all of the things you said you did in your assessment
- Applying your Information Security Policy and keeping it up to date

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, log in to your portal.

What you need to do will be outlined on your dashboard under 'Task Center'.



Your next step

Schedule your scan and be scan compliant

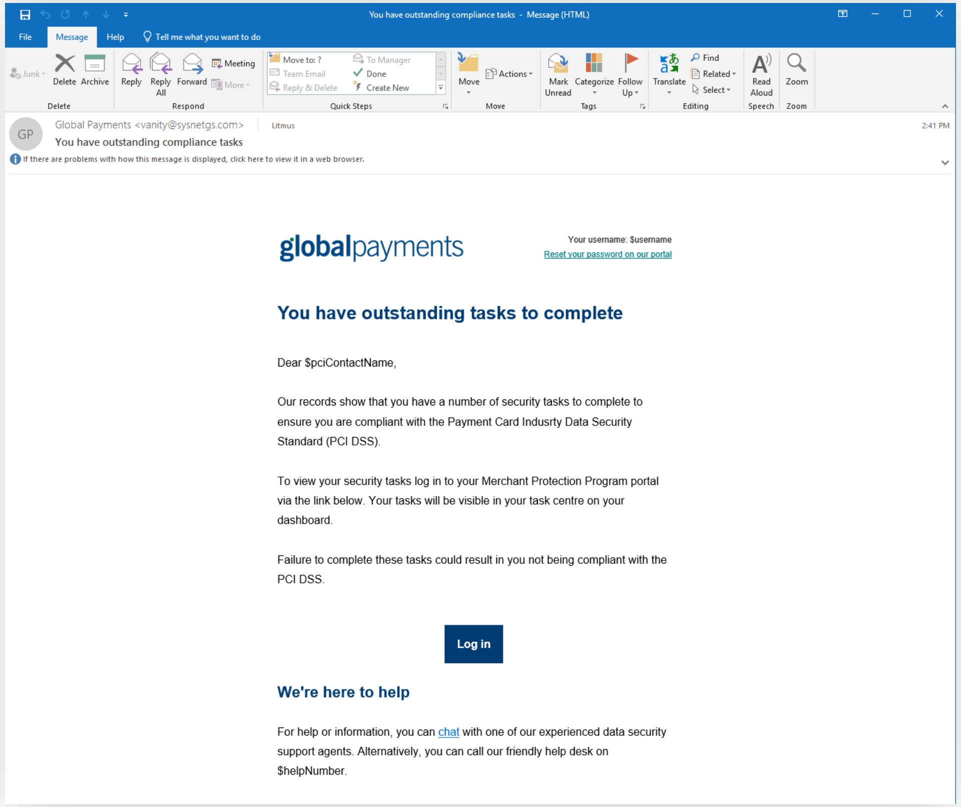
As you have one or more devices connected via the internet you have scanning tasks to do.

To maintain your compliance you will need to run an external vulnerability scan every three months.

You're not compliant

1 Task center

You have 1 unresolved tasks to complete



Global Payments <vanity@sysnetgs.com>

2:41 PM

You have outstanding compliance tasks

If there are problems with how this message is displayed, click here to view it in a web browser.

Your username: $username
Reset your password on our portal

You have outstanding tasks to complete

Dear $pciContactName,

Our records show that you have a number of security tasks to complete to ensure you are compliant with the Payment Card Indusrty Data Security Standard (PCI DSS).

To view your security tasks log in to your Merchant Protection Program portal via the link below. Your tasks will be visible in your task centre on your dashboard.

Failure to complete these tasks could result in you not being compliant with the PCI DSS.

We're here to help

For help or information, you can chat with one of our experienced data security support agents. Alternatively, you can call our friendly help desk on $helpNumber.

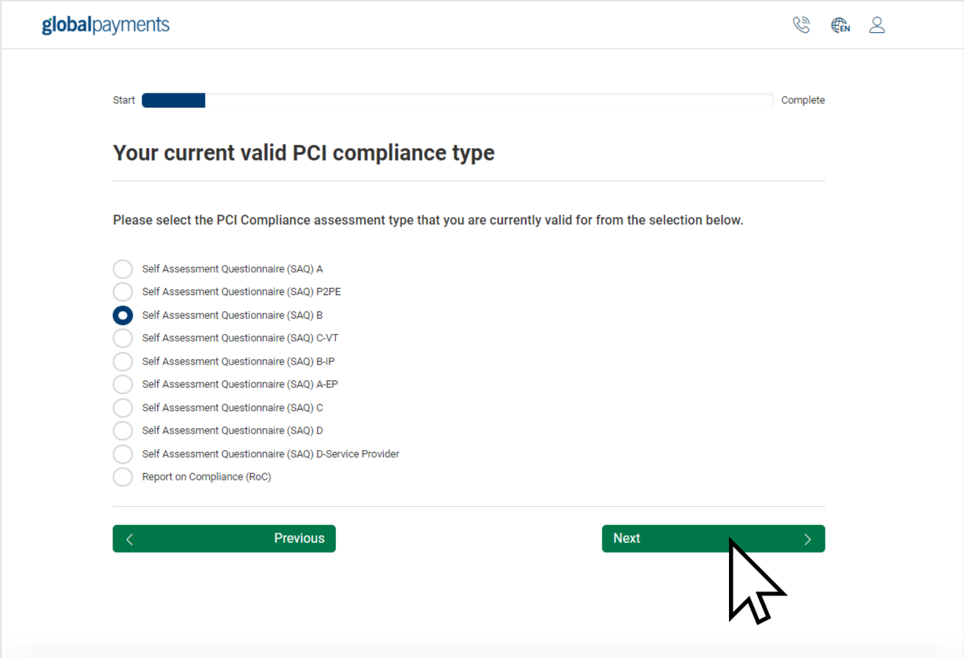
globalpayments

## Uploading an existing attestation

Already have a valid Attestation of Compliance?

# Uploading existing Attestation of Compliance

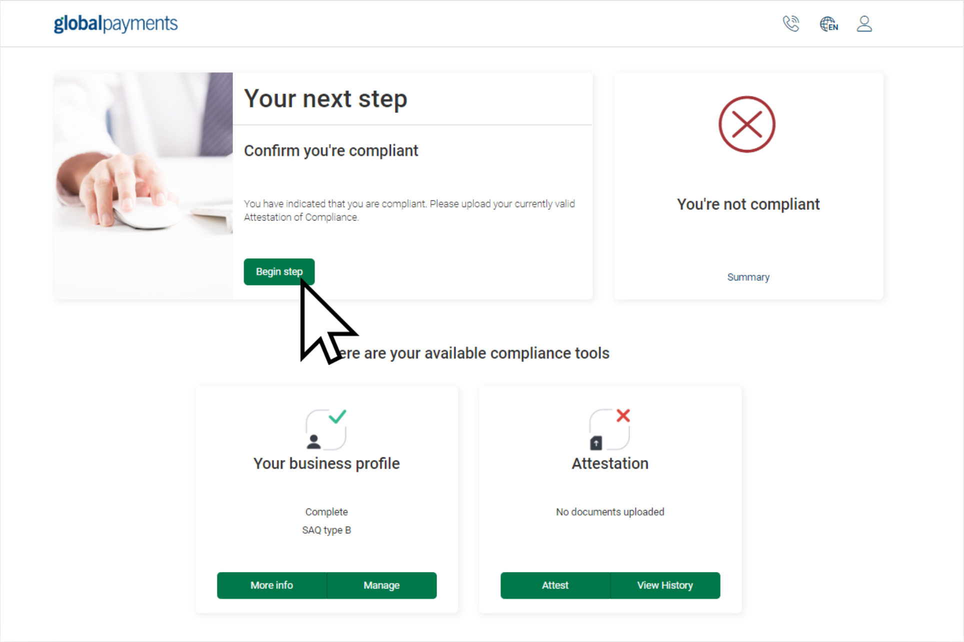
- **If you select that you have an existing attestation of compliance, you will then be asked two questions:**
  - The PCI Compliance assessment type of your business. You can find this on your **existing** certificate.
  - You'll also need to confirm if you use a third party to store or process card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



## 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
○ Self Assessment Questionnaire (SAQ) D-Service Provider
○ Report on Compliance (RoC)



Your next step

Confirm you're compliant

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

You're not compliant

ere are your available compliance tools

Your business profile

Complete
SAQ type B

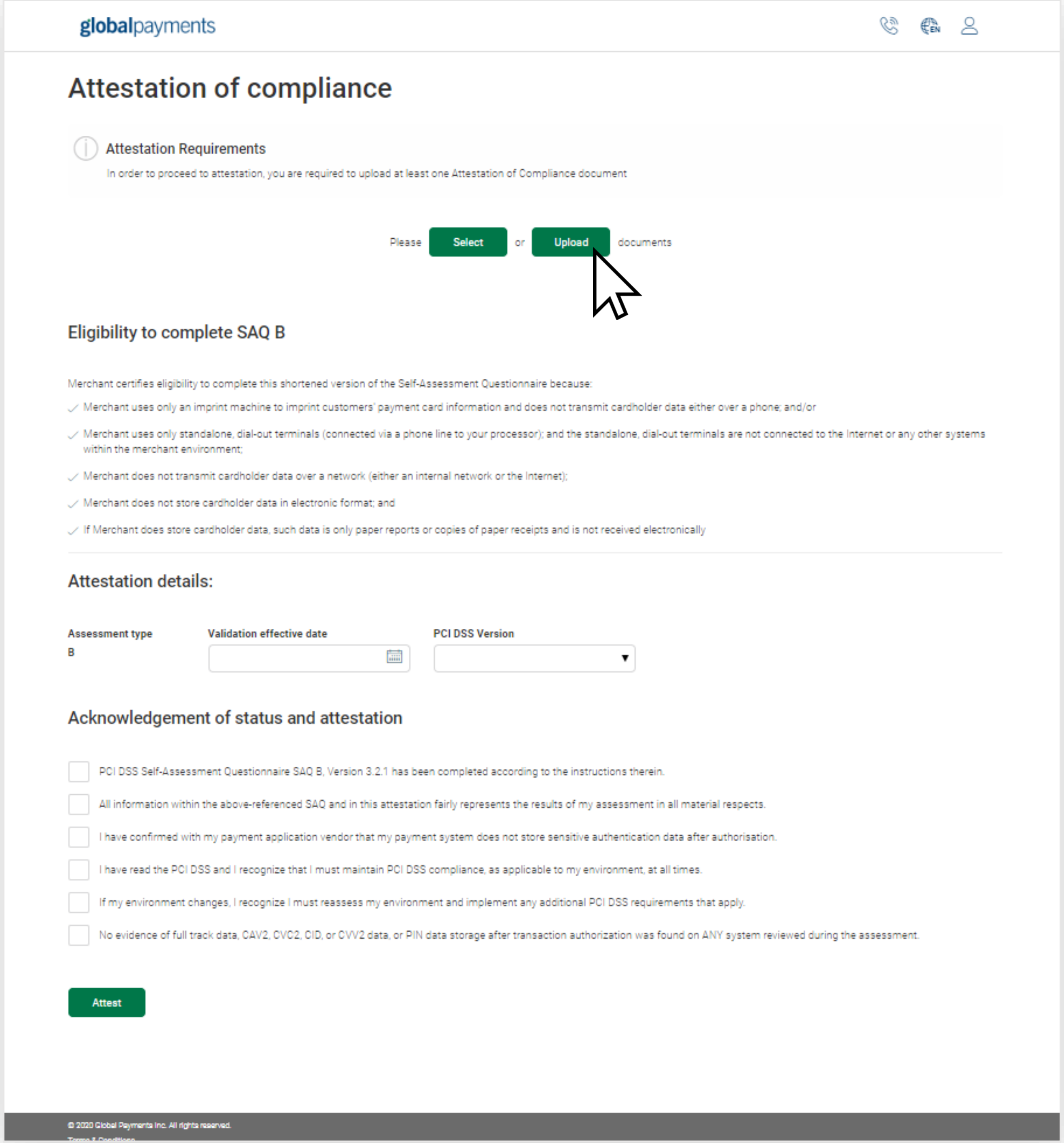
Attestation

No documents uploaded

# 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 | Validation effective date | PCI DSS Version |
|---|---|---|
| B | | |

### 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.

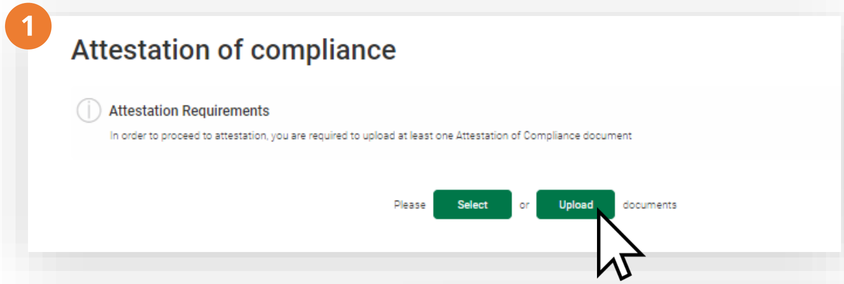
□ No evidence of full track data, CAV2, CVC2, CID, or CVV2 data, or PIN data storage after transaction authorization was found on ANY system reviewed during the assessment.

Terms & Conditions

# 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’

1



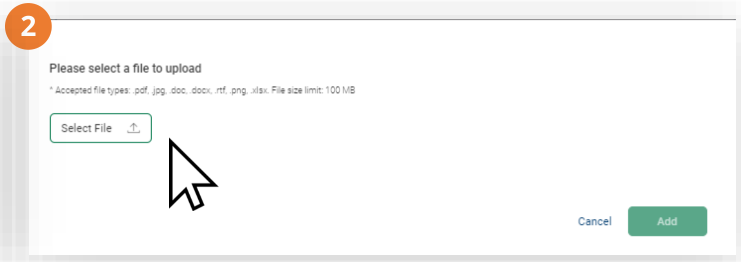
Attestation of compliance

Attestation Requirements

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

Please Select or Upload documents

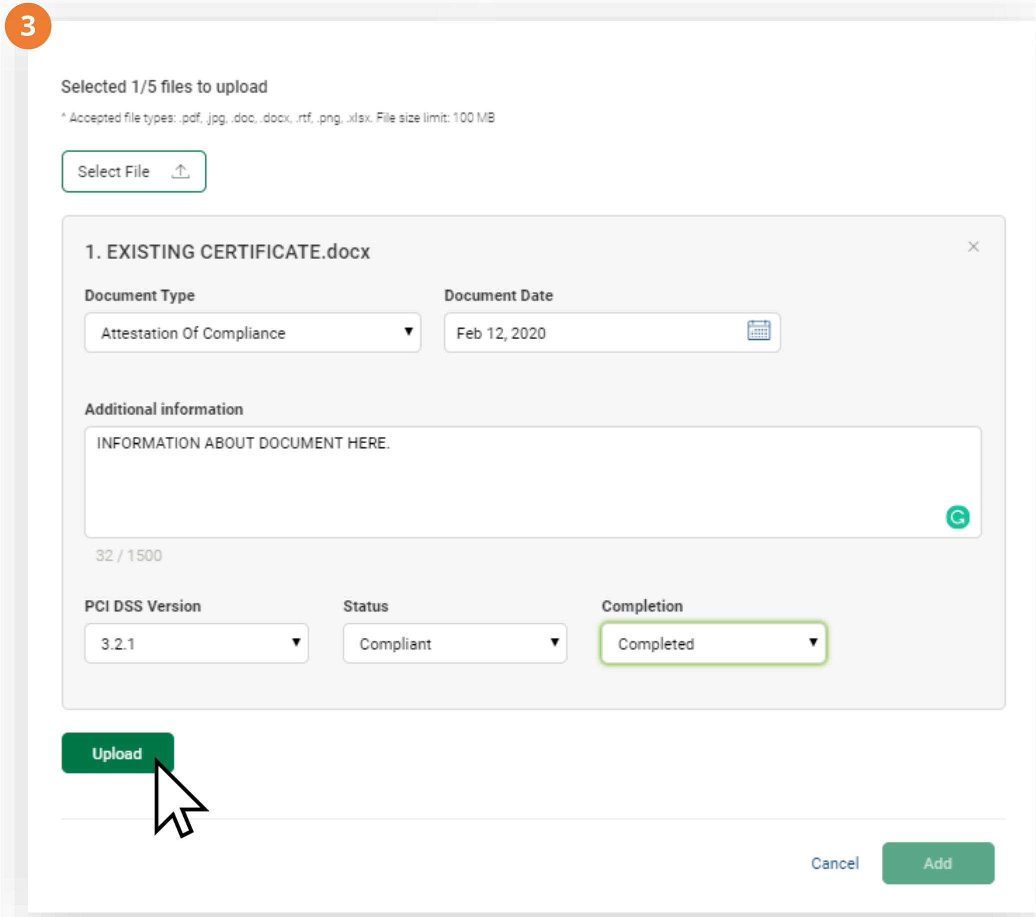
2



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. EXISTING CERTIFICATE.docx

Document Type: Attestation Of Compliance

Document Date: Feb 12, 2020

Additional information: INFORMATION ABOUT DOCUMENT HERE.

32 / 1500

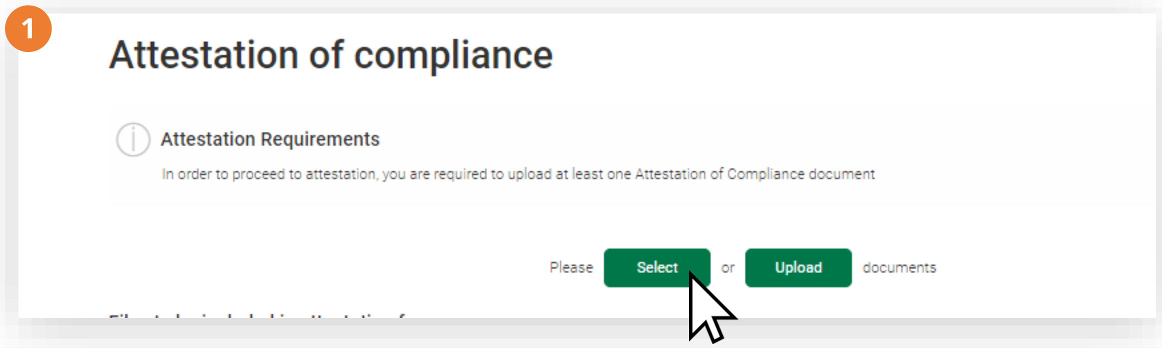
PCI DSS Version: 3.2.1

Status: Compliant

Completion: Completed

# Uploading existing Attestation of Compliance

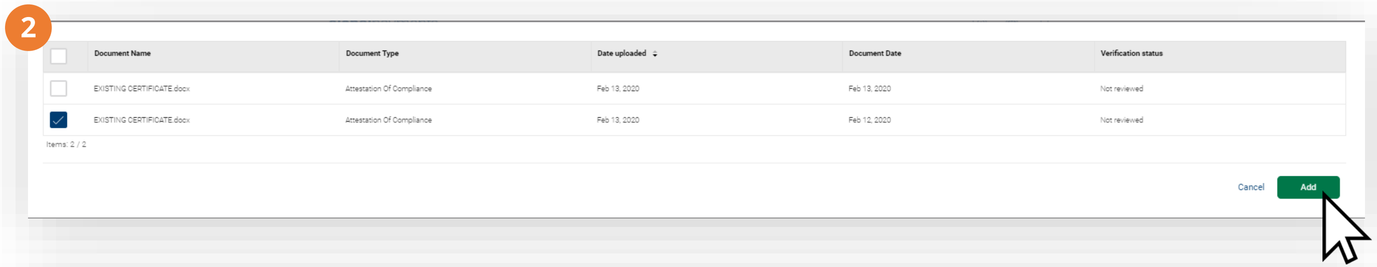
- **Select from your uploaded documents to attach to the attestation**
    - Click ‘Select’ from the main screen
    - From the list of uploaded documents, select the ones you wish to attach to this attestation. Click ‘Add’
    - The documents you wish to include will now appear on the main screen


1

## Attestation of compliance

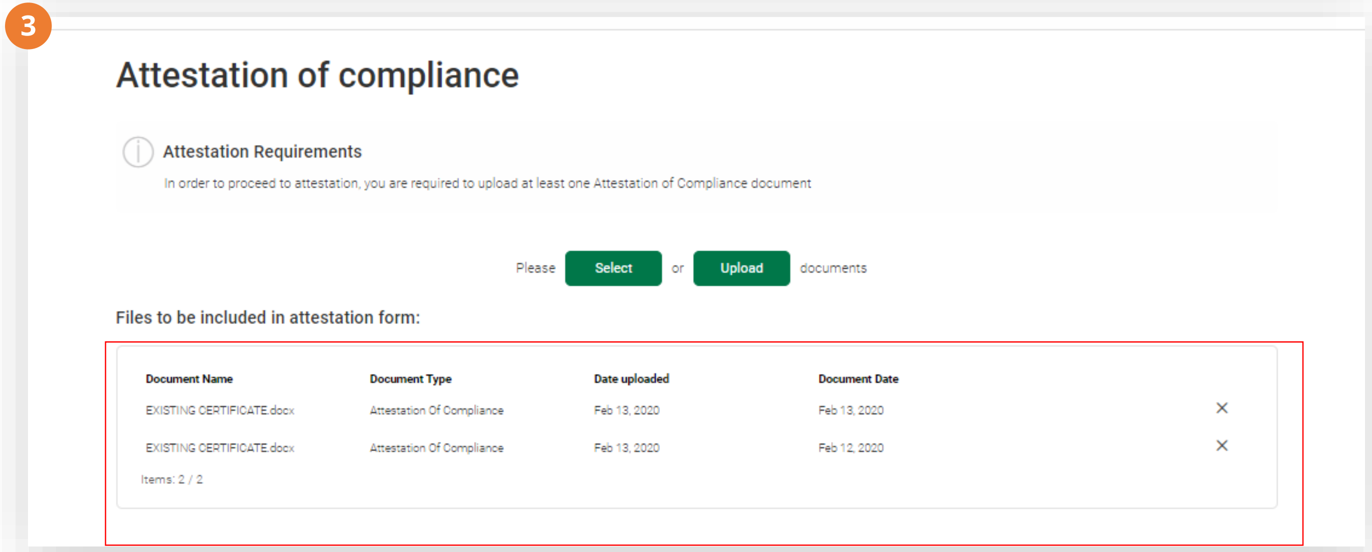
Attestation Requirements

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


2

| □ | Document Name | Document Type | Date uploaded | Document Date | Verification status |
|---|---|---|---|---|---|
| □ | EXISTING CERTIFICATE.docx | Attestation Of Compliance | Feb 13, 2020 | Feb 13, 2020 | Not reviewed |
| ☑ | EXISTING CERTIFICATE.docx | Attestation Of Compliance | Feb 13, 2020 | Feb 12, 2020 | Not reviewed |

Items: 2 / 2


3

## Attestation of compliance

Attestation Requirements

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

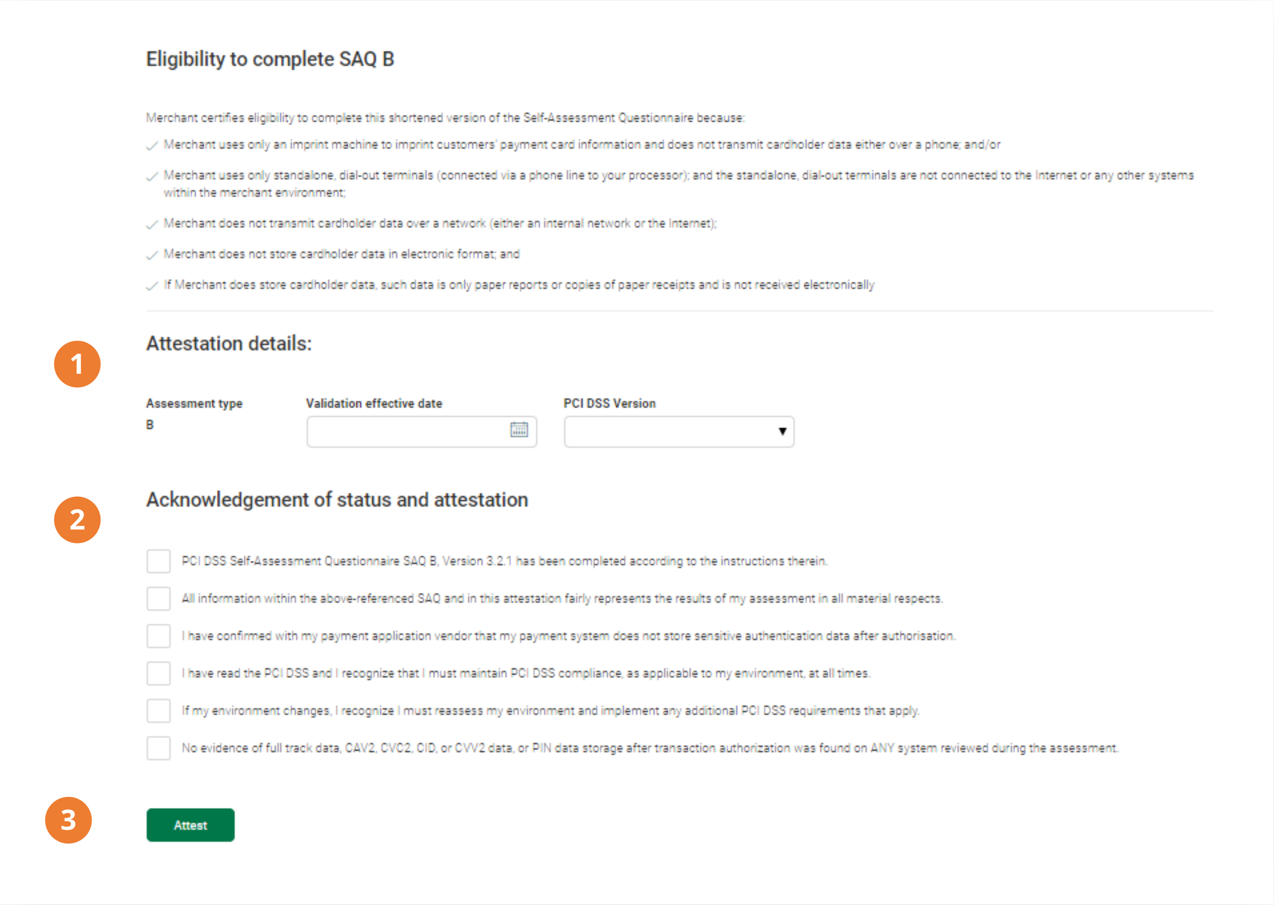
Files to be included in attestation form:

| Document Name | Document Type | Date uploaded | Document Date | |
|---|---|---|---|---|
| EXISTING CERTIFICATE.docx | Attestation Of Compliance | Feb 13, 2020 | Feb 13, 2020 | × |
| EXISTING CERTIFICATE.docx | Attestation Of Compliance | Feb 13, 2020 | Feb 12, 2020 | × |

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

1

### Attestation details:

| Assessment type | Validation effective date | PCI DSS Version |
|---|---|---|
| B | | ▾ |

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

3

## Thank you

# THANK YOU