VIKINGCLOUD™

ECTAA
THE EUROPEAN TRAVEL AGENTS'
AND TOUR OPERATORS' ASSOCIATIONS

Live Webinar

Webinar is starting soon

Understanding PCI DSS

Avoid risk and financial consequences

Speakers:

Christian Möller
Director Transport and Distribution
ECTAA

Natasja Bolton
Client Engagement Manager
VIKINGCLOUD

VIKINGCLOUD™ | ECTAA THE EUROPEAN TRAVEL AGENTS' AND TOUR OPERATORS' ASSOCIATIONS

You will **receive the recording**

Handout **available to download**

Live Q&A; **Please ask questions**

Live **poll** during the webinar

Please **complete the survey**

VIKINGCLOUD™ | ECTAA THE EUROPEAN TRAVEL AGENTS' AND TOUR OPERATORS' ASSOCIATIONS

Live Webinar

Understanding PCI DSS

Avoid risk and financial consequences

Speakers:

CHRISTIAN **MÖLLER**
Director Transport and Distribution
ECTAA

NATASJA **BOLTON**
Client Engagement Manager
VIKINGCLOUD

Our Agenda

What We Are Discussing Today

- Background to the PCI DSS
- Why the PCI DSS
- Data Breaches & the Consequences
- Aim of PCI DSS
- How to comply with the PCI DSS
- Exploring PCI Manager
- Conclusion

POLL

Background to the PCI DSS

Payment Card Industry Security Standards Council (PCI SSC)

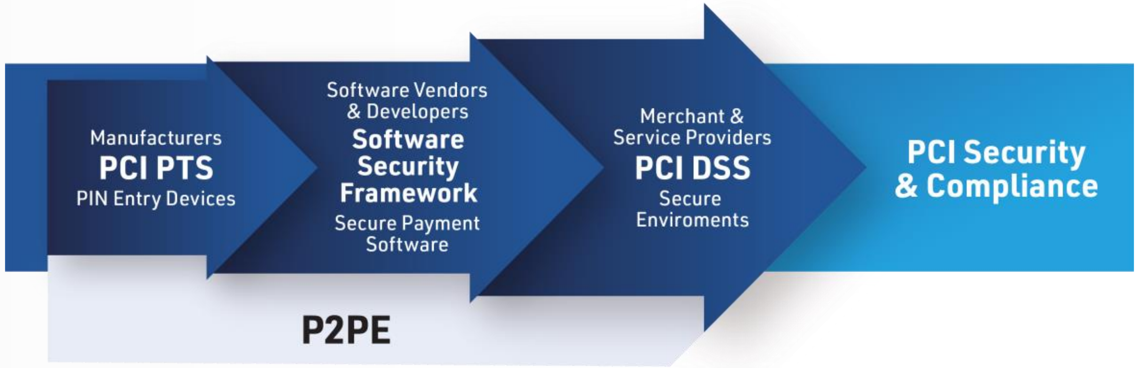
Background to the PCI DSS

PCI SSC

- ✓ Independent body founded in 2006 by the **card payment brands**
- ✓ Develops and maintains **PCI standards:**

PAYMENT CARD INDUSTRY SECURITY STANDARDS

Protection of Cardholder Payment Data


Manufacturers
PCI PTS
PIN Entry Devices
Software Vendors & Developers
Software Security Framework
Secure Payment Software
Merchant & Service Providers
PCI DSS
Secure Enviroments
PCI Security & Compliance
P2PE

Ecosystem of payment devices, applications, infrastructure and users

(after: PCI DSS Quick Reference Guide v3.2)

The card payment brands:

- ✓ Define PCI **Compliance Programmes**
- ✓ Those programmes require **merchant compliance** with the PCI Data Security Standard (DSS)

AMERICAN EXPRESS JCB mastercard VISA DISCOVER GLOBAL NETWORK

What is the PCI Data Security Standard (DSS)?

Background to the PCI DSS

Global data security standard adopted by the payment card brands.

Applies to:

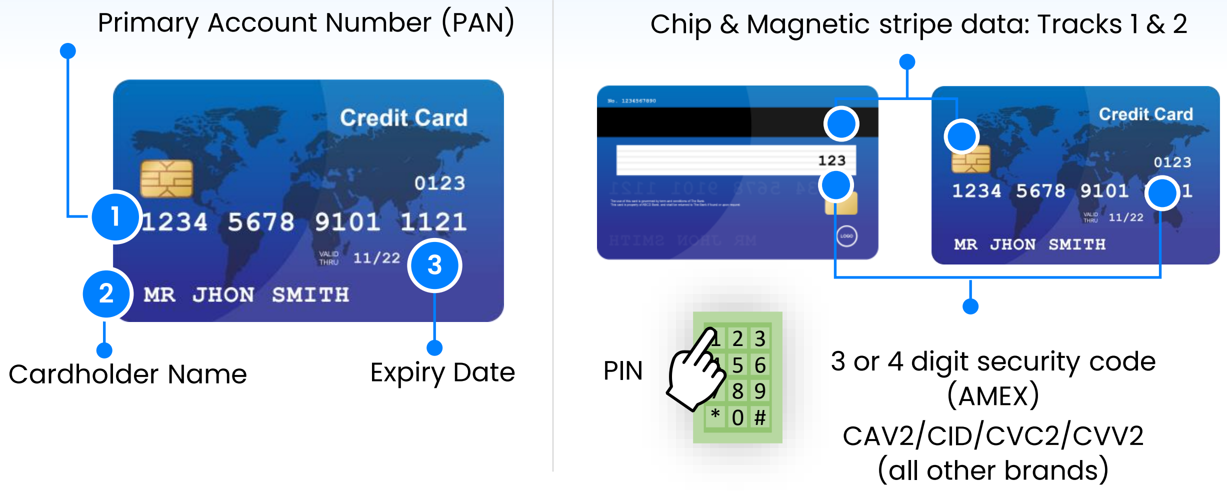
- All entities involved in payment card processing (incl. merchants, processors, acquirers, issuers, and service providers)
- All other entities that **store, process or transmit** (or could **impact the security of**) account data

PCI DSS is **not new:**

- PCI DSS v1.1 launched in **2006**
- PCI DSS v2.0 in **2010**
- Current PCI DSS v3.2.1, since **2018**

PCI DSS

Baseline security best practices for protecting Account Data **(Cardholder Data and Sensitive Authentication Data)**



Primary Account Number (PAN)

Cardholder Name

Expiry Date

Chip & Magnetic stripe data: Tracks 1 & 2

PIN

3 or 4 digit security code (AMEX)
CAV2/CID/CVC2/CVV2 (all other brands)

Applicability of PCI DSS

Background to the PCI DSS

PCI DSS applies to environments where account data is **stored, processed** and/or **transmitted:**

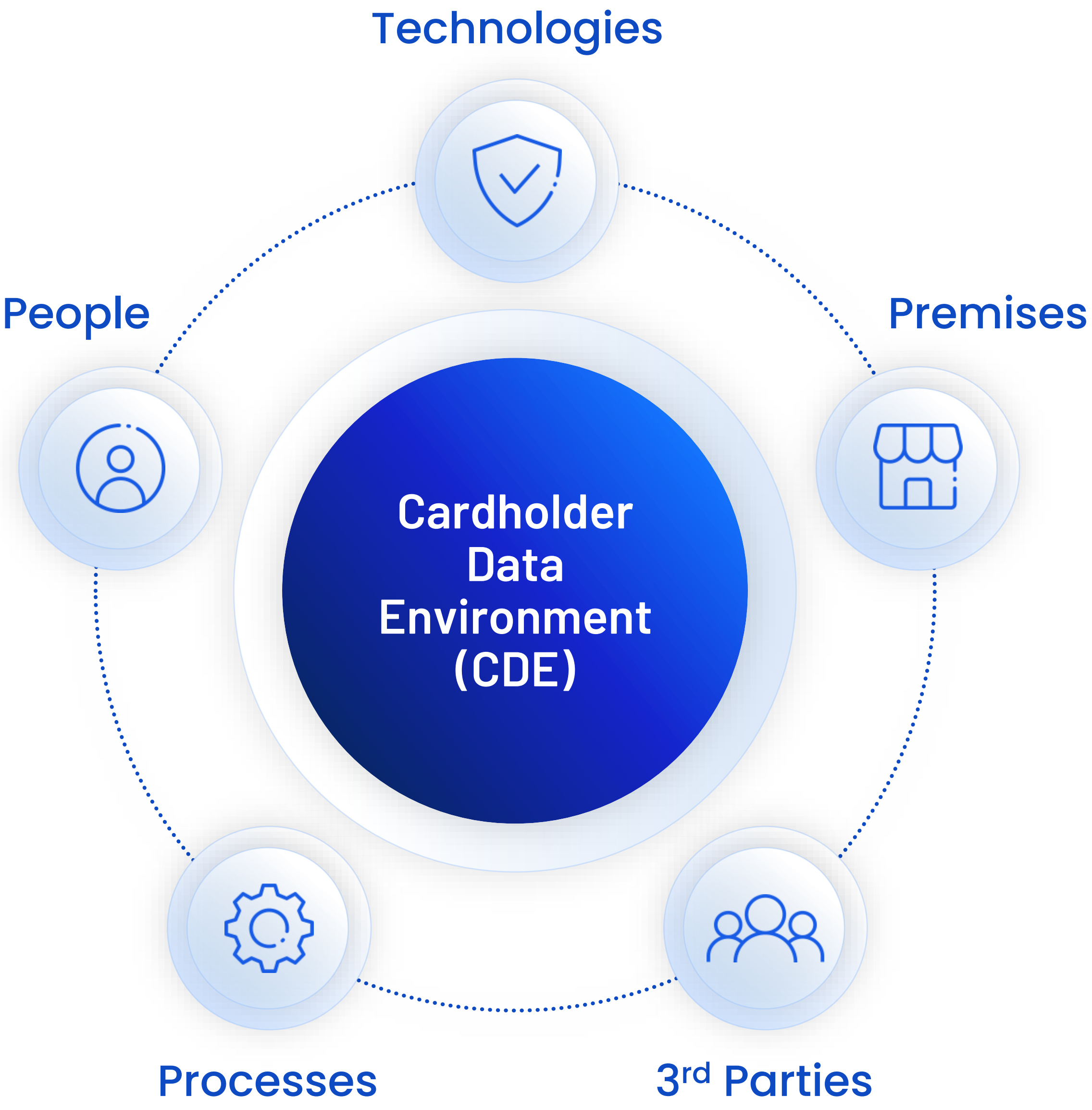
Account data:

- ✓ Is personal data (PII) and a target for criminals
- ✓ Attackers exploit weaknesses in the CDE to gain unauthorised access to account data:

  a data breach

PCI DSS security controls:

- ✓ Protect the CDE
- ✓ Help businesses prevent, detect and respond to data breaches
- ✓ Include requirements for policies, procedures and technical security measures



What is the PCI DSS

A high-level overview

PCI DSS Goals	Requirements Summary
Build and maintain a secure network	• Use of firewalls to protect your network, secure wireless networks • Securely configure and administer all systems
Protect cardholder data	• Sensitive data retention and disposal policies • Secure storage of card data and mask Primary Account Numbers on display • Encrypt transmission of cardholder data across open, public networks
Maintain a vulnerability management program	• Use anti-virus software, vulnerability and patch management for all systems • Software/application development practices and secure coding
Use strong access control measures	• Restrict access to cardholder data by business need to know • User identification and authentication requirements, incl. secure remote access • Physical access controls and tamper inspection of card reading devices
Regularly monitor and test networks	• Log and monitor access to systems and cardholder data • Vulnerability scan / test the security of systems and networks
Maintain an information security policy	• Organisational information security policy, roles and responsibilities, usage policies, security awareness • Management of service providers • Incident response plan

Why PCI DSS

Why PCI DSS

“

Protecting customer payment card information from unauthorised use, exposure and potential fraud is ***key in delivering the trust*** *your customers and partners expect.*

To achieve this:

IATA Accredited Travel Agents must achieve and maintain PCI DSS compliance.

Implications of non-compliance or inaccurate compliance assessment:

- IATA **Risk Event** registered
- Potential for **non-compliance charges** levied by your acquirer(s) / merchant services provider
- Failure to have appropriate technical and organisational measures to ensure the protection of personal data – a **breach of GDPR**
- Greater risk of **card data (account data) breach**

Data Breaches

and their Consequences

What is a card data breach?

Data breaches and their consequences

Any event that could lead to the **unauthorised exposure, compromise** and **misuse** of payment card details and hence to **card fraud.**

Three primary ways attackers gain **unauthorised access:**

- Stolen credentials
- Phishing (social engineering)
- Exploitation of vulnerabilities

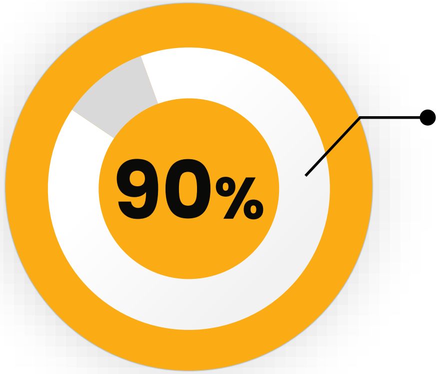
95% of breaches are **financially motivated**

Travel Industry Breaches

- **2019:** Nearly 70% of travel buyers said, their travelers were **affected by a payment-related data breach** from an outside vendor, such as a hotel, airline or retailer, in the previous year
- **May 2023:** Cyberattack on French travel agency
  - Computer intrusion (LockBit ransomware infection)
  - **8000+ customers' passport details, phone numbers and addresses** published on the darkweb
  - Data leak followed travel agency's refusal to pay the ransom demanded

Data Breaches

The reality



of customers who suffered a data breach last year had a turnover of **below 1m transactions** per year (UK-based acquirer statistic)

Merchant e-commerce websites:

the predominant payment channel being attacked in UK and Europe.

Most breached merchants

do not publicise the fact

so there is a lack of awareness within the merchant community.

It can be months until a breach is identified, during which time **all cards being accepted** are likely to be **at risk.**

2023 mean time to **identify a breach:**

204 days
(6+ months)

2023 mean time to **contain a breach:**

72 days
(2+ months)

(IBM Cost of a Data Breach 2023)

Card Fraud

Data breaches and their consequences

Remote purchase (Card Not Present) fraud

- Criminals use stolen card details to buy something online, over the phone or through mail order
- Use card details obtained by scams (such as phishing) or from data breaches (such as web skimming)

Face to face (Card Present) fraud

- In retail stores and ATMs
- Involves the use of:
  - Counterfeit cards (criminal creates a fake card using information obtained from the magnetic stripe)
  - Legitimate cards, and often the PIN, stolen by fraudsters

As a merchant accepting and processing payments directly from cardholders you are on the front line of the battle to:

✓ **Keep payment data safe** from theft and exploitation

✓ Prevent **card fraud**

$165 USD

Average cost per record involved in a data breach

(IBM Cost of a Data Breach 2023)

Every fraudulent transaction costs businesses

3.49 times the lost transaction value, on average

(LexisNexis Fraud Multiplier)

3.01 E-commerce merchants

3.13 Retailers

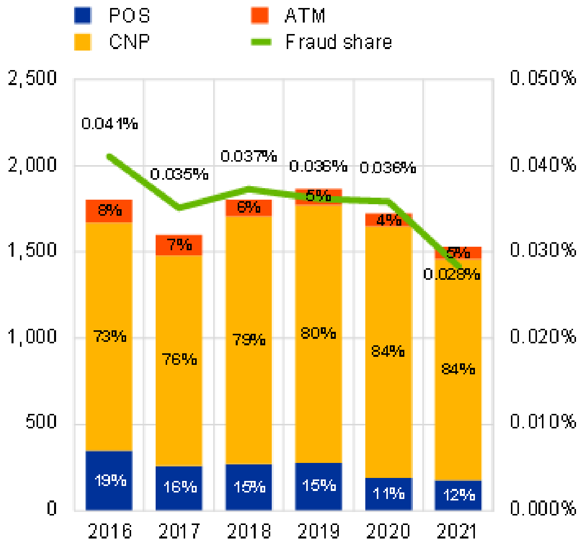
Card Fraud in Europe

Data breaches and their consequences

€1.53 billion

Total Value of Card Fraud 2022

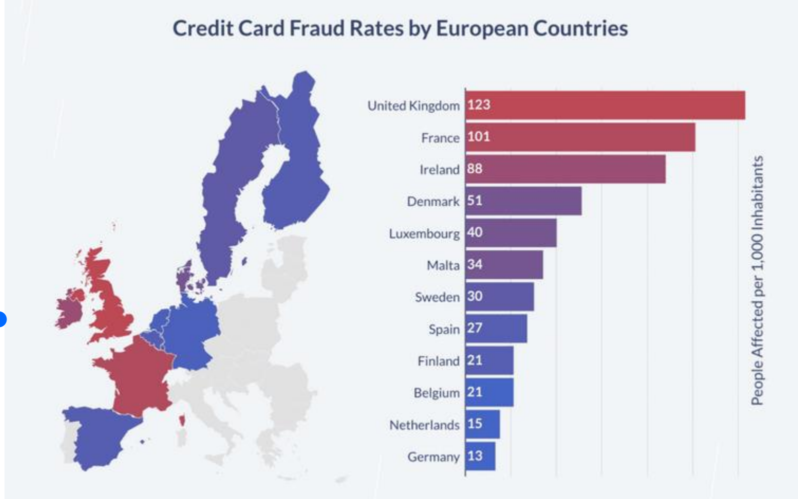
(left-hand scale: total value of fraud (EUR millions); right-hand scale: value of fraud as a share of the value of transactions)



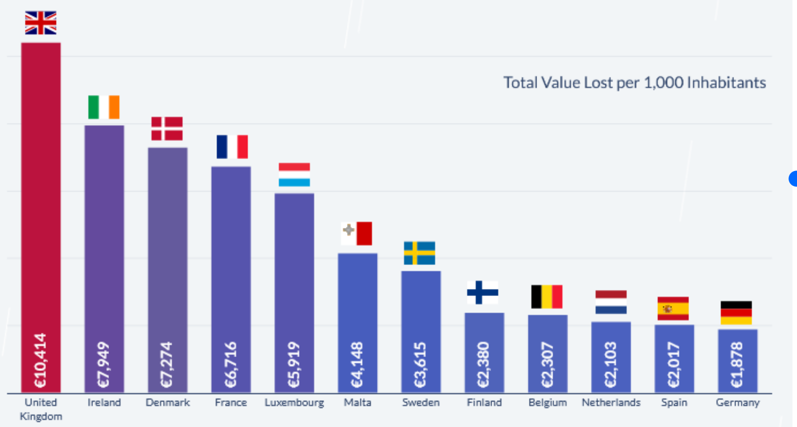
(2023 European Central Bank card fraud report)

Credit card fraud varies widely across Europe:

(2021 Uswitch Online fraud report)



No. of people affected per 1,000 inhabitants



Amount of money lost (€) per 1,000 inhabitants

Aim of PCI DSS

To reduce financial fraud through **heightened data security capabilities** of whoever processes payment card information.

Businesses adhere to best practice security requirements (PCI DSS):

To help them **prevent, detect and respond to data breaches.**

Help **avoid the costs** associated with data breaches, including:

- ✓ **Investigation and remediation costs**
- ✓ **Legal costs**
- ✓ **Loss of revenue**
- ✓ **Lost opportunity costs**

How to comply with the PCI DSS

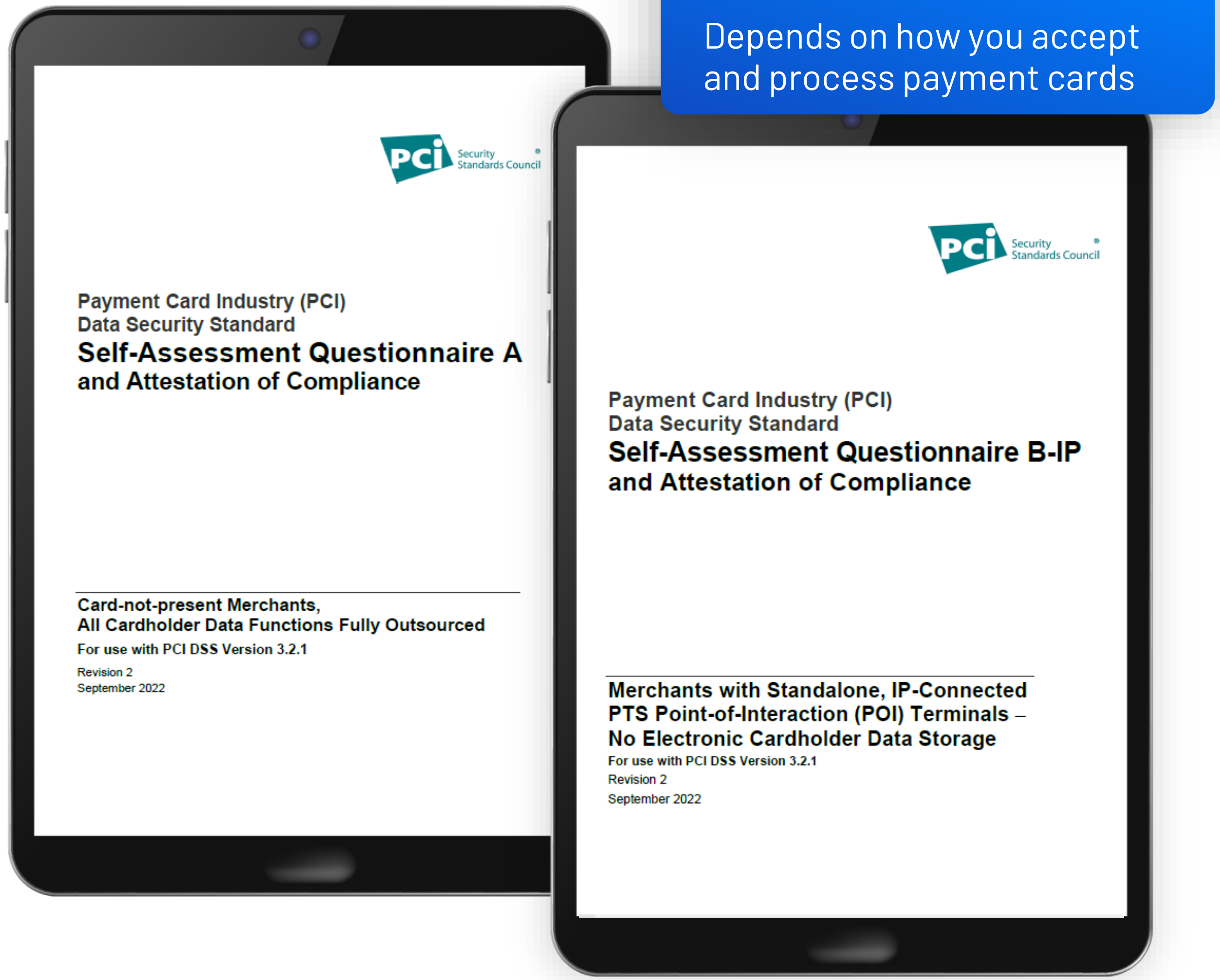
PCI DSS compliance reporting

How to comply with the PCI DSS

- Specified by the payment brand PCI Compliance Programmes
- For merchants at lower levels (of transaction processing):
  - **Self-Assessment Questionnaire** (SAQ)
  - Supported by an **external network vulnerability scan** (If applicable to your environment)
- Eight SAQ types:
  - Address common **payment processing methods**
  - Contain an appropriate set of PCI DSS security measures

YOUR SAQ TYPE

Depends on how you accept and process payment cards



Payment Card Industry (PCI)
Data Security Standard
Self-Assessment Questionnaire A and Attestation of Compliance

**Card-not-present Merchants,
All Cardholder Data Functions Fully Outsourced**
For use with PCI DSS Version 3.2.1
Revision 2
September 2022

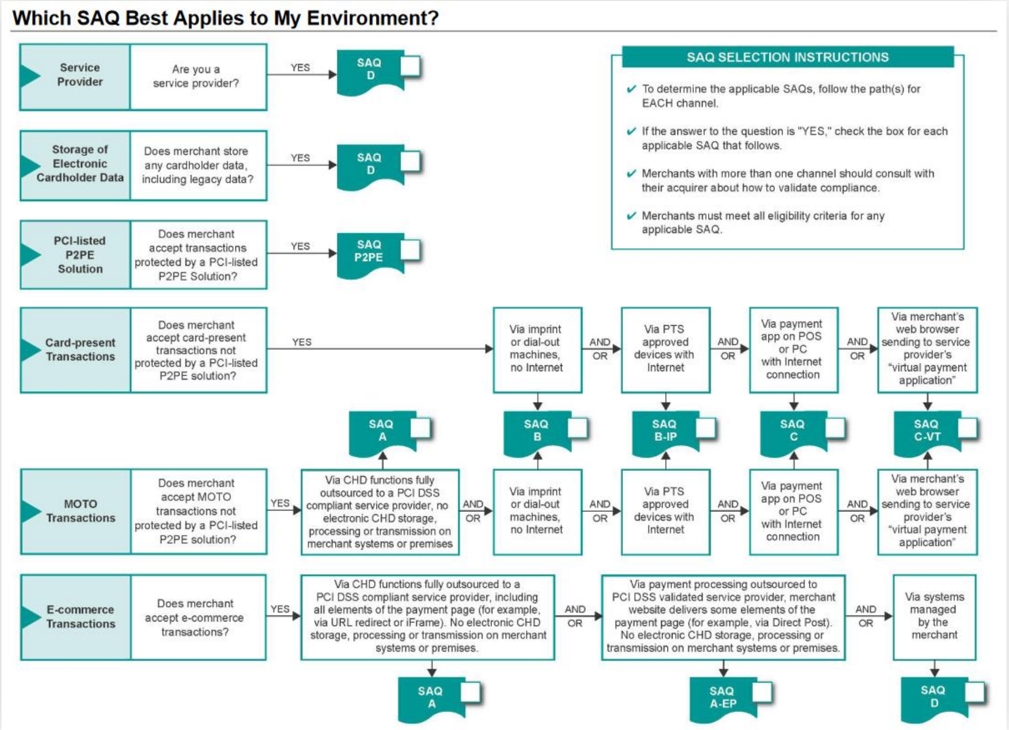
Payment Card Industry (PCI)
Data Security Standard
Self-Assessment Questionnaire B-IP and Attestation of Compliance

Merchants with Standalone, IP-Connected PTS Point-of-Interaction (POI) Terminals – No Electronic Cardholder Data Storage
For use with PCI DSS Version 3.2.1
Revision 2
September 2022

Selecting your SAQ type

How to comply with the PCI DSS

Follow the PCI SSC flowchart:



Which SAQ Best Applies to My Environment?

SAQ SELECTION INSTRUCTIONS

- ✓ To determine the applicable SAQs, follow the path(s) for EACH channel.
- ✓ If the answer to the question is "YES," check the box for each applicable SAQ that follows.
- ✓ Merchants with more than one channel should consult with their acquirer about how to validate compliance.
- ✓ Merchants must meet all eligibility criteria for any applicable SAQ.

Service Provider: Are you a service provider? YES → SAQ D

Storage of Electronic Cardholder Data: Does merchant store any cardholder data, including legacy data? YES → SAQ D

PCI-listed P2PE Solution: Does merchant accept transactions protected by a PCI-listed P2PE Solution? YES → SAQ P2PE

Card-present Transactions: Does merchant accept card-present transactions not protected by a PCI-listed P2PE solution? YES → Via imprint or dial-out machines, no Internet → SAQ B; AND OR Via PTS approved devices with Internet → SAQ B-IP; AND OR Via payment app on POS or PC with Internet connection → SAQ C; AND OR Via merchant's web browser sending to service provider's "virtual payment application" → SAQ C-VT

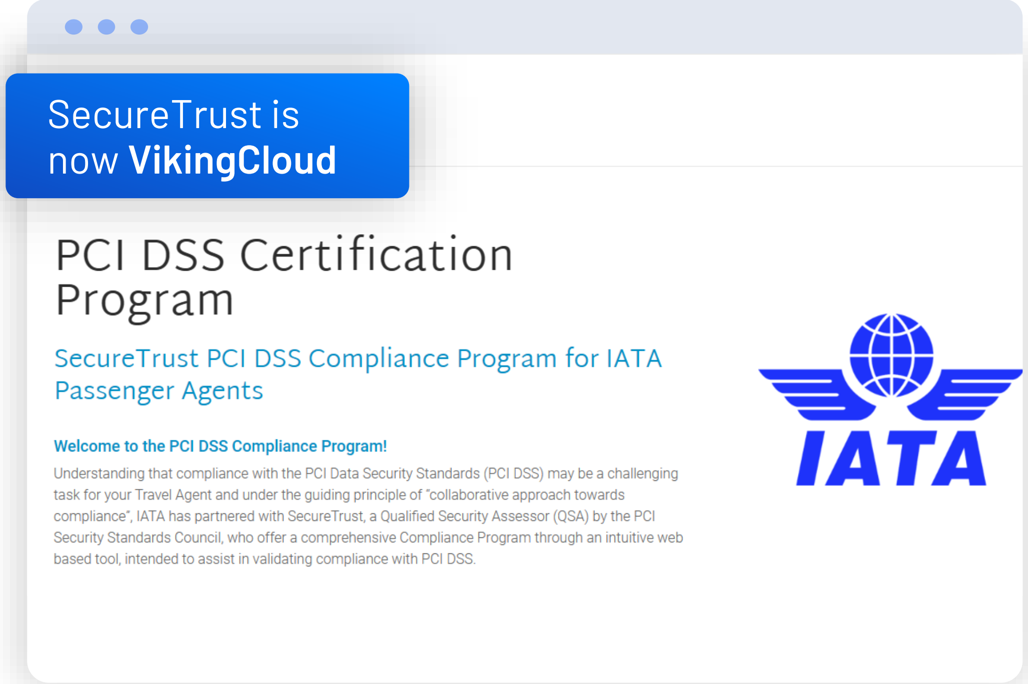
MOTO Transactions: Does merchant accept MOTO transactions not protected by a PCI-listed P2PE solution? YES → Via CHD functions fully outsourced to a PCI DSS compliant service provider, no electronic CHD storage, processing or transmission on merchant systems or premises → SAQ A; AND OR Via imprint or dial-out machines, no Internet → SAQ B; AND OR Via PTS approved devices with Internet → SAQ B-IP; AND OR Via payment app on POS or PC with Internet connection → SAQ C; AND OR Via merchant's web browser sending to service provider's "virtual payment application" → SAQ C-VT

E-commerce Transactions: Does merchant accept e-commerce transactions? YES → Via CHD functions fully outsourced to a PCI DSS compliant service provider, including all elements of the payment page (for example, via URL redirect or iFrame). No electronic CHD storage, processing or transmission on merchant systems or premises. → SAQ A; AND OR Via payment processing outsourced to PCI DSS validated service provider, merchant website delivers some elements of the payment page (for example, via Direct Post). No electronic CHD storage, processing or transmission on merchant systems or premises. → SAQ A-EP; AND OR Via systems managed by the merchant → SAQ D

(from: PCI DSS Self-Assessment Questionnaire Instructions and Guidelines, v3.2.1 r1)

OR

Sign up for the SecureTrust PCI Manager:



SecureTrust is now **VikingCloud**

PCI DSS Certification Program

SecureTrust PCI DSS Compliance Program for IATA Passenger Agents

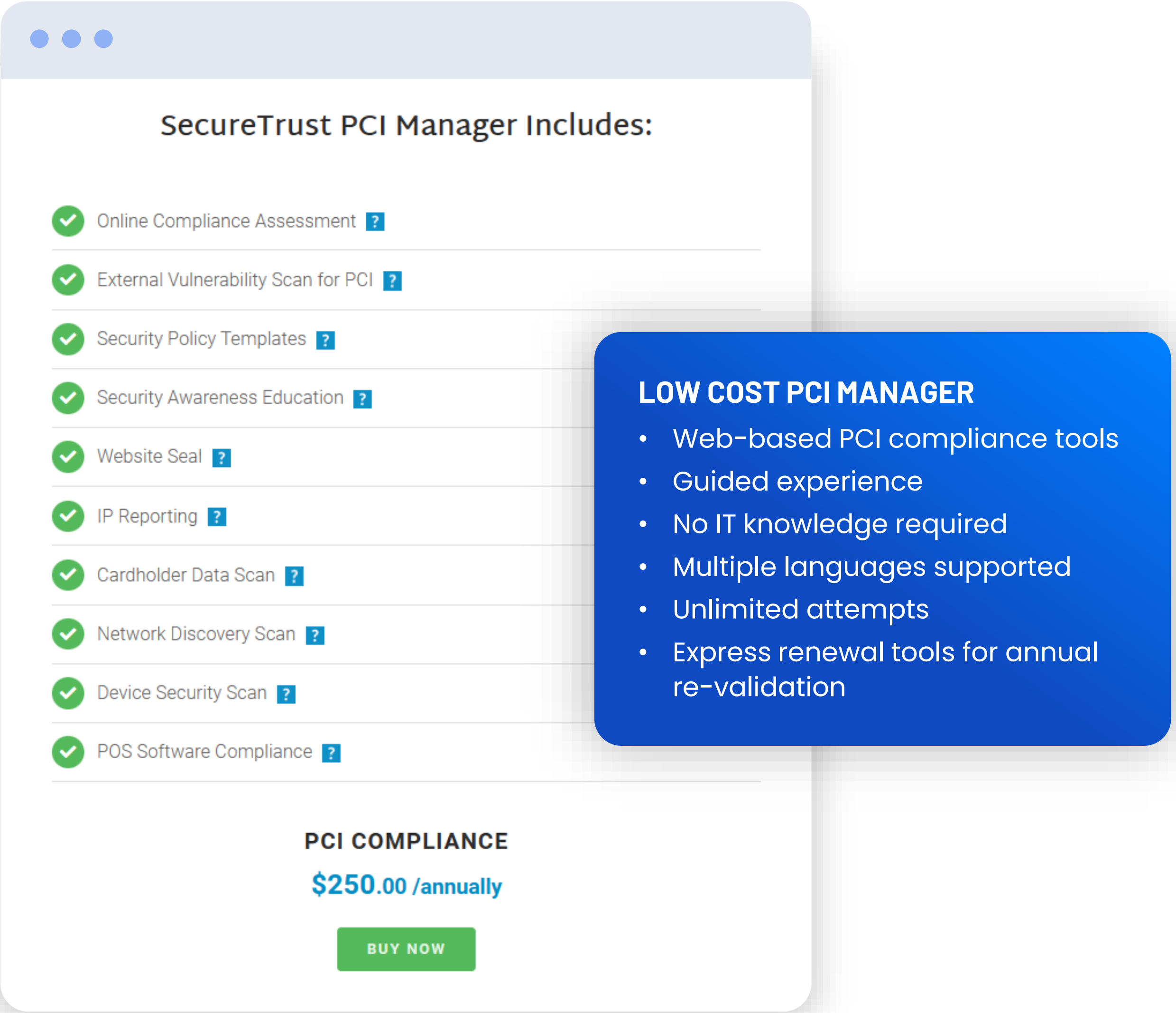
Welcome to the PCI DSS Compliance Program!

Understanding that compliance with the PCI Data Security Standards (PCI DSS) may be a challenging task for your Travel Agent and under the guiding principle of "collaborative approach towards compliance", IATA has partnered with SecureTrust, a Qualified Security Assessor (QSA) by the PCI Security Standards Council, who offer a comprehensive Compliance Program through an intuitive web based tool, intended to assist in validating compliance with PCI DSS.

SecureTrust PCI Manager

How to comply with the PCI DSS

- **Simplifies compliance assessment and reporting**
- **Wizard Tool – 'Guide Me'**
  - Makes sure you complete the right PCI DSS **Self-Assessment Questionnaire** (SAQ)
  - Hides requirements that **do not apply** to your business
  - Helps you set up **vulnerability scanning** (if applicable)
- **Downloadable PCI Attestation of Compliance (AoC)**
  - For **submission to IATA**



SecureTrust PCI Manager Includes:

- ✓ Online Compliance Assessment ?
- ✓ External Vulnerability Scan for PCI ?
- ✓ Security Policy Templates ?
- ✓ Security Awareness Education ?
- ✓ Website Seal ?
- ✓ IP Reporting ?
- ✓ Cardholder Data Scan ?
- ✓ Network Discovery Scan ?
- ✓ Device Security Scan ?
- ✓ POS Software Compliance ?

PCI COMPLIANCE

$250.00 /annually

LOW COST PCI MANAGER

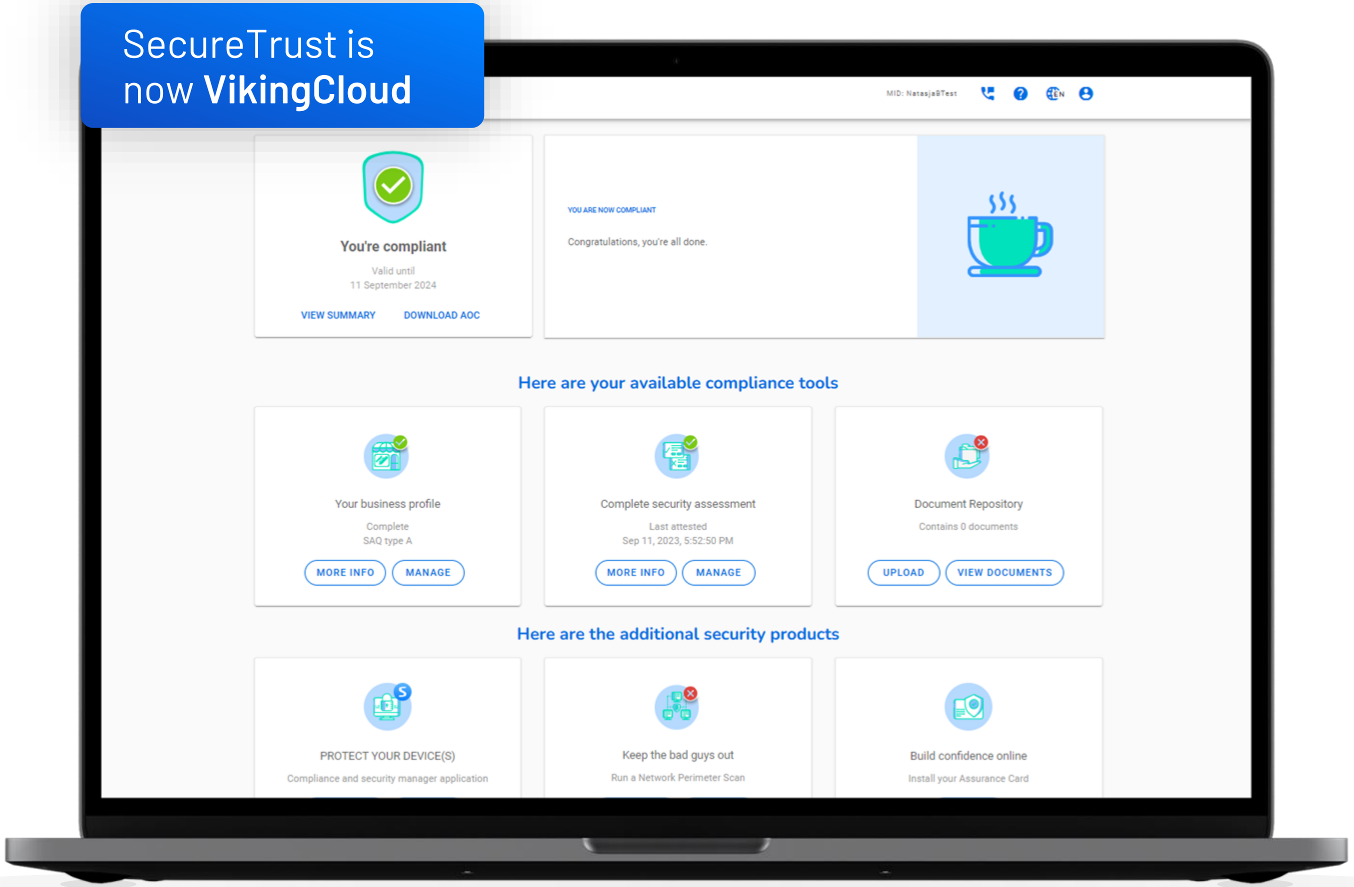
- Web-based PCI compliance tools
- Guided experience
- No IT knowledge required
- Multiple languages supported
- Unlimited attempts
- Express renewal tools for annual re-validation

PCI Manager: what’s included

How to comply with the PCI DSS

- **Report your PCI DSS compliance**
  - Streamlined and simplified journey
- **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**
  - Multi-language support (German, Spanish, French-Canadian, English)
- **Included Security Tools**
  - Take additional steps to defend against hackers and malware

SecureTrust is now **VikingCloud**



You're compliant

Valid until 11 September 2024

YOU ARE NOW COMPLIANT

Congratulations, you're all done.

Here are your available compliance tools

Your business profile
Complete
SAQ type A

Complete security assessment
Last attested
Sep 11, 2023, 5:52:50 PM

Document Repository
Contains 0 documents

Here are the additional security products

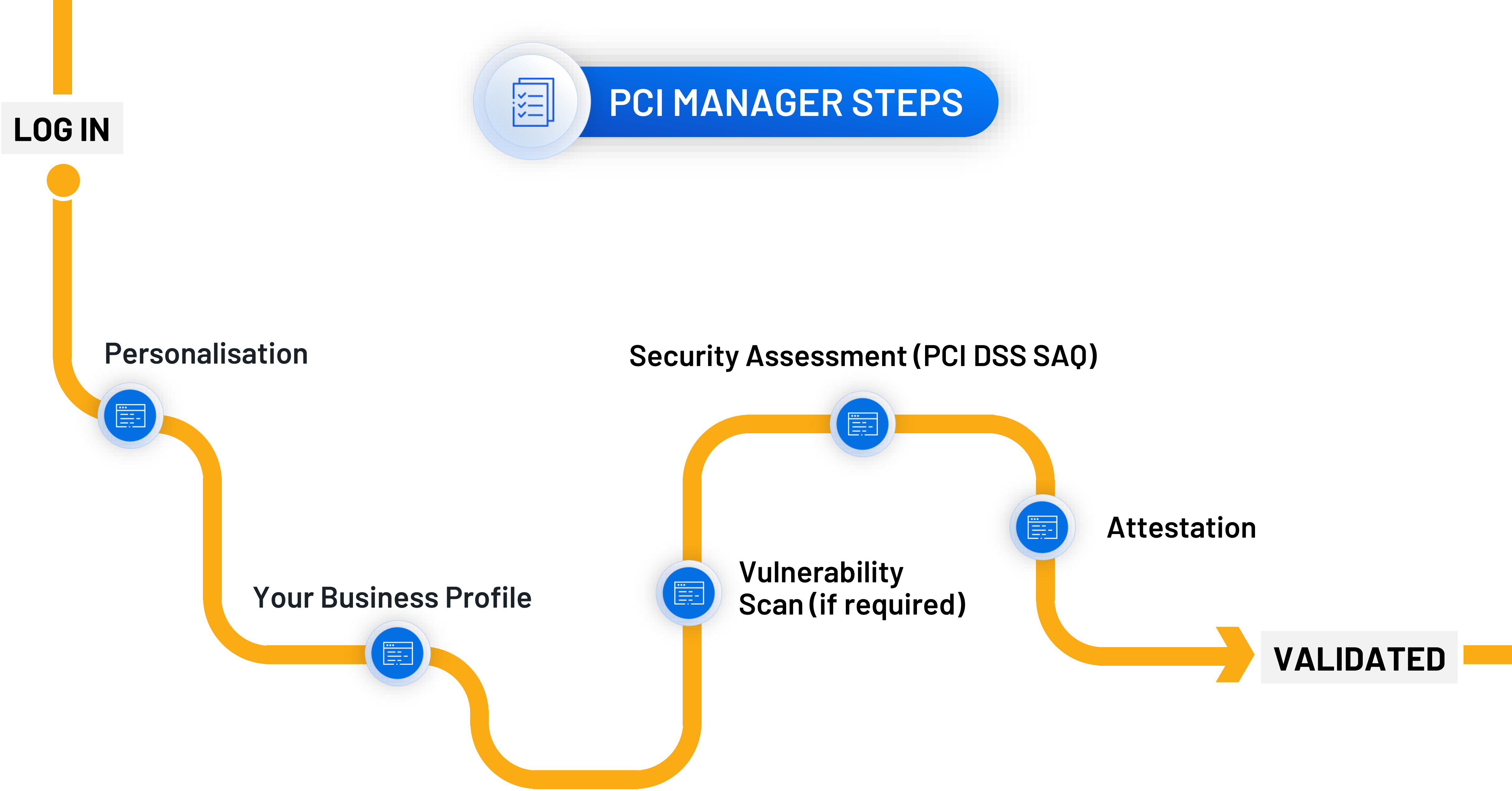
PROTECT YOUR DEVICE(S)
Compliance and security manager application

Keep the bad guys out
Run a Network Perimeter Scan

Build confidence online
Install your Assurance Card

Exploring PCI Manager

PCI MANAGER STEPS



LOG IN

Personalisation

Your Business Profile

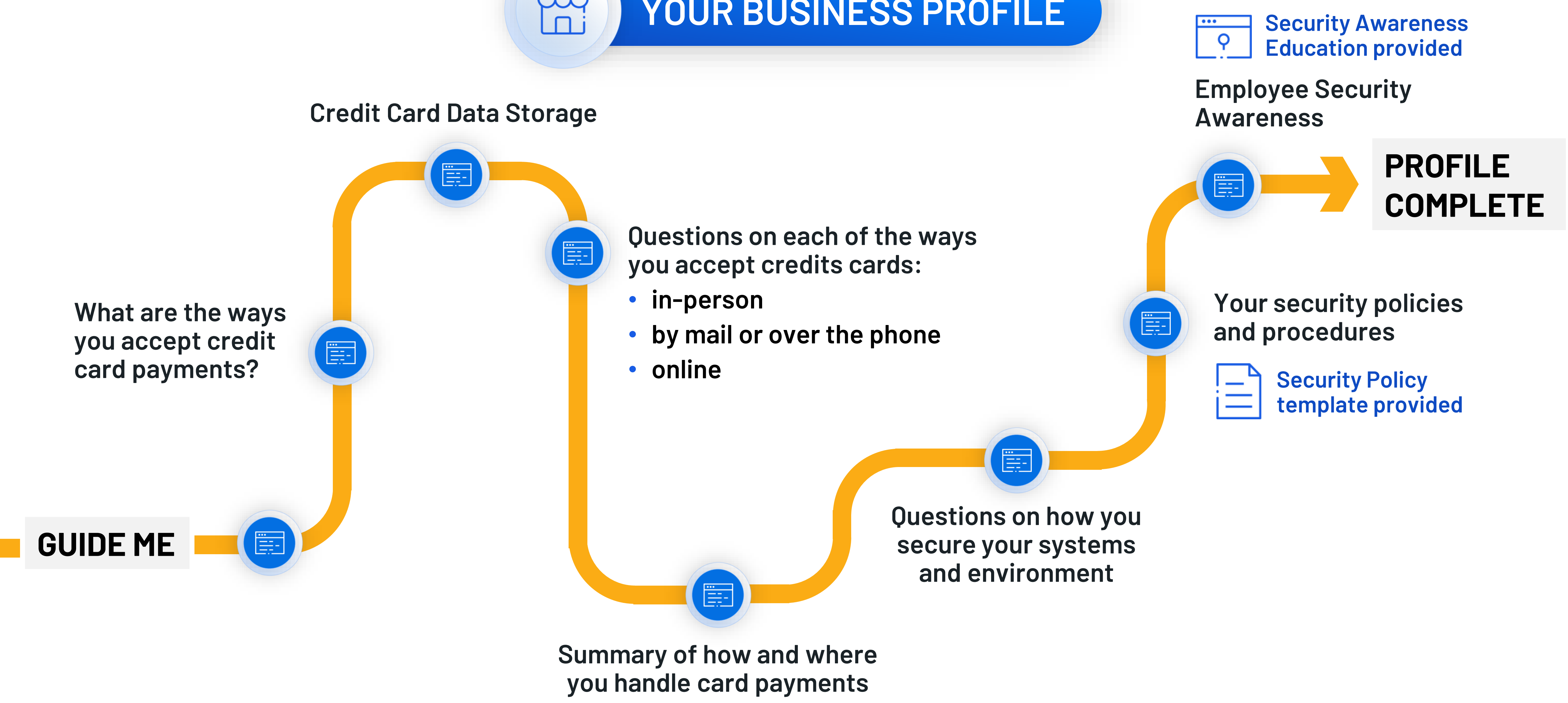
Vulnerability Scan (if required)

Security Assessment (PCI DSS SAQ)

Attestation

VALIDATED

YOUR BUSINESS PROFILE



GUIDE ME

What are the ways you accept credit card payments?

Credit Card Data Storage

Questions on each of the ways you accept credits cards:

- in-person
- by mail or over the phone
- online

Summary of how and where you handle card payments

Questions on how you secure your systems and environment

Your security policies and procedures

Security Policy template provided

Employee Security Awareness

Security Awareness Education provided

PROFILE COMPLETE

What are the ways you accept credit card payments?

Your Business Profile

How do you accept credit cards? Select all that apply.

☑

My business has a physical location where payments with a credit card are made in-person.

In-store card payments

? ☑

My business allows payments with a credit card by mail or over the phone (MO/TO).

Over the telephone or by mail order

? ☑

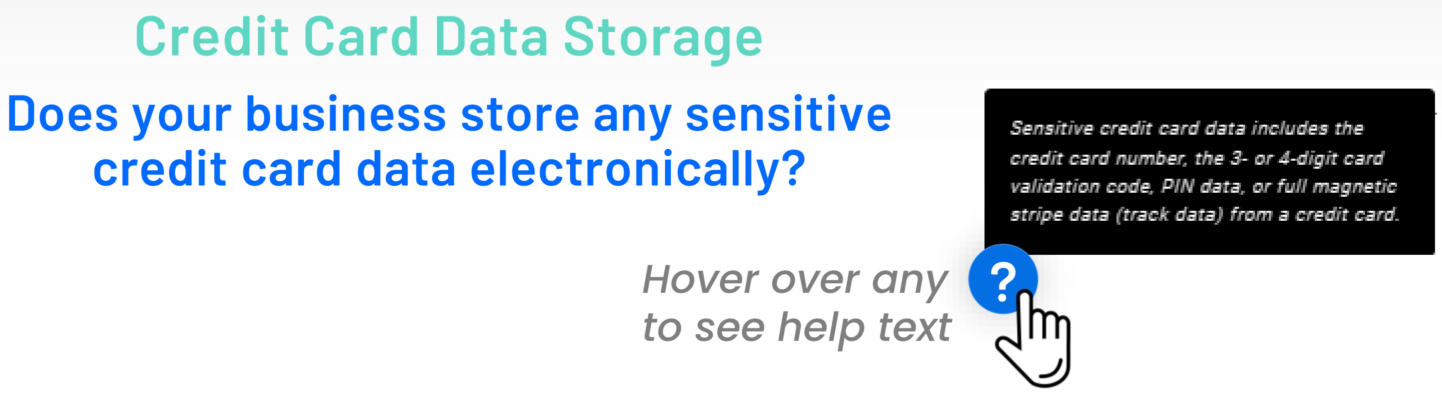
?

My business has a website where payments with a credit card are made online.

Online e-commerce card payments

Credit Card Data Storage

Your Business Profile



Credit Card Data Storage

Does your business store any sensitive credit card data electronically?

Sensitive credit card data includes the credit card number, the 3- or 4-digit card validation code, PIN data, or full magnetic stripe data (track data) from a credit card.

Hover over any ? to see help text

- **Card data storage example:**
  - Holidays deposits taken as one-off payments; customer card details retained electronically for future balance payments
- Card data held as a 'token' (alias) is **not considered** electronic storage of card data
- A token (alias) is returned by your Payment Service Provider, on completion of the initial payment, that you:
  - **Can use** to trigger subsequent or recurring payments
  - **Cannot exchange** for the full card details

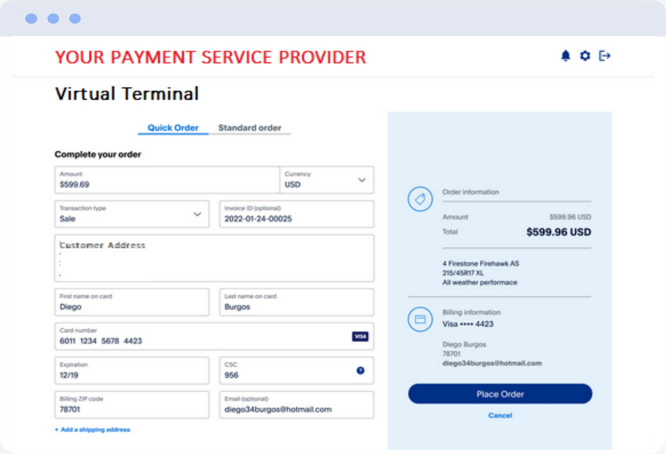
Questions on each of the ways you accept credits cards

In-person

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

☑ Pinpad Terminal

☑ Virtual Terminal



Virtual Terminal

Complete your order

Amount: $599.69
Currency: USD
Transaction type: Sale
Invoice ID (optional): 2022-01-24-00025
Customer Address
First name on card: Diego
Last name on card: Burgos
Card number: 6011 1234 5678 4423
Expiration: 12/19
CSC: 956
Billing ZIP code: 78701
Email (optional): diego34burgos@hotmail.com

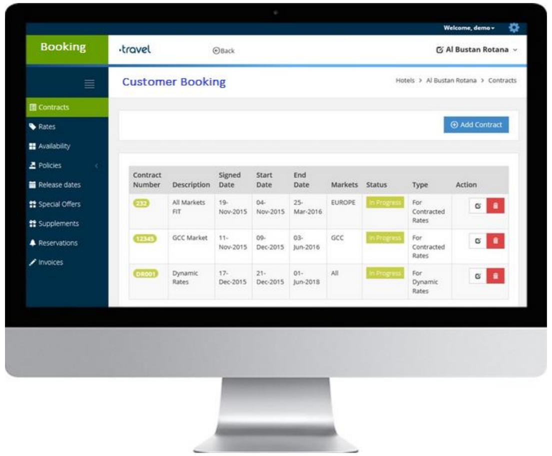
Order information
Amount $599.96 USD
Total **$599.96 USD**

4 Firestone Firehawk AS
215/45R17 XL
All weather performace

Billing information
Visa •••• 4423

Diego Burgos
78701
diego34burgos@hotmail.com

☑ Payment Application



Customer Booking

Hotels > Al Bustan Rotana > Contracts

Contract Number	Description	Signed Date	Start Date	End Date	Markets	Status	Type	Action
232	All Markets FIT	19-Nov-2015	04-Nov-2015	25-Mar-2016	EUROPE	In Progress	For Contracted Rates	
12345	GCC Market	11-Nov-2015	09-Dec-2015	03-Jun-2016	GCC	In Progress	For Contracted Rates	
DR001	Dynamic Rates	17-Dec-2015	21-Dec-2015	01-Jun-2018	All	In Progress	For Dynamic Rates	

Questions on each of the ways you accept credits cards

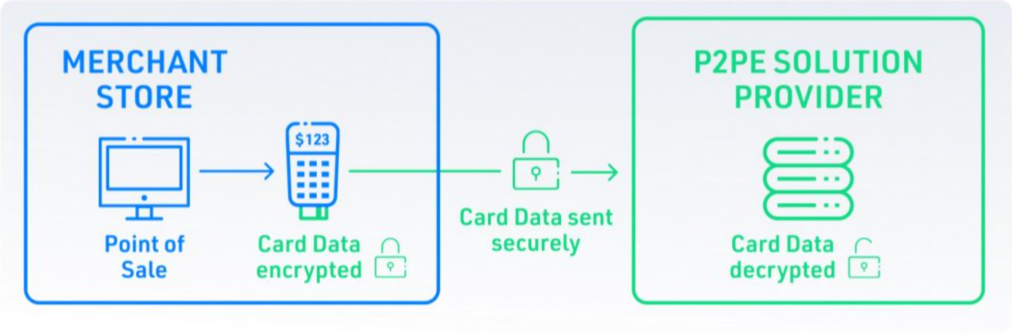
In-person

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

☑ Certified Point to Point Encryption (P2PE)

□ No equipment; I use only paper or a telephone.

A PCI SSC-listed Point to Point Encryption (P2PE) solution:



MERCHANT STORE

Point of Sale → Card Data encrypted

Card Data sent securely →

P2PE SOLUTION PROVIDER

Card Data decrypted

https://listings.pcisecuritystandards.org/assessors_and_solutions/point_to_point_encryption_solutions

- You use an imprint device with carbon-copy paper to capture the credit card number
- Services where you call a number and key in the purchase information.

Questions on each of the ways you accept credits cards:

By mail or over the phone

For your mail and/or telephone orders who collects the credit card numbers from your customers?

My business:

- call handlers in your business take the card details over the phone

A third-party service provider:

- you may never receive the credit card numbers

Questions on each of the ways you accept credits cards: online

online

Does your business have administrative control over any part of your web site?

Yes, if you can:

- ✓ Control the website look-and-feel
- ✓ Access the servers that run the website
- ✓ Administer the web server
- ✓ Install plug-ins, patches or updates

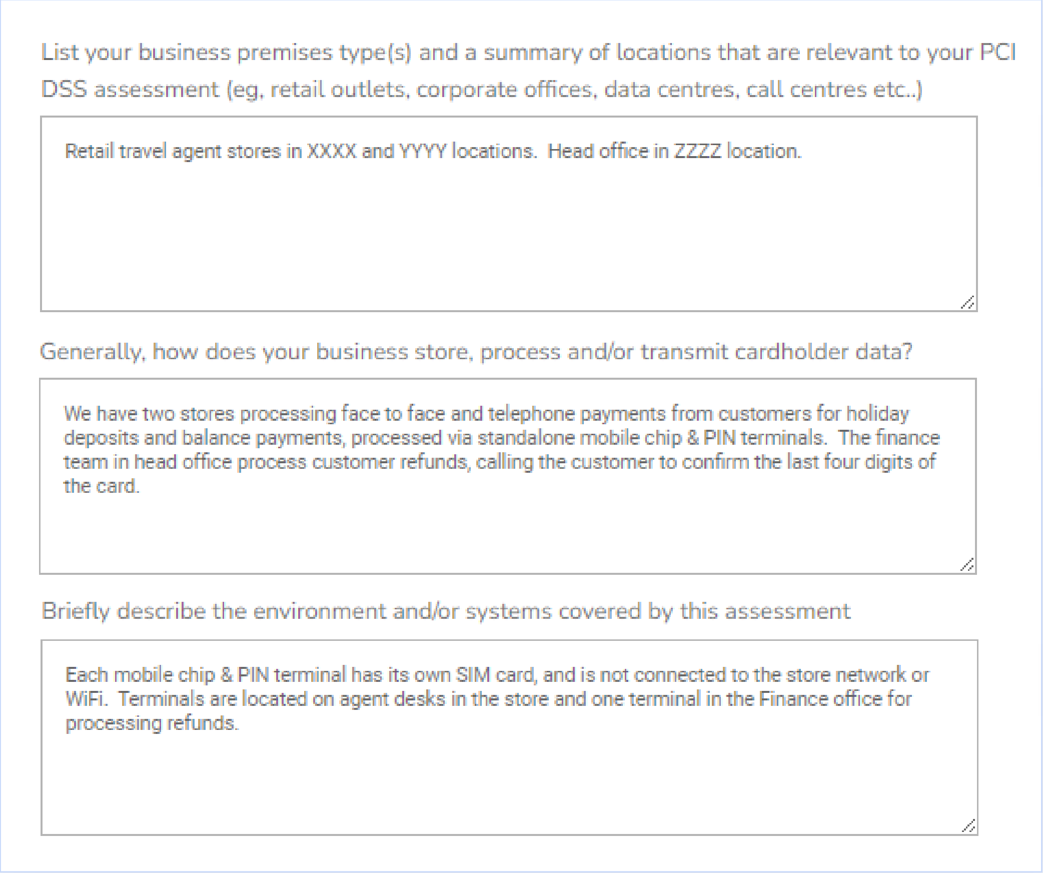
OR

No, you rely on a third-party provider for all website administration

A summary of how and where you handle card payments

Your Business Profile

Forms part of your PCI DSS Attestation of Compliance (AOC)



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..)

Retail travel agent stores in XXXX and YYYY locations. Head office in ZZZZ location.

Generally, how does your business store, process and/or transmit cardholder data?

We have two stores processing face to face and telephone payments from customers for holiday deposits and balance payments, processed via standalone mobile chip & PIN terminals. The finance team in head office process customer refunds, calling the customer to confirm the last four digits of the card.

Briefly describe the environment and/or systems covered by this assessment

Each mobile chip & PIN terminal has its own SIM card, and is not connected to the store network or WiFi. Terminals are located on agent desks in the store and one terminal in the Finance office for processing refunds.

1. List the **locations in scope** for this assessment

2. Describe how card data is **handled** and card payments are **accepted** by your business.

3. Describe the **systems / cardholder data environment(s) in scope** of your assessment.

   The system / environment(s) that **facilitate how** your business handles and accepts card payments

Questions on how you secure your systems and environment

Your Business Profile

Your answers:

- May trigger further profile questions
- Will pre-populate security assessment questions
  - e.g. as ‘Yes’ or ‘Not Applicable’

Topics include:

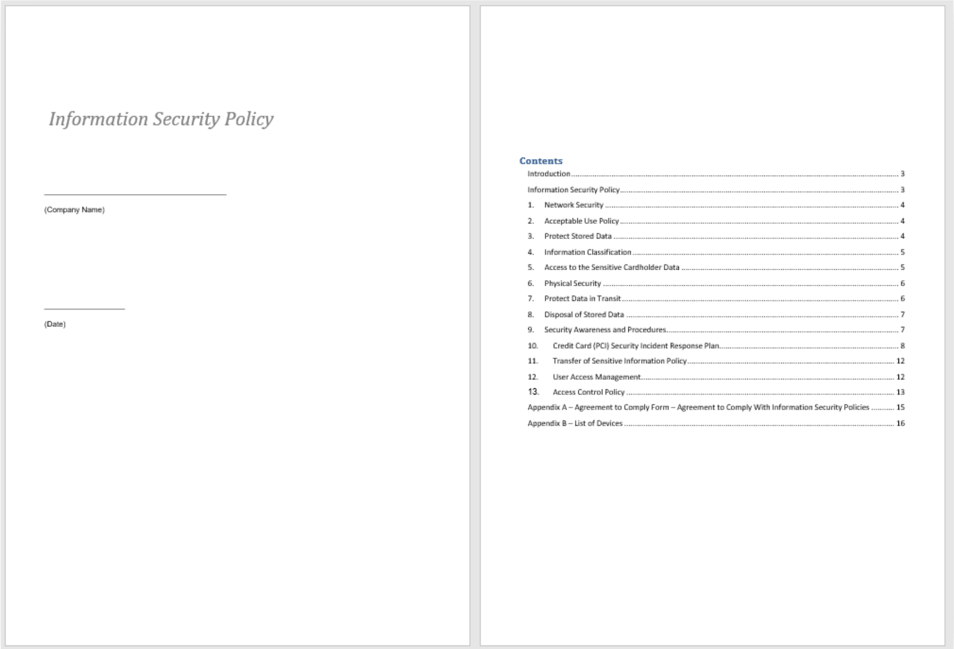
- ✓ How you secure your business network and systems
- ✓ How you protect and securely destroy paper documents with credit card data
- ✓ How you keep track of and protect your POS devices
- ✓ Third-party service provider relationships
- ✓ Your use of wireless networks
- ✓ Controlling physical access to areas where account data is present

Your security policies and procedures

Your Business Profile

Do you have written security policies and procedures that address the protection of paper with credit card numbers such as receipts and the physical security of your card processing devices?

- **Template information security policy available for download**
- **Make sure all employees and contractors:**
  - ✓ Are familiar with your security policies
  - ✓ Have access to your policy document(s) and all related procedures for reference
  - ✓ Understand their responsibilities regarding protecting credit card data
- **Policy template covers PCI DSS security topics, including:**
  - ✓ Protecting your Internet connection
  - ✓ Securing your POS devices
  - ✓ Physical protection of account data, etc.



Information Security Policy

(Company Name)

(Date)

Contents

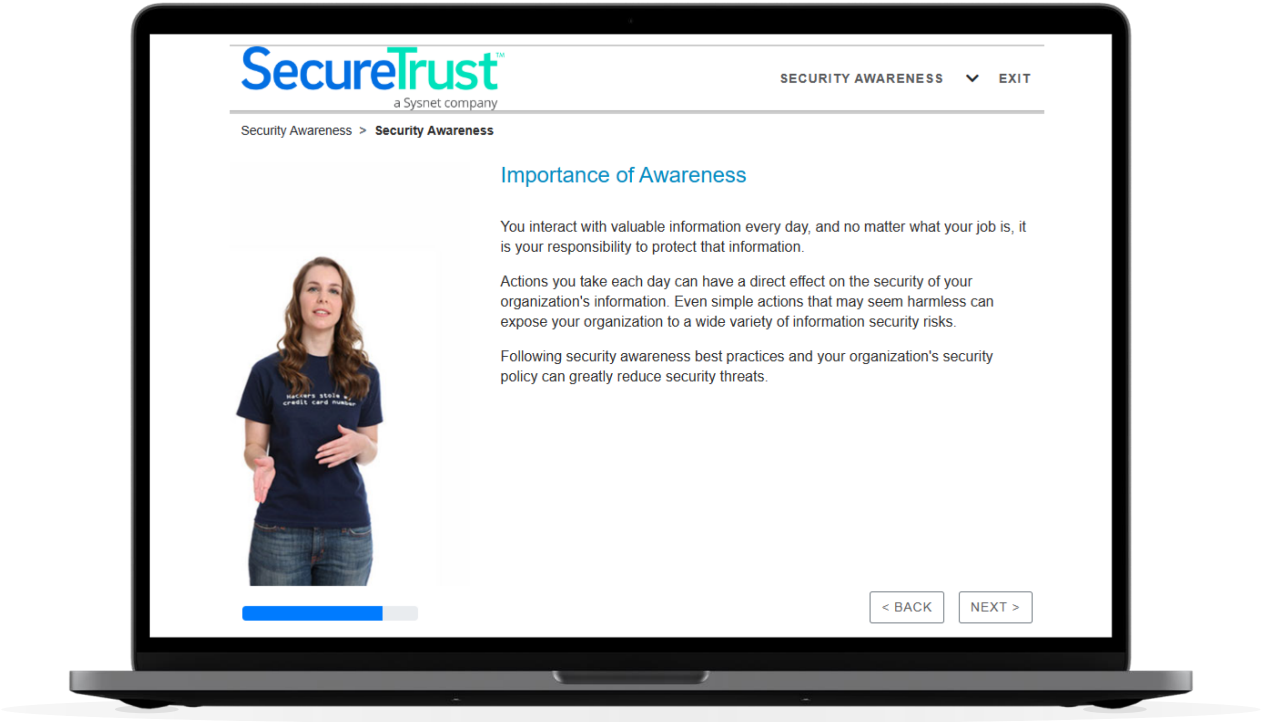
Security Awareness Education

Your Business Profile

Do you have a formal training program for all relevant employees that teaches them about security as it relates to credit cards, paper with credit card numbers on them and the devices that process credit card transactions?

Online Security Awareness Education is provided, including:

✓ Payment Card Industry Overview
✓ Information Security
✓ Security Awareness Overview
✓ Sensitive Information
✓ Secure Practices for Associates



Security Awareness > **Security Awareness**

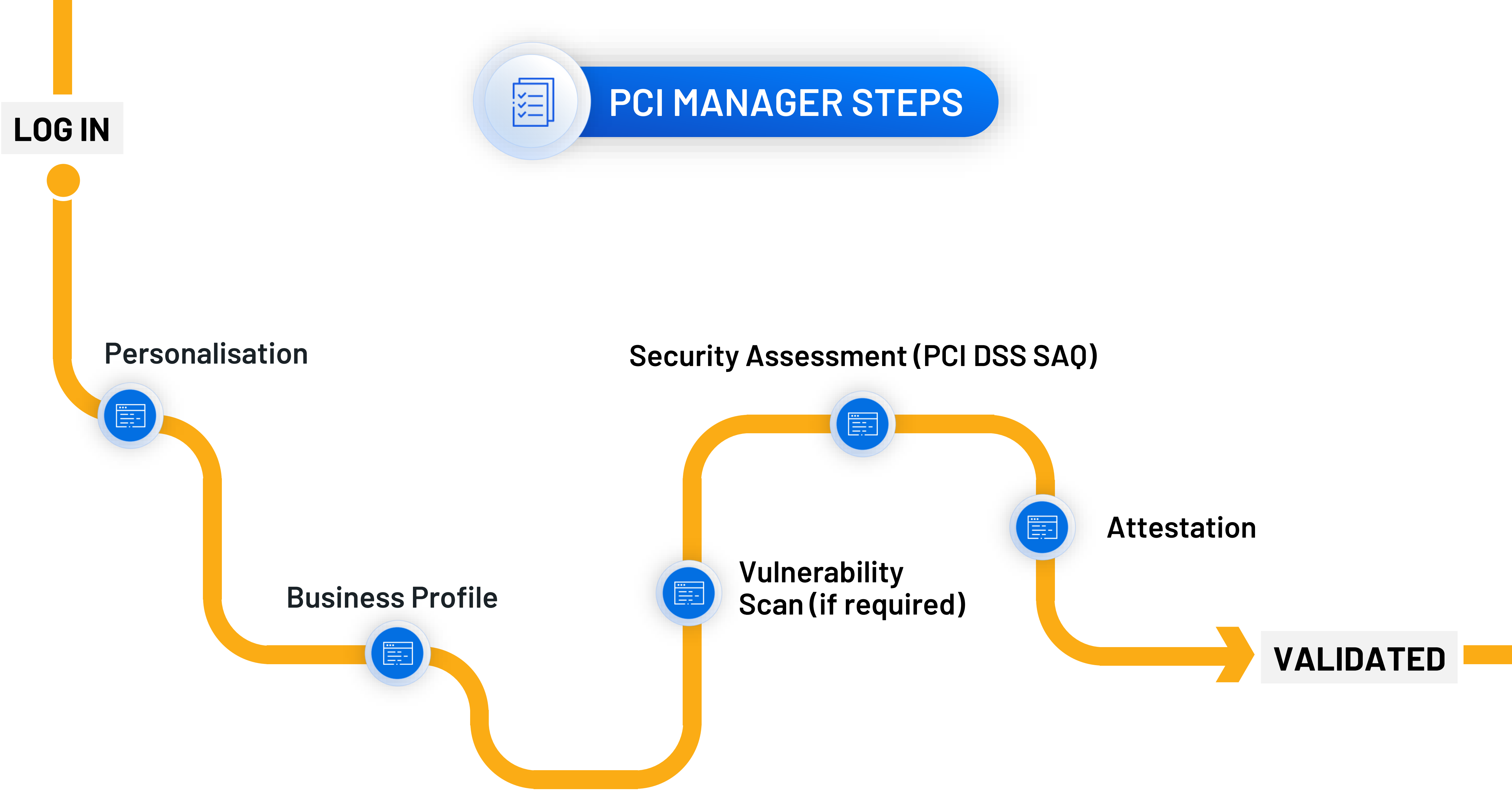
Importance of Awareness

You interact with valuable information every day, and no matter what your job is, it is your responsibility to protect that information.

Actions you take each day can have a direct effect on the security of your organization's information. Even simple actions that may seem harmless can expose your organization to a wide variety of information security risks.

Following security awareness best practices and your organization's security policy can greatly reduce security threats.

PCI MANAGER STEPS



LOG IN

Personalisation

Business Profile

Vulnerability Scan (if required)

Security Assessment (PCI DSS SAQ)

Attestation

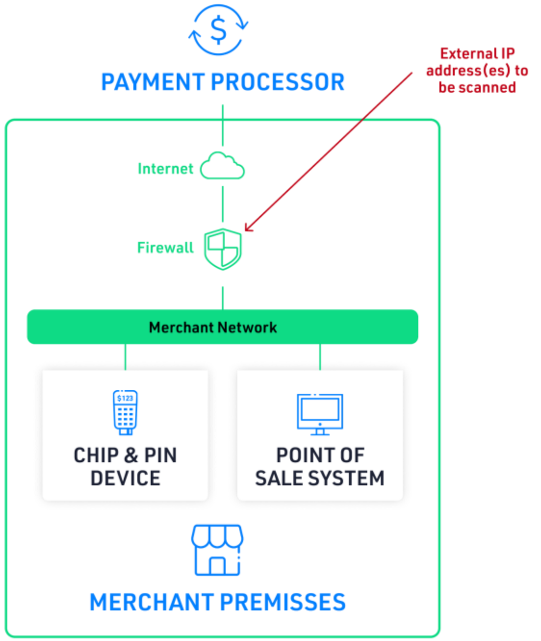
VALIDATED

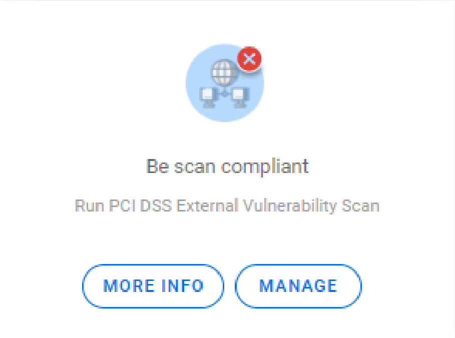
Vulnerability Scans

PCI Manager

- May be required based on Your Business Profile:
- Scans detect vulnerabilities **(security weaknesses)** affecting your Internet-facing systems

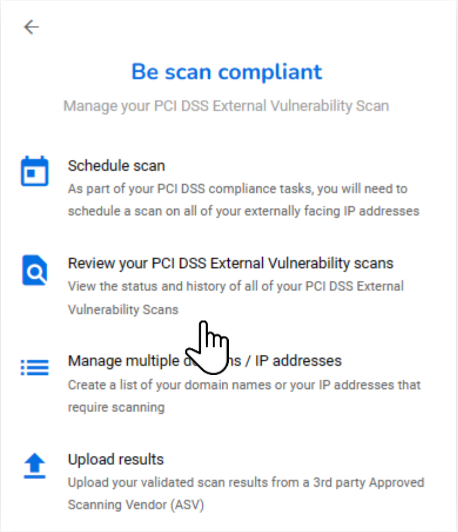
Scan the Internet IP addresses of all externally accessible systems that are **part of your CDE**, or **provide a path to** your CDE





Be scan compliant

Run PCI DSS External Vulnerability Scan



Be scan compliant

Manage your PCI DSS External Vulnerability Scan

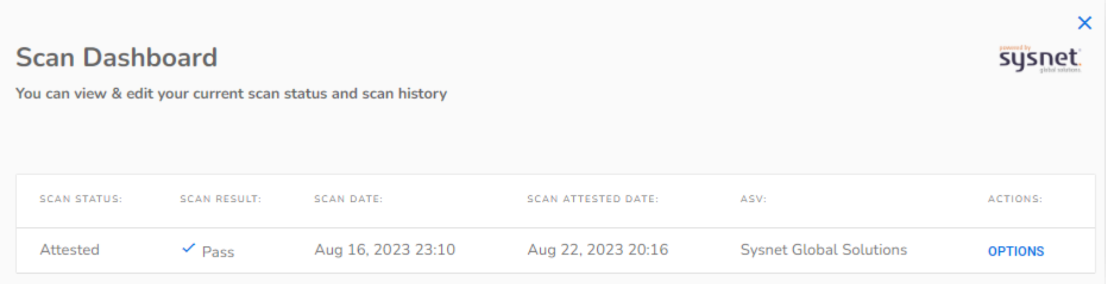
Schedule scan
As part of your PCI DSS compliance tasks, you will need to schedule a scan on all of your externally facing IP addresses

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)

- PCI Manager User Guide and Scan widget guides set-up, review and attestation of scans:



Scan Dashboard

You can view & edit your current scan status and scan history

SCAN STATUS:	SCAN RESULT:	SCAN DATE:	SCAN ATTESTED DATE:	ASV:	ACTIONS:
Attested	✓ Pass	Aug 16, 2023 23:10	Aug 22, 2023 20:16	Sysnet Global Solutions	OPTIONS

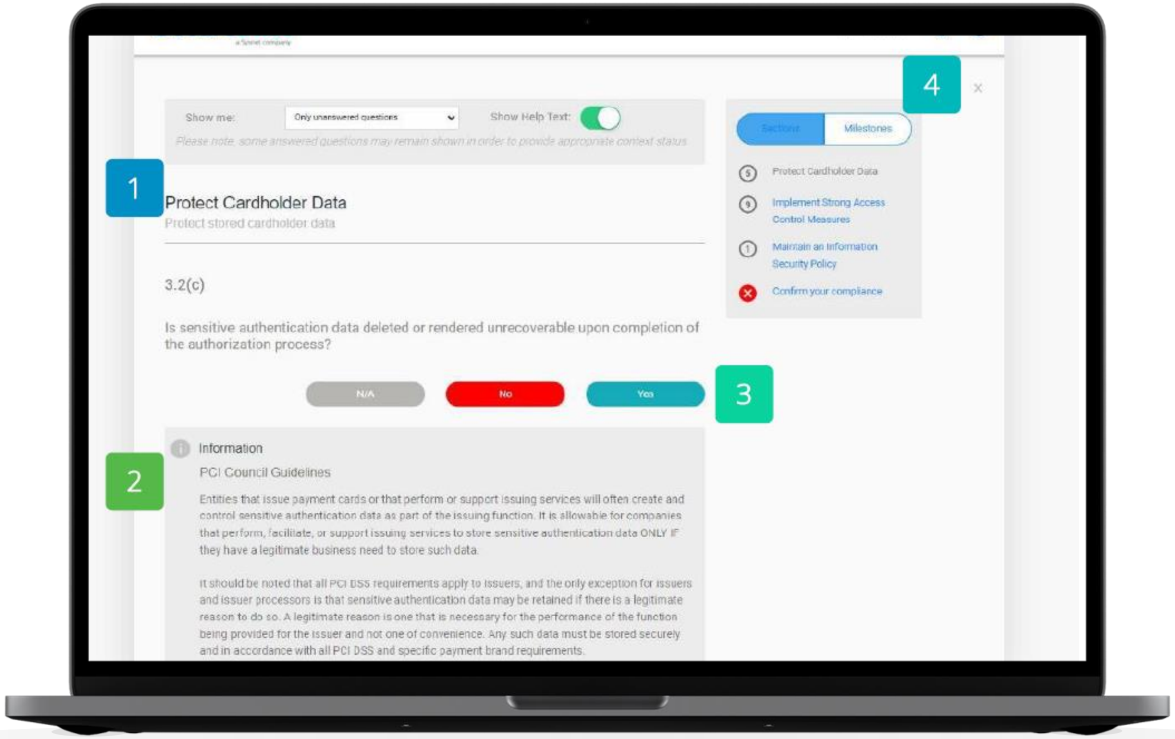
- Reminder emails sent when your next scan is due

Security Assessment

PCI Manager

- **Assess your measures to protect and secure your business against the applicable PCI DSS Requirements.**
- **Your 'Guide Me' business profile:**
  - ✓ Determines the **number** and **complexity** of the assessment questions
  - ✓ **Pre-populates** questions that do not apply or that you have already answered

1. You are guided through the questions.
2. More information is available in the box underneath each question.
3. Work your way through the questions, answering 'Yes', 'No' or 'N/A'
4. Box on the right shows your progress and the number of unanswered questions remaining.



Show me: Only unanswered questions

Show Help Text: ●

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

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

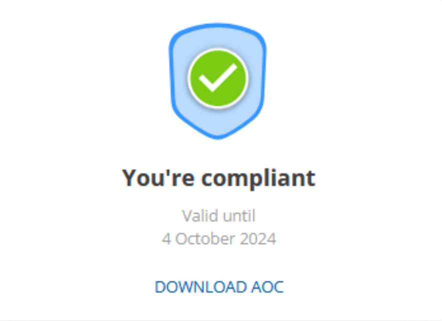
Entities that issue payment cards or that perform or support issuing services will often create and control sensitive authentication data as part of the issuing function. It is allowable for companies that perform, facilitate, or support issuing services to store sensitive authentication data ONLY IF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

Attest to your compliance

PCI Manager

- Attest to your compliance:
  - Confirm the information you provided is correct.
- Select 'Confirm your Attestation'
  - Your SAQ is **valid for one year**.
- **Your renewal date is shown on your dashboard:**

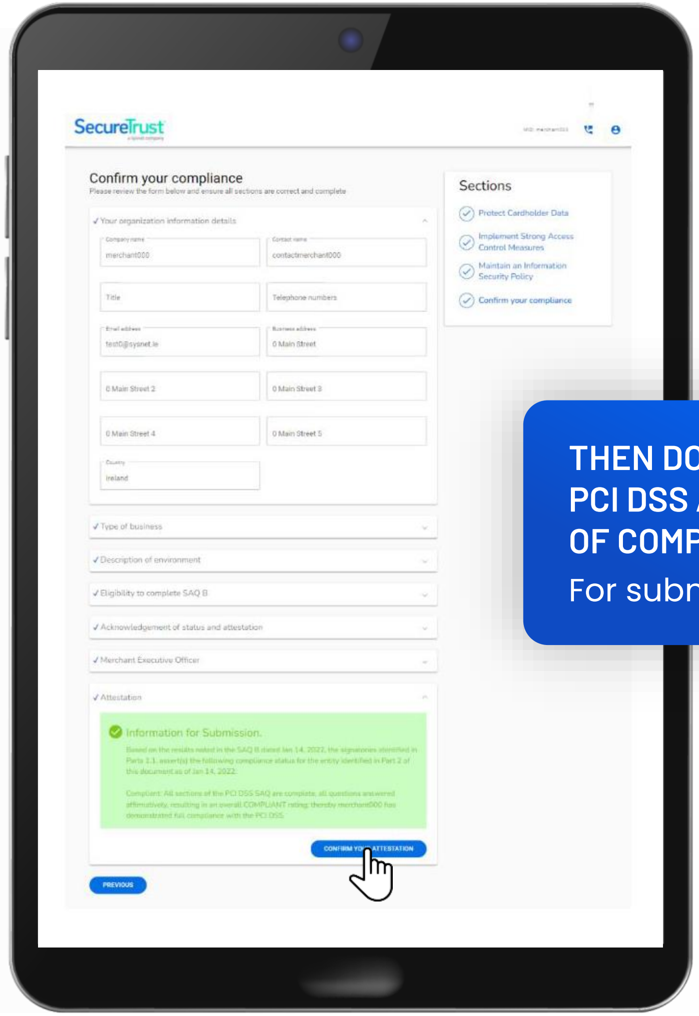


You're compliant

Valid until
4 October 2024

DOWNLOAD AOC

- Reminder emails are sent when it's time to:
  - Complete your next scan (if required for your business)
  - Revalidate your PCI DSS compliance.



SecureTrust

MID: merchant000

Confirm your compliance

Please review the form below and ensure all sections are correct and complete

✓ Your organization information details

Company name: merchant000	Contact name: contactmerchant000
Title	Telephone numbers
Email address: test0@sysnet.ie	Business address: 0 Main Street
0 Main Street 2	0 Main Street 3
0 Main Street 4	0 Main Street 5
Country: Ireland	

✓ Type of business

✓ Description of environment

✓ Eligibility to complete SAQ B

✓ Acknowledgement of status and attestation

✓ Merchant Executive Officer

✓ Attestation

Information for Submission.

Based on the results noted in the SAQ B dated Jan 14, 2022, 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 Jan 14, 2022.

Compliant: All sections of the PCI DSS SAQ are complete, all questions answered affirmatively, resulting in an overall COMPLIANT rating; thereby merchant000 has demonstrated full compliance with the PCI DSS.

CONFIRM YOUR ATTESTATION

PREVIOUS

Sections

- Protect Cardholder Data
- Implement Strong Access Control Measures
- Maintain an Information Security Policy
- Confirm your compliance

THEN DOWNLOAD YOUR PCI DSS ATTESTATION OF COMPLIANCE (AOC)

For submission to IATA

POLL

Understanding the PCI DSS

Conclusion

PCI DSS Compliance.

Avoid risk and financial consequences

- Don’t think *“a breach won’t happen to me and my business”*; there are risks to your business
- You and your business are not alone with PCI DSS
  - SecureTrust PCI Manager is just one of the solutions available to address your risks
  - The available tools simplify and guide you in your implementation of PCI DSS
- PCI DSS compliance does not have to be a significant expense:
  - It is risk-based data security based on your business’ exposure to and handling of card data
  - National associations and ECTAA can connect you with experts
  - QSA Companies are available to help you
- Compliance with the PCI DSS not only helps you meet IATA obligations;
  - Its good data security practices help you with your obligations to other industry bodies and regulators

Further guidance and resource links

Understanding PCI DSS

Today's presentation deck:
Click on Handouts pane or icon in the GoTo Webinar toolbar. Or download from: https://www.ectaa.org/en/media/webinars

IATA PCI DSS & Travel Agent Compliance Requirements
https://www.iata.org/en/services/finance/pci-dss/

SecureTrust PCI DSS Compliance Program for IATA Passenger Agents
https://www.securetrust.com/iata/

PCI Security Standards website:
https://www.pcisecuritystandards.org/

PCI DSS Self-Assessment Questionnaires (SAQs) downloadable from:
https://www.pcisecuritystandards.org/document_library/?category=saqs#results

PCI Information Supplements and Guidance from:
https://www.pcisecuritystandards.org/document_library e.g. Guidance for PCI DSS Scoping and Segmentation, Protecting Telephone-based Payment Card Data

PCI Merchant Resources:
https://www.pcisecuritystandards.org/merchants

VikingCloud Resources:

- Blog: https://www.vikingcloud.com/blog
- PCI DSS v4.0 eBooks: https://www.vikingcloud.com/ebooks/
- PCI DSS and v4.0 merchant information website: https://pciportal.info/

VIKINGCLOUD™ | ECTAA

THE EUROPEAN TRAVEL AGENTS'
AND TOUR OPERATORS' ASSOCIATIONS

Thank you.
Questions?

Maria Messo | Sales Director, European region
Call: +46 (0) 708 270 280
mariamesso@vikingcloud.com

SecureTrust PCI DSS Compliance Program for IATA
https://www.securetrust.com/iata/
PCI Manager: https://managepci.com/
Call: +1 312 267 3212; **Email:** support@securetrust.com

VIKINGCLOUD.COM in

BRINGING SECURITY
AND COMPLIANCE
TOGETHER

VIKINGCLOUD™

BUSINESS UNINTERRUPTED.

Confidentiality and Proprietary Information Notice

All information contained herein is the confidential and proprietary information of VikingCloud.

These materials are provided for informational purposes only and do not constitute a representation or warranty by VikingCloud. The information contained herein may not be reproduced, published or distributed to any third parties without the express prior written consent of VikingCloud.

VikingCloud and the VikingCloud logo are trademarks of VikingCloud, Inc. and/or its affiliates in the United States and other countries.