Barclaycard Data Security Manager

Face to Face – before you begin checklist

The following check-list can be used prior to completing your PCI DSS profile to help you gather the information required of you for your PCI DSS assessment.

You may be required to provide information about some or all of the following with regards to your Face to Face card payment processing environment:

NB: you are not recorded as PDCI DSS compliant until you have ticks in all the boxes on the home screen.

Checklist	Yes	No	N/A
The type of Point of Sale (POS) device/application you use: e.g. a Counter-top POS terminal (fixed or mobile), Integrated/Electronic POS terminal, Payment Application, Mobile Device, or Virtual Terminal	☐	☐	☐
The Make and Model of all Payment Terminals, PIN Entry Devices (PED) and/or PIN Pads (this is usually written on the terminal device)	☐	☐	☐
If you use a terminal that is not supplied by Barclaycard you will need to know the following:-			
• How your Point of Sale (POS) device/application sends the card information **to the acquirer/processor** for authorisation (e.g. over dial-up, internet, gprs)	☐	☐	☐
• If using an internet based device/application, do you have sufficient isolation of that device on the network, so that any other services or applications connected within your network cannot and do not have any connection with the devices/applications within your card environment?	☐	☐	☐
• The Vendor Name, Payment Application Name, Version and expiry date of Payment Applications e.g. on the Payment Terminal (such as Ingenico LLC, Universal EMV POS, V1.0x, 28/10/2019) or on your ecommerce website, in your suppliers documentation.	☐	☐	☐
• Are Payment Applications validated as compliant with the requirements of the Payment Application Data Security Standard (PA DSS) as published by the PCI Security Standards Council	☐	☐	☐

Your POS device may connect via a PSTN (Public Switched Telephone Network)/Telephone line, wirelessly using GPRS/3G or other mobile network, wirelessly via the Internet, wired direct via the Internet.

You can look up your Payment Application for compliance status at:

https://www.pcisecuritystandards.org/approved_companies_providers/vpa_agreement.php

Any third party you use that touches cardholder data by storing, transmitting and/or processing cardholder data should be registered on the VISA Europe Merchant Agent List (link below), and where applicable the VISA Inc. and MasterCard service provider programs.
https://www.visamerchantagentslist.com/

http://usa.visa.com/merchants/protect-your-business/cisp/service-providers.jsp

http://www.mastercard.com/us/company/en/whatwedo/complaint_providers.html

Make sure you can describe your cardholder data environment (i.e. description of the people (including third parties), premises, processes and technologies involved in the processing (entry, viewing, recording/printing), transmission (receipt/sending) and/or storage of cardholder data (both hard copy and electronic). This information must be included on your Attestation of Compliance (AOC) document.

There is a new requirement to carry out a minimum of an annual inspection of your POS terminals and to help with this there is a very useful document on skimming prevention/detection on the PCI SSC website

https://www.pcisecuritystandards.org/documents/Skimming_Prevention_At-a-Glance_Sept2014.pdf

Should you require any helpdesk support (via phone or online chat) this information will help us guide you in the right direction.