PCI DSS Training – Merchant ID Managers 2019

Introduction

- The University is required to comply with the Payment Card Industry Data Security Standard (PCI DSS) – which is a worldwide standard set up to help businesses (merchants) process card payments securely and reduce card fraud.

AMERICAN EXPRESS
DISCOVER
MasterCard
PCI Security Standards Council
VISA
JCB

Introduction

- This is a requirement of our contract with our acquirer, Global Payments, who manage all of our credit and debit card payments.
- A credit or debit card breach would lead to:
  - the immediate cessation of taking payments by this method – and thus cause severe disruption and loss to your Division. The University takes >£120m on credit and debit cards;
  - UoB-wide reputational damage (a loss of confidence in our security standards from students and customers)
  - heavy fines (up to £500k)
  - Very expensive and disruptive investigations and remedial procedures

globalpayments

Introduction (cont.)

- Several Divisions within the UoB process debit/credit card transactions and we have set ourselves up as having a number of separate Merchant IDs across the organisation.
- The UoB has a PCI DSS Policy which was approved on the 27th February 2017 – it is a requirement of all Merchant ID (MID) Managers, as well as any Heads of Division where payments are taken, to have read and understood the Policy, which can be found at http://www.bristol.ac.uk/infosec/policies/docs/
- This training is supplementary to the main Policy and is mandatory for all MID Managers and their deputies. Heads of Division have responsibilities within the Policy and have the opportunity to receive training.
- No staff member should handle cardholder data unless they have a business need and explicit authorisation to do so.
- ALL staff (including casual staff) who come in to contact with cardholder data MUST understand the basic principles of PCI DSS, the risks of various types of fraud and the incident response procedure before they start within their roles. Staff should receive training from their MID manager or Deputy MID manager on this. One useful resource for MID managers is the PCI DSS handout for Front of House staff. MID Managers are responsible for retaining records of this training and must make these available for inspection.

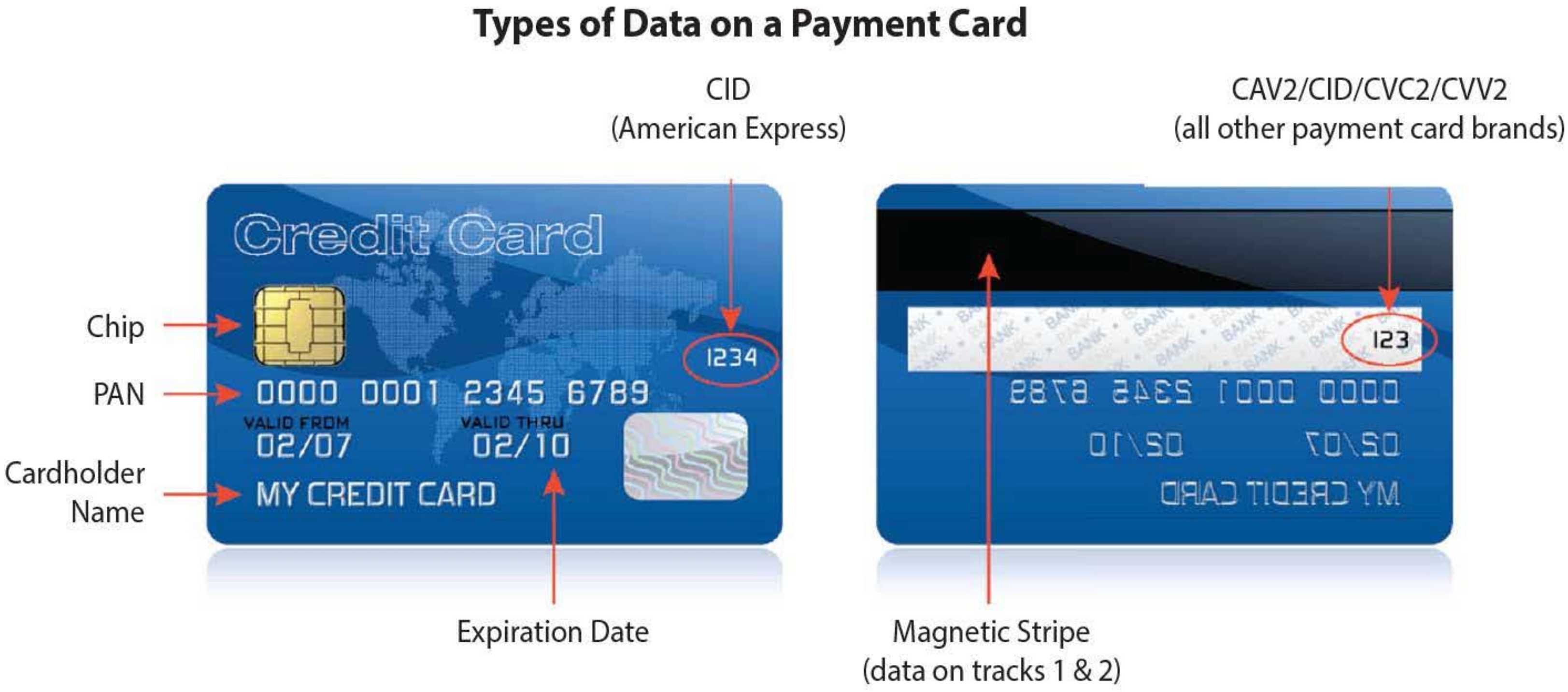
PCI DSS Governance

- UOB strategy and approach is to prevent any cardholder data being transmitted or stored on our systems, so taking them out of scope.
- The PCI Policy provides authorisation for the Information Security Assessor (ISA), Information Security Manager, a Finance Services Manager, or any of their representatives, to inspect any systems, databases, or physical areas of the University where cardholder data might be processed or stored.

Cardholder Data

- The PCI DSS standard is a requirement for any merchant that processes, transmits or stores Cardholder Data and is intended to help protect our customers from fraud.
- Complying with PCI DSS requirements does not guarantee that a security breach will not occur, but it reduces the risk.
- What is Cardholder Data?
  - **Primary Account Number (PAN)** – this is the 16 digit number on the front of the card
  - **Cardholder's Name**
  - **Expiry Date**
  - Card Verification Code or Value (**CVC/CVV/CVC2/CVV2**) – the rightmost 3 digit value printed in the signature panel area on the back of the card

Cardholder Data



Point-of-Sale (POS) Terminals

- POS terminals must be of a type approved by the Income Office.
- The model, serial number, security features and location of all terminals must be recorded and supplied to the Income Office.
- New or replacement terminals should be delivered to the Income Office to minimise opportunities for tampering, and so that the asset list can be accurately maintained. If this is not possible (e.g. emergency replacement) a secure procedure should be in place for receiving new terminals and the Serial Number must be reported to the Income Office (cash-office@bristol.ac.uk) as a priority.
- Devices must be stored securely when not in use, and checked daily for tampering or substitution. POS terminals must never be left unattended.
- Terminals must be returned to the Income Office when no longer required. The Income Office Manager will arrange for the MID to be deactivated.
- MID Managers should set up procedures to follow in relation to regular inspections of POS terminals.

Point-of-Sale (POS) Terminals (cont.)

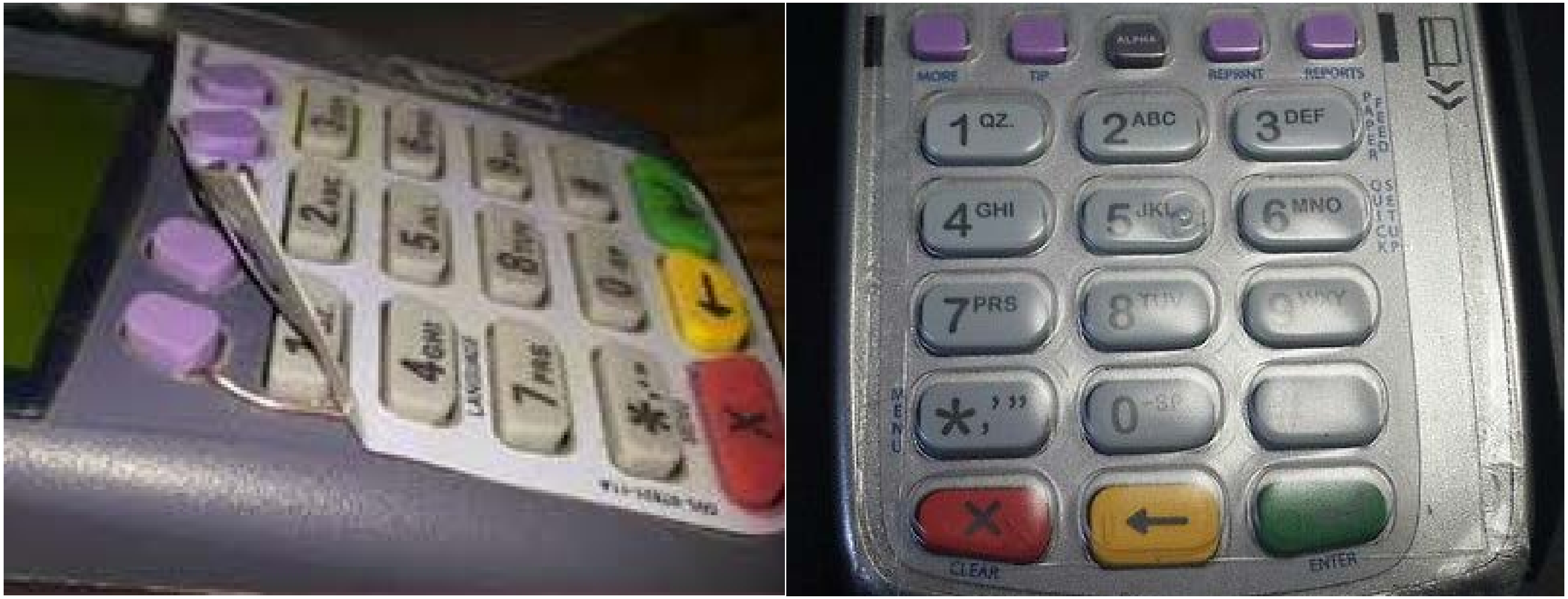
- Any suspicion of tampering must be reported in line with the Incident Response Procedure (see later slide).
- A default supervisor password is provided with new terminals and must be changed (to one of the MID Manager's choosing) during set-up. These passwords are usually required for refunds, batching and configuration changes. The password must only be shared with other relevant senior staff where absolutely essential, for instance with shift supervisors. When any of these staff leave, the password MUST be changed.
- Refunds should only be made to the original card the sale was made from.
- POS terminals should not be taken abroad or used at any location other than the merchant ID number they are linked to.
- CVC/CVV numbers and PINs must NEVER be stored after authorisation (although there may be circumstances in which a CVC/CVV is required to be securely stored **prior** to authorisation.

Compromised Point-of-Sale (POS) terminals

POS terminals need to be protected against tampering which can lead to Cardholder Data being skimmed.

Techniques to skim card details include:

Theft of terminals from sales areas of the University (including desks/offices)



Added overlays with skimming and key-logging hardware

Swapping good terminals for compromised terminals or installing malware while posing as a service technician

Swapping a good terminal for a compromised terminal, using large items to block attendants’ line of sight.

Shipping compromised terminals to merchants under the guise of a terminal upgrade and requiring the good terminals to be returned to the criminal

Handling Cardholder Data – Cardholder not present

- Cardholder Data must not be transmitted or requested to be transmitted via end-user messaging technologies such as email, instant messaging or SMS. If unsolicited Cardholder Data is received via such means, this must be notified to the Information Security Manager and the data securely deleted.
- If you receive an email containing cardholder data either reply from a new email or delete the cardholder details before replying. Don't just reply as you will re-submit the information.
- When receiving card details over the telephone be aware if you have to repeat the number back to the cardholder, as you may be overheard. Consider whether it is necessary and who may be able to hear you.

Handling Cardholder Data – Cardholder not present

- When receiving card details over the telephone, do not write down the cardholder details unless there is a defined business need, you can store it securely and can dispose of it securely (Shred-It bin) immediately after authorisation. It is best practice to directly process all payments directly through the POS terminal.
- University staff and students shall not store credit and debit cardholder data on local hard drives, shared storage (myFiles), cloud storage solutions, or any removable media (memory stick, CD/DVD) under any circumstances.
- Any Cardholder Data stored on University of Bristol systems must be reported to pci-dss@bristol.ac.uk immediately upon discovery.
- Telephone calls must not be recorded and Voice Over Internet Protocol (VOIP) must not be used.

Handling Cardholder Data – Cardholder present

- Cards must always remain visible to the Cardholder at all times.
- Merchant copy of receipts must be stored securely, and destroyed within 12 months.
- Security cameras must not be placed in such a position that Cardholder Data can be recorded, for instance the input of PINs in to a terminal.

INCIDENT RESPONSE PROCEDURE: Responding to a suspected breach of a POS terminal

- DO NOT SHUT DOWN the suspected POS terminal.
- IMMEDIATELY DISCONNECT the network cable from the back of the machine or base to contain and limit the exposure.
- DOCUMENT all steps taken. Include the date, time, location(s), person/people involved and action taken for each step.
- LABEL the machine ‘Do not touch unless directed by the PCI Incident Response Team’
- REPORT the incident to the PCI Incident Response Team

Reporting a breach (08:00-17:00 Monday to Friday)

- A breach might be discovered by our acquirer or a member of staff.
- Once the Incident Response Procedure has been completed, immediately contact a member of the PCI DSS Incident Response Team below (priority order):
    1. Matt Osborn – Information Security Manager, phone: (0117) 39 41151
    2. Rob Logan – Associate Director of Financial Operations and Procurement, phone: (0117) 42 82690
    3. Angela Nansera – Income Office Manager, phone: (0117) 928 7908
    4. Jason Smerdon – Group Finance Director, phone: (0117) 42 82585
    5. Robert Kerse – Chief Operating Officer, phone Rebecca Attwood (PA to COO): (0117) 39 40631
- All of the above are members of an Incident Response Team and they will immediately invoke our Incident Response Plan.
- Staff should inform their Supervisor, MID Manager and/or Deputy MID Manager as soon as possible after detecting the breach.

Reporting a breach (out-of-hours)

- Once the Incident Response Procedure has been completed immediately email PCI-DSS@bristol.ac.uk with the details of the breach and who can be contacted for further information.

- Please use ‘BREACH’ in the heading of the email and remember not to include any cardholder data.

- Staff should inform their Supervisor, MID Manager and/or Deputy MID Manager as soon as possible after detecting the breach.

Further training

- External training is available from the HEI/FE sector Special Interest Group (SIG) which may be beneficial for some MID managers, particularly those with large numbers of outlets.
- For further details please contact either Rob Logan or Angela Nansera.
- Please also let us know of any staff changes to the MID Manager/Deputy so that training can be arranged.

Thank you

For general queries relating to PCI DSS policy or procedure, please email pci-dss@bristol.ac.uk