Bite-sized training: Customer Not Present Card Transactions
Created: 18/05/2021

WARWICK
THE UNIVERSITY OF WARWICK

What is PCI DSS?

The Payment Card Industry Data Security Standards (PCI DSS) are the minimum Standards of security required to safeguard payment card transactions. The PCI Security Standards Council, who are responsible for ensuring the standards remain relevant as technology evolves, created these Standards. With the current version of the standards issued in May 2018 being v3.2.1. The University is contractually obliged, through our acquirer Global Payments, to obtain PCI DSS compliance. By maintaining the standards, we reduce the risk of exposure to payment card fraud for our students, staff and customers.

What is a Card Not Present (CNP) transaction?

'Card not present' means a transaction where the customer and their payment card are not present at point of sale. The card details are provided through a phone call or mail. Card details are **never** taken by email or other electronic communication means.

At the University, CNP transactions are processed using a Payment device (sometimes known as a PED or PDQ).

What do I need to do?

- Complete a daily visual check of the devices to ensure they have not been tampered with. Complete the daily log as evidence of review.
- Questions to ask when checking the device would be - Are there any unusual attachments; has the serial number been changed or tampered with; have the cables been tampered with; has the device been moved?
- Ensure the receipts only print the last four digits of the customer's card number. This is referred to as the card number being truncated.
- Ensure supervisor passwords are only known to supervisors and passwords are changed at a minimum when staff changes occur.
- Ensure the device is always visible to a team member.
- Ensure the device is stored in a secure location when not in use or cannot be observed.

Awareness is key!

- Look out for unusual behavior around the device.
- Is anybody hanging around the device in a suspicious manner?
- Is anyone 'shoulder surfing' or using a phone camera while customers are entering card data?
- Is the payment card in full sight of the customer at all times? There should be no need for anyone other than the customer to handle the card.
- Challenge vistors to your department/outlet, requesting review, access or swap out any of your payment devices. Ask to see ID/Credentials.

The PCI principles that particularly apply to 'face to face' transactions are:

Respond to concerns.

- If you suspect something is wrong, notify your supervisor/line manager immediately.
- Do not use the device, and let others know not to use it.
- For concerns with a device integrated with a till please contact Atia Chaudry Atia.Chaudry.1@warwick.ac.uk
- For concerns with a standalone device please contact Catherine Wallis c.wallis.1@warwick.ac.uk
- Ensure your query/concern has also been logged with the IT helpdesk.

For more information, please refer to the PED/PDQ user guide.