Card Payment Policy – Operating Guidelines

Appendix

When we process or store cardholder data, we have a responsibility to protect our customers from theft and fraud by ensuring that we use and store their data in a secure way.

What is PCI DSS?

PCI DSS stands for "Payment Card Industry Data Security Standards". PCI DSS is a set of requirements developed by the five card brands: VISA, MasterCard, AMEX, JCB and Discover. Their aim was to put together a common set of security principles. The purpose of PCI DSS is to ensure that businesses are reducing the risk of card data theft and fraud and therefore providing a secure environment for their customers to make payment.

Any employee who comes into contact with cardholder data needs to be aware of PCI DSS, and how they as an individual can reduce the risk of cardholder data theft and fraud.

Why is PCI DSS important to the University?

If we process, transmit or store cardholder data, we have a responsibility to secure it and protect our customers from fraud. Because it is considered so important, compliance with PCI DSS is a requirement of our contract with our acquirer, Lloyds Cardnet, as well as other software and service providers. Being compliant shows we have worked to reduce the risk of data theft and to provide a secure payment environment for our customers.

The consequences of a security breach resulting in customer card data being accessed by an unauthorised party can be wide-ranging:

- Inconvenience and distress to our customers – card data theft and fraud can be very upsetting, and take time to resolve.
- Financial sanctions – the University could be fined if card data is lost.
- We could be assessed as a high risk merchant. We would need to have external verification of our security, which would be expensive and time consuming for the University.
- The University could have its ability to take card payments removed. This would cause increased workload, and could lead to loss of business.
- Reputational damage – data security breaches can get a lot of publicity, and the trust our customers have in us could be severely damaged.

Complying with PCI DSS requirements does not guarantee that a security breach will not occur, but it reduces the risk, and our liability.

What does PCI DSS relate to?

Primary Account Number (PAN) – this is the long number on the front of the card. If we do not handle or store the PAN, then PCI DSS does not apply. It should therefore only be handled or stored where there is a clear and essential business need to do so. There are a number of situations in which University staff might come into contact with the PAN:

- On the customer's card when they make a face to face transaction.
- This from customers over the phone, fax or by post, when you take Cardholder Not Present transactions.

- Merchant copies of receipts may have the PAN printed on them.

CVC – the authorisation number on the back of the card. This is Sensitive Authentication Data (SAD) and must never be stored after the payment has been authorised. You may come into contact with the CVC when taking a telephone payment, or when processing a mail order transaction. If the CVC is written down during a telephone call, it should be destroyed once the payment has been processed. **We are not allowed to store the CVC after the transaction has been processed.**

Card terminals

Terminal to be kept in a locked office outwith business hours, and if the room is ever left unattended then the terminal needs to be checked to make sure that it has not been tampered with.

Audit log to be completed each day with the date and signature of the member of staff who checked the terminal before the start of each working day to make sure it has not been tampered with.

Employees who takes card payments or handle cardholder data, have a responsibility to carry out their work according to procedures and University policy regarding PCI DSS. By doing this staff are protecting your customer's data from theft, protecting the University from the consequences of a data security breach, and protecting yourself in the event of a breach.

If you are concerned that a process may not be secure, and may put cardholder data at risk, you have an obligation to report this to your manager or the Finance Office.

How does PCI DSS relate to what I do?

The following examples highlight some of the ways you should take PCI DSS into account when dealing with card data. The list does not cover all situations, and some of the scenarios might not be relevant or appropriate to you. If you are unsure how to apply PCI DSS to your processes, please seek advice from your manager.

Remember, the best defence against cardholder data theft is not to store it – if we do not have it, it cannot be stolen from us.

Payments made in person

Employees should not need to handle the customer's card. Once you have entered the amount, the customer should put their card in the terminal for chip and pin transactions, or pass their card over the terminal for contactless transactions. If you do not handle the card, you do not come into contact with the card holder data.

One way in which criminals can obtain card data is by tampering with the card terminals so that the cardholder data can be collected as the payment is being processed. This is called skimming. It is therefore important to ensure that terminals are not tampered with. Portable terminals must be kept out of reach of customers and the public, and stored securely out of hours. You should be able to recognise if a terminal has been tampered with - you may have a reference photo of your terminal, so you can compare the terminal to the photo and identify

any changes. If you think your terminal may have been tampered with, stop using it and alert your manager immediately.

Merchant copies of till receipts that display the PAN must be securely stored at all times in a designated, locked place with restricted access. They must not be left out on a counter.

Telephone payments

If someone calls to make a card payment, ideally you should enter the details straight into the terminal. If the terminal is not available, you should arrange to call the customer back when the terminal is available, and then enter the details directly into the terminal. If this is not possible, and your manager allows, you can write down the details and process the payment when the terminal is available. This should be within one hour of writing the details down:

If a terminal is not available to take a payment when a customer calls and you are not able to call them back later, you can write down the details, if this is allowed by your manager.

The card details should be securely stored in a locked location. The card details should only be kept until the payment has been processed.

Once the payment has been processed, the written card details should be securely destroyed by cross shredding.

It is important to be aware of what is going on around you, and ensure that no-one can overhear the customer's card details while you are processing the transaction:

If you work in a public area, e.g. a reception desk, never read the customer's card details back to them, in case you are overheard. You can confirm part of the number (e.g. the last 4 digits) if necessary.

Calls where card payments are taken must never be recorded, as this counts as electronic storage of the card data.

Card details received by fax

Card data received by fax can be considered secure, as long as the fax machine does not store the image and is located in a secure area which the public cannot access.
If a customer tells you they will be sending details by fax, you could ask them to call before they send it to ensure that someone will be there to receive it, so the details are not left on the fax machine. After the payment has been processed, we are not allowed to store the CVC number and it should be removed from the form and destroyed. The PAN should only be kept if there is a business need to do so, and must be stored securely.

Faxes containing card data should be collected by an authorised team member as soon as they arrive.

If the payment cannot be processed straight away, the card data should be stored securely until it is processed.

After processing, the CVC number, and ideally the PAN, should be removed and securely destroyed by cross shredding.

Card details received by post

Card details received by post must be addressed to and opened by authorised employees. Transactions should be processed as soon as possible, and within 2 working days. After the payment has been processed, we are not allowed to store the CVC number and it should be removed from the form and destroyed. The PAN should only be kept if there is a business need to do so, and must be stored securely.

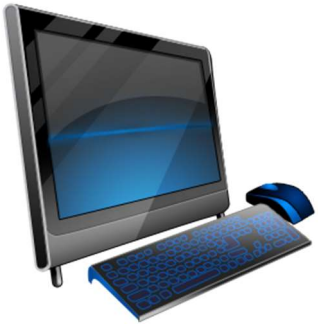
Letters containing card data should be opened by an authorised team member.

The card data should be stored securely until it is processed.

Once the payment has been processed, the CVC number, and ideally the PAN should be removed and securely destroyed by cross shredding.

Payments made online

Online payments should be encouraged where possible as the University and individual team members do not have access to the cardholder data at any time. It also saves time and is more efficient.



Do not impersonate a customer to put a payment through online on their behalf, either over the phone or in person, even if you have their permission. If the customer is unable to pay online themselves, offer an alternative method of payment. Only trained staff working in designated offices should enter a customer's card details online.

Card details received by email

Email is not a secure method for sending or receiving cardholder data, so you should never ask a customer to email their card details to you. If a customer sends them to you in this way, you must not forward them onto another member of staff. They must be deleted without being processed. If we accept and process details sent by email, we are accepting responsibility for the security of delivery, and therefore the email system, which we cannot do.

Card details received by email must not be processed or forwarded on to another email address. You should reply, ensuring all cardholder data has been removed, to advise them that we cannot accept details by email and that they need to provide their details by another method. If you need to keep the email for your records, you must edit the email to remove the cardholder data, and only save the edited version. The original must be deleted.

Physical storage and disposal of card data

Card data should only be retained and stored if there is a business need to do so. If you are unsure if card details should be kept, check with your line manager.

Card data should be securely stored in a locked location, with access to the key recorded.

Card data should be stored for 6 years plus current financial year.

When the card data no longer needs to be stored, it should be securely destroyed by cross-cut

Cardholder data should only be destroyed with your manager's authorisation. If you shred the documents, it must be done using a cross-cut shredder, to ensure the data cannot be reconstructed.

Electronic storage of card data

Card data must **never** be stored electronically – if it is on our networks, there is the potential for unauthorised access. This includes: data stored in files on your computer or network; electronic images, such as efax; recorded telephone calls etc. If you collect CCTV, you must ensure that it cannot capture card data. If you have any card data stored electronically, you must contact the PCI DSS contacts immediately.

What should I do if I suspect someone has gained unauthorised access to card data?

If you believe that an unauthorised person has gained access to cardholder data that the University holds (e.g. if there has been a break in to an area where cardholder data is stored, or you believe a terminal has been tampered with) you must inform your line manager and the PCI DSS contacts at once. If a card terminal may have been tampered with, stop using that terminal and unplug it, but do not change anything and inform the PCI DSS contact immediately.

If you have any questions about PCI DSS, please speak to your manager for guidance. Any further queries should be referred to the Finance Office PCI DSS contacts.

PCI DSS Contacts

Sally Dimeo, Head of Systems and Treasury – 01786 466696.
Dawn Farmer, Finance Systems Support Officer – 01786 467122.