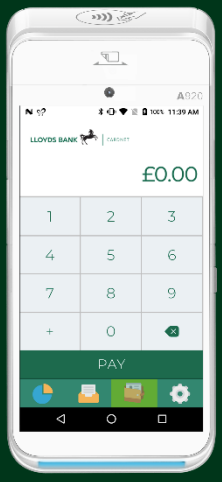
LLOYDS BANK

CARDNET

Cardnet Terminal



PCI DSS: Security Measures for Your Business

This quick look security guide covers the key security points that you need to be aware of as part of your commitment to data security.

This security guide is specific to the method you use to accept card payments, with this guide relating to your Lloyds Bank Cardnet Android mobile payment solution. The solution consists of:

The Cardnet Terminal (PAX A920 PIN Entry Device)

This guide relates only to this method of accepting card payments. If you use any other solution in addition to this, this guide does not apply to that method and you will need to comply with the PCI DSS standards in relation to that product. In addition, this guide and your attested compliance requires your business to not store cardholder data physically or electronically.

You have agreed to comply with all of the statements in this guide. If you no longer agree with any statement, then you will need to get in touch with us so that we can help you to reduce your risk.

Share this guide with all staff members in your business that use the Android mobile payment terminal or handle your customers' payment card details so they are aware of what they need to do to keep your customers' payment card details safe.

Please keep a copy of this guide on your business premises so that all staff members have access to it.

Quick tip

- Cardholder Data – this is the information on a payment card needed to make a card payment.
- Sensitive Authentication Data – is all of the elements of a payment card used to verify the identity of the cardholder. This includes the data contained on the card's magnetic stripe or chip, the card security number (which is the three-digit or four-digit number printed on the card) and the cardholder's PIN and 'PIN block'.

Secure and protect payment card data

- My business collects or processes cardholder data and/or sensitive authentication data only when and where it really is needed.
- My business does not keep or store cardholder data after the initial transaction.
- My business does not keep or store sensitive authentication data after the initial payment transaction has been processed.
- All cardholder data and sensitive authentication data collected is destroyed securely or erased once it is no longer needed for a business reason.
- We destroy or erase cardholder data and/or sensitive authentication data using methods that make sure the information cannot be reconstructed or recovered.
- Keeping payment devices secure
- My business only uses the authorised Lloyds Bank Cardnet mobile payment terminals (PAX A920 PIN entry devices).
- The PIN entry devices are secured and protected against tampering or unauthorised substitution at all times, including when in storage, when not in active use and at points-of-sale.
- I only permit authorised staff to install, configure or operate the mobile payment solution.
- I have kept a record of the location and serial number of the devices and make regular checks to ensure it has not been tampered with or been replaced with a fraudulent device.
- The PIN entry devices are not installed, replaced or returned without prior verification and the identity of any persons claiming to be repair or maintenance personnel is confirmed before access to devices is granted.

Raise security awareness

- My business has an information security policy (included on page 3 and 4 in this guide) that lets my staff know what they need to do to keep my customers' payment card data safe.
- All employees and personnel in my business have been taken through the company information security policy. They understand their role and the responsibility they have in protecting customer cardholder data.
- My business uses induction or orientation sessions to make sure that all new hires, temporary staff and contractors are made aware of the security policies in place.
- My employees are periodically reminded of their security responsibilities.
- Plan of action in the event of a security incident or breach
- My business is prepared in case of a security incident or data breach.
- My business has a security incident response plan (included on page 5 and 6 in this guide) to help us respond quickly and effectively should the worst happen.
- My security incident response plan anticipates the types of incidents my business may experience.
- The people working for my business (whether staff or third party providers) know to report anything that does not seem right.

Information Security Policy

This Security Policy applies to the acceptance and processing of customer present card payments using the approved Lloyds Bank Cardnet Android mobile payment terminal (PAX A920 PIN Entry Device) during the period of your agreement.

This policy applies to:

All parties with responsibility for taking card payments for Face to Face, Mail or Telephone Order transactions are required to understand their responsibilities and meet the requirements set out in this document. This includes and is not limited to all business employees, temporary or agency staff and contractors accepting card payments or handling payment card data.

The only systems that may be used to accept, process, or transmit payment card data are the Lloyds Bank Cardnet-supplied Android mobile payment terminal.

Protecting payment card data

All payment transactions should be processed via the Android mobile payment terminal. No card details should be written down and we recommend that you do not create or hold any documentation showing cardholder data or sensitive authentication. If you do create any such data, this must be held securely and following authorisation of a transaction, this data must be destroyed.

Methods to physically secure any documents containing cardholder data include storing them in a locked drawer, cabinet or safe, or other method that protects against unauthorised access, accidental loss or theft.

Payment card data must not be retained electronically (other than within the Lloyds Bank Cardnet Android mobile payment terminal).

Protecting your device

- Use the Lloyds Bank Cardnet Android mobile payment terminal only as intended by Lloyds Bank Cardnet.
- Lloyds Bank Cardnet Android mobile payment terminals must be received, stored, deployed and used in accordance with the applicable installation and configuration instructions provided.
- Your Lloyds Bank Cardnet Android mobile payment terminal must be secured at all times, including upon delivery, when in storage and in use at points-of-sale, and must be and protected against tampering or unauthorised substitution.
- Do not leave it unattended or in plain view at any time, and make a note of the make, model and serial number of your devices in the following table:

Secure storage location	Make	Model	Device Serial No. / Unique Identifier
<<Location details>>	*XXXX*	*XXXX*	*XYX-111-222-333*

- The list of devices must be updated whenever they are added, moved, replaced or decommissioned.
- Limit access to the Lloyds Bank Cardnet Android mobile payment terminal to authorised staff who have a need to access to or use the device to do their job.
- Make sure only authorised staff, with a job-related need for access, can use the Lloyds Bank Cardnet Android mobile payment terminal.

- Make sure anyone who uses the Lloyds Bank Cardnet Android mobile payment terminal to accept card payments is trained to be aware of and to challenge suspicious behaviour around the devices.
- Regularly check your PIN Entry Devices to ensure they have not been tampered with or substituted.
- Be suspicious of anyone seeking to 'inspect' your devices or offering to 'upgrade' them. Criminals may claim to be repair or maintenance personnel in order to gain access to PIN Entry devices.
- Only allow access to or replacement of devices if this is based on prior notification/agreement with Lloyds Bank Cardnet.
- Be aware of suspicious behaviour around the Android mobile payment terminal (PIN Entry Devices). For example, attempts by unknown persons to gain access to, unplug or open the devices.
- Staff must be trained to report suspicious behaviour and indications of device tampering or substitution.

Security Incident Response Plan

A security incident may not be recognised straightaway, however there may be indicators of a security breach, unauthorised activity, or signs of misuse within the environment.

Look out for any indications that a security incident has occurred or may be in progress. In relation to your Lloyds Bank Cardnet Android mobile payment terminal, indications may include:

- Devices lost, stolen or substituted (terminal serial no./unique identifier no longer matches the device inventory list).
- Changes of Lloyds Bank Cardnet device behaviour when taking payments, for example, chip read of cards starts to fail every time; forcing use of the card swipe.
- Visible damage to the PIN Entry device.
- Non standard stickers covering parts of the device.

Copies of the security incident response plan must be available to all relevant staff members and the Company shall take steps to ensure that all relevant staff understand security incident response plan and what is expected of them.

Testing and Updates

The Incident Response Plan must be checked and tested at least once annually. Testing can be performed using walkthroughs or practical simulations of potential incident scenarios to identify process gaps and improvement areas, and any updates distributed to all relevant colleagues.

Roles and responsibilities

Insert details below:

Job Title/Role	Contact Name	Contact Telephone	Contact Email
Primary incident response contact			
Secondary incident response contact			

What to do in the event of a payment card data breach

If you suspect you have experienced a payment card data breach or your device has been tampered with in any way:

- Stop using the Lloyds Bank Cardnet solution to take card payments, turn off the device.
- Contact Lloyds Bank Cardnet on 01268 567100 (lines open Mon-Sat 8am-6pm).

External Contacts

External Party	Email	Telephone
Lloyds Bank Cardnet – Your Acquirer	CardnetTerminal@lloydsbanking.com	01268 567 100
Local Law Enforcement	n/a	101
National Fraud & Cyber Crime Reporting Centre	Report online: http://www.actionfraud.police.uk/report-a-fraud-including-online-crime-questions	0300 123 2040
For use if you are unable to contact Lloyds Bank Cardnet:		
Visa Europe Data Compromise Team	datacompromise@visa.com	+44 (0) 20 7795 5031
Mastercard	account_data_compomise@mastercard.com	-

Third Party Service Providers

Service Providers are any third-party organisation which processes payment card data on behalf of the business, that payment card data is shared with or that could impact the security of customer payment card data.

The approved service providers for the Lloyds Bank Cardnet mobile payment terminal are:

- PAX (Hardware manufacturer)
- Lloyds Bank Cardnet (Acquiring and Solution supplier (the solution is provided in conjunction with Handpoint)
- Handpoint (Solution supplier, Payment Gateway and Payment Service Provider)

Security Awareness

All parties deploying, storing or using your Lloyds Bank Cardnet mobile payment terminal shall be made aware of the obligations and responsibilities in this guide, including the security policies and procedures, and the importance of maintaining the security of customer payment card data.

The policies and procedures outlined in and required by this document shall be incorporated into business practice to maintain a high level of security awareness.

This guide shall be regularly reviewed with staff, for example by holding periodic security awareness meetings to ensure responsibilities and procedures are understood and adhered to.

This document shall be distributed to all staff, temporary or agency staff and contractors. All new hires, temporary staff and contractors shall be made aware of the security guide upon hire.

All staff must confirm, at least annually, that they understand and will adhere to the security guide.

Any breaches of this policy must be reported to the primary incident response contact. Breaches shall be investigated and reported in accordance with the Security Incident Response Plan if a breach of payment card data is identified. Serious policy breaches may be dealt with under staff disciplinary procedures.