CARDNET

SECURITY GUIDE

How to meet the Payment Card Industry Data Security Standard

July 2022

LLOYDS BANK

This guide covers how to protect:

- your customers' payment data
- your pay-as-you-go mobile card reader by Lloyds Bank Cardnet
- the Lloyds Bank Cardnet app, along with your own tablet or smartphone device.

If you applied for such a card reader, you'll have agreed to comply with this guide. If you no longer agree with any of the statements, you'll need to contact us. This is so we can help you reduce your risk.

The guide is based on the Payment Card Industry Data Security Standard, a global standard to protect payment data.

Your commitment to data security

Tip

Payment data refers to:

- data on a payment card needed to make the payment, such as the the 16-digit card number
- data to confirm the cardholder's identity, held on the magnetic stripe or chip, the security number (three- or four-digit number on the card), or the cardholder's PIN.

Protect payment data

My business:

- only uses the card reader together with the app
- does not write down, keep or store payment data.

Protect the card reader

My business:

- stores and uses the card reader according to the Lloyds Bank Cardnet guides received
- does not leave the card reader unattended or in plain view
- keeps an up-to-date record of the location, make, model and serial number of each card reader as below.

Secure storage location	Make	Model	Serial number or unique identifier
<Location details>	XXXX	XXXX	XYX-111-222-333

Work with authorised personnel only

My business:

- only allows card readers to be installed, replaced or returned after receiving notice from Lloyds Bank Cardnet
- confirms the identity of anyone claiming to be authorised repair or maintenance personnel seeking to 'inspect' or offering to 'upgrade' the card reader
- only allows authorised staff to access and use the card reader, app and mobile devices
- checks regularly for tampering or unauthorised replacement, both when the card reader is and isn't in use.

Protect mobile devices

My business:

- hasn't bypassed mobile device security measures
- only installs software and apps from trusted sources
- only uses mobile devices that continue to receive security updates
- updates mobile devices whenever prompted
- installs app updates as they become available
- locks mobile devices when inactive, using a PIN or passcode
- limits knowledge of access details to authorised staff.

Raise security awareness

My business:

- shares this guide with all colleagues, such as employees, agency staff or contractors who use the card reader and app or handle payment data
- keeps a copy of this guide on business premises, so that those colleagues can access it
- makes all relevant new colleagues aware of the guide through induction sessions
- reminds all relevant colleagues of their security responsibilities from time to time.

Plan for a security incident

My business:

- is prepared in case of a security incident
- has a response plan (as below) to help respond to a security incident quickly and effectively
- has trained relevant colleagues in how to challenge and report anything that doesn't seem right.

Security incident response plan

What do I need to report?

Report:

- any stolen, lost or damaged card reader
- tampering or unauthorised replacement of a card reader (the serial number or unique identifier no longer matches your records)
- changes of app or card reader behaviour
- lost, stolen, or misplaced paper documents or other materials with payment data
- card-skimming devices or non-standard stickers on a card reader.

When do I need to report it by?

Report it as soon as possible or within 24 hours.

Who do I need to call?

Contact Lloyds Bank Cardnet on **01268 567 100**, Monday to Saturday, 8am to 9pm.

What else do I need to do?

- Stop using the card reader and turn it off.
- Delete the Bluetooth link from your mobile device.
- Report the incident to your primary incident response contact (see overleaf).

Your incident response contacts

List at least two people in your business:

Job title or role	Name	Phone	Email
Primary incident response contact			
Secondary incident response contact			

External contacts

Your first call outside your business should be to Lloyds Bank Cardnet, as in the steps above. You may also wish to contact these services:

Name	Email	Phone	Example of when to contact
Visa Europe Data Compromise Team	**datacompromise@visa.com**	**+44 (0)20 7795 5031**	You're unable to reach us.
Mastercard	**account_data_compomise@mastercard.com**	n/a	You're unable to reach us.
Information Commissioner's Office (ICO)	Report online: **https://ico.org.uk/for-organisations/report-a-breach**	n/a	There's been a payment data breach.
Local law enforcement	n/a	**101**	Your card reader has been stolen.
Action Fraud	Report online: **https://www.actionfraud.police.uk**	**0300 123 2040**	Someone has tampered with your card reader.

Testing and updates

You must check the incident response plan at least once a year and pass on any updates to all relevant colleagues.

Also test the plan once a year using walkthroughs or practical simulations of incident scenarios. This will help you find process gaps and what you need to improve.

Find out more

Go to lloydsbankcardnet.com

Call us on 01268 567100
lines open from 8.00am
to 9.00pm Monday to Saturday

Please contact us if you'd like this in an alternative format such as large print, Braille or audio.

Important Information

Calls may be monitored or recorded in case we need to check we have carried out your instructions correctly and to help improve our quality of service.

Please remember we cannot guarantee the security of messages sent by email.

Lloyds Bank plc. Registered Office: 25 Gresham Street, London EC2V 7HN. Registered in England and Wales No. 2065. Authorised by the Prudential Regulation Authority and regulated by the Financial Conduct Authority and the Prudential Regulation Authority.

Lloyds Bank plc is covered by the Financial Ombudsman Service. (Please note that due to the eligibility criteria of this scheme not all Lloyds Bank customers will be covered.)

This information is correct as of July 2022.

Our service promise

If you experience a problem, we will always try to resolve it as quickly as possible. Please bring it to the attention of any member of staff. Our complaints procedures are published at lloydsbankcardnet.com/contactus

LLOYDS BANK

CRD00191 (07/22)