PCI DSS Guidance for Fundraising Staff and Volunteers

Protecting and using information in the correct way is vital to delivering excellent quality services to our supporters and encouraging them to continue their vital support of our work to provode care to terminally ill patients and their families.

Introduction

Donations provided by members of the public using payment cards (credit/debit cards etc) have always been a mechanism for contributions to the work of Marie Curie. With the convenience, wider acceptance and use of contactless transactions, alongside increased spending limits for these transactions, this has markedly increased. Hence facilities to take card payments are increasingly part of face-to-face fundraising events.

To ensure the protection of the card data being processed and to meet compliance requirements under the Payment Card Industry Data Security Standard (PCI DSS), this guidance has been developed to ensure that you know how to handle these devices and process transactions securely.

Failure to comply with the guidance will put Marie Curie at risk of fines and penalties, as well as risk damaging donor confidence in Marie Curie.

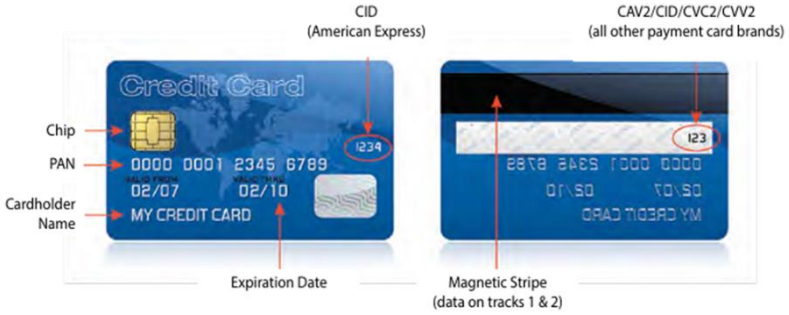
PCI DSS guidance is to be read and signed on joining Marie Curie and refreshed annually.

Learning Objectives

On reading this guidance you will understand:
1. What the Prerequisites for Handling Payment Card Data are
2. What Payment Card Data is and how to handle it safely and securely
3. What an information security incident is and how to report it
4. Where to find further information

What is Payment Card Data?

Payment Card Data refers to the information held on a branded credit/debit card. The following explains the types of data which are considered payment card data.



Marie Curie is a registered charity in England and Wales (207994) and Scotland (SC038731).
Registered as a company limited by guarantee in England & Wales (507597).
Registered Office: One Embassy Gardens, 8 Viaduct Gardens, London, SW11 7BW.

Basic Rules

1. You may only take card payments if you have been trained on how to do so safely and securely using a PDQ or contactless device.
2. You may only take card payments if the customer is present (i.e. standing in front of you with their card in hand).
3. Never handle a customer's payment card unless the customer specifically asks you to do so (e.g. they may require assistance putting the card into the slot). If you are asked to assist, always keep the card in sight of the Customer.
4. Do not speak customer's card details out loud or share them with anyone else.
5. Do not write card data down on paper, type it into e-mails or any instant messaging services.
6. Never enter card data into any unauthorised system.

Tracking the Devices

Please ensure that you update the contactless log provided to you by your Fundraising Manager each time you use a contactless device. The purpose of the log is to ensure that the devices are accounted for and can be located if needed. The log should include the below information:

- Make/model of the device
- Serial number (usually located at the back of the unit)
- Name of the volunteer/fundraising using the device
- Date that the device is being used

Tamper Checks

1. The card payment machines will automatically go into tamper mode and stop working if they detect signs of someone trying to get into the unit. If tamper mode is displayed on your unit, you need to call your Fundraising manager in order to have a replacement unit sent out.
2. Look out for suspicious behaviour, e.g. someone picking up the machine, a child playing with it, etc.
3. For every Fundraising event when you are setting up the device, take a moment to check for signs of tampering:
    - Has the terminal been stored insecurely?
    - Is the terminal serial number different to what it should be?
    - Does the terminal have any marks or scratches?
    - Are any of the screws on the terminal loose?
    - Has anyone tried to change or tamper with the terminal?
    - When switched on, does the terminal screen show any glitches, errors, or issues like spelling mistakes?
    - Are any components missing from the terminal or its box?
    - If the terminal has a card slot, is it obstructed in any way? To test this, insert a non-payment card (driver's license, library card, or similar) to see if it goes all the way into the terminal)

If you answer yes to one or more of the above statements, please do not use the device and contact your Fundraising manager immediately.

Information security Incidents involving Payment Card Data

If you suspect there has been an unauthorised intrusion into the contactless device or access to cardholder data, you must call the IT Service Desk immediately on 0300 330 1298 to instigate the payment card information security incident response procedures. Please also contact your

Fundraising Manager so that they can take the appropriate action to report the incident and mitigate any risk.

Examples of incidents involving or impacting Payment Card Data include:

- If you find a debit card or credit card:
- Give it to your Fundraising manager for action.
- If the manager is not available immediately, call the card issuer's phone number on the back of the card to report it lost and follow their instructions. Lock the card away securely if not asked to destroy it.
- Someone threatens or attempts to bribe you into compromising terminals or Payment Card Data
- You suspect that the security of Payment Card Data may have been compromised because the card payment terminal either:
- Shows signs of tampering or skimming
- It is not operating correctly, e.g. printing the entire card number
- You find a payment card on the floor

Further information

If you have a question about what you can and can't do with payment card data, ask your Fundraising manager or the Information Governance and Security Team.

Also see:

- The full Information Security Standard for Handling Payment Card Data
- Data and Information Policy
- Technology Policy