Imperial College London

Payment Security Management System (PSMS)

Cardholder Data (CHD) Handling Procedures

May 2021 | Release 1.0

Contents

Purpose

To provide a set of procedures to support the handling of cardholder data (CHD) during acceptance, or while being processed within Imperial College London ("Imperial"). This is intended as a set of general procedures and actions that apply to CHD processing which supplement the Payment Information Security Policy and adhere to the requirements of the Payment Card Industry Data Security Standard (PCI DSS).

CHD is desirable data that can be exploited for criminal gain if it falls into the wrong hands. Previous data breaches across many sectors have identified that a lack of guidelines or the existence of weak procedures, have resulted in the unintentional disclosure of CHD or the possibility for data to be accessed in an unauthorised manner. This document intends to address these shortfalls.

1 Scope

This procedure is to set the base principles for accepting, processing, transmitting or storing CHD as a primary or secondary function.

This procedure applies to:

- All individuals within Imperial who are accountable for the management of payment security across the organisation;
- All individuals within Imperial who are responsible for the management of taking payments within their business area;
- All individuals within Imperial who use payment devices to take payments;
- All individuals within Imperial who manage and maintain the hardware and software that is used within the cardholder data environment (CDE) or indirectly supports the CDE.

This procedure document must be followed in conjunction with the Payment Security policies, Imperial's procurement processes and Data Protection policies.

2 Definitions

- **Primary Account Number (PAN): PAN** may also be described as the "account number" or "card number".
- **Cardholder Data (CHD): CHD** consists of the full PAN at a minimum. CHD can also appear as the full PAN plus any of the following: cardholder name, expiration date and/or service code.

- **Sensitive Authentication Data (SAD): SAD** is information that is used to authenticate the cardholder and support the authorisation of the payment. SAD will include but not be limited to:
    - Card validation values (known as CVV, CAV2, CVC2, CVV2 or CID);
    - Track data obtained from magnetic stripe or chip;
    - PIN and PIN blocks.
- **Personally Identifiable Information (PII)** –**PII** is information that when used alone or with other relevant data, can identify an individual. CHD is considered PII.

3 Procedure Actions

There are two key principles that underpin the handling of CHD within Imperial, and they are as follows:

- CHD will only be accepted, processed, transmitted or stored, subject to the documented approval of the Income team and on the proviso a valid business reason exists;
- CHD will exist within the organisation for the shortest time possible and will not be stored after the payment has been processed.

3.1 CHD acceptance

1. CHD can ONLY be accepted from customers via the following methods:
    - Online (eCommerce) via a website and/or payment link facilitated by a compliant third-party payment services provider;
    - Face-to-Face via a payment device that has been provided by and/or approved for use by the Finance Systems Team (see PCI DSS training for further information);
    - Telephone using approved telephone numbers that operate over secure (i.e. encrypted) digital communication lines, analogue telephone lines or mobile (3G/4G/5G) communication technologies. Telephonic payments may be processed in low volumes for:
        - Updating recurring card payment details (if applicable);
        - Debt collection payments;
        - One-off payments due to lack of other methods being unavailable;

- Refunds;
- Donations;

- CHD will not be accepted via email, end-user messaging (e.g. WhatsApp, Facebook messenger), social network posts or other NON-approved communication channels.

2. When processing telephone payments, operators should:

   - Enter the CHD directly into the device or application or website for payment processing;
   - Ensure that they cannot be overheard or overlooked when taking the card payment;
   - Do not repeat back any part of the card data to the client for confirmation.

3. When a refund is required to be made back to a customer's card, the operator should:

   - Establish if the refund can be made by reversing the payment transaction without requiring card data. This should be the preferred option
   - Alternatively, validate the card is the original card that made the payment and follow the relevant Imperial refund instructions

4. Only devices issued or payment services approved by Imperial's Finance Systems team will be used to process payments. For more information about processing card payments, please contact the Finance Systems team (finance.systems@imperial.ac.uk).

3.2 Data at rest

5. The storage of card data under normal circumstances should not be required by the organisation

3.3 Data in transit

There will always be some sort of movement of CHD within Imperial, whether digital transmission or physical movement.

Transmission of CHD in a digital format will only occur during the acceptance and processing and will be protected as follows:

1. CHD shall be encrypted using strong cryptography and security protocols in accordance with the current version of the PCI DSS when transmitted over open, public networks.

2. CHD shall not be sent via end-user messaging technologies, such as email, Messenger, SMS, Skype, WhatsApp, social media or other types of messaging.

3. CHD shall not be sent over Wi-Fi networks. Mobile phone networks (3G/4G/5G) are the only exception.

4. In order to avoid onerous compliance requirements, payment card devices (i.e. payment terminals) which do not have an approved point-to-point encryption (P2PE) certification, must use data connections that are not connected to Imperial's network.

The physical movement of CHD within Imperial may be required based on business need (i.e. moving to location for secure destruction) and suitable levels of protection will be needed as follows:

1. Ensure a valid reason exists for the physical movement of CHD and that approval has been obtained from the Payment Security Committee (pcidsscom@imperial.ac.uk).

2. If the physical movement of CHD is required, only the following physical formats can be moved:

    - Paper forms;

    - Merchant receipts.

3. CHD must **NOT** be digitally transcribed and stored on a memory stick, CD, removable hard drive or other type of digital storage media for physical movement.

4. When moving CHD:

    a. Place CHD in an opaque container (i.e. an envelope) and ensure the outside is clearly marked as "private". Seal the container and place it within a second container that clearly identifies the intended recipient.

    b. When moving the data, use a trusted staff member or courier.

    c. Log the details of the package including when it was dispatched, the content and who couriered it. Notify the intended recipient that the package is enroute and when it may be expected.

    d. On receipt of the data, the recipient must inspect the package for potential tampering. If the seal looks tampered with, the sender must be contacted and a suspected incident raised for investigation.

e. Log receipt of the package, including when it arrived and who delivered it. Confirm to the sender that the package has been received.

f. Keep the package sealed until the point the CHD is ready to be processed, stored securely or destroyed.

3.4 Unsolicited CHD

When CHD has arrived from an unsolicited source or method for a payment, it indicates an underlying issue that needs to be resolved, beyond just dealing with the CHD.

These are suggested procedures for managing unsolicited CHD.

On receipt of CHD from a source or by a method that is not one of Imperial's approved methods or payment channels:

1. Identify the origin of the CHD including, who the original sender was, the communication method used and the time and date of receipt.

2. Contact the sender to inform them of Imperial's accepted methods for handling CHD (accepting payments or processing refunds) and try to ascertain why the sender needed to send their CHD via the unauthorised method or channel. All communications should be documented.

3. Require the sender to make payment or provide the necessary details via one of Imperial's approved secure payment methods or communication channels.

4. Log the receipt of the CHD as an incident using the Payment Security Incident Response Form (https://www.imperial.ac.uk/finance/financial-services/controls--compliance/pci-dss/incident-reporting/) to the PCI DSS Incident Response Team who will initiate the necessary activities to mitigate potential risks to the organisation.

5. Irrecoverably delete or destroy the unsolicited cardholder data as soon as possible. Further information on this is available in coordination with the PCI DSS Incident Response Team and ICT.

6. Review communication of current payment methods. Amend and communicate accordingly in response to reasons the CHD was sent by non-approved channels.

4 Document Management

4.1 Document Owner and Approval

The Payment Compliance Officer is the owner of this document and is responsible for ensuring that it is reviewed in line with the Imperial's review requirements.

A current version of this document is available to all relevant members of staff and is published on Imperial's website.

This procedure has been reviewed and approved by the Payment Security Committee.

4.2 Change History Record

Issue	Description of Change	Approved by	Date of Issue
1.0	PSMSCHProc Introduction	Payment Security Committee	12/05/2021