NHS
Counter Fraud Authority

Credit card fraud

NHS fraud prevention quick guide v2.0 November 2023

Credit cards are commonly used in the NHS for a variety of purchases and transactions, usually for the ordering and/or purchase of goods and services where immediate payment is required or where normal procurement processes do not apply. This quick guide looks at common fraud risks relating to the use of credit cards by NHS organisations.

Credit cards can also be referred to as purchasing cards and are issued to designated staff for making authorised purchases or transactions.

What is credit card fraud?

Credit card fraud can include:

- Unauthorised transactions made using a stolen or cloned credit card.
- Unauthorised transactions made using stolen personal details from a credit card, e.g., goods and services are purchased online or over the phone using stolen card details (this is often referred to as 'card not present' fraud).
- The use of skimming devices to exploit the contactless feature on credit cards where multiple unauthorised transactions of up to £100 can be processed with a card reader.

With a credit card the threats to NHS organisations are exactly the same as those faced by private individuals.

Who is this quick guide for?

This guidance is intended for all staff issued with a credit card for authorised transactions, their managers and for staff working in NHS finance and procurement teams.

How to spot credit card fraud

It is important for staff to remain vigilant to credit card fraud; here are some vulnerabilities to be aware of:

- **Insider threat** – Credit cards can be misused by staff for unauthorised purchases outside of official business. In some cases, employees will test the water and make a small unauthorised purchase to see if it is detected.

- **Poor controls and management** – A lack of oversight and scrutiny of the credit cards in circulation and their use, may encourage lax behaviours and lead to misuse by staff if they go unchallenged.

- **Poor security of credit cards** – Employees may lose cards through theft or negligence, cards may also be skimmed during a legitimate transaction, and financial information stolen and misused.

- **Poor validation process** – Due to emergency incidents and staff level shortages, processes, and procedures to validate credit card usage may not be as stringent as they normally are and can lead to credit cards being used by unauthorised personnel.

How to stop credit card fraud

Controls that mitigate the risk of credit card fraud should be documented clearly in a policy and standard operating procedure (SOP) and staff should be trained on identifying and reporting any risks and breaches. The following controls should be in place for the management of credit cards in use:

- When NHS credit cards are issued to staff for business purposes, an up-to-date policy should be available specifying the terms and conditions of their use, agreed purchase limits, any merchant category restrictions and the escalation process should any breaches of the terms and conditions be identified.

- Where the functionality / service is available, finance teams should freeze or suspend new credit cards in the interim until the card holder has signed the user agreement and been issued with the new credit card.

- An up-to-date list of all employees who have been issued with and authorised to use a credit card should be recorded. Finance and Procurement teams should determine how frequently this list is reviewed.

- A clear process should be in place to ensure that the authorising manager within the Finance or Procurement team are notified of staff leavers to ensure credit cards are

returned and/or deactivated.

- Purchase limits should be agreed and set by the issuing department or manager in consultation with the Finance/Procurement team. Card holders should not split any purchases to avoid transaction or contactless limits. If card usage limits are exceeded, action for escalation should be incorporated within the organisation's policy.

- Once purchase limits have been agreed, parameters should be set within the relevant system or process to ensure that only purchases/transactions within the agreed limits are paid. Line management or director approval should be required if the limit is exceeded.

- Card holders should not 'save' the credit card information with any commercial company or payment gateways when conducting online transactions.

- A maximum limit for transactions should be put on the card.

- All credit card transactions should be checked on a regular basis, at least monthly. This is to identify anomalies, unauthorised spend (purchase and limits) and any potential misuse or fraud.

- If any transactions have been found to breach the NHS organisation's terms and conditions (e.g., spending outside agreed limits), it is recommended that the card is immediately suspended until the matter is resolved. The cardholder should be held to account for any breach and a decision made on whether any disciplinary action should be applied.

- Staff issued with the credit card should be advised to keep the card in a secure place.

- All expired credit cards should be safely disposed of as per the credit card issuer's advice e.g., by cutting or shredding the card and disposing of the pieces so that they cannot be retrieved and pieced together. Particular care should be taken to ensure that the chip and magnetic strip are destroyed.

- Securely destroying communications containing sensitive information from the credit card issuer using a special confidential bin or a shredder.

If you suspect credit card fraud

1. If a card is lost or suspected of being stolen this should be reported immediately and the account should be frozen.

2. If any transactions appear suspicious, the card should be suspended immediately with any further transactions cancelled or frozen.

3. If fraud is suspected the organisation's escalation process should be followed immediately and the Local Counter Fraud Specialist contacted for advice (see also how to report fraud below).

How to report fraud

Report any suspicions of fraud to NHS Counter Fraud Authority online at **https://cfa.nhs.uk/reportfraud** or through the NHS Fraud and Corruption Reporting Line **0800 028 4060** (powered by Crimestoppers). All reports are treated in confidence and you have the option to report anonymously.

You can also report fraud to your nominated Local Counter Fraud Specialist.

Why take action?

Having a policy and SOP in place for the management of credit cards in use ensures there is oversight, holds staff to account and assists in the prevention and detection of fraud. By implementing these recommendations, NHS organisations will reduce their risk of falling victim to credit card fraud and the loss of NHS resources that results from these crimes.

Further information

- The NHSCFA series of fraud prevention quick guides focuses on specific areas of fraud risk vulnerability in NHS finance and procurement and are available to all on NHSCFA's website. They include:
  - Contract splitting (disaggregate spend)
  - Contract reviews
  - Due diligence
  - Suppliers code of practice: preventing fraud, bribery and corruption

- Mandate fraud
- Petty cash
- Buying goods and services

- NHSCFA has developed and published advice and guidance for the NHS on fraud risks relating to COVID-19, which may be helpful. Please visit **NHSCFA's website** for further information.
- The **NHS Fraud Reference Guide** was developed by NHSCFA to include information and definitions for different types of NHS fraud.
- Details of your Local Counter Fraud Specialist.