NHS
Counter Fraud Authority

Purchase card fraud

NHS fraud prevention quick guide v2.1 November 2025

Purchase cards, such as debit cards, virtual and physical 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 purchase cards by NHS organisations.

Who is this quick guide for?

This guidance is primarily for finance and procurement teams to support the implementation of appropriate controls, also for budget holders, managers and staff who have been issued or granted access to a purchase card for authorised transactions.

What is purchase card fraud?

Purchase cards are issued to designated staff for making authorised purchases or transactions.

Purchase 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).

- misuse of purchase cards for personal gain

- 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.

What is virtual credit card fraud (VCC)?

A virtual credit card (VCC) is linked to a real credit card but adds an extra layer of security. VCCs can be used online or in-person transactions when added to a mobile phone-based digital wallet, such as Apple Pay, Google Pay or Samsung Wallet. They generate a random 16-digit card number for every transaction, which expires shortly after use. This makes it nearly impossible for the card details to be reused. VCC fraud refers to the unauthorised use of digital or virtual credit card details to make fraudulent transactions. This can include:

- Unauthorised use of VCC details to purchase goods or services online without the cardholder's consent.

- Misuse of VCCs issued for specific vendors or purposes, where the card is used outside its intended scope.

- Exploitation of weak controls, such as lack of merchant restrictions or insufficient oversight, allowing fraudulent or inappropriate transactions to go undetected.

- Use of stolen login credentials to access virtual card platforms and generate or use VCCs fraudulently.

How to spot purchase card fraud

It is important for staff to be alert to these warning signs as they are key to identifying potential fraud:

- **Unauthorised or unexplained transactions** – Any charges that do not align with the card's intended use, normal business needs, or appear without legitimate justification should be treated as potentially fraudulent and investigated immediately.

- **Repeated small charges followed by a larger transaction** – A pattern of multiple low-value purchases, especially if followed by a significant charge, may indicate a testing strategy commonly used in fraudulent activity.

- **Repeated declined transactions** – Multiple failed attempts to process payments may signal misuse or compromised card details.

- **Unexpected transaction denials** – Legitimate transactions being declined may

suggest the VCC's spending limit has been reached or exceeded due to unauthorised use. (Specific to VCCs)

- **Alerts of compromised credentials** – Notifications about login attempts or access to the VCC management platform that were not initiated by the authorised user may indicate credential compromise. (Specific to VCCs)

- **Transactions outside normal patterns** – Spending in unusual locations, times, or categories compared to typical usage patterns could indicate misuse. (Specific to credit cards)

- **Missing or incomplete documentation** – Charges without receipts, invoices, or supporting evidence could indicate unauthorised expenditure. (Specific to credit cards)

- **Requests for urgent or exceptional use** – Pressure to bypass standard approval processes or validation checks can indicate fraudulent intent. (Specific to credit cards)

- **Lost or stolen cards reported late** – Delayed reporting of missing cards can indicate negligence or an attempt to conceal fraudulent activity. (Specific to credit cards)

How to stop purchase card fraud

Controls to mitigate the risk of purchase card fraud should be documented clearly in a comprehensive policy and standard operating procedure (SOP), and staff should be regularly trained on identifying and reporting any risks and breaches. The following controls should be in place for the mitigation of purchase card fraud:

- A comprehensive policy should be available specifying the terms of use, limits, merchant restrictions, approval and escalation processes. Budget holders and finance teams should check for substantial or recurring credit card payments that should be part of planned procurement, as these may indicate attempts to bypass controlled channels.

- Ensure relevant staff (e.g., finance, budget holder, cardholder) receive ongoing training and updates on expenses, allowances, and purchasing card policies and communicate the consequences of fraudulent claims, including potential disciplinary and criminal action.

- Assign each card to a single employee to ensure accountability. Avoid allocating cards to departments where multiple employees have access. (Specific to credit cards)

- Ensure cardholders sign a declaration confirming they have read, understood, and agreed to comply with the organisation's purchasing card policy before receiving a card.

- Where functionality allows, finance teams should suspend new cards until the user agreement is completed. (Specific to credit cards)

- Ensure cards are returned and/or deactivated immediately when employees leave. (Specific to credit cards)

- Agree maximum limits and implement them within the relevant system. Cardholders must not split purchases to bypass limits. Escalation procedures should be in place for breaches.

- Enable Multi-Factor Authentication (MFA) for all purchasing card systems and platforms to add an extra layer of security against unauthorised access

- Specific merchant category code (MCC) restrictions should be applied to each VCC to limit usage to approved vendors to reduce risk of misuse. (Specific to VCCs)

- VCCs should only be used for the designated vendor or merchant for which they were issued. Any deviation should trigger disciplinary action and escalation. (Specific to VCCs)

- All VCC transaction requests should be reviewed and approved by the appropriate line manager or budget holder before submission to finance. (Specific to VCCs)

- Finance teams should check all transactions at least monthly to identify anomalies, unauthorised spend, and potential misuse. For VCCs, ensure receipts or valid confirmations are submitted for each item, not cumulative spend.

- If transactions violate policy (e.g., spending outside agreed limits), suspend the card until resolved and consider disciplinary action.

- Staff should store physical cards safely to prevent theft or misuse. (Specific to credit cards)

- Cardholders should avoid storing card information with commercial companies or payment gateways. (Specific to credit cards)

- Destroy expired cards by cutting or shredding, ensuring the chip and magnetic strip are destroyed. (Specific to credit cards)

- Shred or use confidential disposal methods for documents containing card details. (Specific to credit cards)

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 purchase 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 the risk of falling victim to purchase card fraud and the loss of NHS resources that results from these crimes.

Further information

- **https://cfa.nhs.uk/fraud-prevention/fraud-guidance**
  - Invoice and mandate fraud
  - Pre-contract procurement fraud and corruption
  - COVID-19 counter fraud guidance
  - NHS Fraud Reference Guide

- For further information visit the **NHSCFA's website**

- Details of your Local Counter Fraud Specialist.

  Organisation name:
  Name:
  Job Title:
  Email:
  Telephone:
  Mobile:
  Address: