Payment Terminals Fraud Alert

MIAA Anti-Fraud Service

May 2022

For GP Practices and Primary Care Networks

Through the NHS Counter Fraud Authority (CFA), we have recently been made aware of a system weakness involving payment terminal machines, which are also known as a point of sale (PoS) terminal or credit card terminal. The weakness relates to the supervisor code for the payment terminal, which had not been changed from the default code and was used to perpetrate fraud.

Background

A payment terminal is a device which interfaces with payment cards to make electronic funds transfers, facilitating debit and credit card payments via various methods including:

- Face to face, using a card machine (chip and pin / contactless)
- Over the phone
- By sending a payment link
- Through a website

As well as accepting payments, terminals can be used to process a refund. In the case of the terminal used for the fraud, a refund could only be processed by entering a supervisor's code.

Any organisation operating payment terminals could be at risk.

How the fraud operates

The NHS organisation victim to this fraud used payment terminals hosted by Worldpay and paying Worldpay to process transactions on its behalf. However, this type of fraud is not limited to Worldpay terminals and processes.

ACTION REQUIRED

MIAA Anti-Fraud Service recommend this alert is distributed to:

GP Staff
for
ACTION &
AWARENESS

MIAA IA 22/23 1
For further information on MIAA's Anti-Fraud Service visit
miaa.nhs.uk

During a regular review of transactions, the NHS organisation noticed that 45 individual direct debit refunds had been processed to 21 separate bank accounts, totalling £230,100.00. All transactions were carried out overnight, on three consecutive dates. This was irregular activity and immediately identified as suspicious.

All transactions were processed on a single payment terminal, and Worldpay confirmed that a card had not been physically presented, with the account details of each account had been physically keyed in. The supervisor code for the payment terminal had not been changed from the original default code.

The payment terminal was physically accessed to perpetrate this fraud, which required the fraudster gaining access to a restricted area that would not have been in use during the hours this occurred. The perpetrators were identified on CCTV as three males, who were detained when they returned to the scene a week later.

This modus operandi is well known in the private sector; however, there has previously been no intelligence that NHS-related premises have been targeted by what is believed to be organised crime.

Prevention advice and action

To protect against this type of fraud please consider the following:

- Consider the review process in place for payment terminal transactions and, if necessary, undertake a proactive review of payment terminal statements to identify any suspicious refund transactions.
- Organisations should ascertain how many payment terminals they have in operation and ensure that these are all securely stored away from public access when not in use.
- All payment terminal 'supervisor codes' should be checked and must be changed from the default code.
- Organisations should consider changing 'supervisor codes' on a regular basis.
- The physical security of payment terminals should be managed in the same way as cash and cheque books. They should only be accessed and used by authorised individuals.
- Guidance should be disseminated to all point of sale and relevant staff.
- Additional vigilance should be exercised when operating payment terminals during working hours, to prevent suspects from distracting staff and taking control of payment terminals.
- Security personnel should maintain physical security of all out of hours staff access points. Members of the public should not be provided access to out of hours staff access points unless the nature of their visit has been confirmed by the staff to be visited.
- All incidents of suspected fraud against NHS organisations should be reported via the NHSCFA by calling **0800 028 4060** or online at www.cfa.nhs.uk/reportfraud. GP Practices / PCNs should contact their local police, or report any incidents via Action Fraud on **0300 123 2040.**

TAKE FIVE TO STOP FRAUD™

ActionFraud
National Fraud & Cyber Crime Reporting Centre
0300 123 2040