

**SCOTTISH
CRIME &
DRUG
ENFORCEMENT
AGENCY**



Scottish Business Crime Centre Liaison Unit

Bulletin 01/2011

Supplier Account Take Over Fraud

March 2011 updated May 2011

Overview

This bulletin is issued by the Scottish Business Crime Centre Liaison Unit of the Scottish Crime and Drugs Enforcement Agency (SCDEA). It is based on assessment of intelligence from the Scottish Financial Crime Group; The National Anti-Fraud Network and NHS Counter Fraud Services. The intention of this bulletin is to promote and support effective business crime information/intelligence sharing between the SCDEA and the Scottish business community. Our aim is to reduce the harm caused by serious organised crime and to make Scotland a hostile environment for serious organised criminals.

Supplier Account Take Over Fraud

An account takeover happens when a fraudster poses as a genuine customer, or supplier, gains control of an account and then makes unauthorised transactions. Any account could be taken over by fraudsters, including bank, credit card, email and other service providers. This activity has now extended to supplier accounts.

Organised criminals purport to be representatives of a genuine supplier company. The fraudsters send letters, facsimiles and/or emails to accounts payable staff and request that the current bank details for genuine supplier companies are changed to bank accounts which the fraudsters have access to. Following that change, genuine business payments to that supplier are diverted to the fraudsters. The genuine supplier companies are unaware and it is only after they make contact with businesses in relation to non-receipt of payment, that the fraud becomes apparent. Often by that time, the fraudsters have emptied the bank accounts that the monies were redirected to.

This fraud continues to grow across the country, it is therefore absolutely essential that this bulletin is shared with all relevant personnel involved in the maintenance of purchase ledger records (and in particular bank account details) to block all fraudulent attempts to inappropriately amend these details.

The scope of this activity is widespread and it has extended to local authorities and other organisations including private sector companies. The fraud is organised in the following way:

- The fraudsters target better known supplier companies, this is possibly as a result of tender documents or publicised creditor lists.
- Often email addresses on letters submitted use domain extensions similar to that of the genuine companies, but which are in fact operated by the fraudsters.

- The fraudsters have called telephone switchboards of target companies asking for contact names responsible for authorising payments in order that correspondence is directed to the relevant staff members.
- Supplier details such as telephone numbers have been requested, presumably to be added to the fictitious requests to add authenticity.
- There are examples of the fraudsters telephoning target companies to chase payment, in the hope that some checks might not be carried out.
- Company Secretary, Finance Directors and other authorised contact details (including signatures) are generally correct – almost certainly having been scanned from published information available from various sources including the internet.

National Anti-Fraud Network

The National Anti-Fraud Network (NAFN) has issued intelligence bulletins to its local authorities. The fraud within local authorities initially centred on requests to change bank details relating to construction companies that are frequently engaged on current capital construction projects within Council areas. This information is widely available through contract award notices and general publicity surrounding what are often significant projects in terms of monetary value.

See the news article:

<http://www.constructionenquirer.com/2010/10/29/swindler-arrested-over-construction-invoice-scam/>

Companies House Fraud

Companies are also at risk because fraudsters can submit fake papers to Companies House and have the details of the director or official address of the company changed. Fraudsters can then run up huge debts in the name of a company which knows nothing about the fraud until it is too late. Companies can prevent fraudsters from changing their details by registering for the 'Proof' system at Companies House. This means that companies can only change their details online using a password and confidential authentication code; and by using a registered email address. These security measures make it significantly more difficult for fraudsters to commit any fraud at Companies House, as long as companies keep the password and authentication code secure. Contact Companies House for more detail on this.

Recommendations

- Remind your staff not to provide genuine supplier company reference information via the telephone.
- Review and verify bank account and single point of contact information for all supplier companies where possible.
- If you receive a letter, which upon verification proves to be false, immediately place it in a suitable document holder to protect it as it may be subject to forensic examination.
- Do not use the details supplied in the letter, fax or email to contact the company.
- Take steps to ensure that appropriate confirmation is obtained from genuine supplier companies regarding any changes to business bank account information or key business personnel information.
- Check all details on any request for change against the information already held. This will include company names, contact numbers, company registration numbers, VAT numbers, addresses, web addresses and all email addresses.
- **DO NOT** use Companies House to verify information.
- Telephone the contact number for the suppliers head office **noted on previously paid invoices** and confirm the change.
- Contact police if attempted fraud is identified.

If you have any queries re this or any other matters please do not hesitate to contact:

Scottish Business Crime Centre Liaison
Scottish Intelligence Co-ordination Unit
Scottish Crime and Drug Enforcement Agency
Direct dial: 01506 524 548
Email: SICU-DESK@scdea.pnn.police.uk

Our Vision

To protect Scotland's communities from serious organised crime

Our Mission

Working every day for the people of Scotland - dismantling serious organised crime

Our Organisational Values

Trust, Commitment and Respect

Disclaimer - Whilst every care has been taken in developing and compiling this document, the SCDEA accepts no liability for any loss or damage caused, arising directly or indirectly, in connection with reliance on its contents.
© SCDEA 2011