Financial Investigation Unit
Cross Border Crime
A Division of the Guernsey Border Agency

FRAUD ALERT

Ref: 01/12

Mandate / Invoice Fraud

An alert has been widely distributed by the National Fraud Intelligence Bureau (NFIB) to the private and public industry and the content of this alert is below. This alert was received on the 21st August and is being distributed through the Financial Intelligence Service for information purposes but also so that members can take steps where necessary to protect their own organisations.

The NFIB is continuing to receive reports relating to bogus invoices purporting to be from genuine service/product providers or false instructions to change the account details for future payments towards ongoing contracts.

A number of public and private sector organisations appear to be the target of this fraud type, and some of these include:

- Educational establishments such as Universities, Schools and Colleges
- Councils
- Airports
- Health Care Providers
- Travel related Industry
- Pharmaceuticals Industry
- Financial Services Industry
- Food and Drink Industry

Losses can vary considerably but often run into hundreds of thousands of pounds and several have exceeded £1 million. Some of the stolen funds have been recovered but inevitably this is not always the case as often the funds are quickly transferred outside of the UK which makes recovery difficult.

The bogus invoice fraud usually involves a genuine invoice being intercepted by unknown means and the account details given for payment are altered to an account under the fraudster's control. The fraud will usually be discovered when the legitimate company sending the invoice chases for non-payment. Some incidents have also involved completely counterfeit invoices being submitted for payment.

Organisations with ongoing business relationships or contracts have been deceived with a diversionary tactic by the fraudster. This involves the fraudster identifying an organisation that make regular payments to a service provider, and this maybe an individual or large company. The fraudster will submit a change of account notification to the remitting organisation. On receipt of the notification the department controlling the organisations finances have then changed the payment details with little or no verification. Funds have then been inadvertently sent to bank accounts under the control of fraudsters.

Where invoices are entirely counterfeit they will not stand up to scrutiny. The counterfeit invoices (and any covering letters) may appear to be printed on company headed paper but are more likely scanned copies from an original document and printed onto paper using a domestic printer. Consequently the company logo may appear less sharp and slightly blurred.

Where bank details have been replaced on an original invoice with the fraudster's bank account details, it may be possible to compare the print against the remainder of the document to identify any alterations. In some cases where no payee account details are shown on the invoice the fraudsters have merely typed an instruction to pay funds to a particular account.

Look out for different contact numbers and e-mail addresses for the company as these may differ to that recorded on previous correspondence. The contact e-mail address may only include a minor amendment giving the impression it is the correct contact address. For example it will look almost identical to the previous e-mail address but may read ".org" instead of ".com" or ".co.uk".

The NFIB would advise that you consider reviewing your anti-fraud measures to ensure that you do not fall victim to this type of fraud. Although not exhaustive, some examples of action you can take to protect yourself are:

- Always confirm change of bank account requests with the company making the change, being mindful not to use the contact details on the letter requesting the change.

- Consider setting up designated single points of contact with companies to whom you make regular payments.

- Instruct staff with responsibility for paying invoices to be cognisant of checking invoices for irregularities and checking out their suspicions with the company requiring payment, again being mindful that contact details on the invoice may not be genuine.

- Consider setting up a system whereby when an invoice is paid you also send an email to the recipient informing them payment has been made and to which bank account. Be mindful of account security and consider including the beneficiary bank name and the last four digits of the account to ensure security.

- Consider reviewing change of account details already acted upon where payment is due at a future date and confirming the authenticity of the request.

- Fraudsters may have found information regarding contracts and suppliers on the victim organisation's own web-sites. Consideration should be given to whether it is necessary to publish information of this type in the public domain as it has been demonstrated that it can be used to facilitate significant fraud.

- For payments over a certain threshold, consider organising a meeting with the company who are requesting payment, and satisfy yourself payment will be sent to the correct bank account and recipient.