

FRAUD ALERT- Invoice Re-direction Fraud:

Publication by:

Banking & Payments Federation (BPFI)

For the attention of:

Irish Businesses

Purpose of Advisory:


To advise that a number of businesses in Ireland have recently fallen victim to a scam involving bogus emails being received that purport to be from an existing creditor. The email generally contains a letter as an attachment, the letter purports to notify the receiver of new (amended) bank account details to which all future payments are to be sent.

Key Details:

1. Irish businesses are increasingly experiencing attempted Invoice Re-direction fraud.
 2. This involves a creditor's beneficiary details being fraudulently altered.
 3. The business is misled into believing that a beneficiary's bank account details have been changed and so funds that are due to be paid out are transferred to a fraudulent account.
 4. Attempts such as this could be successful if the change of details request is not confirmed directly with the source supplier (Use a phone number from your files, not from the letterhead of the suspect letter).
 5. There are various other measures a business can take to safeguard itself against such fraud.
 6. For further details please see below.
-

Background:

There is a growing trend in Payment Fraud involving beneficiary details being fraudulently altered. This bogus invoice fraud usually involves genuine invoice details being intercepted by unknown means, the



beneficiary account details are altered so that payment is redirected to an account under the fraudster's control. The fraud will usually be discovered some time afterwards when the legitimate company sending the invoice queries "non-payment".

What Are the Tell Tale Signs?

The email notifying the change of details may be in the name of someone that the receiver is used to dealing with, however the fraudsters will have created a bogus email account and the sender's name which will carry a minor variation, see following examples:

james.ryanabcd@hotmail.com (genuine)	jamesryanabcd@hotmail.com (bogus)
liz.smythabcd@stantons.com (genuine)	liz.smythabcd@stantonz.com (bogus)

Fraudsters may then submit bogus invoices. These 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 so the company logo may appear less sharp and slightly blurred.

Action:

Although not exhaustive, some examples of action you can take to protect yourself are:

- Make a phone call to a known contact within the firm that appears to be requesting fundamental changes in banking details
- 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.
- Look out for different contact numbers and e-mail addresses for the company as these may differ from those recorded on previous correspondence.
- Consider reviewing change of account details already acted upon where payment is due at a future date and confirming the authenticity of the request.
- 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 concerns with the company requiring payment.

- Consider setting up a system whereby when an invoice is paid you also send an email to the recipient informing them that 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.
- Fraudsters may have found information regarding contracts and suppliers on the victim organisation's own web-sites. Consideration should be given as 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 fraud.
- For payments over a certain threshold, consider organising a meeting with the company who are requesting payment, and satisfy yourself that payment will be sent to the correct bank account and recipient.

This is a general notice issued by the Financial Crime and Security Department of the BPFII on Behalf of BPFII members.

Disclaimer Note: The information contained in this Fraud Alert /Advisory is for general guidance and for information purposes only and is intended to enhance awareness and vigilance regarding this