Invoice fraud (also known as invoice redirection fraud) is a widespread and well-established crime which cost UK businesses almost £93m in 2018. It poses a very real threat to organisations of all shapes and sizes and yet many remain unaware of it. **Here's what to look out for**.

INBRIEF

A BEGINNER'S GUIDE TO ANTI-FRAUD MEASURES | APRIL 2019

FRAUD ADVISORY PANEL

Invoice fraud

WHAT IS INVOICE FRAUD?

A fraudster posing as an existing supplier asks for changes to be made to the banking details you hold for them in your organisation's payment system. This will typically happen in an exchange of emails. Once the new account details are in place any subsequent payment will not reach your true supplier because it is automatically diverted into the pockets of the fraudster.

Criminals are using increasingly sophisticated ways to make their email approaches more convincing. For example, they will try to find out when you make regular payments and then use doctored versions of real supplier emails to infiltrate genuine email chains. Any organisation that makes details of its commercial relationships publicly available – perhaps by listing suppliers on its website – is particularly vulnerable to invoice fraud.

Also be aware that a fraudster might pretend to be you and target your customers with fake invoices.

WARNING SIGNS

Fraudulent invoices and their supporting communications can be incredibly difficult to spot because a lot of work goes into making them look realistic. Even so, there are some common warning signs to watch out for.

- Any request for an existing supplier's bank account details to be changed should be subject to proper scrutiny.
- The reasons given for the change might be suspiciously weak – such as 'we've moved our bank', 'we are using a new account' or 'we've had some problems with our primary bank account' – but not necessarily.
- The new account details are accompanied by an urgent request for payment, perhaps as a faster payment.
- Closer inspection of the email address reveals some small anomaly – perhaps a capital letter O has been replaced by the number 0, or the letter W is in fact a pair of Vs. (You may need to hover your mouse over the email address to see these things properly.)
- The writing style and language is not quite what your contact normally uses.
- The telephone number (as well as the email address) has changed.
- Any logos are blurred or badly cropped.
- Where proof of the new bank details is provided the transactional information has not been redacted. (Genuine businesses normally do this.) In which case you should review the transaction carefully to see if it is 'business-like' and in keeping with what you would expect from an organisation of your supplier's size and type.

TAKING ACTION

If you suspect invoice fraud you should act promptly.

- Do not make the payment in question.
- Tell the real supplier so that they can inform other customers and check their system security.
- Make sure the fraudulent account details are not listed for any of your other suppliers.
- Check online to see if the IP address used for the spoof emails has prompted other reports of abuse.
- Make sure none of your other payments have been compromised.
- Assess the adequacy of your current controls and propose improvements where necessary.
- Report your concerns to Action Fraud (England, Wales and Northern Ireland) or Police Scotland (Scotland).
- Report the matter to your bank.

CHECKLIST

A number of quite simple procedures can help protect your organisation from invoice fraud.

- ✓ Before any payment or money transfer is made always contact the supplier directly to verify changes to account details. Do this either by telephone or in person, using contact details obtained from the supplier's own website or from your own files.
- ✓ When making a first-time payment to a new account transfer a small sum first, then check it has been received before paying the balance.
- ✓ Request formal proof of any change of bank details, with the account name and supporting details clearly visible. Carefully review this for authenticity, checking things like the size, colour and position of logos and fonts.
- ✓ Always issue remittance advices to your suppliers so they know when a payment has been made.
- ✓ Check bank statements regularly and report suspicious transactions immediately to your bank.
- ✓ Do not list your suppliers on your website or in any other publicly available materials unless you are required to do so by law.
- ✓ Never leave sensitive information – such as invoices – in full view. These will often contain information (such as direct debits and bank accounts) invaluable to a fraudster.
- ✓ Alert staff to all unsuccessful frauds so they can be prepared for repeat attempts.
- ✓ Be aware that staff outside finance might also be targets for spoof emails.
- ✓ Encourage staff to be vigilant when they are asked for information about existing suppliers and/or regular payment cycles. Criminals often conduct information-gathering exercises in preparation for the fraud itself.

And, importantly, **trust your instincts.** If you think something is suspicious, it probably is.

FURTHER INFORMATION

Fraud Advisory Panel provides simple and practical guidance to individuals and organisations on common forms of fraud and financial crime.

Get Safe Online provides easy-to-understand information on online safety for businesses as well as individuals.

Take Five (a UK national campaign) publishes straightforward and impartial advice on preventing financial fraud.

ACKNOWLEDGEMENTS

The Fraud Advisory Panel gratefully acknowledges the contribution of Lorie Sutton (ICAEW) in the preparation of this helpsheet.

FRAUD ADVISORY PANEL

Chartered Accountants' Hall
Moorgate Place
London EC2R 6EA UK

T +44 (0)20 7920 8721
E info@fraudadvisorypanel.org
www.fraudadvisorypanel.org

Company Limited by Guarantee Registered in England and Wales No. 04327390
Charity Registered in England and Wales No. 1108863