Fraud - Business email compromise

Do you know the red flags to look out for?

If you work in the international supply chain, you are at risk of being unwittingly exposed to many types of payment fraud during the normal course of business. The methods used are often sophisticated and involve the complicity of multiple parties internationally. The proceeds of fraud often feed into other criminal activity such as drug smuggling, people smuggling, modern day slavery and terrorism.

With business transactions and communication handled almost exclusively online in today's fast-paced digital environment, there is an increased risk of fraud, making due diligence more critical than ever. This document looks at the most common methods of payment fraud in the global supply chain and the preventative measures you can take to mitigate the risk.

What are the risks?

Which types of fraud are most common in my industry?

PAYMENT FRAUD

Typically, this will involve a fraudster pretending to be a business you make regular payments to, instructing you to make a payment to an alternative account. The fraudster will monitor email traffic waiting for a suitable payment request to be made. They will copy style and language to ensure they remain undetected. Often the email address they use will be almost identical to the address you would usually correspond with - occasionally the email address will be identical.

CEO FRAUD

A common type of payment fraud is CEO fraud, where an apparent internal email instruction purporting to come from a senior member of staff requests that you make an urgent transfer of funds to a new customer or to a beneficiary account created to appear similar to that of an existing customer.

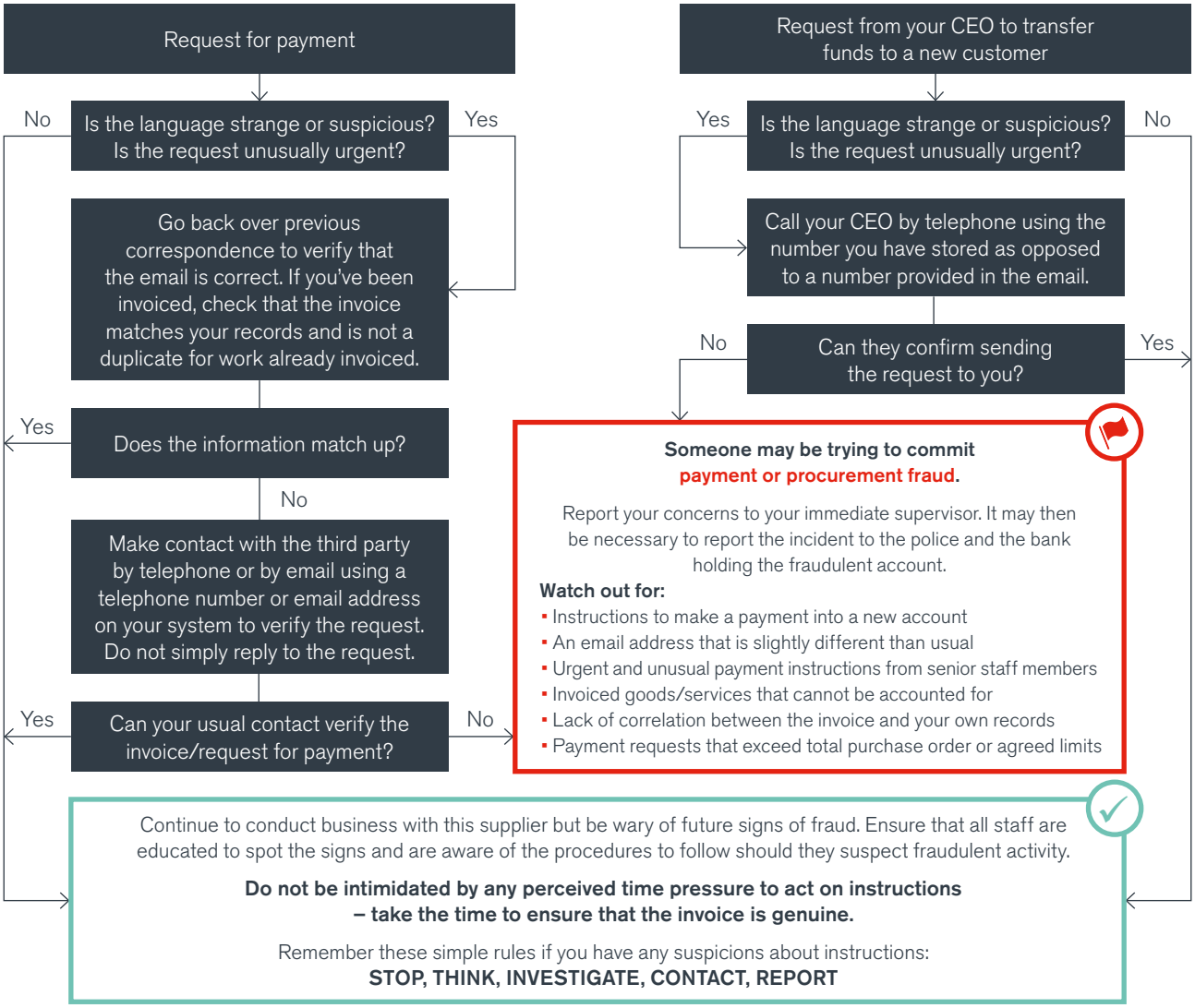
PROCUREMENT FRAUD

In the global supply chain, it is common for businesses to rely on subcontractors to undertake services; however, this can leave you exposed to fraudulent invoicing by fraudsters purporting to be a subcontractor.

Fraudsters infiltrate computer systems and monitor email traffic to gather the information they need to commit fraud. Often, a fraudulent invoice is difficult to reconcile with a specific appointment or it could be a duplicate of a previous purchase order but with different banking details.

The fraudster may use tactics such as citing negative effects on credit ratings, commercial standing and threatening legal action in the event of non-payment to force the transaction through.

To avoid becoming the victim of fraud, consider the following guidelines when you receive correspondence at work:



TT CLUB
IS MANAGED
BY **THOMAS MILLER**

For more information
Please contact us at **riskmanagement@ttclub.com**
or visit us as **ttclub.com**