

Buyer Impersonations

Advice on how to avoid being caught out

Buyer Impersonations are on the increase.

Impersonations, as the name suggests is where fraudsters impersonate established credit worthy companies by placing orders in their name but requesting delivery to a rogue trading address or offering to pick up the goods themselves. Suppliers then invoice the legitimate company to be told the goods were not ordered by them.

The main goods targeted by this type of fraud tend to be Food (fruit, veg, meat) and IT related products, however the threat is open to all.

Points to look out for that could indicate an impersonation:

- A professional looking website but with little functionality
- The buyer is generally not interested in price/no or little negotiation
- An unusually short period between first contact, order and delivery requested
- The buyer requesting to collect goods themselves often in unmarked vehicles
- The buyer changing delivery address at short notice
- Conflicting sectors, the buyer being in a different trade sector to the supplier
- Buyer being too ready to supply information requested such as trade references, accounts etc

What can you do?

Suppliers should carry out checks to ensure their customers are genuine:

- Take a contact name, land line phone number and website address
- Impersonators usually use mobile telephone numbers and gmail/hotmail email addresses so beware
- When reading any documents supplied ask yourself if the grammar and spelling used are what you would expect from a professional business.
- Do not rely on contact numbers provided by the buyer, look up alternatives for the company and ring those asking to speak to the individual, that will enable you to verify if that person actually works for the company or whether they are using genuine names that when contacted for real have no knowledge of the contract referred to
- Beware of fake websites, always search for an alternative to the address you've been given as impersonators often setup very convincing secondary sites with a slight difference in name to that of the genuine site
- Google street view the delivery address provided to validate its authenticity

- Beware of last minute changes to delivery address, don't change the delivery destination once goods are in transit, educate vehicle crews to deliver only to the specified destination and to report any attempt to change the delivery destination before off-loading the goods
- Beware of urgent or casual orders from existing customers, insist they follow usual purchasing procedures
- Request a VAT number and check it's validity on the EU site link below:
http://ec.europa.eu/taxation_customs/vies/

We recommend that if suppliers feel they have been hit, in the first instance report it to the police but also report it to Action Fraud which is the UK's national fraud reporting centre.

