Atradius
Managing risk, enabling trade

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 with little or no 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
- A director of the business placing the orders
- An email address that differs from the website domain name

What can you do?

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

- Take a contact name, land line phone number, website address - and check them out
- 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 set up very convincing secondary sites with a slight difference in name to that of the genuine site
- www.whois.com/whois provides a free service where you can check the creation date of email/web domains to help clarify the authenticity of a business. A recently created domain name (with a short validity) for a long established business should raise concern
- 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 specified destinations and to report any attempt to change delivery destination before off-loading goods
- Beware of urgent or casual orders from existing customers, insist they follow usual purchasing procedures
- https://betacompanieshouse.gov.uk provides direct free online access to UK Companies House and the filed documents where checks of the registered trade against the goods being ordered are recommended
- Be alert to our T400 warning condition used on genuine businesses where we are aware that impersonation has taken place and extra due diligence is recommended

If suppliers feel they have been targeted we recommend reporting it to Action Fraud, the UK's national fraud reporting centre.

Tel:0300 123 2040

Web: www.actionfraud.police.uk

Each point in isolation would not necessarily point to fraud however when you start seeing several points in existence that is when suspicions should be raised.

Atradius Credit Insurance N.V.
3 Harbour Drive
Capital Waterside
Cardiff, CF10 4WZ

Tel.: +44 (0)29 2082 4000

www.atradius.com

UK Branch Registration: FC033828/BR018915
Atradius Crédito y Caución SA de Seguros y Reaseguros

ATR_FS_Buyer Impersonation.UK.19.001