Exporting Cargo – Fraud Issues

Even with increased IT security and fraud awareness, the truth is that no one is immune to fraud.

Fraudsters are more refined than ever before and many scams are instigated by organised crime groups. These groups are dangerously sophisticated – they have multi-layered schemes in place, including having great knowledge about the industry and the targeted business. They possess a large number of bogus documents such as contracts of sale, insurance policies, and bills of lading or a fake website and personal ID. Some groups even hire personnel to pick up consignments or take meetings.

Common types of fraud in logistics contracts

Payment frauds

One of the most abundant frauds is payment scams.

These require (in comparison to the other types of fraud) the least amount of knowledge on the fraudster's part. These frauds make victims transfer their payments to a bank account owned by the fraudsters instead of the bank account owned by the genuine business.

An example of such fraud is an email from an accounts department of a carrier asking to transfer the payment money to a different bank account than usual. The new bank account belongs to the fraudster, rather than the carrier.

Another example is when the shipper is insisting on payments to be sent to a personal/ third party account rather than the legitimate company account due to, for example, high banking rates incurred by the shipper's bank.

These emails can be so well disguised to look like they are coming from a long-standing business partner, that these will not raise any level of suspicion - while the opposite should be true. Such fraud can easily be prevented by calling the company or accounts department, on the number stated on their website or other independently provided documents, and confirming the bank details and reasons for the change of instructions.

A subcategory of payment fraud is CEO fraud – targeted at the staff in accounts departments pressuring them

Tel: 0344 967 0793 | Email: info@LA-Law.com | www.lesteraldridge.com

to transfer money to another bank account or pay certain invoices with urgency. Such emails would appear as if they were coming from senior managers of the business, when, in reality, these would come from fraudsters spoofing and impersonating these managers.

This can also be prevented by calling the person requesting the transfer to confirm the request (by dialling the phone number from an employee directory) and/or checking the instructions with superiors.

Identity of carrier fraud

Such fraud necessitates an additional layer of sophistication from the fraudsters – producing falsified documents and policies, creating fake websites, responding to queries and having expansive knowledge of the industry to be able to convince industry professionals to believe them. Given the value of the goods or payments the fraudsters can extract from the customers or shippers, it is a lucrative business where creating the additional layer of opacity pays off.

Such fraud can start innocently – with a shipper searching for a carrier or freight forwarder with the internet, usually looking for the cheapest or the best value for money option. The shipper finds a lucrative ad and contacts the supposed carrier for a quote and further information – which the fraudster happily provides. Negotiations go well and the carrier takes possession of the goods to ship to the required destination. Problems will start appearing on the way – the shipper might be required to pay additional VAT, port fees or licences without being provided with any legitimate documents to support the additional fees from the carrier. Without payment of the additional fees, the goods would not be delivered to the consignee. In reality, the goods may not have been shipped and instead could have been sold to third parties.

Ten tips to avoid fraud

We believe these simple, yet effective tips can easily be incorporated into the day-to-day business and be a valuable weapon in the fight against fraud:

1. When searching for a carrier, always use legitimate websites, possibly run by an association, rather than user-created content websites such as Gumtree or Alibaba.

2. Check for grammatical errors, differences in the company name throughout the website and other communication, legitimacy of their place of the business address and their email address.

3. Check the reviews of the shipper and their website for more information which can be reviewed and confirmed.

4. Complete due diligence on the business partners – do you know who you are dealing with?

5. If receiving documents, make sure these are full copies of the documents including full terms and

Tel: 0344 967 0793 | Email: info@LA-Law.com | www.lesteraldridge.com

conditions; check for grammatical and factual errors.

6. Only allow verified persons to the warehouse and if they are not scheduled to pick goods up, do not let them enter unless verified with higher management levels.

7. Query every single unexpected charge (such as VAT, port fees not planned for) and demand to see the original documents supporting the charge.

8. Before transferring any payment, double-check the bank account details, that the account belongs to the company and call the company to confirm these details.

9. Check your bank statements carefully and report any suspicious activity to your bank.

10. Be sceptical – if you are unsure of anything – query it and escalate it to your superiors

Once a victim of fraud, it might be very difficult and expensive to track the fraudsters down and prove a case against them. Further, it is hard to establish whether, if tracked, the fraudsters would be able to pay back the stolen money.

Whilst most businesses are legitimate, please remember – prevention is always better than cure and the above tips are not conclusive and foolproof advice.

If you have any questions or concerns regarding the above article or your current situation, please contact our specialist Marine Lawyers on 02380 827416 or by emailing online.enquiries@LA-law.com.

Tel: 0344 967 0793 | Email: info@LA-Law.com | www.lesteraldridge.com