

International trade law: Payment of falsified invoice on account fraudster

Unfortunately, it regularly happens that email accounts are hacked. This may happen especially in international trade, where parties mainly communicate by email. The question is who bears the risk if the buyer pays the price on an account of the fraudster based on a falsified invoice.

What went wrong?

In a recent case before a Dutch court the buyer of a quantity of metal made a payment based on an invoice contained in an e-mail falsified by an unauthorized third party. As a result the purchase price was not received by the seller. The seller claimed payment from the buyer.

The buyer took the position to have fulfilled his payment obligation, because the payment had already been made. The payment was made based on the false invoice, but the buyer assumed that the bank account number specified concerned seller's bank account and therefore the buyer assumed that the payment was justified. Furthermore, the circumstance that a fraudster apparently gained access to the e-mail traffic between seller and buyer by hacking into the system of the seller, should be at the risk of the seller according to the buyer.

Decision of the Courts

In this case, the parties continued their dispute from the District Court to the Court of Appeal and finally to the Supreme Court.

District Court

The Court honoured the seller's claim to payment of the invoice.

The Court decided, that if a third party declares something for another (i.e. the seller), that other person can generally rely on the fact that the statement did not originate from him, even if the person to whom the statement was addressed, assumed and could reasonably assume that the statement did originate from that other person. However, the court held that the recipient is protected in the confidence that the statement originates from that other person if there are special circumstances. These circumstances must be of such a nature that they lead to the conclusion that justified trust of the recipient is attributable to the other (i.e. the seller). The confidence that the false invoice with the wrong bank account number

originated from the seller is insufficient to deem that the seller is bound by the contents of the false invoice. Taking all the circumstances into consideration, the Court also decided that the seller did not act so negligently that the resulting fraud should remain at its risk.

This means that the District Court held that buyer is not protected in the belief that the false invoice came from the seller. The buyer has not satisfied its payment obligation by paying to the fraudster and must therefore still pay to the seller.

Court of Appeal

The Court of Appeal annulled the judgment of the District Court and rejected seller's claims after all.

In the opinion of the Court of Appeal there were special circumstances. For example, the emails which were sent to buyer, came from the correct email address of the seller. That email address was also used by seller on previous orders and the invoices were sent from this email address to the buyer as well. The subject of the emails was also always the same. The seller prescribed the method of invoicing, whereby its payment requests were sent to buyer by email. Furthermore, the seller did not use a same account number for each invoice. The designated bank and account number differed per order. It was also not unusual for the shipping documents to be adjusted in the meantime, for example because the delivery conditions or the size of the order changed. In that sense, the amendment of the shipping documents was no cause for concern for the buyer. In the light of this, the Court of Appeal was the opinion that there were special circumstances. These special circumstances were of such a nature that the buyer could assume that the invoices were sent by the seller.

Supreme Court

The Supreme Court upheld and confirmed the judgment of the Court of Appeal.

What does this mean for you?

One of the factors that may play a role in the decision of the courts is to what extent the parties have taken adequate precautions to prevent a third party from falsely sending invoices. The buyer and seller may be expected to explain what efforts they have taken to find out how the third party could have falsely pretended to be one of them and what the outcome is of these efforts.

It is difficult to completely prevent fraud. But at least you can take appropriate measures. For example, to take technical security measures to prevent hacking as much as possible and to recognise hacking. Furthermore, it is wise to have regular contact with the seller by telephone and not only or mainly by email. On the phone you can check more easily whether the emails and/or invoices have indeed been sent by the seller and if the current situation matches with the emails. If the invoice states a payment

not to the same or already recognised account number, it is wise to contact the seller in advance by telephone and to check whether the new or different account number is correct.

June 2021