# CYBER RISKS IN COMMODITIES SALE CONTRACTS – MISDIRECTED PAYMENT

## The risk of payments under a sale contract being fraudulently diverted is a key concern for commodities traders.

In a typical scenario, an imposter gains access to electronic communications between seller and buyer to a trade. The buyer then receives an invoice and makes payment to the bank account details specified therein, only to discover subsequently that the invoice was sent by the imposter, not the seller, and the funds have been diverted to another bank account. Sophisticated imposters can produce convincing documents and use email addresses highly similar to those of the genuine seller.

If a payment is misdirected in this way, under English law, who is responsible? Can the risk of such a cyber attack be expressly allocated between the parties to a sale contract? How can commodities traders protect themselves?

## Who bears the risk?

Many commodities sale contracts require payment to be made by an electronic transfer of funds. The payment clause often specifies that payment must be made to the intended recipient's account (usually the seller). A recent English high court decision indicates that in these circumstances, the buyer's obligation to pay is satisfied only when payment is received into the correct account[1]. If the buyer makes a payment but it does not reach the intended recipient's bank account, the buyer will have to make a further payment to the seller to avoid being in breach of contract. In this scenario, it is the buyer who bears the risk of making a misdirected payment due to having been misled by fraudulent payment instructions.

## Allocating Risk under the Contract

The increasing frequency of cyber attacks has led many commodities traders to seek to allocate risk expressly in their sale contracts. Since there is currently no market standard cyber risks clause for use in commodities contracts, a bespoke clause is required.

## Cyber Risks Clauses - General

Drafting a cyber risks clause for a sale contract can be challenging, as it is not possible to include all possible scenarios without making it unduly lengthy. We recommend a focus on specific areas of concern. Cyber risks clauses typically include provisions which:

- Place express responsibility on parties to have in place procedures, systems and appropriate staff training to minimise the risk of a cyber security incident occurring (a requirement of good "cyber hygiene"). This is sometimes done by reference to ISO standards.
- Specify parties' obligations to mitigate and resolve the impact of a cyber security incident, which may include an obligation to cooperate with a contractual counterparty.
- Provide for a limitation and/or exclusion of liability in the event of a cyber security incident. A buyer in a strong commercial position may seek to insert a provision which provides some relief in the event of a failure to pay due to a cyber security incident.

## Drafting a Cyber Risks Clause - GTCs

When drafting a new cyber risks clause for use in a commodity trader's preferred general terms and conditions (GTCs), it is important to ensure that the clause is consistent with the definitions and other provisions. Consider in particular whether cyber risks are already covered. For example:

- **Could it be force majeure (FM)?** In some cases, cyber security incidents may be covered by FM clauses. However, a cyber incident which leads to a payment being diverted will usually not constitute FM; FM clauses commonly exclude any events which affect the performance of a payment obligation (notably the FM clauses in the BP GTCs 2015[2] and SCoTA v8[3]). Depending on the language used in the FM clause, it may also be important to consider whether the cyber incident was reasonably foreseeable and preventable.
- **What about the limitation of liability clause?** This may apply to a loss resulting from a cyber security incident. Consider whether it carves out losses resulting from negligence. If there is uncertainty, it is preferable to state expressly whether the clause is intended to apply where a buyer's payment has been fraudulently misdirected.

We can assist you in reviewing your GTCs and drafting a suitable cyber security clause for a commodities sale contract if required.

## Practical tips for dealing with payment fraud and diverted payments

We recommend that you have in place comprehensive due diligence and cyber security protocols, and perform audit checks to ensure the correct processes are being followed.

If a payment is diverted, there are options available. The paying party should immediately contact the relevant bank(s) as they may be able to place a temporary hold on the account. If possible, redress should be sought from the third party fraudster, often by obtaining a freezing injunction over the bank account. Action could also be taken against the bank for security/data protection failures, or recovery can be made under an appropriate insurance policy.

For further information, please contact:

**MARTINA KELLY**
Senior Associate, London
**T** +44 (0)20 7264 8155
**E** martina.kelly@hfw.com

1 K v A [2019] EWHC 1118 (Comm) at para. 29 *"The contractual obligation is to make payment to the seller's bank for the account of the sellers [...]"*.

2 BP Oil International Limited General Terms & Conditions for the Sale and Purchase of Crude Oil and Petroleum Products 2015 Edition - clause 65.2.2.

3 globalCOAL's Standard Coal Trading Agreement (SCoTA) version 8 – clause 15.3

**HFW has over 600 lawyers working in offices across the Americas, Europe, the Middle East and Asia Pacific. For further information about our commodities capabilities, please visit www.hfw.com/Commodities**

**hfw.com**



Americas | Europe | Middle East | Asia Pacific