Fraud Alert Fake President

With Euler Hermes as your Fidelity insurer, you have a strong partner to stand by you when you need protection from fidelity risks. But we do not only want to be there for you when a loss has already taken place. It is our aim to protect your company from the dangers which may threaten it. For this reason we would like to warn you about specific fraud scenarios which have been responsible for causing a large number of losses in recent years, some of them quite high.

Scenario 1: Fraud through criminals assuming a false identity – "Fake President Fraud"

In this type of scam, the perpetrators masquerade as being from the insured company's top management – mostly as a member of the board of management- and send an email or fax to an employee who is responsible in the company for carrying out bank transactions, asking them to execute an urgent money transfer. They try to make the employee believe that this is a highly confidential matter which must be kept secret at all costs, and which is vital for the strategic course of the company. The victims, who on the one hand feel flattered by the special trust shown in them by the board and on the other are under great pressure due to the alleged importance of the transaction, in most cases execute such transfers without delay. The money is nearly always transferred to foreign bank accounts, mostly in Asia and Eastern Europe. If the fraud is exposed, the accounts there are almost always already empty or it is extremely difficult to recover the money due to the foreign legal system.

Frequently, employees in the foreign branches or subsidiaries of the company are targeted. That makes it more difficult for them to contact the responsible bodies in the company personally to verify that the alleged instructions are really coming from them.

Scenario 2: Fraud through diverting payment flows – "Payment Diversion"

In these cases, the fraudsters masquerade as business partners or suppliers of the insured company and manage, by giving fake information, to get payments for goods delivered or services rendered diverted onto different account numbers from those previously registered. This form of fraud functions by sending a forged notice to the insured company that the bank connections previously agreed with them have changed, and that payment transactions should be made in future to the new account number.

Scenario 3: Fraud through identity theft – "Fake Identity Fraud"

In this fraud scenario, too, the perpetrators masquerade as an existing customer or a new customer of the insured company and send a written order for goods. Plausible reasons are then given for switching the delivery to a divergent delivery address. Since the identity of an already existing firm is used, the fraud victims do not at first smell a rat. The fraud often only comes out when payment does not arrive on time and a reminder is sent to the real customer. When the delivery address is then checked by the police, the premises are found to be deserted - and the goods have of course long since been moved somewhere else.

What can you do?

- Implement clearly demarcated processes and responsibilities in your company. If it is at all possible, the "four eyes principle" should be introduced for all relevant financial transactions. Set up clear rules to be followed in cases which are out of the ordinary, for instance when unusually high or urgent payments need to be made.

- Verify the payment information or the email order. If possible, a call should be made to employees you already know at the customer or to the head office of the alleged customer. For this, do not use the telephone number given in the email, but, for instance, the one in your own internal records or on the customer's website.

- The details given of changes to the bank account data or divergent addresses for the recipients of a payment should similarly be verified by a safe method such as sending a letter or confirmation of the account with calling back to authenticate it.

- Encourage your employees to get back to the alleged sender or at least to inform their direct superior if they receive a communication purporting to be from the company's board which appears unusual in its style or contents or the expressions used, or perhaps even contains spelling or grammar mistakes.

- Involving the police – in the event of an attack, you should file charges.

- **Inform all your employees worldwide about this type of fraud scenario, make them aware of the danger and put appropriate codes of practice in place to deal with it.** Especially those employees who work in sensitive areas in the finance departments should be made aware of this danger.

This information sheet is intended for your general information only and can under no circumstances be construed as providing cover. The scope of your cover can be seen from the Schedule to your Policy, the General Conditions of Fidelity Insurance agreed in each case and the statutory provisions of the German Insurance Contract Law (VVG).

Please note that it is only our **GCI VSV Premium** – within the valid sublimit (Losses – caused by third parties) which cover – in principle - the claims scenarios described by us above, in particular "FAKE PRESIDENT" FRAUD.

For more information: http://www.eh-cybercrime.de

Mit besten Grüßen

Rüdiger Kirsch

Euler Hermes Deutschland
Niederlassung der Euler Hermes SA