PAYMENT FRAUD OVER THE INTERNET – WHAT SHOULD YOU DO?

Checklist

"FAKE PRESIDENT FRAUD":
in this type of fraud, the fraudsters pretend to be high-ranking managers of the company – mostly a board member or managing director– and ask a staff member who is responsible in the company for bank transactions by email or fax to make an urgent money transfer. By assuming this false identity, payments are transferred to external accounts.

„PAYMENT DIVERSION FRAUD":
fraud through the redirecting of payment flows, e. g. by giving new account details of a supplier which are alleged to have changed.

Act at once!

"Everything comes to him who waits" according to the proverb – but sometimes the exact opposite is true: reacting as swiftly as possible is of the essence in cases of so-called Fake President and Payment Diversion fraud. The criminals are online in the internet and using its speed; operating across borders is part of their plan and is intended to make it as difficult as possible for the victim to get the assets/money that have been misappropriated back. The only way you can thwart them is by acting fast and effectively. That is why you should follow the instructions recommended below, which give you, in our experience, the best chance of recouping or at least reducing the loss you have suffered or in the best case avoiding it entirely:

1. INFORM YOUR BANK IMMEDIATELY

of the loss and provide them with all the available documents.

- Ask them to stop the transfer[1].
- If the money has already been transferred, ask the bank (if necessary get in touch with their management) to send a SWIFT[2] message **without delay** to the recipient bank that the transaction is suspected to be criminal fraud, requesting them to execute a reverse transfer of the sum and to report suspected money laundering.
- Get the bank to **give you a copy** of the SWIFT message for your records.

[1] In electronic banking, the transfer will as a rule already have been made.

[2] Banks communicate globally via the so-called SWIFT system. Secure messages can be sent between banks extremely fast via this.

2. MAKE SURE THAT NO MORE PAYMENTS ARE MADE and that any further emails received from the suspected fraudsters are passed on immediately to the responsible department of your company.

3. SECURE ALL DOCUMENTATION AVAILABLE which has directly or indirectly any bearing on the event of loss both electronically and in paper form such as:

- emails
- bank statements
- transfer orders
- telephone memos etc.

4. NOTIFY THE LOSS TO US AND SEND US ALL THE AVAILABLE DOCUMENTATION IMMEDIATELY.

- We can agree together with you what measures need to be taken, also abroad, in order to stop any further outflows of your money.
- The sooner you contact us, the better the chances of us finding together a way to recuperate the loss or at least contain it.
- The longer you wait, the better chances the criminals have to transfer the money onwards, making it more difficult or even impossible to recover it.

5. REPORT THE OFFENCE TO THE RESPONSIBLE PUBLIC PROSECUTOR'S OFFICE AND PREFER CHARGES attaching all the relevant documentation you have.

- Decide together with them the best way to proceed, especially as regards any requests for legal support in foreign jurisdictions.
- Obtain the case file number and wherever possible the name of the employee in charge of the case at the public prosecutor's office and
- pass this information on to us.

6. MAKE YOUR EMPLOYEES AWARE OF THE DETAILS OF OUR FRAUD WARNING AND ALERT THEM TO THE FOLLOWING WARNING SIGNALS:

- new persons suddenly appear in an existing email correspondence.
  – Check the email addresses.
  – The criminals often use email addresses which are very similar to real ones which you probably already know, and often differ only by a single letter or character.
- You should be suspicious if you receive an email from a member of the company's management asking you to execute transfers of high amounts to foreign accounts, and should always get confirmation of this through other channels, especially when you are requested to keep it strictly confidential and to bypass the normal procedures.
  – The person contacted is often told to carry out the transaction involving a law firm which then gets in touch with you to give further instructions.
  – Check whether the law firm and the lawyers who purport to be acting for it actually exist. Involving a law firm is a ruse designed to put further pressure on you and to bolster the appearance that the transfer you are asked to make is a legal and bona fide transaction.
- Be suspicious when a business partner requests payment to be switched to a different account from the one he has been using for years and ask your contact person at the business partner to confirm this, e.g. in writing and sent by normal post. **When you reply, do not under any circumstances use the contact data given in the suspicious email.**
- The criminals often try to swear you to secrecy by referring to the German public authorities, for instance the BaFin[3].
  – Be careful to check the spelling of the alleged person from the BaFin. This is often based on English names.
  – As a rule, it turns out that the BaFin or another authority given are not even responsible for the transaction in question and mentioning them is, here too, only intended to increase pressure and create the impression that the transaction is perfectly legal and above board.

[3] BaFin = Bundesanstalt für Finanzdienstleistungsaufsicht (Federal Financial Supervisory Authority)

Euler Hermes Deutschland Niederlassung der Euler Hermes SA 22746 Hamburg home address: Gasstraße 29, 22761 Hamburg
Phone +49 (0) 40/88 34-0 Fax +49 (0) 40/88 34-77 44 info.de@eulerhermes.com www.eulerhermes.de

15 5503 1120