

COMMON FRAUD SCHEMES IN THE CEE REGION

Fraud schemes such as "Fake President Fraud", "CEO/CFO FRAUD" or "CEO Email Scam" are an increasing phenomenon in the CEE Region. Based on a rather simple but highly effective scenario perpetrators target companies and – either by telephone or e-mail – succeed in convincing the companies' officers to make money transfers to foreign bank accounts.

Extent of damages

According to the most recent figures published by the FBI, this scheme has already caused losses in the amount of USD 3.1 billion, with over 22,000 victims in at least 79 countries affected from October 2013 through May 2016.

What is a "Fake President Fraud"?

The perpetrators introduce themselves to a company's financial officer or someone in the finance department as a high-level management member and instruct them to execute an immediate and urgent transfer of monies from the company's bank account to other foreign accounts (mostly in offshore jurisdictions). The fraudsters succeed in convincing the companies' officers that they are indeed the senior management member that they purport to be. They use an identical or slightly changed e-mail address that appears very similar to the authentic one, and convince the financial officer that he or she has been chosen to assist the high level management member in an important transaction due to their outstanding performance in the past and their reputation as a trustworthy and reliable person. Sometimes the modus operandi includes telephone calls to the financial officer as well as calls from alleged external legal advisors. By doing so they build up trust.

Typical Example

"Dear XYZ,

Please make yourself immediately available for a very urgent and highly confidential acquisition which keeps me busy the last months. Your assistance takes priority over all other tasks. Because of your impeccable working performance and your loyalty towards our company in the past, I have chosen you for this very important transaction.

You will correspond with our legal advisor, Mr. ABC. I fully trust Mr. ABC, therefore, please follow all of his instructions carefully. Because I will be very busy over the next days, Mr. ABC will provide me with daily updates.

To avoid the risk of an unwanted early release, please do not discuss this acquisition with anybody personally. If you have any questions, please do only contact me via this e-mail address.

Please confirm when you have read and understood this e-mail.

Mr. ABC will contact you asap.
Best regards,
Your CEO"

What do we know about the fraudsters?

Most of the money is transferred to offshore bank accounts (in particular in Asia). Currently, it is not clear according to which criteria fraudsters choose their targets. Since the fraudsters are often aware of internal regulations and working methods of the target company, it may be assumed that the victim has been observed for a certain amount of time. Sometimes "insiders" may be involved.

Returning the money

Since the fraud is often not detected immediately and involves money transfers to numerous bank accounts in various countries, finding and recovering the money by legal enforcement can be very difficult, time consuming and costly. Very often only a small portion of money, or nothing, can be recovered.

Immediate legal measures are essential (e.g. freezing of bank accounts). Establishing a good working relationship with the local and international authorities will also enhance the chances for success in retrieving monies.

What to do when you have become a target of such a fraud?

- Act swiftly to remain in control and set up an emergency team of lawyers and IT-experts.
- Assessment of loss and situation: find out which accounts and which banks in various jurisdictions are affected.
- Secure all data immediately and send all people who may be involved home.
- Call the police and file a complaint.
- Contact "asset tracers", which are companies specialized in aimed, discrete localization, identification and retrieval of financial assets which are in the unlawful possession of a third party.
- Immediately select investigators and define the scope of the investigation.

How to Mitigate the Risk – Essential To Dos:

What can you do to protect your company and to avoid the risk of such an incident?

- Make your employees aware of the "Fake President Fraud" and similar social engineering schemes and train them how to avoid becoming a target of such fraudsters.
- Put in place robust guidelines and processes on how payment transactions are to be handled.
- Implement a financial authority limits policy that provides employees with clear directions with respect to the approval process.

- If possible, no payment instructions (at least not above a certain amount) should be given by phone or by email.
- Regularly review the information the firm makes public on its website or in social media, such as employee positions, email addresses and phone numbers, and consider removing public information about your employees who are working in crucial areas, such as the finance department.

Should you require assistance in updating and amending internal rules, please do not hesitate to contact Wolf Theiss.

Authors:

Angelika Hellweger

Florian Pechhacker

About WOLF THEISS

Wolf Theiss is one of the leading law firms in Central, Eastern and Southeastern Europe (CEE/SEE). We have built our reputation on a combination of unrivalled local knowledge and strong international capability. We opened our first office in Vienna almost 60 years ago. Our team now brings together over 340 lawyers from a diverse range of backgrounds, working in offices in 13 countries throughout the CEE/SEE region.

For more information about our services, please contact:

**Clemens Trautenberg**

Partner

clemens.trautenberg@wolftheiss.com

T: +43 1 51510 5750

**Angelika Hellweger**

Counsel

angelika.hellweger@wolftheiss.com

T: +43 1 51510 5202

This memorandum has been prepared solely for the purpose of general information and is not a substitute for legal advice.

Therefore, WOLF THEISS accepts no responsibility if – in reliance on the information contained in this memorandum – you act, or fail to act, in any particular way.

If you would like to know more about the topics covered in this memorandum or our services in general, please get in touch with your usual WOLF THEISS contact or with:

Wolf Theiss
Schubertring 6
AT – 1010 Vienna

www.wolftheiss.com