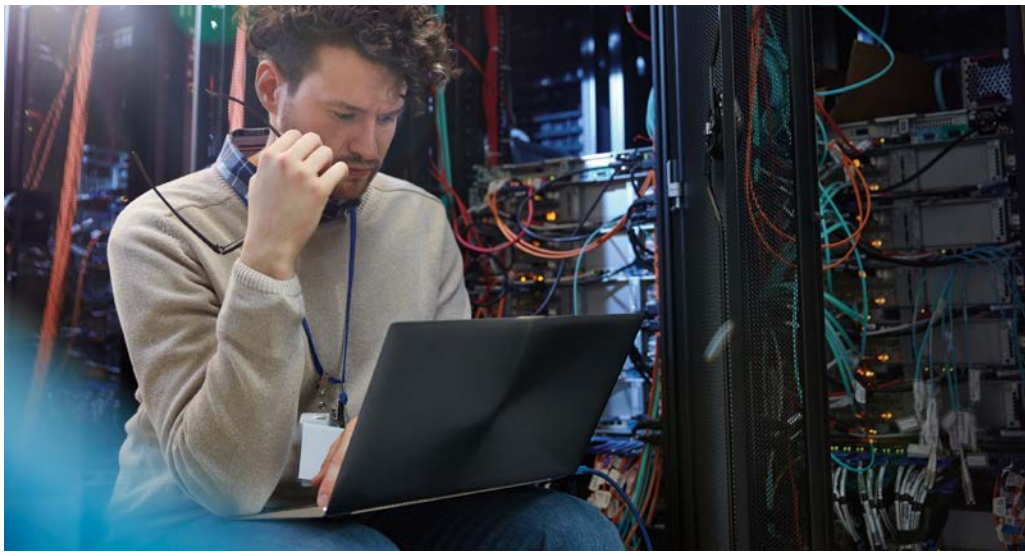
CREDIT SUISSE

Fraud in payment transactions – how you can protect your company

Fraud in payment transactions leads to substantial financial losses for Swiss companies and is becoming more prevalent. What are the warning signs and how can you actively protect yourself and your company?



Business email compromise

Compromised business email addresses constitute one of the greatest cyberthreats to individual companies as well as to the economy as a whole. Below you can see how this kind of fraudulent activity is carried out:

1

Espionage

- Perpetrators gather publicly available information about the company and its employees.
- Perpetrators infiltrate the IT infrastructure of the company or of a business partner (e.g. using a phishing attack).

2

Deception

- Perpetrators contact the company's finance department via email.
- The perpetrators allege that a payment is due and should be made to a previously unknown bank account.

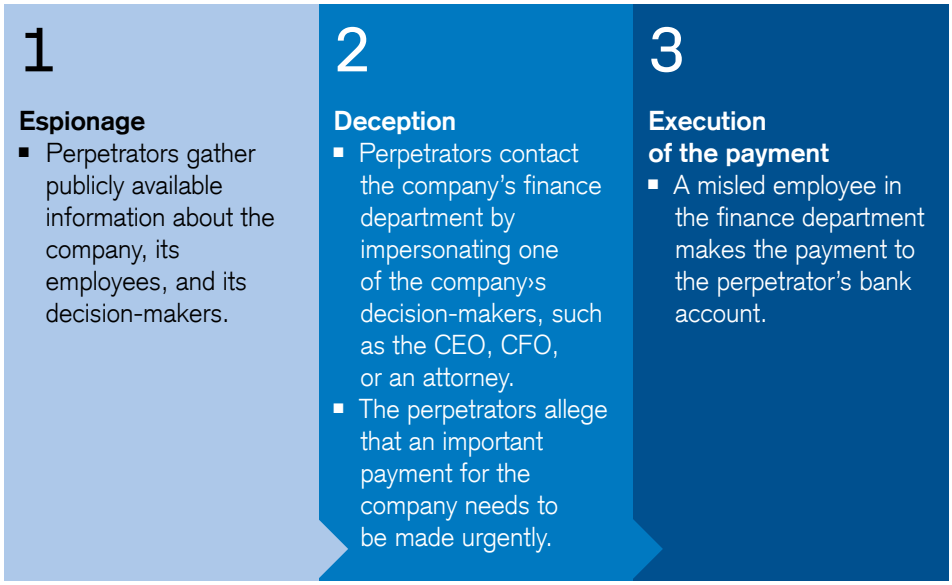
3

Execution of the payment

- A misled employee in the finance department makes the payment to the perpetrator's bank account.

CEO fraud

Successful CEO fraud attacks can bring your company to financial ruin since fraudsters want to access your company's assets. Below you can see how this kind of fraudulent activity is carried out:



Things you need to know:

- Any company, regardless of size, industry, or domicile can be targeted by fraudsters.
- A poorly protected IT infrastructure opens the door to fraudsters.
- Email communication is not secure and can be manipulated.

As a company, you can take action to combat these risks. By taking the following behavioral measures, you can make it difficult for fraudsters to succeed in their attempts and thereby avoid financial losses.

How to protect yourself:

- Ensure your IT infrastructure is protected in line with the latest standards.
- Establish different communication channels with your clients and suppliers and keep these up to date (e.g. telephone, mobile, email, postal address).
- If a business partner gives you payment instructions that differ from the instructions you already have, such as a different bank or account number, verify these. Please note: Do this using a secure channel, e.g. a telephone number that has already been verified.
- Implement accounting processes that prevent fraudulent transactions from being executed, for example by:
  - Making the relevant internal departments aware of business email fraud and CEO fraud.
  - Avoiding sole signing authority.
  - Encouraging your employees to immediately report suspicious activity or incidents that they notice to an internal central office.
- Check what information you want to publish about your company and your employees. Keep the information published to a minimum.
- Consider filing criminal charges if you are affected by fraud, even if you have not suffered any financial damage.
- In the event of an incident, inform your house bank immediately. This allows your bank to take the necessary protective measures and to claim back a fraudulent transaction in a loss event.

Please do not hesitate to contact your client advisor if you have any questions.

CREDIT SUISSE (Switzerland) Ltd.
P.O. Box 100
CH-8070 Zurich
credit-suisse.com

SMMI 3 C2614 12.2020