COVID-19 Cyber fraud and scams

Scammers and cyber crooks did not take long to adapt their usual fraud to this uncertain period caused by the Covid-19, refinishing notably their sadly notorious "CEO Fraud" to the present circumstances.

While all companies face great challenges dealing with continuity plans, reduced working hours of employees, cash pooling strategies to balance the accounts as well as restructuration projects in order to optimize the condition and the management of their cash flows, the floating triggered by the simultaneous global home office creates greater than ever opportunities for fraudsters.

With the surrounding fear of a forthcoming chaos, the internal daily routines are by essence considerably disrupted and the status of emergency is presumed by all and hardly questioned at all echelons of the hierarchy in these unprecedented times. The fraudsters do no longer need to be that creative to convince non extra-cautious accountants in remote working to approve and release damageable banking transfers.

None of the below tips are new but with the significant increase of scams experienced of the last couple of weeks, a gentle reminder would not harm.

Checks to be carried out

- **Adapt your existing business checks** and respective payment process to the current situation to ensure an **enhanced control** despite the remote status of employees and/or shortage of manpower; in any event **do not reduce/ interrupt the normal chain** of control in place.
- Monitor employees at risk and **maintain regular contact with them** in order to keep them quickly appraised with the ongoing changes and/or project decided by the management.
- Secure your conference calls, internal ones inclusive, with **updated access code** when the topics are sensitive.
- Ensure that **all employees precisely verify** the email address of any author sending payment instructions or requesting sensitive information; look for spelling errors or odd acronyms in the email address.
- **Ignore direct messages** (emails, social-media, WhatsApp, ...) coming from **an unsolicited and unknown source allegedly Covid-19 related** (Governmental body, health institutions and authority, charities, ...), or **at least run further verifications** through different channels and without precipitation.
- **Prohibit employees to use their private email** address for professional purposes and set the mandatory rules that **no (significant) payment is made if processed through such email address**, unless recipient, reason and IBAN are confirmed beforehand orally.
- Raise **awareness to malicious attachments, links**, Apps to all sort of updates associated with COVID-19 and **do never open them**; we are already abundantly updated by mass media.
- Remind employees to **avoid disclosing their credentials to disguised COVID-19 business** and organisation and to strictly **limit new logins** with safe and recognized online shopping websites, with caution.
- **Update (and improve)** your anti-malware software and make sure that all your employees use duly protected computers at all times (even if private device).
- Where possible, **differ instruction date and settlement date** by the remitting bank, to allow further scrutiny and to increase chance of funds to be recalled.

In the unfortunate case of a fraud

- Time is of essence, you will blame yourself later about the lack of control and diligence
- Immediately call the remitting bank or the online payment platform in order to block payment and ask them to instantly send a Swift recall message to the receiving bank
- Immediately call and send letter to the recipient's account bank warning them about a suspicious entry of funds [to be detailed for ease of identification] and urging to block and return the funds.
- In case of international fraud (notably when the receiving bank is abroad), file a criminal complaint with the Swiss Office of the Attorney General and call their relevant service +41 58 462 06 85 as you are probably not the sole victim of said scam (the receiving account might be already blocked).
- Reassess your system's weaknesses and risks

Contact
Rodolphe Gautier
lic. iur., Attorney at Law
Partner
Telephone +41 58 658 30 40
rodolphe.gautier@walderwyss.com