International Law Office

Importance of IT security measures in banking relationships: clients may bear risk of being hacked

14 August 2020 | Contributed by Walder Wyss

AUTHORS

Jürg Schneider

Hugh Reeves

Lucas Nanchen

On 9 July 2020 the Federal Supreme Court issued a ruling (4A_9/2020) addressing the liability of a securities trading company when hackers break into and use a client's email account to send transfer orders.(1)

Facts

In 2014, a Turkish resident (the client) transferred some of his assets to a Swiss securities trading company (the company) whose assets were deposited in an online bank account. The client and company were bound by an 'execution only' contract, which contained a so-called 'risk transfer clause'. Under this clause, the client expressly authorised the company to accept instructions given, in particular by email, and execute them immediately under any circumstances, even without written confirmation. According to the contract, the client assumed all risks, even in case of an error by the company as to the client's identity and released the company from any liability for damages that the client could incur in relation to the use of email, fax, telephone or any other transmission medium. The only exception was in case of the company's gross negligence.

At the end of 2015, hackers took control of the client's email account, allowing them, without the client's knowledge, to use his email address, read emails sent to the company, delete emails and send new ones. In one month, the hackers sent eight transfer orders to the company ordering the sale of shares and the transfer of funds to a UK account. In total, the hackers managed to extract €34,000 and £357,000 of the client's assets. As soon as the hackers used a slightly different email address, the company stopped the transactions and asked the client for confirmation.

Decision

The Federal Supreme Court analysed contractual practices between financial institutions and their clients and the (contractual) allocation of risk between the parties. In particular, it noted that banks would, absent any contrary agreement, have to bear the risks arising from payments to an illegitimate beneficiary. However, it is customary for the general terms and conditions of banks or other finance companies to include a risk transfer clause, thereby moving the risk to their clients. Any financial consequences resulting from an undetected lack of legitimation or forgeries, except in the event of gross negligence by financial institutions can therefore be contractually allocated to their clients. Absent any gross negligence by a financial institution, clients therefore bear the risk of third parties hacking into their email accounts. This also applies when clients act diligently and in cases of pure happenstance (ie, an unpredictable event outside clients' control).

Importantly, the Federal Supreme Court considered that banks do not have to take extraordinary measures to verify a signature's authenticity, which would be incompatible with a swift processing of operations, nor do they have to systematically presume the existence of forgery or tampering. This also applies in the case of email instructions. Consequently, the bank's responsibility is not engaged unless a quick look at transfer requests shows at first glance serious signs of identity usurpation (eg, spelling or language mistakes that are unusual for clients whose identity has been usurped); in such cases, any oversight could constitute gross negligence and hence the bank would have to bear the financial loss.

In the case at hand, the Federal Supreme Court considered that the hackers had used sufficient sophistication in imitating the client's writing style so as not to raise any serious indications of email abuse. In addition, the

transfers were made to a reputable bank in the United Kingdom. As a consequence, the Federal Supreme Court considered that the company was not grossly negligent. Because of the risk transfer clause, the client had to bear the financial losses.

Comment

This case is a stark reminder of the importance for anyone using online accounts and online (email) communications to properly secure their IT systems against hackers and other malevolent third parties. In case of any suspicious activity, it is necessary to immediately assess the situation and react accordingly.

As this case shows, clients of securities trading companies (or other financial institutions) may suffer the consequences of their lack of IT security and bear the risk of any financial loss, even though they were not at fault.

For further information on this topic please contact Jürg Schneider, Hugh Reeves or Lucas Nanchen at Walder Wyss by telephone (+41 58 658 58 58) or email (juerg.schneider@walderwyss.com, hugh.reeves@walderwyss.com or lucas.nanchen@walderwyss.com). The Walder Wyss website can be accessed at www.walderwyss.com.

Endnotes

(1) Intended for publication in the official case law collection of the Federal Supreme Court.