EFT fraud - risk management, rights and recourse

By Louis Podbielski

13 Nov 2019

Paying by electronic funds transfer (EFT) is so convenient for running one's home or business, with us being able to make payments from our smartphones and laptops. But this convenience does not come without risks.

Louis Podbielski, Case Law Product Manager at LexisNexis South Africa

Criminals are experts at intercepting emails from senders, inserting their own bank details and sending the email on so that it looks like the genuine sender's email and address. Once your money reaches these fraudulent accounts, it gets spirited away and you still owe the person, shop or supplier that was supposed to receive the funds in the first place.

Despite FICA requirements on bank accounts, the case law shows that you have little chance of recovering the money or catching the culprits. In *Galactic Auto (Pty) Ltd v Venter [2019]* (LP) a businessman bought a Ford Ranger that he urgently needed for a new business project. He did an EFT in response to an email that he received and was expecting from the car dealership.

He took delivery of the Ford Ranger, with it later emerging that the transfer had gone into a fraudulent account. The dealership then claimed the R380,000 purchase price from him. In this case, the court found that he should have verified the account number, before making the transfer and that he still owed the car dealer the money.

Criminals are also known to target attorneys because they often have large amounts in their trust accounts, and they regularly make substantial payments to new payees. In the case of *Fourie v Van der Spuy and De Jongh Inc [2019]* (GP), the client put funds into the attorneys' trust account, but due to a fraudulent email, the attorneys paid over R1,7 million into an account from which the money disappeared.

Whaling attacks a heightened threat

5 Jan 2016

The court noted that the Attorneys Fidelity Fund had issued a risk alert to attorneys, warning that cyber risks were increasing and that attorneys must take adequate risk mitigation measures. The court found that the attorneys should have taken precautions and that they were liable, especially based on their duty of care towards the client.

These two cases show that the risk of EFT fraud is becoming so real and that parties cannot merely accept bank details supplied by email, even if the email appears genuine and seems to come from the correct sender, at the expected time. Precautions must be taken to verify the bank details, before making the transfer.

Matthew Klein (Acting Judge) sums up the situation in the *Fourie* case:

> *"[1] This is a judgment on a matter pertaining to cybercrime, it is a matter of innocent people being dragged into cases where emails are hacked, and payments are made to unknown hackers. The victims then litigate against one another.[25] The rate at which cybercrime occurs makes the internet a very unsafe working area."*

But what can individuals and businesses do to reduce risks? A basic precaution would be to check the payee's telephone number on their website, or by dialling Telkom's Directory Enquiries on 1023, dial that number, and have a staff member read out their account details.

Save yourself from mobile hacking - Q&A with Simeon Tassev

Lauren Hartzenberg 30 Mar 2016

Some banks are now offering an Account Verification Service as part of their online banking, where the payee's details and account number can be checked.

But would these measures be enough to satisfy the court, especially for attorneys who have the duty of care in safeguarding their client's funds in a trust account?

Cyber expert Graham Croock of nCyber and Associates says, "It is not sufficient to rely on verification of bank account details only. While this is an added control and often relied on, the problem arises with identity theft where the details will test positive if checked against bank records."

He gives the following advice:

- The most effective controls to prevent EFT fraud relate to awareness training of all staff and system access controls embedded in accounts payable software and bank software.
- Cyber Risk Management is now imperative for all businesses and particularly law firms who tend to rely on IT service providers for the implementation and management of cyber controls.
- Change control procedures must incorporate specially focused attention on any system where bank details can be

changed, and it is here where access controls are critically important.
- Patch management, End Point protection and disabling of account defaults are key controls, which need constant monitoring and effectiveness assessment.

“By performing comprehensive cyber risk assessments, system control weaknesses can be identified and mitigated prior to successful phishing and whaling attacks or hackers accessing and changing bank details,” Croock says.

ABOUT THE AUTHOR

Louis Podbielski is a Case Law Product Manager at LexisNexis South Africa.