COX | YEATS
attorneys

Durban: Ncondo Chambers, Vuna Close, Umhlanga Ridge, Durban I Dx 50, Durban
P O Box 913, Umhlanga Rocks, 4320
Tel: 031 536 8500
Sandton: 4 Sandown Valley Crescent, Sandton, 2196 I Dx 33 Sandton Square
Tel: 010 0155 800
Cape Town: Unit 16, 10 Pepper Street Chambers, Cape Town, 8000
Tel: 021 879 2516
Website: www.coxyeats.co.za

July 2023

CYBERCRIME: CHECKS AND BALANCES OR BE HELD LIABLE

INTRODUCTION

Communication in transactions routinely takes place by way of e-mail. It is common for e-mails to be "hacked" by fraudsters. Fraudsters then mislead the person transferring money into believing that the transfer of funds into the fraudster's bank account is in accordance with the agreement between the transacting parties, this is more commonly known as "Business E-mail Compromise". Both parties are victims of the fraud so, who should bear the loss?

This question was considered in the now infamous decision in ***Hawarden v Edward Nathan Sonnenbergs Inc*** (the "**ENS Case**") where a large law firm was found to be liable for the loss of a buyer in a conveyancing transaction and now more recently in the case of ***Jan Jacobus Gerber vs. PSG Wealth Financial Planning (Pty) Ltd*** (the "**PSG Case**"), where a financial planning firm had to compensate a client for payments made from the client's investment portfolio on the instructions of a fraudster.

The PSG Case is an important reminder to businesses (particularly those in the professional services and investment industry) and clients on what can and should be done to avoid loss.

THE PSG CASE FACTS

In the PSG Case, Mr Gerber had an investment portfolio with PSG Wealth Financial Planning (Pty) Ltd (**PSG**) which was managed by a Mr Fisher. In 2019 Mr Fisher received an e-mail (purportedly from Mr Gerber) to change his banking details and thereafter to pay money out of funds earmarked for retirement into this "new" bank account.

Unbeknownst to Mr Fisher, and his secretary, a fraudster had hijacked the plaintiff's e-mail address. To "verify" the new bank account the fraudster provided PSG with a letter under the guise of the bank's official stamp purporting to be confirmation of new account bank details.

Mr Fisher conducted an internal bank verification process with PSG's client services department. Client services identified a risk associated with the account and instructed Mr Fisher to further verify the new bank account details. Despite this, Mr Fisher instructed his secretary to make the first payment which she did. A call was made to Mr Gerber thereafter, not to confirm the banking details as client services had requested, but simply to confirm that a payment to Mr Gerber's bank account had been made (without any context, to which Mr Gerber raised no objection).

Several further payments were made into the fraudsters bank account thereafter.

When the fraudster continued to ply their trade and tried to access Mr Gerber's wife's funds everyone involved became aware of the scam. Mr Gerber then sued PSG for damages.

THE PSG CASE DECISION

On an analysis of the contract between the parties, and section 11 of the General Code of Conduct for Financial Service Providers and Representatives, the court found that there was a duty on PSG to protect Mr Gerber against gross negligence and fraud including implementing measures (technological and otherwise) to eliminate that risk.

PSG unsuccessfully argued that there was an implied duty on Mr Gerber to implement measures to avoid his e-mail from being hacked. The court found no basis for this duty in law or any evidence that Mr Gerber had not taken steps to this effect. It also rejected the argument that PSG had relied on a representation made by Mr Gerber as he had taken no actions in the series of events.

Accordingly, the court found in favour of Mr Gerber on the basis that PSG failed to comply with its obligation to protect Mr Gerber from fraud and entered judgement against PSG for all amounts paid to the fraudster together with commission and other charges and interest thereon.

THE ENS CASE DECISION

The court found that a duty of care exists on the person handling the transaction to warn the client of the dangers of cyber hacking and to take precautionary action to prevent the fraud from eventualizing, regardless of how or why the clients e-mail was hacked. In such circumstances, the risk of cyber hacking is foreseeable and the failure to safeguard the safety of the transaction is negligent.

KEY TAKEAWAYS

In both the PSG Case and the ENS Case, employees failed to comply with their internal fraud prevention policies and to make a simple clear and unambiguous telephonic call to the person whose money they were dealing with to confirm their banking details, which in both instances would have likely avoided the fraud from being successful.

Further, it appears that businesses will unlikely be able to "*pass the buck*" onto ordinary individuals and the courts will be reluctant to impose any duty on them to protect themselves against cybercrime, especially where there is a duty on the other party to take precautionary measures to prevent the fraud and associated financial loss.

Regardless of the obligations of a service provider, whenever an individual makes a payment or authorises a payment, they could avoid the time and cost of litigation after a fraud occurs by having taken the initiative themselves to call ahead and confirm the bank account details before actioning that payment. An added proviso should also be included in correspondence advising the client of the risks of cyber hacking and what steps should be taken to avoid such fraud from occurring.