hbgschindlers attorneys

Liability for Cyber Crime

By **Dominique Lobban** (Candidate Attorney), released by **Charissa Kok** (Partner)

12 November 2024

Edward Nathan Sonnenberg Inc. v Hawarden

INTRODUCTION

It is no secret that cybercrime is at an all-time high, with technology constantly evolving at a rate nearly impossible to keep up with. It remains more important than ever, especially in the legal sector, that companies and law firms do everything in their power to protect themselves and their clients from being hacked, payments intercepted, and sensitive information leaked. A recent matter brought to the Supreme Court of Appeal has highlighted the question of liability for cybercrimes, more specifically, whether companies and law firms have a legal duty to protect their clients and/or third parties against business email compromise (**"BEC"**), a type of cybercrime used by scammers to mislead victims into paying money or divulging confidential information by compromising email addresses, and furthermore, how wide this the duty's scope is.

CASE LAW

In the recent matter of Edward Nathan Sonnenberg v Hawarden 2024 ZASAC 90, the SCA was tasked with determining who bore the liability for the BEC which ultimately led to the theft of R5.5 million.

The facts set out that Hawarden wanted to purchase a property for the amount of R6 million in May 2019. Pam Golding Properties (**"PGP"**) was the real estate agent mandated by the seller of the property to market the property. In an email dated 23 May 2019, PGP corresponded with Hawarden congratulating her on her purchase and informing her of the R500 000.00 deposit. The court noted the significant of this email as it contained a warning of the risks of cybercrime and advised her to verify all banking details prior to effecting payment. To this extent, Hawarden heeded the advice and telephonically confirmed the banking details of PGP before making her deposit.

The seller had appointed Edward Nathan Sonnenberg Inc. (**"ENS"**) as the conveyancers, who confirmed receipt of the deposit amount and put Hawarden in contact with their offices directly for the transfer. During August 2019, Hawarden corresponded with ENS through a representative, Maninakis, in order to effect payment of the balance amount, being R5.5 million.

Hawarden was to sign a guarantee, which Maninakis sent the paperwork for in an email on 20 August 2019. Unbeknown to both Maninakis and Hawarden, this email was intercepted by a cybercriminal who had illegally gained access to ("hacked") Hawarden's email account sometime prior. A day later, Hawarden received Maninakis' email with fraudulent banking details altered by the hacker and sent to Hawarden using Maninakis' email address. Hawarden thereafter called Maninakis for a discussion in which she decided she would transfer the outstanding amount directly to ENS. Maninakis agreed and said an email would follow with the guarantee requirements and their banking details for a direct transfer.

Maninakis indeed sent this email with their banking details on an FNB letterhead, which contained a warning of the dangers of cybercrime and fraud, however, this email was intercepted by the hacker as well, who altered the banking details and sent the documentation on to Hawarden from an email address almost identical to Maninakis', save for two switched letters.

On 22 August 2019, Hawarden attended at her bank, Standard Bank, to seek assistance in making the payment, where she spoke to both a Mr Carrim at ENS and Maninakis regarding the payment, which was now going to be by way of EFT. Hawarden confirmed telephonically that she had the emails containing ENS' banking details and would proceed. Importantly, Hawarden did not confirm the banking details with ENS telephonically nor with the Standard Bank consultant assisting her when she made payment to the altered banking details.

Hawarden emailed proof of payment to Maninakis, which was intercepted by the hacker and altered to reflect that the payment would take up to 48 hours

to reflect. Maninakis' replying email was intercepted to show fraudulent investment mandates and the cybercrime warning were removed. In this period, the money was withdrawn by the hacker and FNB was unable to recover it by the time they were notified of the fraud. The fraud was only discovered on 29 August 2019. Hawarden instituted proceedings against ENS for the recovery of the R5.5 million, basing her claim on the fact that ENS owed her a legal duty to exercise a degree of skill and care - on the level of a reasonable conveyancer specialising in property transfers - to advise her on safe payment practices and warn her about BEC dangers. She further pleaded that the reasonableness of imposing a legal duty on ENS and to hold it liable for damages suffered by her in breach thereof was supported by public policy and legal norms in accordance with constitutional norms, being that she is elderly and a lay person without the knowledge and experience to protect herself against sophisticated cybercriminals, therefore ENS should have done so.

The Johannesburg High Court as the court a quo found in favour of Hawarden on the basis that all creditors in the position of ENS owe a legal duty to their debtors to protect them from the possibility of their accounts being hacked.

ENS appealed the High Court's decisions to the Supreme Court of Appeal (the "SCA"), who disagreed with the High Court's untenable postulation of duty placed on creditors. The SCA determined that in order for Hawarden's delictual claim to succeed, the element of wrongfulness arising from an omission causing pure economic loss would need to be more closely analysed. Hawarden's claim was based off pure economic loss caused by an alleged wrongful omission. The SCA relied on several judgments when assessing this claim. Home Talk Development (Pty) Ltd and Others v Ekurhuleni Metropolitan Municipality[1] was used to show that:

> "...negligent conduct in the form of an omission is not regarded as prima facie wrongful. Its wrongfulness depends on the existence of a legal duty. The imposition of this legal duty is a matter for judicial determination, involving criteria of public and legal policy consistent with constitutional norms."

This was further emphasised in the Constitutional Court case of Country Cloud Trading CC v MEC[2] which said that "...there is no general right not to be caused pure economic loss. So our law is generally reluctant to recognise pure economic loss claims, especially where it would constitute an extension of the law of delict" and further that the test for wrongfulness as set out in Le Roux[3] "...should not be confused with the fault requirement. The test assumes that the defendant acted negligently or wilfully and asks whether, in the light thereof, liability should follow".

From the above, the court determined that our law does not generally hold persons delictually liable for loss caused by another party's omission. In this case, regard must be had to the fact that Hawarden was not a client of ENS, her loss occurred outside of an attorney-client relationship, Hawarden's loss was not a result of any failure in ENS' system but rather because her email was hacked, and Hawarden had been warned in PGP's letters of this very risk. Furthermore, Hawarden had, in her payment of the deposit amount, heeded PGP's warning and confirmed the banking details telephonically. She was aware of this way of authentication but did not do so with the payment to ENS despite speaking to Carrim and Maninakis at the time, nor did she ask Standard Bank to verify the banking details while she was in their offices making payment. It was open to Hawarden to ensure she was paying to the correct bank account, and she had ample means at her disposal to protect herself. The court further determined that any warning at the point of their dealing would have been useless as her email had already been compromised prior and the risk had already materialised.

The SCA ultimately found that the findings of the High Court would have profound implication for not just attorneys, but for all creditors and thus the court a quo should have declined to extend the ambit of liability. The Country Cloud matter set out that "...if claims for pure economic loss are too-freely recognised, there is the risk of liability in an indeterminate amount for an indeterminate time to an indeterminate class" and that this vulnerability to risk should be an important criterion to consider when looking at wrongfulness claims based on pure economic loss. In the Two Oceans case, it was also held that when considering vulnerability to risk, the criterion "will ordinarily only be satisfied where the plaintiff could not reasonably have avoided the risk by other means". It is evident in this case that Hawarden could reasonably have avoided the risk by either asking Carrim or Maninakis to verify the account details of ENS or asked the bank to verify the account details while she was there.

The court further emphasised that, after weighing up her options, Hawarden chose to forgo the original plan of a bank guarantee in favour of an EFT and this fact should not be excluded from consideration when imposing responsibility on her for her own failure to protect herself against a known risk.

COURT HELD

Taking into consideration the above facts and arguments, the SCA therefore found that there is no shift in responsibility for Hawarden's loss on to ENS and her argument before the court a quo should have failed. The Appeal was upheld with costs.

CONCLUSION

The above judgment has distinguished and clarified on whom liability sits in terms of cybercrimes and BEC. It shows that it is also up to the lay person/debtor to ensure they are protecting themselves against cyber criminals. They too have a duty to ensure they are doing their due diligence when opening, sending and receiving emails, especially where it pertains to making electronic payments. The duty does not only sit on companies and firms to ensure they have protection and security measures in place, but on the client too - as any undue burden poses the risk of opening the door to a flood of claims for pure economic loss.

VALUE

The analysis of the judgment shows that financial institutions/creditors are not the only party responsible for due diligence in respect of making/receiving payments. The lay person also has a duty to ensure that they are making payment to the correct account and that their accounts have not been compromised. They must do so by actually taking the steps recommended to them by financial institutions/creditors.

[1]*Home Talk Development (Pty) Ltd and Others v Ekurhuleni Metropolitan Municipality 2018 (1) SA 391 (SCA).*
[2]*Country Cloud Trading CC v MEC, Department of Infrastructure Development, Gauteng 2014 (12) BCLR 1397 (CC).*
[3]*Le Roux and Others v Dey (Freedom of Expression Institute and Restorative Justice Centre as Amici Curiae) 2011 (3) SA 274 (CC).*

Charissa Kok
(Partner)

Dominique Lobban
(Candidate Attorney)