CONTRACTUAL LIABILITY FOR CYBERCRIMES – WHO BEARS THE BRUNT?

Category: Commercial Law,IT Law
written by Mathando Likhanya | May 20, 2024



South Africa has seen a rise in cybercrime with an estimated[1] annual impact of R2.2 billion on the economy. There has been a number of reported incidents impacting various sectors, both private and public within the healthcare, retail and IT industries to name a few. The financial and legal sectors have not been exempted from the scourge of cybercrime, with the sectors predominantly affected by business email compromise.

Business email compromise ("**BEC**") refers to a type[2] of cybercrime whereby a criminal illegally accesses a user's email account and misrepresents themselves as if they are the user. In recent years, we have seen businesses and customers approaching the courts for redress after they have fallen victims to what the courts have described as a "universally recognised scourge".[3] This article looks at two recent court judgements in order to briefly unpack the courts' approach to contractual liability for cybercrimes.

Jan Jacobus Gerber v PSG Wealth Financial Planning (Pty) Ltd

In this case, Mr Jan Jacobus Gerber ("**Mr Gerber**") and PSG Wealth Financial Planning Proprietary Limited ("**PSG**") entered into a written contract for the management of a share portfolio and provision of financial services. The contract contained a provision in terms of which PSG was under a duty to protect Mr Gerber from, *inter alia*, gross negligence and fraud. Furthermore, the contract incorporated, by reference, the General Code of Conduct for Financial Service Providers and Representatives ("**the Code**"). In terms of the Code, PSG was obliged to effectively employ resources, procedures and appropriate technological systems that can eliminate as far as reasonable possible, the risk that clients will suffer financial loss as a result of, *inter alia*, fraud and negligence.

Based on the above, Mr Gerber alleged that PSG was obliged to exercise the necessary skill, care, and diligence to ensure that the monies held by it did not fall prey to fraud. By failing to do, PSG breached its obligation which than led to his loss. In its defence, PSG admitted liability to protect against fraud, save for fraud committed by means of cybercrime because Mr Gerber failed to protect his computer system from being hacked. In pursuance of this defence, PSG sought to imply a tacit term to the effect that Mr Gerber had a duty to prevent hacking of his system.

In deciding whether PSG had established a tacit term, the court applied the officious bystander test. It found that importing the tacit term would be counter intuitive, as this would render the protection against technological fraud meaningless if the client has to assume the obligation to prevent hacking of its systems. The court also found that PSG did not establish a tacit term contended for. In addition, the court found that the assumption of contractual obligations must be construed in the context that cybercrime is a universally recognised scourge.

This case is very critical precedent in establishing who bears liability where loss has been suffered as a result of business email compromise. Given the rise in cybercrimes, it has become critical that financial and legal service providers recognise the gravity of their duty to protect their clients against cybercrime.

***Hawarden v Edward Nathan Sonnenbergs Incorporated* [2023] 1 All SA 675 (GJ)**

In this case, Judith Hawarden ("**Ms Hawarden**") brought a delictual claim against Edward Nathan Sonnenbergs Incorporated ("**ENS**") for damages to the sum of R5,5 million (five million five hundred thousand rands) for pure economic loss. The claim arose out ENS' failure to warn Ms Hawarden of the danger of BEC, a duty Ms Hawarden argued was owed to her. The BEC ensued when Ms Hawarden was in the process of concluding a transaction for the purchase of property, for which ENS acted as conveyancers.

The court found that ENS owed Ms Hawarden a general duty of care that arose the moment ENS accepted the brief to act as a conveyancer in the transaction. This is because even though at that point Ms Hawarden was not ENS' client, she was in the care of ENS. Therefore, ENS' duty included a duty to warn Ms Hawarden of the known risk of BEC and to take the necessary precautions and to protect itself against BEC. From this case, it is clear that although there was no contract in place between Ms Hawarden and ENS, the court still held ENS liable for the BEC.

It is unclear whether the approaches taken by the courts in the above judgements will be the prevailing principles in relation to BEC. However, what is clear is that the duty of care owed towards clients extends to the duty to protect against BEC. Organisations need prioritise and make sure that such is reflected through the development of internal policies and procedures to ensure that clients are at all times protected against BEC.

Written by Mathando Likhanya and Tshepiso Hadebe.

Contact us for more good, clear and precise advice!

---

[1] Metadata Simnikiwe, “Cyber crime’s annual impact on SA estimated at R2.2bn”, April 4, 2023, https://www.itweb.co.za/content/JN1gPvOAxY3MjL6m

[2] SABRIC, “Business Email Compromise”, https://www.sabric.co.za/stay-safe/business-email-compromise/

[3] Gerber v PSG Wealth Financial Planning (Pty) Ltd (36447/2021) [2023] ZAGPJHC 270, paragraph 100