

Financial services company ordered to pay client more than R800k lost in cybercrime fraud

By Tania Broughton

3 Apr 2023

The High Court in Johannesburg has [ordered](#) a financial services company to pay a client more than R800,000 stolen by fraudsters through email cybercrime.



Image: The Gauteng High Court in Johannesburg has ordered Edward Nathan Sonnenbergs to pay R5.5m plus punitive costs to Judith Hawarden.
Archive photo: Ashraf Hendricks/GroundUp

- PSG Wealth Financial Planning has been ordered to pay a client more than R800,000 stolen by fraudsters through email cybercrime.
- The fraudsters had hacked a client's email and requested via email for the client's investment shares and some of his wife's investment to be paid out to a new bank account.
- PSG argued that while it had a duty to protect the client's money, it could not be liable for loss under circumstances in which the client had been hacked.
- But the Judge found that PSG had not complied with its own policy to protect its clients from cybercrime.

Judge Denise Fisher ruled in favour of Jan Jacobus Gerber who sued a PSG Wealth Financial Planning for the loss he sustained due to the unlawful electronic transfer of money intended for his retirement that he had invested with the company.

Judge Fisher said it had become routine for business to be conducted via email and it had now become common for these emails to be accessed remotely by fraudsters. She said business email compromise (BEC) had become rife and that both parties had been victims of the fraud.

“The question is, who should bear the losses,” she said.

Judge Fisher said Gerber had a share portfolio which had been managed by PSG, through its representative Jonathan Fisher, for more than a decade.

Gerber had a share and cash portfolio with investments totalling R855,413 as at September 2019. This could be liquidated and paid out at Gerber’s request.

The Judge said that the contact between Fisher and Gerber was rare. The dealings entailed no more than a monthly statement, detailing his account activity, sent via email to Gerber.

Then, in October 2019 there was a “somewhat unusual request” when Fisher received an email, purportedly from Gerber, requesting to liquidate R250,000. The email also provided details of a new bank account with FNB.

Fisher emailed back, asking for confirmation of the new account. An email was sent back, containing a letter, ostensibly from FNB, which appeared to have an official bank stamp and reflected that the account had been opened in 2002.

Judge Fisher said PSG branches were run on a franchise system, and as part of that agreement, were given access to a central client service which could verify bank account details. The FNB account details were sent for verification. The report came back that the identity attached to the FNB account did not match Gerber’s details. It showed that the account had in fact only been opened less than three months prior, and the phone number and email address were not valid.

However, Fisher said these verification reports were often unreliable. His personal assistant Jocelyn van Stavel emailed Gerber to confirm that this was his account.

“Unsurprisingly, came the response from the hijacked email that the payment should be made into it,” Judge Fisher said.

When Van Stavel made a “courtesy” call to Gerber to let him know the money had been paid, Gerber had been driving and responded ‘goed so’ (‘that’s fine’) – although he did not know what she was referring to.

A second email from the hacker soon followed asking for more money, which was paid out, effectively wiping out Gerber’s investment.

Judge Fisher said the emboldened hacker was alerted by Van Stavel that Gerber’s wife also had an investment account. The hacker then requested R400,000 from his wife’s account. But when that email arrived, Van Stavel testified that “something didn’t look right”.



Leading law firm ordered to pay victim of cyber crime

Tania Broughton 17 Jan 2023



Fisher then contacted his clients, who both confirmed they had not asked to withdraw any funds.

A subsequent investigation revealed that Gerber's email had been hacked, and all the emails to and from PSG were diverted to a separate file which did not appear in his inbox or outbox.

PSG argued that while it had a duty to protect Gerber's money, it could not be liable for loss under circumstances in which his computer system had been hacked. This was a "tacit term" of the agreement, it said.

But Judge Fisher said to import such a term would be counterintuitive. "The protection against technological fraud would be meaningless if the client had to assume the obligation to prevent hacking. After all, PSG is paid handsomely for the services provided, including the provision of fraud protection," she said.

"There is no evidence that Gerber did anything or failed to do anything to protect his system from being hacked. He testified that his system was password protected and that he had an effective virus protection installed. This was not challenged."

Judge Fisher said the contracts dictated that instructions had to be given via email and "arguably [PSG] thus assumed the risk of employing this system of communication".

The Judge said the call to Gerber had been a "courtesy call", not one seeking confirmation that the monies were to be paid into another bank account.

PSG had not established that it complied with its contractual obligations to protect Gerber against cybercrime, she said. Judge Fisher ordered PSG to pay Gerber R811,488.98, plus interest and the costs of the application.

Published originally on [GroundUp](#)

© 2023 GroundUp. This article is licensed under a [Creative Commons Attribution-NoDerivatives 4.0 International License](#).

For more, visit: <https://www.bizcommunity.com>