

Leading law firm ordered to pay victim of cyber crime

By [Tania Broughton](#)

17 Jan 2023

Court judgment has consequences for companies that invoice via email.



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

- Judith Hawarden received an email from what she thought was Edward Nathan Sonnenbergs (ENS) with the details of the account into which she paid the balance of money owed on a property sale.
- But the email was forged and the money stolen. Hawarden sued ENS for the money.
- In finding for Hawarden, the Gauteng High Court criticised ENS for relying on email, which is insecure, for invoicing her. The case likely has profound consequences for how companies invoice clients.
- ENS also had to pay punitive costs for the way it handled the case.

One of South Africa's leading law firms has been held liable for R5.5m which a property buyer intended to deposit in its trust account. The money was stolen as a result of fraudsters manipulating emails from an employee of the firm.

Johannesburg High Court Judge Phanel Mudau has ruled that Edward Nathan Sonnenbergs (ENS) must pay Judith Hawarden R5.5m, plus interest, and pay the legal costs of the lawsuit on a punitive scale.

In her arguments, Hawarden claimed that ENS owed her a duty of care, and that in corresponding with her, it also had a legal duty to warn her of the danger of “business email compromise (BEC)”, that this was on the increase and that it was already prevalent.

She said the firm should have warned her, before she made any payment, that she should verify the account details, and it should have loaded its trust account details on online banking systems so that the account number would not have to be sent out on unprotected and unsafe emails.

ENS denied liability, claiming that Hawarden herself had been negligent in using an electronic transfer without ensuring that the bank details were correct.

The case dates back to 2019 when Harwarden put in an offer on a Forest Town property through Pam Golding Properties for R6m.

She paid a deposit of R500,000 directly to the estate agency.

The seller appointed ENS as the conveyancing attorney.

Hawarden received an email from Eftyhia Maninakis, a secretary in the property division of the law firm, with details of what was still required in order for the sale to go through and the option of providing a bank guarantee for the outstanding amount.

What Hawarden did not know was that this email was fraudulent, that a fraudster had intercepted the genuine email and altered the firm’s bank account details.

In response to this email, Hawarden telephoned Maninakis a few days later. Maninakis confirmed that she could transfer the outstanding amount in cash directly to ENS.

Hawarden received an email from what appeared to be Maninakis’s email later that day - what she believed was a follow up to their earlier conversation.

That email contained the firm’s bank account number, as confirmed by First National Bank.

What Hawarden did not notice was that the email address was from ensafirca.com - not ensafrica.com.

[Read the judgment](#)

Judge Mudau said the emails actually sent by ENS had been intercepted and forged and the bank account details were incorrect.

Further correspondence between Hawarden and Maninakis was also intercepted by the fraudsters, including an investment mandate which contained several warnings about BEC. This was after payment had been made but before the fraud was discovered.

The money was paid into the FNB account but was transferred out and the bank was unable to retrieve the misappropriated funds.

Hawarden, who has now retired, said in her evidence during the trial that nothing in the two emails alerted her to the fact that they were fraudulent and that she knew nothing of the dangers of business email compromise.

She said after she paid the money into the fraudsters' bank account, she received a statement of account from ENS, to make a second payment. At the foot of that account was a warning urging readers to telephonically verify the firm's banking details, a warning which had been absent on previous communications.

In evidence, Hawarden conceded that she had, during and after her divorce, dealt with large amounts of money - and that she had heeded the BEC warning on the Pam Golding correspondence - but said she trusted ENS implicitly and "assumed they would take care of anything that was not safe".

Hawarden called a digital forensic expert witness, Anton Van't Wout, who prepared a video demonstration for the court showing the ease with which an email can be altered. He suggested alternative safer ways of communicating safer information.

He testified that there was no reason why ENS could not have used a secure portal.

Another witness, attorney Mark Heyink, an expert in information and communications technology law, testified that this type of cyber crime was a well-known risk.

Under cross examination he conceded that most attorneys sent invoices to clients by way of ordinary emails and PDF attachments and that his evidence reflected what ought to be done, not what actually happens.

ENS led the evidence of Maninakis who said she had not known that PDF documents could be manipulated until this incident.

She said she had not sent the initial mandate letter with the fraud warnings to Hawarden because she did not know at that stage that Hawarden was going to pay the money in cash, rather than by bank guarantee.

She also thought Hawarden was in "safe hands" because she was liaising with her own bank on the issue.

Judge Mudau said Hawarden blamed ENS for her loss because, she said, the firm should have done more to protect her and used more secure means to communicate with her. She contended that ENS was well aware of this type of fraud.

"The evidence in this case shows that BEC attacks are rife, especially in the conveyancing industry. The parties' experts agree that BEC has been around for many years.

"ENS contends that if this court holds ENS liable, it would expose all conveyancers, big and small alike, to claims of the same kind by third parties, with whom they have no relationship, for losses they suffered at the hands of fraudsters who hacked their own email accounts.

"ENS contends that the ripple effect thereof would not only extend to all firms of attorneys but indeed to all businesses who send their invoices, with their banking details, to their clients by email which is a near universal practice for all firms.

"ENS submits that it is the responsibility of the debtor, who chooses to make an electronic payment, to ensure that it is paid into the right account," the judge wrote.

He said while Hawarden was not a client of ENS, the firm owed her a general duty of care as a purchaser of property.

"ENS, as Hawarden contends, had control over the way its bank account details were conveyed to her. It chose to do this by way of an unprotected email attaching its bank account details as a PDF document which could be easily manipulated as the evidence clearly established.

"ENS failed to safely communicate its bank details using technical safety measures ... Hawarden depended on [ENS] to act professionally."

The judge said the fact that most businesses sent their banking details by emails did not absolve the law firm from unsafe behaviour “which it knew at the time was unsafe and knew to take precautions”.

“Viewed objectively, Hawarden cannot be faulted for placing her trust in the firm who she believed was a very large and reputable firm.

“I have no difficulty in finding that the firm’s banking details were financially sensitive information and needed to be treated as such, that the risk of BEC was foreseen by ENS ... and that sending bank details by email is inherently dangerous.

“The risk of loss to Hawarden was highly foreseeable by ENS.

“The interests of society demand that a legal duty is recognised in this case,” Judge Mudau said.

Punitive cost order

The judge awarded a punitive cost order because ENS breached Hawarden’s privacy by including irrelevant documents about her divorce and other investments and business dealings in the court papers. Hawarden had made her hard drive available to ENS to conduct a forensic investigation to determine where the hacking occurred. ENS breached an undertaking not to copy certain documents on her hard drive.

This article was [originally published](#) on [GroundUp](#).

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