JUTA
POPIA PORTAL

ISSUE NO 21 • WHAT WE THINK ABOUT ... *GERBER V PSG WEALTH FINANCIAL PLANNING* • MAY 2023

WHAT WE THINK ABOUT ...
GERBER V PSG WEALTH FINANCIAL PLANNING

1. OVERVIEW

Another day, another data breach! Recently (in March 2023), the South Gauteng High Court handed down another interesting judgment related to liability for financial loss caused by cybercrime. To be more specific, in the judgment of *Gerber v PSG Wealth Financial Planning*[1], the judge had to deal with the following issue:

> 'The crime is typically committed in anonymity by means of remote engagement using the internet and other systems. It is usually of the nature of a confidence trick – the perpetrators trick the person who has control over the transfer of rights in the money into believing that the transfer into the account controlled by the fraudster is in accordance with legitimate instructions. Both parties are victims of the fraud. The question is: Who should bear the loss which it occasions?'[2]

These are our immediate thoughts on the issues raised in this case.

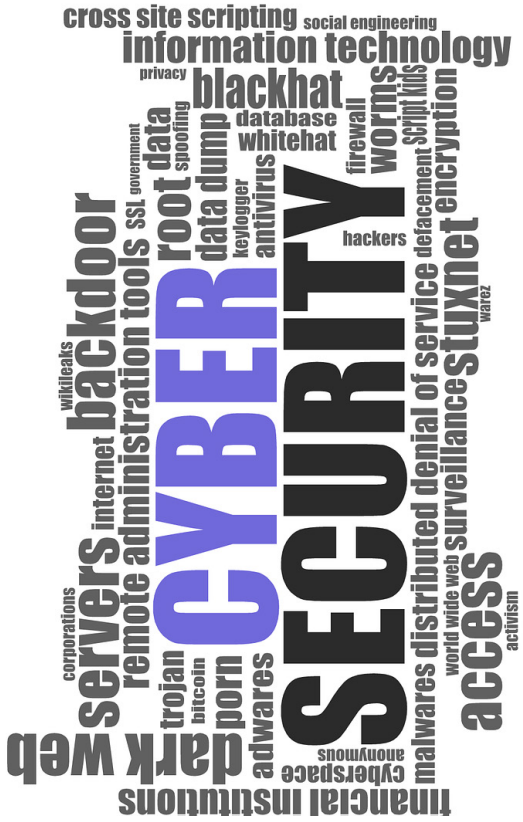

Photo: TDarwin Laganzon from Pixabay

2. WHY IS THIS CASE RELEVANT TO DATA PRIVACY COMPLIANCE?

Photo: stock.adobe.com

While this case does not mention POPIA, it deals with a topic very central to Condition 7 of POPIA ('Security Safeguards). While most responsible parties worry about being fined by the Information Regulator if they have a data breach, this case highlights the associated contractual liability risks.

3. SO, WHAT ACTUALLY HAPPENED?

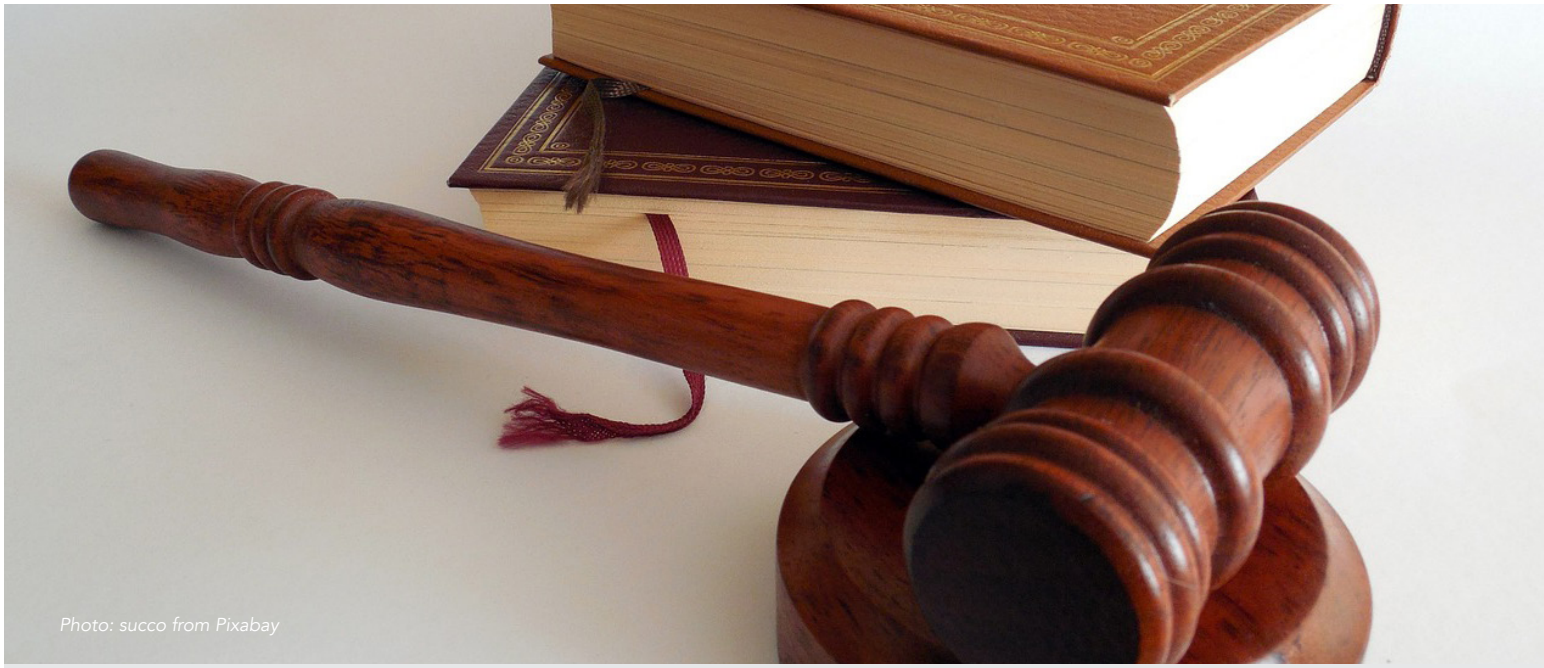

Photo: succo from Pixabay

Gerber (the party who brought the legal action) was a longstanding client of PSG Wealth Financial Planning ('PSG', the party being sued). Gerber had numerous investments with PSG, and Mr Fisher managed his investment portfolio. The nature of the relationship which existed was that Gerber put funds at Fisher's disposal to invest on his behalf, and Fisher had discretionary power to reinvest dividends and to buy and sell shares on Gerber's behalf.

In 2019, Gerber's email was hacked by cybercriminals, and they contacted PSG impersonating Gerber. Here, the cybercriminals (purporting to be Gerber) requested that PSG liquidate a portion of Gerber's investments and transfer them into a different bank account from the one PSG had on file. PSG did ask for a bank statement from this new bank account. In response, the cybercriminals sent a forged bank letter confirming the bank account's ownership and age details.

As a centralised security safeguard to prevent this type of crime, PSG, as an organisation, provides its franchises with access to services such as bank account verification checks and account control and payments. Here, PSG did do a bank account verification check, and the bank account did not pass this check. Additionally, the bank in question was unwilling to confirm telephonically whether the bank account belonged to Gerber. Fisher and his administration staff maintained that the results of bank account verification checks were often unreliable and could not be considered conclusive evidence of whether a bank account was fraudulent. The bank advised that the funds could be paid into the bank account at Gerber's own risk. PSG did ask via email if Gerber was willing to assume this risk, and the cybercriminals (again purporting to be Gerber) confirmed that the payment must be made. PSG subsequently made this payment. The cybercriminals (encouraged by their first success) purported to be Gerber again and requested more of Gerber's investments to be liquidated and the funds paid into another bank account. PSG's administration staff got suspicious this time and contacted Gerber's wife directly to confirm this request. This conversation resulted in PSG discovering that Gerber had no knowledge of the previous requests or payments and that fraud had occurred.

Later during the court case, Gerber claimed that PSG was contractually obligated as his financial services provider 'to exercise the necessary skill, care and diligence to ensure that the monies held by it in trust did not fall prey to fraud, that it breached this obligation and that such breach led to his loss'.[3] PSG denied liability and used the following grounds as defences:

- that PSG's contract with Gerber incorporated a tacit term to the effect that PSG would not be liable for losses under circumstances where Gerber's computer system was hacked due to his own negligence;
- that Gerber was negligent in that he did not take all reasonable steps to protect his computer system against hacking; and
- estoppel.

4. WHAT DID THE JUDGE DECIDE?

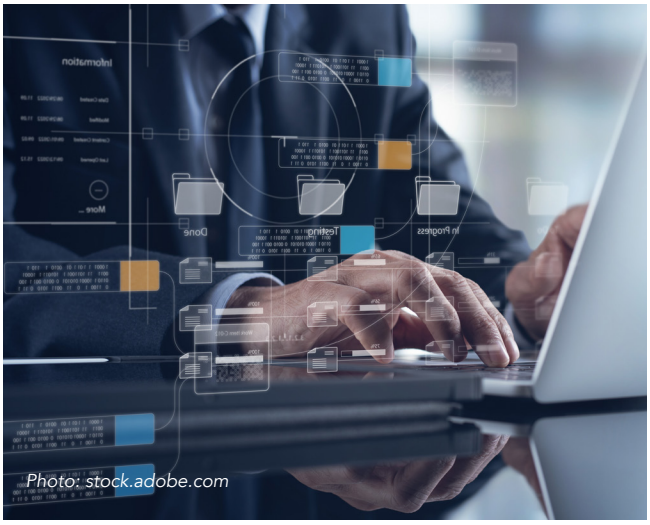
Photo: stock.adobe.com

The judge ultimately held that PSG was contractually liable to compensate Gerber for the financial loss he suffered due to the cybercriminals' conduct on the following bases:

- that PSG had not established the tacit term contended for;
- that PSG's contractual obligation to its clients 'was to have and effectively employ the resources, procedures and appropriate technological systems that can reasonably be expected to eliminate as far as reasonably possible, the risk that the clients will suffer financial loss through theft or fraud';[4]
- that PSG had ignored their own security safeguards in regard to [4] *Gerber v PSG Wealth Financial Planning* at paragraph 99. harge their contractual obligations as described above; and
- the defence of estoppel raised by PSG was also unsuccessful in these circumstances.

5. WHAT DO WE THINK ABOUT THIS?

5.1. IN GENERAL


Photo: ublicDomainPictures from Pixabay

We 100% agree with the judge's conclusions that PSG had a contractual obligation towards Gerber to employ procedures and technological systems to eliminate threats as far as reasonably possible and protect his investments from fraud or theft and that PSG failed in discharging this contractual obligation.

The only point we have some differences of opinion on is using the case of *Hawarden v Edward Nathan Sonnenbergs Inc.*[5] as a precedent for establishing an obligation to take specific actions in this example. We have based this opinion on the fact that the facts of these cases differ in quite a material way. In the *Hawarden v Edward Nathan Sonnenbergs Inc.* example, the cybercrime victim's own email systems were compromised. The cybercriminals in question then impersonated an Edward Nathan Sonnenbergs email address to provide the victim with an incorrect bank account. Edward Nathan Sonnenbergs Inc's systems were never actually compromised, and their staff did not fail to comply with their internal security safeguards. Whereas in this case, PSG's employees clearly failed to comply with the security safeguards that PSG had put in place to prevent this type of fraud.

5.2. UNDER POPIA

We think that this legal case would hold water if it had been brought under POPIA. The facts of this case align with our interpretation of the duty imposed on responsible parties by sections 19 and 20 of POPIA. [6]

Additionally, in this scenario, PSG is evidently the responsible party, and Gerber is the data subject.[7] Therefore, regarding section 91(3) of POPIA, Gerber (or the Information Regulator on his behalf) could institute a civil action for damages against PSG for a breach of POPIA.

6. FURTHER READING

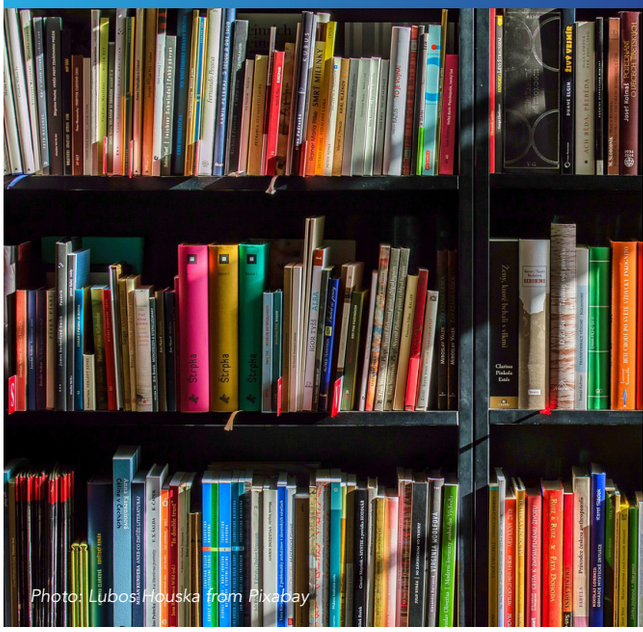

Photo: Lubos Houska from Pixabay

We discuss the duties of a responsible party concerning implementing security safeguards for protecting personal information and liability in relation to data breaches, specifically in Chapter 5.

We discuss civil liability for damages under POPIA in Chapter 19.

We discuss the other recent case of Business Email Compromise ('BEC') fraud, *Hawarden v Edward Nathan Sonnenbergs Inc.*, in our March 2023 newsletter article 'What we think about ... *Hawarden v Edward Nathan Sonnenbergs Inc.*'