

SOUTH AFRICA / JUDGMENT

Gerber v PSG Wealth Financial Planning (Pty) Ltd (36447/2021)

[2023] ZAGPJHC 270 (23 March 2023)

[2023] ZAGPJHC 270

COURT

South Gauteng High Court, Johannesburg

BEFORE

Fisher

CASE / FILE NUMBER

36447/2021

Source: saflii.org · Research copy typeset by Esheria. Not court-issued or certified.

Source record

FLYNOTES:

DUTY TO PROTECT AGAINST CYBERCRIME
CONTRACT
– Financial loss – Cybercrime – Universally
recognised as a scourge – Contractual obligations
to clients
– Client's email hacked and funds paid out to
fraudster's account – Duty to employ procedures
and
technological systems to eliminate threats as far as reasonably
possible – No scope to import a proviso that the
client has
the duty to prevent hacking – Investment company liable.
IN THE HIGH COURT OF
SOUTH AFRICA
GAUTENG LOCAL
DIVISION, JOHANNESBURG

Case No:

36447/2021
NOT
REPORTABLE
OF
INTEREST TO OTHER JUDGES
NOT
REVISED

In the matter between: JAN
JACOBUS
GERBER Plaintiff
And
PSG
WEALTH FINANCIAL PLANNING (PTY) LTD
Defendant

Coram: FISHER J

Heard: 17 January 2023

Delivered: 23 March 2023
ORDER
I

make an order which reads as follows:

1.
The defendant is to pay the plaintiff the amount of R811 488.98;
2.
The defendant is liable for interest on such amount at the statutorily prescribe rate on the amount of R250 000.00 from 8 October 2019 (being the date of the first payment) and on the amount of R561 488.98 (which comprises the second payment of R550 000.00 and the commission and fees of R11 488.96 charged by the defendant) from 18 October 2019 (being the date of the second payment);
3.
The defendant is to pay the costs of suit.

JUDGMENT

Fisher J

[1] This case involves a claim in contract for loss sustained due to the electronic transfer of the plaintiff's funds which were under the control of the defendant into the bank account of a fraudster.

[2] In this technological age the regulation of financial relationships routinely takes place by way of email. It has become common for these emails to be accessed remotely by fraudsters and for the victim's

computer system to be hijacked. This has become known as 'hacking' and the persons who commit this type of crime as 'hackers.'

[3] Types of hacking include crude extortion using sophisticated destructive software (known as malware) which is installed on the computer system remotely with ransom then being sought the hackers for its removal; corporate espionage and money transfer fraud.

[4]

It has been recognised by this court and others that this latter type of fraud, which has become known as Business Email Compromise (BEC) fraud, is rife.[1]

- [5] 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?
- [6] The application of the settled legal principles in relation to determining negligence in claims in delict and the nature and scope of contractual relationships can be complex in this esoteric cyberspace where what can and should have been done to prevent the hacking of the system is often difficult to determine.
- [7] It is helpful to discuss the applicable principles with the material facts in mind. I thus move to deal first with these facts.

Material

facts

- [8] The plaintiff has a share portfolio which has been managed by the defendant for in excess of a decade. The portfolio was managed by Mr Jonathan Fisher in his capacity of representative of the defendant for some years prior to the events which led to this case.
- [9] As at September 2019 the plaintiff held investments with the defendant in a total amount of R 855 413. This amount was held in shares and cash and these amounts could be liquidated and paid out in cash to the plaintiff on his request. The aim was however that the investment serves as retirement fund for the plaintiff and his wife. She also held a portfolio in her own name.
- [10] Until the hacking incident, which took place, over the period 03 October 2019 to 05 November 2019, the relationship had been uneventful.
- [11] The account was a discretionary account, meaning that the plaintiff put funds at the disposal of Mr Fisher who could operate on the account as he saw fit as far as the reinvestment of dividends and the usual buying and selling of shares was concerned. The aim was obviously to get as high a return on these share trades as possible so that the investment grew.
- [12] It was thus not necessary that the plaintiff have much, if any, personal contact with the defendant's

staff or Mr Fisher. Such contact was rare. The dealings between the parties entailed no more than a monthly statement being sent via email to the plaintiff setting out details of the brokerage activity on the account.

[13] On 03 October 2019 there was a somewhat unusual request which appeared to emanate from the plaintiff; the plaintiff sought the liquidation and payment of more than a quarter of his portfolio. This was something that he had never sought in all the years that the account had been managed by the defendant. As I have said, the purpose of the investment was to fund retirement. The amount sought to be liquidated was R 250 000.

[14] There was a further change alluded to in the email; a change of bank details from the plaintiff's

Nedbank account which had been on record for years to an account at First National Bank (FNB).

[15] Mr Fisher wrote back obligingly by return email. He said all was in order with the withdrawal and that it would take three days for the funds to be made available. Mr Fisher's email was carbon copied to his personal assistant Ms Jocelyn van Stavel.

[16] Mr Fisher noted pertinently in the return email that the bank account mentioned was different from that which the defendant had on record for the plaintiff. He asked that a current FNB statement be sent showing the new details. Presumably this was an attempt to verify that the account was not fraudulent.

[17] An email was then forthcoming in response. It did not contain a bank statement as requested. Instead, it contained a letter – ostensibly from FNB. The letter is dated 30 September 2019 and appears to bear an official bank stamp reflecting that date. It purports to provide details of a bank account held in the name of the plaintiff. It reflects that the bank account was opened in 2002 which would make it 17 years old. It states that, if the reader, has any queries the writer can be contacted at a mobile telephone number provided. Ms van Stavel was again copied in this response.

[18] The PSG branches such as the plaintiff are run on a franchise system. As part of the franchise arrangement, they are afforded the use of central client services provided by the main PSG entity. The central services include bank account verification checks and account control and payments. This facility clearly has, as a main function, the protection against BEC fraud.

[19] On 04 October 2019 Ms van Stavel, instructed by Mr Fisher, sent an email to central client services

asking that the plaintiff's 'new account' be verified and loaded so that payment could be made thereto.

[20] A document which is indicated as being from the Bank Verification Panel of PSG shows that the search failed. Details of the verification check disclosed to Mr Fisher and Ms van Stavel inform that (i) the identity attached to the account did not match the client details; (ii) the account was not more than three months old and (iii) neither the phone number nor email address attached to the account was 'valid'.

- [21] This information notwithstanding, there was a persistence as to the loading of the bank details. Mr Fisher and Ms van Stavel testified that these verification reports were often unreliable and that thus that they were not regarded as conclusive evidence of a fraudulent account.
- [22] Client services furthermore conveyed that, when asked, FNB was not willing to confirm telephonically that the account belonged to the plaintiff.
- [23] It was made clear that client services had identified a risk attached to the account and that consequently it would not accept any liability which arose from payment into the account. It thus required confirmation from Ms van Stavel that payment could indeed be made into the account at the risk of the defendant.
- [24] Ms van Stavel, duly instructed by Mr Fisher was undeterred. She next sent an email to the plaintiff's email address asking for his confirmation that the account was indeed his and that payment could be made into his account. Unsurprisingly, came the response from the hijacked email account that the payment should indeed be made into the nominated account.
- [25] The first personal communication between the parties occurred on 08 October 2019. Ms van Stavel telephoned the plaintiff on his mobile phone. He was driving at the time and on his way to a mining site where he was working. She merely informed him that 'the money' would be paid into his account that day. He responded 'goed so' ('that's fine') – although he did not know to what she was referring.
- [26] Ms van Stavel testified that this was a 'courtesy call' to let him know that the money had been paid.
- [27] Later that day an email was sent from the hijacked email account asking for proof of payment.
- [28] It is common cause that the plaintiff had no knowledge of the payment.
- [29] The hackers had thus successfully achieved payment of R250 000 of the funds from the plaintiff's account into the fraudulent account. They decided to continue with the deceit.
- [30] On 15 October 2019, there was further activity from the email address. An email was sent to Ms van Stavel thanking her for the previous successful transaction and requesting an additional payment to the FNB account. The email was copied to Mr Fisher.
- [31] It was confirmed by Ms van Stavel per return email that this would be done.

[32] On 18 October 2019 there was a communication from the plaintiff's email address asking when payment would be made. The reply came from Ms van Stavel that it would be forthcoming that same day.

[33] Payment was again duly made into the fraudulent account, thus wiping out most of the plaintiff's investment.

[34] Emboldened by the success, the hacker sought a further source of payment. Ms van Stavel was asked for a statement for all the plaintiff's investments. This was duly forwarded.

[35] Ms van Stavel, trying to be helpful, inquired if the plaintiff wanted a statement relating to his wife's portfolio as well. The answer came back in the affirmative. There followed a request for a withdrawal of R400 000

from Mrs Gerber's investment account.

[36] On 05 November 2019, an email was sent under cover of which a letter purporting to be confirmation of details of a banking account for the payment to Mrs Gerber. It had a similar get-up to the previous letter.

[37] Ms van Stavel testified that the email of 05 November 2019 'didn't look right'. She indicated that the language and syntax of the covering email was not grammatically correct in Afrikaans, which she spoke fluently.

[38] She thus approached Mr Fisher, who was in his office, and indicated her disquiet. Mr Fisher testified that he had, by this stage, had a conversation with a colleague in the same brokerage field who had related that hacking had taken place in relation to one of his clients in a similar way.

[39] This insecurity led to a call being made by Mr Fisher to Mrs Gerber. He asked her about the liquidation of the R400 000 investment of her portfolio. She indicated that she knew nothing about it and referred Mr Fisher to her husband.

[40] In the meantime, telephonic contact had been made with the plaintiff and he had confirmed that he too knew nothing of the requested transaction.

[41] It finally dawned on all concerned that they had been duped.

[42] A subsequent investigation conducted by the plaintiff some months later revealed that the plaintiff's

Microsoft Outlook email account had been hacked. The emails to and from PSG were diverted by the hacker to a separate file on the

account and thus did not feature in the inbox and outbox files. In this way the selected correspondence remained hidden until it was too late.

[43] Against this background I now turn to examine the claim and the defences raised thereto.

[44] The defendant seeks to import a tacit term into the contract which it contends excludes its liability. It also denies, in any event, that it breached the express terms of the contracts.

[45] The defendant pleads an alternative claim of estoppel. I will deal with the contractual defences and the estoppel defence in turn.

The claim and defences raised in contract

[46] The claim is based on the alleged breach of written contracts in terms of which the defendant undertook to manage the plaintiff's share portfolio and provide financial advice. The contractual relationship between the parties comprises two written agreements, an 'Advice Agreement' and a 'Product Agreement'.

[47] It is not in dispute that under the express terms of these agreements the plaintiff had the duty to protect the plaintiff against gross negligence and fraud.

[48] It is also not in dispute that under the General Code of Conduct for Financial Service Providers and Representatives ("the Code") which was expressly imported into the contractual relationship and specifically Section 11 of the Code, the defendant was obliged to 'at all times 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 clients, product suppliers and other providers or representatives will suffer financial loss through theft, fraud, other dishonest acts, poor administration, negligence, professional misconduct or culpable omissions.'

[49] The plaintiff thus pleads generally that the defendant was obliged 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.

[50] It was furthermore a term of the agreements that the plaintiff was obliged to provide all instructions

to the defendant in writing via email or fax. The reference to a fax would appear to be an anachronism as they are no longer in common usage having been supplanted by the email.

[51] The defendant accepts that it had the duty to protect the plaintiff's money against fraud but pleads a tacit term to the effect that the plaintiff would not be liable for loss under circumstances where the plaintiff's computer system was hacked due to the plaintiff's negligence. It alleges that the plaintiff was negligent in that he did not take all reasonable steps to protect his computer system against hacking.

[52] In essence, the defendant admits liability to protect against fraud, save fraud perpetrated by means of cybercrime where the plaintiff failed to take reasonable steps to protect his computer system from being hacked.

[53] The defendant must prove the tacit term. If it fails, it is left with a case in contract that it took reasonable steps to prevent the fraud.

[54] I now deal with the tacit term.

The tacit term

[55] The obligation of the defendant to protect against fraud is express. As I have said, the background and context to such obligation must be seen to include the prevalence of cybercrime in the financial service industry. In the face of this express term, the plaintiff seeks to imply a tacit term to the effect that the client had a duty to prevent hacking of his system.

[56]

A tacit term is an unexpressed provision of the contract which derives from the common intention of the parties as inferred by the court from the express terms of the contract and the surrounding circumstances.[2]

[57]

A tacit term cannot be imported into a contract on any question to which the parties have applied their minds and for which they have made express provision in the contract.[3]

[58] Thus, the defendant would have to show that the express duty of the defendant to protect its client against fraud is conditional on the client taking certain steps. These steps are not specifically pleaded.

[59] The defendant, on the other hand, was obliged to have and effectively employ the resources, procedures and appropriate technological systems that can reasonably be expected to eliminate the risk that its clients will suffer financial loss through fraud.

[60] Clearly, that there was a risk of hacking taking place is contemplated by this term.

[61] It makes sense that hackers will focus their efforts on infiltrating areas of commercial enterprise that involve large money transfers. Professions such as attorneys and financial services have started warning clients that bank account numbers will never change without specific human interventions from the firm. These warnings are often a standard message on all correspondence.

[62]

In *Hawarden v ENS*[4], claim in contract on the basis of an implicit term in favour of the client, it was found by this court that precautions which the defendant attorney was obliged to take would have prevented the fraud regardless of how or why the plaintiff's email was hacked. In my view, the same position holds sway on the facts of this case.

[63]

A test commonly applied by our courts[5] to determine the basis of which a tacit term can be imported into a contract is known as the 'officious bystander test.' It emerges from the following famous dictum of Scrutton LJ in *Reigate v Union Manufacturing Co (Ramsbottom) Ltd and Elton Cap Dyeing Co Ltd*[6]

'A term can only be implied if . . . it is such a term that it can confidently be said that if at the time the contract was being

negotiated someone had said to the parties, "What will happen in such a case" they would both have replied, "Of course so and

so I will happen; we did not trouble to say that; it is too clear." Unless the Court comes to some such conclusion as that, it ought not to imply a term which the parties have not expressed.'

[64] In applying the officious bystander test to determine the existence of tacit term, the express provisions of the agreement, the circumstances surrounding the conclusion of the agreement and the conduct of the parties subsequent thereto must be considered.

[65] The defendant, in effect, seeks to import a proviso into the fraud protection. It would have the term read that the defendant must protect the funds and not pay them to an illegitimate source provided that, if the client does not take reasonable steps to make his computer system inviolable to hacking, the protection will not apply.

[66] To my mind, to import such a proviso into these protections would be counter-intuitive. The protection against technological fraud would be meaningless if the client had to assume an obligation to prevent hacking of its system. After all, the defendant is paid handsomely for the services provided, which include the providing of fraud protection.

[67] An important gloss of the bystander test is that the tacit term contended for must be capable of precise formulation.

[68] Trollop JA in *Desai and Others v Greyridge Investments (Pty) Ltd*[7] in dealing with a proposed tacit term said the following:

'I do not think that it is either clear or obvious which of those forms of the term should prevail, and hence that none can be implied. The

reason is that the implication of a term depends upon the inferred or imputed intention of the parties to the contract . . . and once there is difficulty and doubt as to what the term should be or how far it should be taken it is obviously difficult to say that the parties clearly intended anything at all to be implied.'

[69] On this score, it is difficult, in the absence of an expert understanding of the technicalities of hacking, to determine precisely what needs to be done to protect the system. This difficulty is exacerbated by the fact that it is notorious that cyber-criminals develop their technologies and tactics to meet preventative measures as they evolve.

[70] I thus find that the defendant has not established the tacit term contended for. It is thus not necessary to consider whether a breach of such clause has been established by the defendant and whether such breach was causative of the loss.

[71] In any event, there is no evidence that the plaintiff did anything or failed to do anything to protect his system from hacking. He testified that his system was password protected and that he had an effective virus protection

software installed. This was not challenged.

[72] The defendant contends that the plaintiff must show that he did all he could to protect his email. This is not so. Defendant relies on the tacit term and the breach thereof. It is thus for the defendant to formulate the term, to show what steps should have been taken in compliance with the term and that these steps were not taken.

[73] Counsel for the defendant points out that there was some contradiction in the evidence of the plaintiff and his wife as to whether the passwords were physically accessible. He says this is relevant to the plaintiff's failure to comply with his obligations to keep his system safe. In this regard Mrs Gerber testified that the password was kept in a file in the plaintiff's study while the plaintiff testified that it was kept in a safe. This discrepancy is not material; it is not in the contemplation of either side that the email was physically sourced from study or safe. It is not in dispute that this was a virtual hacking. This evidence is thus irrelevant.

[74] Furthermore, and merely as an aside, it is not beyond the realm of possibility or even probability that the plaintiff's email was sourced from a hacking of the defendant's system and that the process started there. As was testified to by Mr Fisher, his colleague alerted him to similar fraudulent activity in relation to one of his client's

portfolios.

[75]

The upshot of these speculations may be that without firm evidence that either one or the other of the parties allowed the infiltration of one or the other of their systems, hacking must be regarded as an inevitable and intractable scourge. It is also not irrelevant that the contracts dictated that the manner in which the instructions had to be given was via email. Arguably, the defendant thus assumed the risk of employing this system of communication[8].

[76] Having failed in establishing the tacit term, the defendant is thus left with the defence in contract that it complied with the express terms of the agreement.

- [77] Clearly, on the facts, it did not. The deficiencies in the checking process were clear. The defendant ignored its own protocols. The checking machinery yielded the result that the account was not verified as being legitimate. The defendant however took the decision to override this information. This was notwithstanding that PSG client services pertinently pointed out that it had identified a risk that the account was not that of the plaintiff and that it would not bear this risk. I am informed from the Bar that there is no insurance for the fraud in issue and that loss resulting therefrom will be borne by the defendant if it does not succeed in its defences.
- [78] At very least, one would expect that the information relating to the bank account which was conveyed by client services would have triggered a further and more careful scrutiny of the letter provided as verification of the account. This is more so the case as Mr Fisher's own request for a bank statement was not complied with. A bank statement would have afforded greater detail as to the veracity of the account. The fact that it was not provided should have raised a concern in the first place.
- [79] Responsible and careful attention to the purported letter as against the bank account check would have revealed that the account was less than three months old whereas the letter states that the account in question was opened in 2002 – i.e. that it had been held by the plaintiff for more than fifteen years. This is a glaring anomaly.
- [80] The fact that the account was newly opened would, to my mind, be an indicator that it may have been opened for a nefarious purpose. The bank account verification process was specifically directed at whether the account was less than three months old. The fact that the discrepancy was not picked up shows that there was a lack of attention to the purported proof of the new account as being that of the plaintiff. The letter was simply taken at face value. This, to my mind, does not amount to the taking of steps to protect the investment against fraud. In fact, on the contrary.

The estoppel

[81]

When a person (the representor) has by words or conduct made a representation to another person (the representee) and the latter,

believing the representation to be true, acted thereon and would suffer prejudice if the representor were permitted to deny the truth of the representation made by him, the representor may be precluded (estopped) from denying the truth of the representation.[9]

- [82] The estoppel in this case is raised on two bases: first, that the plaintiff's system was hacked and thus the plaintiff through his negligence allowed the misrepresentations to be made; second, that the defendant when

telephoned by Ms van Stavel failed to question the statement that monies were to be paid into his account thus creating the impression

that he had sought such payment.

[83] I deal with each basis in turn.

The plaintiff's negligence facilitated the fraud.

[84]

This basis entails reliance on what is known in our law as the facilitation theory. This theory absent proof of calculated deception on the part of the defendant has long been discredited in our law[10].

[85] This was succinctly declared by Corbett J in *O K Bazaars* at 287H-288B as follows:

"As in the present instance, cases of estoppel by negligence often involve the fraudulent conduct of a third party and the complaint

against the person sought to be estopped is that his negligence permitted or facilitated the fraud. In this situation our Courts have rejected, as being too broadly stated, the so-called "facilitation theory", viz. that where-ever one of two innocent parties must suffer by the acts of a third, he who has enabled such third person to occasion the loss must sustain it (see Grosvenor Motors' case, supra at p.425; see also Connock's (S.A.) Motor Co. Ltd v Sentraal Westelike Ko-operatiewe Maatskappy Bpk., 1964

(2) S.A. 47 (T) at p.48). It has, on the contrary, been held that such cases must be adjudged by the ordinary general principles relating to estoppel by negligence; and, of course, the fraudulent intervention of a third party is an important factor in determining whether the conduct of the person sought to be estopped proximately caused the other's mistaken belief and resultant loss; and whether this result was reasonably foreseeable."

[86]

The defendant relies on *Mosselbaai Boeredienste (Pty) Ltd v OKB Motors CC*[11], a judgement of the Full Bench of the Free State Division. That case involved a sale transaction between two dealers in motor vehicles. Payment was made by the respondent into a fraudulent bank account, the payment details having emanated from a fraudulent invoice sent from the appellant's computer system. The appellant argued that the respondent was negligent in paying the purchase price into a bank account without verifying that such account was that of the appellant and that, in these circumstances, the defendant should bear the consequences of its negligence. The respondent, argued that the security in respect of the appellant's computer system was compromised through the negligence of the appellant, enabling the false invoice to be sent to the respondent. The respondent thus raised an estoppel which succeeded in the trial court and was upheld on appeal by the Full Court.

[87] It is argued on this authority that as the indications are that the fraud emanated from the hacking of the plaintiff's system and not that of the defendant, the plaintiff should bear the loss.

- [88] Apart from the fact that Mosselbaai cannot be construed as being authority for the general proposition that if the fraud emanates from one party's system, that party must bear the loss, the facts of that case are distinguishable. In Mosselbaai there was direct evidence that the fraud had been perpetrated internally on the appellant's system in that the password and user-names were not changed for years and were widely known by current and ex-staff members. There was no outside or remote accessing of the system. There was also no contractual protection accorded to either party.
- [89] On general principles, the case for estoppel by facilitation must fail on two bases. First, the defendant has not established that anything the plaintiff did or failed to do resulted in the hacking and it is just as probable that the details of the email addresses of clients were obtained from the defendant's system. Second, the plaintiff had no duty to protect his email system. On the contrary, the plaintiff was protected by a contract which put the duty to prevent fraud of this nature on the defendant.
- [90] Even if it had been shown by the defendant that the plaintiff was negligent, this does not absolve the defendant of his admitted contractual obligations. The proximate cause of the loss was not the hacking, it was the failure to employ the necessary and contractually prescribed vigilance when monies held in trust were sought to be paid into a different account.
- [91] In the circumstances the defendant cannot succeed on the estoppel defence on the first basis.

The telephone call

- [92] Mr Fisher attempted to suggest that his systems and protocols went further than merely the bank account checks. He indicated that it was part of the defendant's protocol that the client be spoken to personally when payment was to be made so that it could be confirmed that payment was being made into the correct account. He testified that the plaintiff misrepresented the position in the face of this protocol.

- [93] Ms van Stavel however characterised the call she made as a 'courtesy call'. On any basis the call cannot be construed as seeking confirmation that monies were to be transferred from the investment account of the plaintiff into a different bank account from the one on record with the defendant. The information given by Ms van Stavel was that payment would be made into the plaintiff's account. The plaintiff was not alarmed by this as he probably would have been had he been told that payment was to be made out of his investment account into a FNB account. This stands to reason. To the extent that the telephone call was meant to confirm that the account was a valid account such inquiry would have been express. The defendant explains that he believed the reference to be to internal transactions in his investment account. He concedes that such a call was never made previously but he explains that this did not concern him. He had no knowledge of the internal processes of the defendant and no reason to question the call.

[94] The plaintiff's confirmation on a query from his financial service provider that money could be paid into his account cannot, to my mind, be construed as a representation.

[95]

The situation would be different if the telephone communication was directed at confirming the plaintiff's new bank account details. Had this been done and the plaintiff, for some reason, confirmed the account to be his, it would arguably be the case that the defendant must be found to have taken all reasonable steps to verify the account and that it was thus not in breach of its contract. The case would thus not be decided on the question of the plaintiff's negligent misrepresentation but in contract.[12]

[96]

In any event, on the estoppel, it was the defendant's onus to show that the representation was clear and unequivocal and that Ms van Stavel reasonably understood the representation to mean that payment of the plaintiff's monies held by the defendant could be made into a new bank account.[13] The test for representation by conduct is whether the representor should reasonably have expected that the representee may be misled

and whether the representee acted reasonably in construing the representation.[14] The defendant failed to establish these aspects on the facts.

[97] As I have said, on Ms van Stavel's evidence, the call made by her was merely a courtesy call. It was not directed at confirming the bank account details or the instruction to pay. It is common cause that there was no indication given that information was being sought from the plaintiff. He was simply informed that payment would be made to him by his financial service provider. He had no reason to question this information. Dividend payments were made to his account in the normal course of the share brokerage that took place in terms of the agreements. The purpose of his investment was that it grows in, inter alia, this manner.

[98] Thus, the defendant has not made out a case for estoppel on the second basis either.

Conclusion

[99] The contractual obligation of the defendant 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.

[100] The assumption of these contractual obligations must be construed in the context that cybercrime is universally

recognised as a scourge. There is no scope to import a proviso into the term to the effect that the plaintiff has the duty to prevent

hacking. This would be counter-intuitive. A major and arguably the main reason for the protection under the agreement is cybercrime. Why would the plaintiff then assume responsibility for cybercrime?

[101] The defendant has not established that it complied with its contractual obligations to protect the plaintiff against cybercrime.

[102] The defendant has furthermore not established the estoppel defences raised.

[103] In relation to the quantum, the plaintiff's claim initially consisted of a claim relation to the loss of dividends

as a result of the fact that shares were sold to obtain the liquid funds. However, during the proceedings the plaintiff conceded that it would seek only the loss as at date of the breaches contended for which is the total paid by the defendant into the FNB account - being R 800 000 and with commission and fees charged by the defendant in the amount of R11 488.98 and interest on such amounts at the prescribed rate.

Order

In the circumstances I make the following order:

4. The defendant is to pay the plaintiff the amount of R811 488.98;
5. The defendant is liable for interest on such amount at the statutorily prescribe rate on the amount of R250 000.00 from 8 October 2019 (being the date of the first payment) and on the amount of R561 488.98 (which comprises the second payment of R550 000.00 and the commission and fees of R11 488.96 charged by the defendant) from 18 October 2019 (being the date of the second payment);
6. The defendant is to pay the costs of suit.

D FISHER

JUDGE OF THE HIGH COURT

APPEARANCES

For the Plaintiff: Adv. R. Bekker

Instructed by: Cox Yeats Attorneys

For the 1st Respondent: Adv. P Van der Berg SC

Instructed by: Thyne Jacobs Incorporated

[1] See for example Harwarden v ENS handed down in this court by Mudau J on 16 January 2023 under case number 13849/2020 , Jurgens and Another v Volschenk (4067/18) [2019] ZAECPHC 41 (27 June 2019); Fourie v Van der Spuy and De jongh Inc. and others

[2019] JOL 45848 (GP).

-
- [2] Alfred McAlpine & Son (Pty) Ltd Transvaal Provincial Administration 1977(4) SA 310 T 327.
- [3] See Airways Inc v SA Fire and Accident Insurance Co Ltd 1965(3) SA 150 (A) 175 C
- [4] Op cit, n 1
- [5] See for e.g. :South African Mutual Aid Society v Cape Town Chamber of Commerce 1962
- (1) SA 598 (A) at 606 ; Alfred McAlpine & Son (Pty) Ltd v Transvaal Provincial Administration 1974
- (3) SA 506 (A) op 533A - B ; Wilkins NO v Voges [1994] ZASCA 53; 1994
- (3) SA 130 (A) at 137A – D; Techni-Pak Sales (Pty) Ltd v Hall 1968
- (3) SA 231 (W) at 236H - 237
- [6] 1918] 1 KB 592 (CA) (118 LT 479 at 483)
- [7] Desai and Others v Greyridge Investments (Pty) Ltd[7] 1974
- (1) SA 509 (A) at 522H - 523A
- [8] See Maartens v Pope 1992 (4) SA 883 (N)
- [9] Oakland Nominees (Pty) Ltd v Gelria Mining 8 Investment Co (Pty) Ltd 1976
- (1) SA 441 (A) 452A-H
- [10] cf, for e.g, Union Government v National Bank of South Africa Ltd 1921 AD 121 131 138; and Grosvenor Motors (Potchefstroom) Ltd v Douglas 1956
- (3) SA 420 (A) 425F-H). O K Bazaars (1929) Ltd v Universal Stores Ltd 1973
- (2) SA 281 (C) (Ok Bazaars):
- [11] Mosselbaai Boredienste (Pty) Ltd v OKB Motors cc 2021 3DR 3059 (FB).
- [12] See Lillicrap, Wassenaar and Partners v Pilkington Brothers (SA) (Pty) Ltd 1985
- (1) SA 475 (A).
- [13] Southern Life Association ltd v Beyleveld NO 1989(1) SA 496 (A).
- [14] Concor Holdings (Pty)Ltd t/a Concor Technicrete v Potgieter 2004(6) SA 491 (SCA)

Source & reproduction note

Judgment wording, source notices and original paragraph numbers are retained. Esheria supplies the layout and this PDF's page numbers; these are not the source pagination. This is a research copy, not an official or certified court document. Check quotations, citations and publication restrictions against the original source before relying on it.

ORIGINAL SOURCE <https://www.saflii.org/za/cases/ZAGPJHC/2023/270.html>

CASE PAGE <https://chat.esheria.ai/case-law/south-africa/gerber-v-psg-unknown-topic-agpjhc-2023--6a3ea51e3b1caa91298149a1>

Prepared on 10 October 2026 · Esheria