Editorial note: Certain information has been redacted from this judgment in compliance with the law.

IN THE HIGH COURT OF SOUTH AFRICA

FREE STATE DIVISION, BLOEMFONTEIN

Reportable:	**YES/NO**
Of Interest to other Judges:	**YES/NO**
Circulate to Magistrates:	**YES/NO**

Case no: A43/2021

In the matter between:

MOSSELBAAI BOEREDIENSTE (PTY) LTD **APPELLANT**

t/a MOSSELBAAI TOYOTA

and

OKB MOTORS CC t/a BULTFONTEIN TOYOTA **RESPONDENT**

CORAM: **LOUBSER, J *et* BUYS, AJ *et* MGUDLWA, AJ**

HEARD ON: **02 FEBRUARY 2024**

DELIVERED ON: 07 MARCH 2024

JUDGMENT BY: BUYS, AJ

Introduction

[1] This is a judgment in the appeal to the full court by the appellant in terms of which the following relief is sought:

> "1. That the appeal be upheld with costs;
>
> 2. That the order granted by the Court on 17 March 2021 be set aside and replaced with the following:
>
> > "1. The defendant's counterclaim is dismissed with costs.
> >
> > 2. Judgment is granted against the defendant in favour of the plaintiff as follows:
> >
> > 2.1 Payment in the amount of R159 353.76;

2.2 Payment of interest on R159 353.76, calculated at a rate of 10.5% per annum from 8 February 2018 to date of payment;

2.3 Costs of suit, including preparation, traveling and counsel's costs at an increased scale.""

[2] This appeal is with special leave to appeal granted by the Supreme Court of Appeal on 9 June 2023 to determine the merits of the appeal.

[3] This appeal is against the order and judgment by the Bultfontein Magistrates' Court under case number 119/2018 ("the court *a quo*"). I do not deem it necessary to deal with the history of the matter from the date the Notice of Appeal was filed until special leave to appeal was granted on 9 June 2023.

Pleadings

[4] The appellant instituted action against the respondent for payment in the amount of R159 353.76, interest on the said amount calculated at the rate of 10.5% per annum from 8 February 2018 until date of payment and costs of suit.

[5] It appears from the summons that the appellant's claim premised from a verbal agreement concluded between the appellant and the respondent on 7 February 2018 in terms of which the appellant agreed to purchase from the respondent a Toyota Etios 1.5 Sprint HB motor vehicle ("the vehicle") for the amount of R159 353.76 ("the purchase price").

[6] The purchase price was due and payable by the respondent to the appellant upon delivery of the vehicle to the respondent on 8 February 2018.

[7] The respondent failed to pay the purchase price, and is consequently in breach of the agreement, therefore the purchase price is due, owing and payable by the respondent to the appellant.

[8] The respondent, in response to the appellant's claim, raised a special plea of estoppel on the following grounds:

[8.1] The appellant sent an invoice to the respondent with the banking details […] Account, Branch code […] and Bank account number […].

[8.2] The respondent acted in accordance with the information received from the appellant and made payment to the account number on the invoice on 8 February 2018.

[8.3] The appellant, or its representatives acting on behalf of the appellant, made the representation that the appellant's correct banking details appeared on the invoice referred to *supra*. The respondent accepted the correctness of the information on the said invoice when it made the payment referred to *supra*.

[8.4] The appellant is estopped from claiming that the account number referred to *supra* is incorrect.

[9] Over and above the special plea of estoppel raised by the respondent, the respondent furthermore denies being in breach of the agreement, and based this denial on the payment made into the bank account provided by the appellant. The respondent further pleads that the representation made by the appellant was made as a result of negligence of the appellant and/or its representatives, in that the appellant's electronic mail system was "*spoofed*".

[10] Simultaneously with its plea, the respondent delivered a conditional counterclaim. The respondent's cause of action in the conditional

counterclaim is based on the same averments referred to *supra* in the special plea and plea over, namely:

[10.1] The representation made by the appellant and/or its representatives was as a result of the appellant's electronic mail being "*spoofed*", creating an opportunity for a third party to change the appellant's bank account details on the invoice.

[10.2] The appellant acted negligently in that it failed to ensure that its electronic mail system was secure and could not be "*spoofed*".

[10.3] The respondent suffered damages in the amount of R159 353.76 as a result of the false representation.

[11] The appellant first and foremost denies that itself and/or any of its representatives made false representations to the respondent and pleads further in replication that the invoice received by the respondent was not received from the appellant and was also not sent by the appellant. The appellant denies further that the banking details on the invoice are its banking details, and avers further that the allegations contained in the respondent's special plea are insufficient to sustain a defence of estoppel.

[12] The appellant denies any representation as a result of negligence, but pleads in the alternative that if the respondent succeeds in proving that it suffered damages, such damages were caused by the respondent's own negligence in that it failed to ensure that the account into which the purchase price was paid was indeed that of the appellant. This alternative averment finds support in the allegation that all Toyota dealers, including the respondent, were notified by Toyota South Africa (Pty) Ltd of fraudulent activity regarding banking details which notification warned Toyota dealers of the alleged "*spoofing*" relied on by the respondent. The respondent failed to pay attention to the

warning, alternatively failed to take reasonable steps to avoid being the victim of the known fraudulent activity of "*spoofing*".

Evidence on behalf of the respondent

[13] The respondent had the duty to begin and called three witnesses, namely Mr André Olivier, Mrs Martie Aletta Steyn and Mr Malcolm Gregg Botha.

[14] Mr Olivier, being the dealer principal of the respondent, testified that:

[14.1] He is responsible for the administration and general management of the respondent's business.

[14.2] Mrs Steyn was the respondent's salesperson who conducted the negotiations and/or discussions with the appellant regarding the purchase of the vehicle.

[14.3] Mrs Steyn provided him with the invoice which she received from the plaintiff. He perused the invoice and authorised the invoice for payment, whereafter the invoice was given by Mrs Steyn to Mrs Marieke Smith to process the payment. The payment was authorised by Mrs Charlene Nel on the electronic banking system of the respondent after it was processed by Mrs Smith.

[14.4] He testified about the procedure followed during February 2018 by the respondent for the payment of invoices, namely "Die faktuur kom in. Jy kyk na die faktuur. Daar word bevestig ook dat alles op die faktuur kan mens nou sê wettiglik lyk. Ons het niksvermoedend onraad gemerk nie. Die faktuur het 'n 100 persent reg gelyk. Die faktuur is afgeteken en dan het die proses verder geloop.".

[14.5] The incorrect invoice was received from sales2@mbtoyota.co.za and payment was made in terms thereof into the incorrect account. On 15 February 2018, Mrs Steyn received a telephone call from Mr Maritz of the appellant, who informed her that the appellant has not received

payment. It was later established that the monies were paid into the incorrect account.

[14.6] During cross-examination, Mr Olivier testified that he was aware of the circular issued by Toyota South Africa to all Toyota dealerships during November 2017 in which dealers were cautioned about fraudulent activities regarding transactions whereby banking details on invoices were fraudulently changed. He further testified as follows regarding his knowledge of the said circular:

> "Ek het wel kennis gedra daarvan en dit is hoekom ons die goed met die nodige omsigtigheid hanteer het."

[14.7] Mrs Steyn informed him, when she provided him with the invoice for approval, and after he enquired from her whether the bank account details on the invoice were verified and confirmed by the appellant, that she spoke to Mr Maritz who confirmed that the bank account details were correct.

[14.8] He accepted that if the appellant's electronic mail was hacked, the appellant would not have been aware of the fact that the incorrect invoice was sent to the respondent on 7 February 2018.

[15] Mrs Steyn, the then sales assistant at the respondent, testified as follows:

[15.1] She contacted dealerships to enquire about the availability of a Toyota Etios vehicle. When she contacted Mr Maritz at the appellant, he indicated to her that the appellant has an Etios vehicle available and he requested her to provide him with the necessary particulars for purposes of issuing an invoice to the respondent for and in respect of the vehicle. She provided the required information to Mr Maritz *via* electronic mail, and also requested Mr Maritz to provide the respondent with the appellant's banking details.

[15.2] She received an invoice on 7 February 2018 from sales2@mbtoyota.co.za and took the invoice to Mr Olivier, who signed it off, whereafter she took the documents to Mrs Smith to process the payment. It was only established that payment was made into the incorrect account when Mr Maritz requested her later in February 2018 to provide him with proof of payment.

[15.3] During cross-examination, Mrs Steyn, conceded that in hindsight, she first should have contacted Mr Maritz telephonically to confirm the bank account details on the invoice received by her. In her own words she testified "As ek terugdink dan sou ek hulle eers gebel het om te bevestig die bankbesonderhede." However, at the time of the transaction, she did not do so as she did not have any reason to doubt the correctness of the bank account details on the invoice. She further testified that she could have verified the bank account details telephonically, which she did not, because it was not the procedure at the time, and therefore she accepted that it was a mistake on her side not to verify the bank account details telephonically.

[15.4] She did not inform Mr Olivier that she had confirmed the correctness of the bank account details on the invoice. However, when confronted with Mr Olivier's version that she informed him that she did verify the correctness of the bank account details, she testified that she was uncertain and cannot remember what Mr Olivier said, but according to them (Mr Olivier and herself), they accepted the banking details on the invoice to be correct.

[15.5] Mr Maritz did not intentionally provide her with the incorrect invoice and he did not have the intention to defraud the respondent. She was also not aware of the circular distributed by Toyota South Africa.

[16] The evidence of Mr Botha, who testified as an expert, has not been disputed, and for this reason his evidence and conclusions in his report does not have to be evaluated for purposes of this appeal. However, Mr Botha expressed the view that a third party had access to the lock-in credentials for the sales2@mbtoyota.co.za electronic mail account and could have, through such access, changed the content of the invoice as well as the payment confirmation which was sent by Mrs Steyn to Maritz.

Evidence on behalf of the appellant

[17] The appellant called two witnesses, namely Mr Gabriel Willem Andreas Maritz and Mr Petri Esterhuizen.

[18] Mr Maritz, being employed by the appellant as sales manager since 2014 testified that:

[18.1] Mr Johan Griesel from the respondent contacted him about the availability of an Etios vehicle. Thereafter, Mrs Steyn dealt with the matter on behalf of the respondent. He indicated to Mrs Steyn that the appellant has an Etios available and that she must provide him with the invoice details in order for him to make out an invoice to the respondent for the purchasing of the vehicle from the appellant.

[18.2] He made use of the electronic mail address sales2@mbtoyota.co.za (previously used by Mr Johan du Toit).

[18.3] After he received an email from Mrs Steyn on 6 February 2018 with the information as requested, he gave instructions to the administrative clerk of the appellant, Mrs Antoinette Oosthuizen, to generate an invoice for and in respect of the transaction. He received the original invoice and placed it in the vehicle for the driver who would collect the vehicle to take the original invoice to Bultfontein.

[18.4] Mrs Steyn requested him telephonically to send a copy of the invoice to her, whereafter he approached Mrs Oosthuizen to obtain a copy of the invoice. He took the copy of the invoice and scanned it to his computer from a Cannon scanner situated opposite his office. He then sent the scanned copy of the invoice *via* electronic mail to Mrs Steyn on 7 February 2018. This electronic mail contained a message to Mrs Steyn, being "*Faktuur op Etios Uiteindelik!*".

[18.5] He did not attach the incorrect invoice with the incorrect account details to his electronic mail to Mrs Steyn on 7 February 2017. The scanned copy of the invoice contained the correct banking details of the appellant.

[18.6] He received a proof of payment from Mrs Steyn, which proof of payment recorded the correct bank account details of the appellant. However, on 9 February 2018, the dealer principal of the appellant, Mr Stefan Janse van Vuuren, informed him that the payment does not reflect in the appellant's bank account. This sparked telephonic and electronic correspondence between Mrs Steyn and himself, and on 15 February 2018, it was established that the invoice which was received by Mrs Steyn was changed and payment had been made into an incorrect account. Neither Mrs Steyn nor any employee of the respondent telephonically requested him to confirm the bank account details in the invoice which was received by the respondent on 7 February 2018. Had they telephonically requested him to verify the bank account details, he would have realised that the invoice received by Mrs Steyn contains the incorrect account number and that the invoice has been changed. This would have prevented the respondent from making the payment into the incorrect bank account.

[18.7] He was aware of the circular issued by Toyota South Africa during November 2017, and as a result thereof, it was common practice to

telephonically verify the banking details before any payment is made. Since his employment at the appellant, he is unaware of any similar incident where electronic mails which clients and/or other dealerships received from sales2@mbtoyota.co.za have been hacked and invoices or other documents sent from this electronic mail address were changed.

[18.8] He did not know the password to the sales2@mbtoyota.co.za electronic mail account, and he is not acquainted with computers. Whenever he required assistance, Mr Petri Esterhuizen assisted him. He further testified that he did not give any person the authority to change the bank account details on the invoice or to work on his computer.

[18.9] When he was appointed to replace Mr Johan du Toit as sales manager, the computer previously used by Mr du Toit was given to him, and all documents and records which were generated by Mr du Toit was deleted from the computer.

[19] Mr Esterhuizen testified as follows:

[19.1] He was previously employed by the appellant as a sales person, during which he was also responsible for the management of the electronic mail accounts and systems of the appellant. He is employed at Hashtag, an IT business which was established by Mr Janse van Vuuren, since 2017.

[19.2] Afrihost, being the host of the mbtoyota domain used by the appellant, provides the server for and in respect of the mbtoyota domain. Hashtag administers the mbtoyota domain on behalf of the appellant.

[19.3] He was involved in the setup of the electronic mails for the appellant, including sales2@mbtoyota.co.za. Hashtag has access, with the necessary passwords obtained from Afrihost, to the appellant's electronic mail domain registered on the Afrihost server.

[19.4] He agrees with the Mr Botha's conclusion that a third party had access to the login credentials for the sales2@mbtoyota.co.za electronic mail account. However, the incident is the first incident of such kind at the appellant since 2013.

[19.5] The passwords to the electronic mail accounts and Afrihost's server were used by him and the other two employees of Hashtag to manage the mbtoyota domain. They had to have access to the passwords to perform their duties. He and the other two employees could, by using the passwords to the electronic mail account, send electronic mails from such account. However, he trusted the other employees, and according to him, the electronic mail system used by the appellant was safe and secured. He also testified that the password for sales2@mbtoyota.co.za has not been changed for the past five years and that previous employees, prior to the incident, know the password.

Judgment of the court *a quo*

[20] In its judgment dated 17 March 2021, the court *a quo* found on a balance of probabilities that the respondent is successful with its defence of estoppel and consequently dismissed the appellant's claim with costs, including preparation, traveling and counsel's costs at an increased scale.

[21] The court *a quo's* judgment in favour of the respondent referred to *supra* is based the following findings:

[21.1] No representation regarding the correctness of the banking details reflected on the incorrect invoice was made by the appellant to the respondent as Mrs Steyn, on behalf of the respondent, testified that she did not phone Mr Maritz to confirm the banking details.

[21.2] A third party had access to the sales2@mbtoyota.co.za electronic mail address from which the electronic mail with the incorrect invoice was received by Mrs Steyn on 7 February 2018. This constitutes a representation by conduct.

[21.3] The respondent believed the information on the incorrect invoice as being correct, acted thereon by making payment and will suffer prejudice if the appellant is not estoppel.

[21.4] The appellant had knowledge of cybercrime experienced by dealerships as a letter in that regard was sent to all dealerships.

[21.5] The appellant conceded that:

[21.5.1] There is no way the respondent could have known that the incorrect invoice did not come from Mr Maritz himself and was incorrect.

[21.5.2] The only way that the sales2@mbtoyota.co.za electronic mail address could have been used was if the person using it had the username and password, and consequently, the appellant conceded further that only a person with knowledge of the password could have attached the incorrect invoice. Mr Esterhuizen also conceded during cross-examination that a third party had access to the login credentials of the sales2@mbtoyota.co.za electronic mail account.

[21.6] The court *a quo* further found:

> "If the Plaintiff had only taken the necessary care with the password used to gain entrance to the domain they have prevented their loss. The Plaintiff was negligent and failed to exercise the safety measures a reasonable person, after being warned of Cybercrime, would have taken. Failure to do so was at their own peril."

[21.7] Central to the dismissal of the appellant's claim, is the court *a quo's* finding that the incorrect invoice received by the respondent from Mr Maritz's electronic mail account constituted a misrepresentation by the appellant, which was the result of the appellant's negligence and failure to exercise the safety measures a reasonable person would have taken after being warned of cybercrime.

Grounds of appeal

[22] The appellant's appeal against the judgment and order of the court *a quo* is based on the various grounds in respect of the findings of fact and rulings of law set out in detail in the appellant's notice of appeal. However, in his heads of argument, Mr Pienaar, on behalf of the appellant, submitted that the appeal in essence turns on the following main issues (I am in agreement with this submission):

[22.1] Whether the fact that the incorrect invoice was received on 7 February 2018 by the respondent from the sales2@mbtoyota.co.za electronic mail address, being the electronic mail address used by the appellant, constituted a representation by conduct by the appellant to the respondent that the incorrect account depicted on the incorrect invoice is the appellant's correct bank account.

[22.2] Whether the respondent had to ensure that payment is made into the appellant's correct bank account and had to, before making payment to the appellant, confirm the correctness of the bank account details depicted on the invoice which the respondent received by electronic mail.

[22.3] Whether, should it be found that the incorrect invoice received from sales2@mbtoyota.co.za constituted a representation by conduct by the appellant, such representation was the proximate cause of the payment which was made by the respondent into the incorrect bank account.

Estoppel

[23] The essence of the doctrine of estoppel by representation is that a person (the representor) is precluded or estopped from denying the truth of a representation previously made to another person (the representee) if the representee, believing in the truth of the representation, acted on the representations to the representee's detriment.[1]

[24] A party, in this instance the respondent, wishing to rely on estoppel, has the onus to plead and prove the essentials for estoppel,[2] namely:

[24.1] There was a representation by words or conduct of a certain factual position,[3] namely that the incorrect invoice contained the appellant's correct banking details;

[24.2] The representee (the respondent in this instance) acted to its detriment on the correctness of the facts as represented. There must be a causal connection between the representation and the act;[4]

---

[1] Amler's Preceedings of Pleadings, Ninth Edition, Harms at page 187.

[2] Absa Bank Limited v IW Blumberg and Wilkinson 1997 (3) SA 669 (SCA) at 677G.

[3] Universal Stores Ltd v OK Bazaars (1929) Ltd 1973 (4) SA 747(A) at 761.

[4] Stellenbosch Farmers Winery Ltd v Vlachos t/a Liquor Den 2001 (3) SA 597 (SCA) at paras 17-20; Van Deventer v Ivory Sun Trading 77 (Pty) Ltd 2015 (3) SA 532 (SCA) at par 44 and Absa Bank Ltd v De Klerk 1999 (1) SA 861 (W).

[24.3] The representation was made negligently;[5] and

[24.4] The representor could bind the appellant by means of the representation.[6]

[25] The respondent relied on a representation by conduct, caused by the appellant's negligence, and not on a representation by words. The latter finds support, firstly in Mrs Steyn's confirmation during evidence that Mr Maritz never personally confirmed the correctness of the bank account details on the incorrect invoice, and secondly, it is not the respondent's case that Mr Maritz or the appellant intentionally provided the incorrect invoice to the respondent. The respondent relied on a representation.

[26] To succeed with a defence of negligent representation by conduct, the respondent also had to prove that:

[26.1] the appellant was negligent in that it failed to ensure that its electronic mail system was secured;

[26.2] the appellant should have reasonably expected that its conduct could result in its electronic mails to be intercepted and changed and could mislead the respondent; and

[26.3] such negligence effectively contributed to the making of the representation, as alleged, and caused the respondent to act to its detriment.[7]

[27] The respondent had to establish that:

---

5 Info Plus v Scheelke 1998 (3) SA 184 (SCA).

6 NBS Bank Ltd v Cape Produce Co (Pty) Ltd 2002 (1) SA 396 (SCA).

7 Info Plus v Scheelke *supra* at 194F; Leeuw v First National Bank 2010 (3) SA 410 (SCA) at paras 11 and 16 and Concor Holdings (Pty) Ltd t/a Concor Technicrete v Potgieter 2004 (6) 491 (SCA) at 495B.

[27.1] the appellant's negligence was the proximate cause of the respondent's action, namely the payment being made by the respondent into the incorrect bank account;[8]

[27.2] its reliance on the representation was reasonable, namely, that it did not have information which put it upon enquiry; and

[27.3] it exercised reasonable care and diligence to learn the truth.[9]

[28] Even if the appellant negligently failed to secure its electronic mail domain, the respondent failed to prove that the negligence was the proximate cause to its action, and the conspectus of the evidence showed that the respondent's reliance on the representation was not reasonable. The following evidence should be emphasised:

[28.1] It is common cause that the respondent did not take any steps to verify or confirm the bank account details as contained in the incorrect invoice before making payment to the appellant.

[28.2] Mr Olivier admitted that he had knowledge of the circular of Toyota South Africa, wherein the dealers attention was drawn to similar cybercrime activities. Despite this knowledge, no attempts were made by him or the respondent to verify the bank account details on the incorrect invoice. However, Mr Olivier testified that the said circular was the reason why the respondent handled these things, being payments, with the necessary caution.

[28.3] Mr Olivier furthermore testified that, based on the indication by Mrs Steyn that she confirmed the bank account details depicted on the

---

[8] Grosvenor Motors (Potchefstroom) Ltd v Douglas 1959 (3) SA 420 (A) at 425-426 and Stellenbosch Farmers' Winery Ltd v Vlachos t/a The Liquor Den *supra* at paras 17-19.

[9] The Law of Estoppel in South Africa, JC Sonnekus, Third Edition, page 122, par 5.1 and page 211, par 6.

incorrect invoice with the appellant, he approved the invoice for payment.

[28.4] Mr Olivier did not approve the invoice for payment based on any representation made by the appellant, but based on the representation made by Mrs Steyn, namely that she confirmed the banking details and that such details were correct. This version of Mr Olivier, which was accepted by the court *a quo*, did not rely on a representation by the appellant, but on the representation made to him by Mrs Steyn referred to *supra*. This representation by Mrs Steyn induced the respondent to act to its detriment.

[28.5] Despite some contradictions between the evidence of Mrs Steyn and Mr Olivier as to the verification of the banking details by Mrs Steyn and whether she informed Mr Olivier that the banking details on the incorrect invoice have been confirmed by the appellant, it is evident from the respondent's version, especially the evidence of Mr Olivier, being the person who was responsible to approve the invoice before payment would be made, that the alleged negligent representation by the appellant did not induce the respondent to act at its detriment.

[29] I am in agreement with Mr Pienaar's submissions that:

[29.1] If the respondent took the necessary steps, in fact a simple telephone call would have sufficed, to confirm the bank account details stated on the incorrect invoice before payment was made, it would have been informed by the appellant that it is indeed the incorrect bank account details. This would have resulted that payment into such incorrect account would not have been made. This process, according to Mr Olivier, was in fact the process followed by the respondent at the time he approved the invoice for payment.

[29.2] The respondent's own conduct caused it to pay the monies into the incorrect bank account. The respondent acted at its own peril and cannot rely on the alleged negligent representation made by the appellant.

[29.3] The court *a quo* erred by ignoring the respondent's obligation to have acted reasonably, particularly in circumstances where it was aware of similar cybercrime activities.

[29.4] The court *a quo* failed to apply the principles regarding the doctrine of estoppel correctly to the facts, namely, it erred in:

[29.4.1] not finding that the payment by the respondent was not the cause or result of any representation by the appellant, but in fact the result of a misrepresentation by the respondent's own employee;

[29.4.2] not finding that any negligence on the part of the appellant was not the proximate cause of the payment which was made into the incorrect bank account.

[30] For the reasons set out *supra*, the respondent should not have succeeded with the defence of estoppel in the court *a quo*.

Negligence

[31] Mr Pienaar referred to *Kruger v Coetzee*[10] wherein the test for negligence has been authoritatively stated as follows:

> "For the purposes of liability *culpa* arises if –
>
> (a) a *diligence paterfamilias* in the position of the defendant –
>
> (i) would foresee the reasonable possibility of his conduct injuring another in his person or property and causing him patrimonial loss; and

[10] 1966 (2) SA 428 (A) at 430.

(ii) would take reasonable steps to guard against such occurrence; and

(b) the defendant failed to take such steps."

[32] The respondent had the onus to prove on a preponderance of probabilities that the appellant was negligent.[11]

[33] In terms of its conditional counterclaim, the respondent claims that, because of the appellant's alleged negligent or fraudulent misrepresentation, the respondent has suffered damages in that it paid the amount of R159 353.76 into the incorrect bank account.

[34] It is not in dispute that Mr Maritz and the appellant were not aware that a third party had access to Mr Maritz's electronic mail account. However, the court *a quo's* finding in respect of negligence is based on the evidence of Mr Esterhuizen, namely:

[34.1] The evidence of Mr Esterhuizen cannot be seen as unbiased and objective, and he was not an honest witness.

[34.2] Hashtag had the necessary access, with the necessary passwords obtained from Afrihost, to the electronic mail domain registered on Afrihost.

[34.3] Mr Esterhuizen and the other two employees of Hashtag, who had access to the password of the appellant's electronic mail account, could have send electronic mails form the account. This, regardless Mr Esterhuizen's evidence that he not only trusted the other two employees of Hashtag, but that the electronic mail system used by the appellant was safe and secured.

---

[11] Ntsala v Mutual & Federal Insurance Co Ltd 1996 (2) SA 184 (T) at 190.

[34.4] Mr Esterhuizen agreed with the conclusion of Mr Botha, namely that a third party had access to the login credentials for sales2@mbtoyota.co.xa electronic mail account, and this unknown third party could have intercepted and changed the electronic mails. Neither Mr Botha nor Mr Esterhuizen could give an opinion on the manner in which the third party obtained access to the login credentials of the above electronic mail account.

[35] The appellant pleaded in its plea to the respondent's conditional counterclaim that, should the respondent succeed in proving that it suffered damages, that such damages were caused by the respondent's own negligence in that it failed to ensure that the bank account into which the purchase price was paid was indeed the bank account of the appellant.

[36] Mr Pienaar, on behalf of the respondent, submitted that the respondent failed to make out a case that the reasonable person, in the same position as Mr Maritz and/or the appellant, would have foreseen and prevented the fraudulent use of sales2@mbtoyota.co.za or the fraudulent change of its invoice, and could have prevented the fraudulent electronic mail to Mrs Steyn on 7 February 2018. Mr Pienaar further submitted that the respondent has not given any evidence on what should have been done by the appellant to secure its electronic mail account and to show that the appellant's conduct did not meet the requirements of the reasonable person test.

[37] Mr Berry, on behalf of the respondent, submitted that if the appellant took reasonable steps to ensure the passwords of its electronic mail accounts were regularly changed, the spoofing would not have occurred. Mr Berry relies specifically on the evidence of Mr Esterhuizen, namely that the relevant password has not been changed for five years and various previous employees have knowledge of the password.

[38] I am in agreement with Mr Pienaar's submissions *supra*, more specifically that the respondent has failed to make out a case that the reasonable person, in the same position as Mr Maritz and/or the appellant, would have foreseen and prevented the fraudulent use of sales2@mbtoyota.co.za or the fraudulent change of its invoice, and could have prevented the fraudulent electronic mail to Mrs Steyn on 7 February 2018, and furthermore that the respondent has not given any evidence on what should have been done by the appellant to secure its electronic mail account and to show that the appellant's conduct did not meet the requirements of the reasonable person test. These submissions are also supported by the evidence of Mr Esterhuizen, namely that he trusted the other two employees of Hashtag and that the appellant's electronic mail system was safe and secured.

[39] The uncontested evidence on behalf of the respondent, namely that the respondent failed to verify the appellants bank account details before the payment was made, resulted in the incorrect payment being made. This finding is supported by the evidence of Mr Olivier, namely, that he was not only aware of the circular issued by Toyota South Africa referred to *supra*, he also acted with the necessary caution, and only approved the invoice for payment after he received confirmation from Mrs Steyn, that the appellant's bank account details were verified as correct.

[40] Mr Pienaar referred to the principles applied in cases where cheques have been intercepted as enunciated in *Eriksen Motors (Welkom) Ltd v Protea Motors, Warrenton,*[12] namely:

> "… when a debtor tenders payment by cheque, and the creditor accepts it, the payment remains conditional and is only finalised once the cheque is honoured. Any risk of fraudulent misappropriation should be borne by the debtor since it is the debtor's duty to seek out its creditor. But where the creditor stipulates the mode of payment

[12] 1973 (3) SA 685 (A) at 693.

> and the debtor complies with it, any inherent risk in the stipulated method is for the creditor's account."

[41] Mr Pienaar submitted that the principles set out in *Eriksen Motors (Welkom)* are equally applicable to the payment made by the respondent into the incorrect account. I agree with Mr Pienaar's submission in this respect, especially considering the following:

[41.1] The respondent's primary obligation in terms of the contract was to make payment of the purchase price, and this obligation could only have been discharged by payment of the purchase price to the appellant.

[41.2] To discharge the respondent's obligation, Mrs Steyn requested the appellant's bank account details from Mr Maritz, and this was undoubtedly done to effect payment by means of electronic transfer of the purchase price into the appellant's bank account. The evidence shows that the method of payment was not specifically stipulated by the appellant.

[41.3] Because payment was not made into the appellant's bank account, the respondent has not complied with its obligations in terms of the contract, and consequently the respondent is still liable for payment of the purchase price.

[42] Mr Pienaar also referred to various High Court judgments dealing with the question as to who should bear the loss where payment is electronically made to a creditor, which is fraudulently intercepted by a third party.

[43] In *Galactic Auto Pty Ltd v Andre Venter*[13] ("*Galactic Auto*") the plaintiff sold a motor vehicle to the defendant, and later instituted action against the defendant for payment of the purchase price, which the plaintiff alleged was

[13] [2019] ZALMPPHC 27.

not paid. The defendant raised a defence of estoppel and in the alternative instituted a counterclaim based on alleged misrepresentation by the plaintiff in that the plaintiff, through its representatives, made a misrepresentation to the defendant which was false and caused the defendant to believe that the purchase price was paid to their bank account and received by them when it was not the case. From the common cause facts, it was established that the plaintiff's electronic mails had been intercepted by a hacker who also changed the bank account details provided to the defendant, and upon receipt of the banking details, made payment into the fraudulent bank account.

[44] The court held in *Galactic Auto* that "if the defendant had only verified the banking details he would have prevented the loss. His failure to do so was at his own peril".[14] The court found in favour of the plaintiff (the creditor) and relied on the principles summarised in *Mannesmann Demag (Pty) Ltd v Romatex*[15] where payment has been intercepted and misappropriated by a thief, namely:[16]

> "When a debtor tenders payment by cheque, and the creditor accepts it, the payment remains conditional and is only finalised once the cheque is honoured. (Eriksen Motors (Welkom) Ltd v Protea Motors, Warrenton, and Another 1973 (3) SA 685 (A) at 693; Christie The Law of Contract in South Africa at 413.) Until that happens a real danger exists that the cheque may be misappropriated or mislaid and that someone other than the payee may, by fraudulent means, convert it into cash or credit, for instance, by forging an endorsement or by impersonating the true payee. That risk is the debtor's since it is the debtor's duty to seek out his creditor." (emphasis added)

[45] In *Fourie v Van der Spuy & De Jongh Inc*,[17] ("*Fourie*") cybercrime was also at the centre, which resulted in an attorney making payment of monies which had to be paid to his client, in a wrong account. The court held as follows:

---

14 At par 49.
15 1988 (40 SA 383 (D) at 389 F - 390 D.
16 Galactic Auto *supra* at par 51.
17 2020 (1) SA 560 (GP).

> "[23] It is common cause that the second respondent has failed to pay over the balance due to the applicant. In this regard the second respondent has failed to discharge her obligation to the applicant and that should be the end of the matter.
>
> [24] It cannot be disputed by the respondents that had the second respondent confirmed or verified the new bank details with the applicant, the fraud simply would not have occurred. It is abundantly clear from the facts that no verification process was followed and that the firm would have to carry the loss, not the applicant." (emphasis added)

[46] In *Hawarden v Edward Nathan Sonnenbergs*[18] ("*Hawarden*") the plaintiff was the purchaser of immovable property and the defendant the appointed conveyancer in the sale transaction. The plaintiff made an electronic payment of the amount of R5 500 000.00 into what she believed was the bank account of the defendant. The details of the bank account was obtained by the plaintiff from an electronic mail received from a secretary in the employ of the defendant. Unknown to the plaintiff, her electronic mail account was hacked, and the account details intercepted and altered by an unknown fraudster, resulting in the payment being made into the incorrect account. The plaintiff, in terms of a delictual claim, alleged that the defendant had the duty to exercise sufficient care in the conduct of the transaction, to warn the plaintiff of the dangers of business electronic mail compromise and to communicate its bank details in a safe manner.

[47] Based on the evidence, the court concluded in *Hawarden* that the defendant had a general duty of care to the plaintiff, as purchaser of property, and because it knew and understood the risk of business electronic mail compromise, it had to take the necessary precautions to ensure the accuracy and safety of its transmissions. In finding in favour of the plaintiff, the court held that, viewed objectively, the plaintiff cannot be faulted for placing her trust in the defendant who she knew was a very large and reputable law firm. On

---

[18] 2023 JDR 0079 (GJ).

her version, which the court accepted, the plaintiff did not think she needed to seek advice as she was dealing with a law firm whose reputation went before it.[19]

[48] I agree with Mr Pienaar's submission that *Hawarden* is distinguishable from the facts in in this matter. Not only was the respondent in the present matter aware of the possibility of cybercrime when payment was made into the incorrect bank account of the appellant, but on Mr Olivier's own version, he approved payment to be made after he confirmed with Mrs Steyn that the bank account details on the incorrect bank invoice were verified with the appellant.

[49] In *André Kock en Seun Vrystaat (Pty) Ltd v Snyman N.O.*[20] ("*André Kock*") the applicant claimed payment of the purchase price from the respondents for livestock sold and delivered to the respondents. The applicant sent its invoice by electronic mail to the respondents. The electronic mail was intercepted by an unauthorised third party. This invoice was reconfigured by replacing the applicant's banking details with the hacker's details, whereafter it was sent to the respondents as if it emanated from the applicant's electronic mail account. The respondent then paid the purchase price due to the applicant into the hacker's bank account. It was the applicant's case that a forensic investigation conducted by a forensic expert determined that the respondents' electronic mail account was compromised. The respondents disputed liability on the ground that there was no conclusive evidence that the fraud emanated from its electronic mail account.

[50] In conclusion, and in finding in favour of the applicant, the court held in *André Kock* that the respondent's liability to pay the applicant would have only been discharged by payment to the applicant; that where a payment is effected by way of an electronic funds transfer, the responsibility of verifying the creditor's banking details before making the payment lies squarely on the debtor; and

---

19 At paras 117 – 127.

20 2022 JDR 1792 (FB).

that the respondent had merely assumed that the electronic mail received was from the applicant and then went on to make a payment into the banking account provided in the said electronic mail without having taken any steps to verify such information.[21]

[51] In *Gerber v PSG Wealth Financial Planning (Pty) Ltd*[22] ("*Gerber*") the plaintiff held investments with the defendant in the form of shares and cash. As a result of a fraudulent electronic mail request, which purported to be emanating from the plaintiff, the defendant paid from the plaintiff's funds into a fraudulent account. The plaintiff claimed payment of the monies based on the breach of contract by the defendant. The defendant firstly relied on a tacit term of the contract, namely that it would not be liable for loss under circumstances where the plaintiff's computer system was hacked due to the plaintiff's negligence and secondly raised estoppel, based thereon that the plaintiff's system was hacked and thus the plaintiff, through his negligence, allowed a misrepresentation to be made to the defendant in respect of the incorrect account details.

[52] The court held in *Gerber* that the defendant did not establish the contended tacit term[23] nor was there any evidence that the plaintiff did anything or failed to do anything to protect his system from hacking.[24] The court further held that:

> "[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

---

21 At paras 8 and 9.

22 [2023] JOL 58352 (GJ). See also Lester Connock Commencement Fund v Brough Capital (Pty) Ltd [2023] ZAGPJHC 1329.

23 At paras 55 – 70.

24 At pa 71.

> 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." (emphasis added)

[53] In *Hartog v Daly and Others*[25] ("*Hartog*"), the appellant, a practicing attorney, had to pay monies which were available from a sale transaction to the third respondent (referred to *infra* as "Patrick"). The electronic mail, providing the appellant with the banking details of Patrick was spoofed by a fraudster, resulting in the payment being made by the appellant into a fraudulent account. It was the appellant's case that the respondents are to be held liable for the loss as the mandate given to the appellant had a tacit term to the effect that the respondents will exercise the utmost caution when instructing the appellant to make payment, and that they would do all that was reasonably possible to ensure the integrity of the electronic mails addressed to the appellant and keep and maintain their data security.

[54] The full court in *Hartog* held that the appellant did not prove the existence of a tacit term referred to *supra*.[26] Consequently the court held that there is no need to make any finding regarding where the compromise occurred which enabled the fraudster to send an electronic mail to the appellant and which resulted in him making payment into an account other than the one to which payment should have been made, because the appellant breached the mandate agreement by not making payment of the proceeds of the sale into the bank account of Patrick and remains responsible for such payment.[27]

---

25 2023 JDR 0189 (GJ).
26 At paras 41 – 73.
27 At paras 80 – 81.

[55] Mr Berry, on behalf of the respondent, submitted that the judgments referred to *supra* are distinguishable from the facts of this matter. His submission finds support in the contention that the appellant and the respondent are both motor dealerships and they do not stand in any judiciary relationship towards one another – they dealt with one another at arm's length. Mr Berry further submitted that the judgments referred to *supra* are distinguishable based thereon that estoppel was not raised in these judgments as a defence and secondly a counterclaim based on negligent misrepresentation has not been instituted as with this matter. I disagree with these submissions, especially considering that:

[55.1] The defendant in *Galactic Auto* raised a defence of estoppel and in the alternative instituted a counterclaim based on alleged misrepresentation, and in *Gerber* the defendant relied on a tacit term of the contract, namely that it would not be liable for loss under circumstances where the plaintiff's computer system was hacked due to the plaintiff's negligence, and secondly it raised estoppel, based thereon that the plaintiff's system was hacked and thus the plaintiff, through his negligence, allowed a misrepresentation to be made to the defendant in respect of the incorrect account details.

[55.2] No judiciary relationship existed in the matters of *Galactic Auto* and *André Kock*.

[56] Mr Berry furthermore submitted that any obligation on a buyer, the respondent in this instance, to first verify an account number provided to effect payment, especially if the account number was received from the sellers own electronic mail address, takes the obligation/duty of the respondent too far. Mr Berry further submitted that the seller, the appellant herein, has a duty to ensure the security measures are in place, and that it failed to do so, which ultimately led to the loss suffered by the appellant, especially where the appellant was aware of cybercrime. I disagree with these submissions, firstly, on the

respondent's own version, Mr Olivier approved the payment after he received confirmation that the bank account was verified, secondly, no evidence was presented by the respondent showing that no security measures were in place to protect the appellant's electronic mail account and/or what the appellant should have done to secure the electronic mail account.

[57] I agree with Mr Pienaar's submission that the principles and findings referred to *supra* in *Galactic Auto*, *Fourie*, *André Kock*, *Gerber* and *Hartog* are correct and applicable to the facts in this matter. I consequently do not align myself with Mr Berry's submissions referred to *supra*.

Conclusion

[58] Central to the appellant's case is that a person who sends an electronic mail is generally unaware of any fraudulent access to his or her electronic mail account and is unaware that the electronic mail which is received by the recipient has been intercepted, hacked and changed. The golden threat in the judgments referred to *supra* places an obligation on the purchaser to ensure that the bank account details contained in the invoice is in fact correct/verified and that payment is made to the seller and not to an unknown third party. Failure to do so, and where payment is made into an incorrect bank account, such incorrect payment does not extinguish the purchaser's obligation and liability to pay the debt.

[59] The respondent did not discharge its onus to prove the defence of estoppel or the cause of action underlying its delictual claim in terms of the conditional counterclaim.

[60] On the respondent's own version, it was aware of the existence of cybercrime and therefore acted at its own peril when it made payment without verifying the correctness of the bank account details. Had the respondent made a simple telephone call to Mr Maritz, it would have established that the invoice

received was fraudulently changed and would not have made payment into the incorrect bank account. This was conceded by Mrs Steyn.

[61] The evidence established clearly that the interception of the electronic mail at the appellant's electronic mail domain was not the proximate cause of the payment into the incorrect account. The proximate cause of the payment into the incorrect bank account was in fact the approval of the payment by Mr Olivier after having been satisfied that the bank account details have been verified. The bank account details were in fact never verified, and consequently the respondent acted at its own peril when the payment was made into the incorrect bank account.

[62] I am in agreement with the appellant's submissions that the court *a quo* erred in not dismissing the respondent's plea of estoppel and its conditional counter claim and not granting judgment in favour of the appellant.

[63] Accordingly I make the following order:

1. The appeal is upheld with costs;

2. The order granted by the Court on 17 March 2021 is set aside and replaced with the following:

"1. The defendant's counterclaim is dismissed with costs.

2. Judgment is granted against the defendant in favour of the plaintiff as follows:

2.1 Payment in the amount of R159 353.76;

2.2 Payment of interest on R159 353.76, calculated at a rate of 10.5% per annum from 8 February 2018 to date of payment;

2.3 Costs of suit, including preparation, traveling and counsel's costs at an increased scale."

_____

J.J. BUYS, AJ

I concur

_____

P. J. LOUBSER, J

I concur

_____

S.T. MGUDLWA, AJ

On behalf of the Appellant:	Adv C.D. Pienaar Phatshoane Henney Attorneys Bloemfontein
On behalf of the Respondent:	Adv A.P. Berry Badenhorst Attorneys Bloemfontein