REPUBLIC OF SOUTH AFRICA

IN THE HIGH COURT OF SOUTH AFRICA
GAUTENG DIVISION, JOHANNEBURG

CASE NO: 13849/2020

(1) REPORTABLE: YES
(2) OF INTEREST TO OTHER JUDGES: YES
(3) REVISED: YES

[16 January 2023] **……..**
SIGNATURE

In the matter between:

JUDITH HAWARDEN Plaintiff

and

EDWARD NATHAN SONNENBERGS INC Defendant

J U D G M E N T

Summary: Law of delict- whether the defendant as the conveyancer is liable in delict for pure economic loss - wrongfulness –plaintiff vulnerable to risk- delictual liability established.

The judgment deals with the vexed question of whether or not to impose liability for pure economic loss sustained by the plaintiff who fell victim to cyber- crime through business email compromise ('BEC') as a result of the defendant's negligent omission to forewarn the plaintiff of the known risks of BEC and to take the necessary safety

precautions that are designed to safeguard against the risk of harm occasioned by BEC from eventuating.

The plaintiff purchased an immovable property from a third party seller who appointed the defendant, ENS attorneys, as the conveyancer in the sale transaction. The plaintiff paid the deposit required under the sale agreement and thereafter chose to pay the balance of the purchase price of R5.5 million by way of electronic transfer of funds directly into the defendant's trust account ('the ENS account') for the benefit of the seller pending registration of transfer.

The plaintiff made an electronic payment of the amount of R5.5 million into what she believed was the ENS account, details of which had been emailed to her by a conveyancing secretary in the employ of the defendant. The ENS account details were set out in a pdf attachment under cover of an email. Unbeknown to the plaintiff, her email account was hacked and the email containing the ENS account details was intercepted by an unknown fraudster and altered to reflect the fraudster's bank account details, resulting in the funds electronically transferred by the plaintiff being deposited in the fraudster's bank account as opposed to the ENS account.

Notwithstanding the discovery of the fraud, the defendant called upon the plaintiff to make payment of the balance of the purchase price, which had discernibly not been received by the former as required under the sale transaction. The parties were unable to resolve the impasse that followed, resulting in the plaintiff instituting action against the defendant for the loss of R5.5 million sustained by her as a result of the cyber fraud.

The evidence at trial established that the defendant was aware of the risks of BEC prior to the fraudulent incident and that it had failed to warn the plaintiff of the known risks of email and pdf manipulation or of precautions that could be taken against BEC prior to the plaintiff effecting the electronic payment. It was also not in contention that BEC attacks are rife, especially in the conveyancing industry. Further, the defendant had control over the way in which it conveyed its bank account details to the plaintiff - in an unprotected pdf attachment to an email it transmitted to the plaintiff – whilst technically safe measures, amongst others, multi-channel verification (in-person or telephonic confirmation of bank details) were available to be employed by it to avert cyber fraud.

Held that, a duty of care exists between a purchaser in a conveyancing transaction and the conveyancing attorneys handling the transaction to prevent harm resulting from the conveyancer's failure to warn the depositor of the dangers of cyber hacking and spoofing of emails or of the fact that pdf attachments to emails containing sensitive information such as bank account details are not invulnerable to BEC.

Held, further, that as an experienced conveyancer, the defendant understood the risks inherent in conveyancing transactions by virtue of its own prior knowledge of the dangers of BEC. The risk of BEC was thus foreseeable and the defendant was under a duty to guard against the harm eventuating. Its omission to do so was negligent in the circumstances.

Held, further, that the defendant was the proximate cause of the plaintiff's loss in that it provided its own bank account details and was responsible for their accuracy and for the safety of their transmission. In failing to safeguard the safety of their transmission, the defendant acted wrongfully.

Held, further, that as regards the element of wrongfulness, the plaintiff's loss in a case of this nature is both quantifiable and determinate and the risk of indeterminate liability as a policy consideration that militates against the recognition of liability for pure economic loss is thus averted.

Held, further, that factual causation was established in that but for the negligent transmission by the defendant of its bank account details including its failure to inform the plaintiff, as depositor, of the dangers of BEC, the plaintiff would not have suffered the loss. Legal causation was likewise established as the negligent conduct of the defendant was linked sufficiently closely to the loss suffered by the plaintiff for legal liability to ensue, given that the loss was reasonably foreseeable under the circumstances.

Order: The plaintiff's claim was upheld with costs on the scale as between an attorney and his client including the costs occasioned by the employment of two counsel.

MUDAU, J:

[1] The current action proceedings were launched during June 2020. The plaintiff,

Ms Judith Hawarden (“Ms Hawarden”) issued summons against the defendant, Edward Nathan Sonnenbergs Incorporated (“ENS”), a firm of attorneys which practices as attorneys and conveyancers, for damages in the sum of R 5.5 million plus interest at the applicable prescribed rate per annum to date of payment. The matter served before me in terms of paragraph 8 of Chapter 2 of the Commercial Court Practice Directive.

[2] The matter has its origin in emails and attachments thereto that were received by the plaintiff on 21 August 2019, which were part and parcel of a type of fraud, which has become known as unlawful "business email compromise” “(BEC”) perpetrated by an unknown cybercriminal. The chain of events set in motion by the transmission and receipt of the said emails led plaintiff to transfer the amount of R5.5million - being the outstanding amount due in respect of her purchase of an immovable residential property - into a fraudulent account, which she thought was the bank account of the defendant (“the ENS account”).

[3] The plaintiff’s claim against ENS is delictual in nature. It is one for pure economic loss caused by omission. The pleadings consist of amended particulars of claim and an amended plea, together with requests for trial particulars and replies thereto, with the plaintiff alleging in the amended particulars of claim that ENS owed her a duty of care and that as a consequence of the breach of such duty she suffered damages in the amount of R5.5 million.

[4] Plaintiff pleaded further, alleging that in the course of its dealings with Plaintiff ENS owed Plaintiff a legal duty ("the legal duty"), inter alia, in the relevant communications (whether by letter, email or telephone), to warn Plaintiff of the

danger of BEC and the increase in the prevalence of the BEC type of fraud in particular; to warn Plaintiff, before making any payment to ENS to ensure that she verified that the account into which payment will be made is a legitimate bank account of ENS; and to implement adequate security measures such as password protection of emails and/or attachments thereto or loading the ENS Trust Account as a public beneficiary in the FNB and Standard Bank online banking systems so that the bank account number does not require transmission by the medium of an unprotected and unsafe form of communication. ENS denies that its conduct was wrongful, negligent or caused the loss. The defendant denies, inter alia, that in a phone conversation, the plaintiff was advised or told that the outstanding amount could be transferred directly to the defendant. Instead, the defendant pleads that ENS' Maninakis simply undertook to send the defendant's trust account details "*in case the plaintiff chose to transfer the balance of the purchase price to ENS*".

[5] ENS has pleaded, in the alternative, that the plaintiff was contributorily negligent. To wit, inter alia, that the plaintiff failed to exercise reasonable care to ensure that it was safe to pay the balance of the purchase price by electronic transfer; failed to exercise reasonable care to ensure that the number of the account to which she transferred the balance of the purchase price was correct; and that she failed to ask Ms Maninakis, Mr Carrim (of the defendant) or her own bank whether it was safe to pay the balance of the purchase price to the account number received by email. The issue for determination is whether ENS should be held delictually liable for Ms Hawarden's loss.

Factual Background

[6] The facts are largely common cause. On 23 May 2019, Ms Hawarden entered into an offer to purchase agreement with the David Pitts Family Trust for the purchase of a property, a dwelling house in the suburb of Forest Town, Johannesburg, through the real estate agency of Pam Golding Properties ("Pam Golding"). The purchase price was R 6 million, with a deposit of R 500,000.00 required. The deposit was payable to Pam Golding. The offer to purchase agreement in clause 5.4 was on condition that that the balance of R 5,5 million would be secured by a bank guarantee issued in favour of the seller from a recognised financial institution acceptable to the seller, or by way of another undertaking acceptable to the seller, which would be subject only to transfer taking place. Such guarantee or undertaking had to be delivered by the purchaser to the conveyancer (ENS) within 14 (fourteen) days. ENS was appointed by the seller as the conveyancing attorneys responsible for attending to the transfer and registration of the property.

[7] Ms Hawarden received the news from the estate agent, Mr Prince Lukhele of Pam Golding, that her offer was accepted by the seller. This message was conveyed to her in an email dated 23 May 2019 at 09h15. The email contains the following statement:

> *"Please note that due to the ever present risk (of) cyber-crime we insist that before you make payment of the deposit, you call either Prince Lukhele on 0113800000 or the toll free number on the attachment to verify that the banking details we sent are the* same as the details you have received."

[8] Attached to this email was a letter on Pam Golding's letter head dated 6 September 2016, containing more warnings about "email hacking, phishing

and *scams*" as well as Pam Golding's bank account details. The offer to purchase agreement in clause 5.4 was on condition that that the balance of R 5,5 million would be secured by a bank guarantee issued in favour of the seller from a recognised financial institution acceptable lo the seller, or by way of another undertaking acceptable to the seller, which will be subject only to transfer taking place. Such guarantee or undertaking shall be delivered by the purchaser to the conveyancer (ENS) within 14 (fourteen) days. The plaintiff spoke to Prince Lukhele over the phone at about 09h15 on 23 May 2019, for 153 seconds.

[9] Plaintiff effected payment on 24 May 2019, of the requisite deposit by direct deposit into the trust account of Pam Golding, the estate agents mandated by the seller to market the property.

[10] Subsequently, Pam Golding emailed ENS**,** copying in plaintiff, whereby it confirmed receipt of the deposit and attached a copy of the signed offer to purchase agreement. Upon receipt of this email, ENS responded to Pam Golding**,** copying in plaintiff**,** advising that Ms Shivani Ambaram, a senior associate employed by ENS in the Real Estate or Property Department, would attend to preparing the documentation for submission to the Deeds Office to effect the transfer and registration of the property into the name of Plaintiff.

[11] On 21 August 2019, at 9:03 AM, the plaintiff received an email from one Eftyhia Maninakis ('Ms Maninakis'**)** with email address emaninakis@ensafrica.com,[1] a secretary in the property division of ENS. The email reads as follows:

"Dear Judith,

[1] Underlining own emphasis

With reference to the above matter please see attached a letter with guarantee requirements. In accordance with the signed Offer to Purchase same need to be delivered within 14 days of request by us, i.e by no later than 3 September 2019. We note from the Offer to Purchase, registration is to take place on or about the 1 October 2019. We have requested rates clearance figures and await same from the council. Looking forward to your further communication herein.

Kind Regards,

Eftyhia Maninakis"

[12] The email attached a letter setting out the defendant's guarantee requirements. The defendant sought two guarantees, one in favour of the Standard Bank for credit of David-Pitts Family Trust in the amount of R144 258.06, and another one in favour of First National Bank (FNB) for credit of ENS in the amount of R5 355 741.94. What the plaintiff did not know at the time, however, is that this email was fraudulent. The fraudster had intercepted the genuine email sent the previous day by Ms Maninakis and had altered the defendant's account details to reflect the fraudster's account no "*62821759365".*

[13] In response to the email, plaintiff telephoned Ms Maninakis on 21 August 2019, to discuss the letter and asked whether, if her bank was unable to furnish the guarantees by 3 September 2019, as required in what she assumed to be a letter from ENS, could plaintiff elect to transfer the outstanding amount directly to ENS. Ms Maninakis confirmed that this could be done and stated that she would email two more documents to plaintiff,

namely: a letter to Standard Bank with guarantee requirements; and a document from FNB providing the banking account number of ENS, for purposes of a direct transfer of the balance of the purchase price to ENS. Later, at 16:39 on 21 August 2019, Plaintiff duly received the following email from what appeared to be Ms Maninakis' ENS email address, emaninakis@ensafirca.com[2] and what appeared to be a follow up communication from the telephonic conversation earlier that day. The email reads:

"Dear Judith,

It was nice chatting to you, further to our telephonic conversation please see attached a letter, addressed to Standard Bank, with our guarantee requirements. Kindly remember to ask what Standard Bank will charge you to issue said guarantees. We further attach a copy of our banking details to enable you to attend to the transfer of the balance of the purchase price, in the sum of R5 500 000.00. into our trust account, in the event that you choose to do so, instead of requesting the bank to issue the guarantees. Please do not hesitate to contact me to assist you when you approach the bank, regarding the issuing of guarantees, as they might pose questions that you are not able to answer. Have a good evening and I look forward to your further communication herein.

Kind Regards, Eftyhia Maninakis"

[14] The word "africa" in Ms Maninakis's email address was changed to "afirca" in the email received by plaintiff, which plaintiff did not notice. Two letters referenced in the email were attached thereto, namely: first, a letter on what

[2] Underlining own emphasis

appears to be an ENS letter head, addressed to Standard Bank requesting the necessary guarantees; and second, a letter which appears to be from First National Bank ('FNB') confirming what is alleged to be the banking details of ENS. As indicated above, the emails actually sent by ENS appear, however, to have been intercepted and forged by an unknown hacker in order to perpetrate a type of fraud which has become known as "Business Email Compromise" ('BEC') as plaintiff did not receive the genuine ENS emails and attachments at the time when it was sent to her, but only saw the forgeries, with the fraudulent banking account details provided in the forged communication.

[15] The series of events on 22 August 2019, when Ms Hawarden transferred the R5,5m outstanding amount into the fraudulent account, which she thought was the ENS account, are as follows. Plaintiff went to Standard Bank of SA Limited, Rosebank Branch at which she was a client, to obtain assistance with the transfer of the money to ENS. There she was assigned to Ms Sinethemba Shabalala ("Sinethemba"), a person employed by Standard Bank and acting within the course and scope of her employment. Ms Hawarden discussed the option with Sinethemba of requesting guarantee forms from the bank versus transferring the money directly to ENS.

[16] Sinethemba informed Ms Hawarden that it takes up to 14 working days to provide guarantees. While still at Standard Bank Rosebank, Ms Hawarden called Ms Maninakis to discuss the issue of interest which would be earned on any deposit into ENS' trust account. Ms Maninakis was however not in the office and Plaintiff left a message, requesting details of the rate of interest ENS would offer. Shortly after, Ms Hawarden received a call from Mr Arshaad

Carrim (Carrim), a Senior Associate in ENS's Real Estate or Property department. The interest options were discussed and Mr Carrim advised that ENS offered less interest than the Standard Bank money market.

[17] Ms Hawarden and Ms Maninakis continued to correspond, albeit that their communications were intercepted and altered by the fraudsters to delay detection of the fraud. On 23 August 2019, Ms Maninakis sent to Ms Hawarden an investment mandate to be signed. The investment mandate contained several warnings about BEC and precautions to be taken against BEC. However, this was after the payment had been made, but before the fraud was discovered. In relevant parts, the warnings read: "…acknowledge and agree that:

…3.2. criminal syndicates may attempt to induce me/us to make payments due to ENSafrica into bank accounts that do not belong to ENSafrica;

3.3. this form of fraud may be perpetrated through emails, letters and electronic or other correspondences that may appear to have emanated from ENSafrica;

3.4. before making any payment to ENSafrica, I/we will ensure to verify that the account into which payment will be made is a legitimate bank account of ENSafrica;

3.5. if at any time I/we are not certain of the correctness of the bank account into which a payment due to ENSafrica will be made, I/we will immediately contact ENSafrica;

3.6. ENSafrica will not advise of any change in bank details by way of email or other electronic communication. If I/we receive any communication of this

nature, I/we will report it to ENSafrica…"

[18] The plaintiffs' money was withdrawn during the period between her effecting payment by EFT and plaintiff becoming aware of the fraud. The beneficiary bank into which the outstanding amount was transferred, namely FNB, was unable to retrieve the misappropriated funds.

The oral evidence

[19] Ms Hawarden, now retired and a senior citizen, gave evidence and confirmed the contents of her witness statement that she was the victim of a BEC fraud, but for minor alterations. It is on the 23 May 2019, that she made a deposit into the trust account of Pam Golding, not the 24 May 2019 as reflected in her written statement. Secondly, paragraph 17 of the statement where she said that she had been unable to find my email correspondence at the time of preparing her witness statement, was correct. But since then she found the correspondence with the relevant attachments. She does not know in precise terms how the fraud was carried out other than that correspondence between her and the defendant was intercepted and manipulated. She seldom makes large transactions. She knew nothing of the dangers of business email compromise. Her background is in social activism, and not in business.

[20] Ms Hawarden explained the series of events which led to her paying the outstanding balance of the purchase price for the property into a fraudulent account, as summarised above. She testified that there was nothing in the two emails that could have alerted her to the fact that they were fraudulent, and that she believed that they were genuine. On her version, during their call, Ms Maninakis did not inform her that a direct transfer was a riskier option than

payment by bank guarantee, nor did Ms Maninakis warn her of the dangers of business email compromise.

[21] Ms Hawarden gave evidence that Standard Bank was not in the position to verify the account details because it was an FNB account and in any event did not have cause to question the account details because they were on a formal FNB letterhead. Subsequent to the mistaken payment into the fraudster's account, in late September 2019, the defendant sent a statement of account and its banking details in order so that the plaintiff could make a second (replacement) payment. At the foot of the statement of account was a warning urging the reader to telephonically verify the defendant's banking details before making any payment to the defendant, which warning was absent in its previous communications. A similar, even more explicit, warning appeared in an investment mandate, which was prepared by the defendant for the plaintiff's signature.

[22] In addition, she addressed certain additional issues. The first of these were the circumstances in which the defendant had obtained information and documents from the plaintiff in the run up to the trial. Ms Hawarden explained that the defendant had made a mirror image copy of her computer. She assumed that it wished to do so to establish whether or not the plaintiff had been hacked. The computer held vast amounts of personal information, and its copying caused her a great deal of anxiety.

[23] Ms Hawarden subsequently found out that an enormous amount of information was taken from her computer, much of which appeared to have little relevance to the matter before this court, which included first, her Vodacom cell phone record from January 2019 to December 2019. She could

not understand the relevance of these records, especially those before May 2019, which was when she had her first dealings with the defendant.

[24] The second was a Nedbank Corporate Saver interim statement. Ms Hawarden testified that this account was opened on the advice of Citadel to keep her money required for living expenses. She testified that it was a personal bank account and that she could not understand its relevance to the case. The third item was an email between the plaintiff and her lawyers in her divorce. The plaintiff testified that she was divorced in early 2019, and that the email related to the settlement. She could not understand what relevance it had to the present matter. She testified that its inclusion by the defendant in the trial bundle caused her immense distress and was in breach of an agreement between the plaintiff's attorney and the defendant's attorney.

[25] ENS also included the divorce settlement agreement, in breach of an agreement between the parties' attorneys to remove such material. Ms Hawarden testified that it was humiliating to see matters relating to her divorce in the public domain. Next, the plaintiff's counsel took the plaintiff to various RMB Investment Portfolio Statements. Ms Hawarden testified that this was a record of investments going back ten years, with no apparent relevance to the case. Also included was a 2011 email about the plaintiff's tax affairs. She testified that this also had no apparent relevance to the case and that it appeared to be in breach of the agreement between the parties' attorneys.

[26] The next document was an Alexander Forbes Investment Advice Agreement dated 1 April 2014. Ms Hawarden testified that she had no idea why the agreement would be relevant to the present matter, other than to harass her. The plaintiff's counsel took the plaintiff to an email dated 27 May 2014. Ms

Hawarden explained that it was an email arising out of a meeting with the Solon Foundation, of which she was a trustee. The Solon Foundation is a Swiss Foundation which does work in education in rural South Africa.

[27] Ms Hawarden testified that it was founded by a very private Swiss family, who had appointed the plaintiff as a trustee because they trusted her judgment and integrity. She was not remunerated for her work for the Solon Foundation. Ms Hawarden testified that the email was private and that she had been put in the position where she would have to disclose to the Board that the Solon Foundation's affairs had been made public, and possibly resign her position.

[28] The plaintiff was once again highly distressed by the apparently unnecessary and irrelevant disclosure of this document. In addition, the plaintiff said that the document was disclosed in breach of an agreement between the plaintiff's attorney and the defendant's attorney. The defendant included two further Solon Foundation documents in the trial bundle on Caselines, being the 2017 financial statements for the Solon Foundation and a letter from the foundation's auditors regarding the financial statements. The plaintiff testified that this was sensitive and confidential financial information with no apparent relevance to the case, and that the other trustees would be appalled by its being made public.

[29] Finally, the plaintiff's counsel referred the plaintiff to the memorandum of incorporation of a non-profit company called Compassionate Friends. The plaintiff explained that this was an international organisation set up to support families who had lost children or siblings or grandchildren, as the plaintiff had done. Following the loss of her child, the plaintiff had become a grief counsellor and went on to become the head of counselling and a member of

the executive committee at Compassionate Friends. She later became the chair of the committee and became a member of the CC which held the property from which Compassionate Friends operated. The CC was incorporated as a non-profit company, and the plaintiff remained a director. The plaintiff testified that the inclusion of the memorandum of incorporation of Compassionate Friends had forced her to revisit the most painful event of her life, for no apparent purpose. The plaintiff confirmed that the objectives of Compassionate Friends appeared clearly from the document.

[30] Under cross-examination, the first contention that emerged under cross-examination was that the plaintiff was not a stranger to large amounts of money, or to making substantial transactions. She admitted to having received or paid the following amounts before her transfer to ENS: She received an amount of R5m on 17 May 2019, and an amount of R1m on 18 May 2019. She transferred the R6m on 20 May 2019. She transferred R500,000 from one account to another and then paid it to Pam Golding on 23 May 2019. There were other transactions in June 2019, subsequent to this incident in May 2019.

[31] Ms Hawarden explained, however, that she had been married to a wealthy man and only discovered after her divorce how wealthy her husband had been and that he had managed their finances during the marriage. She also had financial advisors who managed her financial affairs. The plaintiff explained that she meant that she had never transferred such large sums of money prior to the process of buying her house, and not prior to the transfer which she had attempted to make to the defendant. The plaintiff emphasised that she had not conducted large transactions *prior to 2019*. While conceding that she had

made some large transactions, they had all been related to her divorce and the purchase of her house. The plaintiff's husband had agreed to give her R6,000,000.00 towards the purchase of a house as a part of the divorce settlement.

[32] In the email and its attachment, Pam Golding warned Ms Hawarden of the risks of cyber-crime repeatedly. They, in particular, warned her not to rely on banking details sent to her by email but to check them by telephone. Ms Hawarden accepted that she had seen the warnings contained in the Pam Golding correspondence and stated that she had called Prince Lukhele**,** the estate agent at Pam Golding Properties**,** to confirm their bank account details before paying the deposit. She later accepted that her recollection must have been incorrect and that Lukhele must have called her. Nothing turns on this aspect of her evidence.

[33] As to why she had failed to heed Pam Golding's warnings when she made her transfer to ENS, she stressed she failed to heed Pam Golding's warnings because she trusted ENS. When further pressed on why she did not respond to the defendant's email in the same way that she did to Pam Golding's email, the plaintiff elaborated that she trusted the defendant implicitly, and that the Pam Golding experience had occurred three months earlier. She also emphasised that she was going through a difficult time on account of her divorce. She repeatedly stated she trusted ENS, the source of the email and *"assumed they would take care of anything that was not safe*".

[34] Ms Hawarden was invited, under cross-examination, to reconcile the following statement provided in the request for further particulars and in respect of which she failed to make discovery**,** namely**,** that she*" was not aware of the*

prevalence, dangers or nature of business email compromise" given her knowledge of the Pam Golding warnings. She said in response that, "*I must have forgotten. I clearly forgot. I never gave it another thought".* It is common cause that the Pam Golding correspondence containing the fraud warning was sent on 23 May 2019, whereas the defendant's targeted discovery request was dated 4 May 2021, two years later.

[35] Also, when challenged on the statement in her witness statement that the first fraud warning she received was on 25 September 2019, by way of the second investment mandate sent to her, the plaintiff stated that she forgot if she had been warned in the investment mandate that had been received by her on 26 August 2019. In her witness statement, the plaintiff states as follows in relation to the investment mandate received by her on 26 August 2019: "*I cannot find a copy of this investment mandate form and I cannot recall if it contained any warnings about BEC*".

[36] Ms Hawarden stated in her witness statement and in evidence that, "*Standard Bank was not in the position to verify the account details because it was an FNB account*...". The defendant's counsel queried why the plaintiff or her bank could not have verified the bank account details using the FNB stamp which stated that its authenticity could be checked in a certain way. She was further pressed on why she had stated in her witness statement that her bank could not have verified the account details because it was an FNB account. The plaintiff emphasised that she trusted the defendant and that she could not answer for the bank.

[37] The defendant's counsel also took Ms Hawarden through a number of Standard Bank notices warning clients of various cyber frauds, including

"*smishing*", "*fishing/phishing*", and "*vishing*". The plaintiff said that she did not recall the notices but accepted that she would have received them because she was a Standard Bank customer at the time.

[38] The defendant's counsel also turned to the transaction with the defendant. He took Ms Hawarden through the correspondence sent and received by her and Ms Maninakis and the telephone call between them. In particular, the defendant's counsel referred Ms Hawarden to the email sent by Ms Maninakis at 16h18 on 21 August 2019, and the attached letter from FNB, which was addressed to "*Dear valued client…*" and introduced FNB's new letter generation functionality which allowed users to validate the letter. However, this was removed by the fraudsters and not received by the plaintiff.

[39] Counsel also referred her to the instructions in the top right corner of the letter with instructions on how to verify the letter. In response, the plaintiff pointed out that the reference number for the verification of the letter had expired. The defendant's counsel then referred Ms Hawarden to the emails, which she in fact received, pointing out that the FNB fraud warning had been removed and the account details of the defendant altered.

[40] Ms Hawarden conceded that she had informed Ms Maninakis of her decision to go the cash route after making the payment, and that Ms Maninakis then sent her the mandate. It was also put to the plaintiff that she did not care about the fraud warnings contained in the investment mandate. She denied this and stated that she did not consider the fraud warnings because she had already made the payment.

[41] Under re-examination, the plaintiff clarified, inter alia, as follows. On a call

whilst still at the bank, Ms Maninakis asked the plaintiff whether she had taken to the plaintiff's bank Ms Maninakis' email with the letter setting out the defendant's bank account details, and that the plaintiff had confirmed that she had both and would correspond with Ms Maninakis once she had finalised the matter with the bank. The plaintiff was adamant that Ms Maninakis or for that matter, Mr Carrim, at no stage warned her of the dangers of business email compromise.

The plaintiff's first expert witness – Mr Anton Van't Wout

[42] The plaintiff's first expert witness was Mr Anton Van't Wout ("Van't Wout"). Mr Van't Wout confirmed his witness statement without corrections. Mr Van't Wout gave evidence as an expert in the field of digital forensics and data analytics. He conducts digital forensic investigations in his chosen profession. On his version, BEC has been on the rise, and that he and colleagues have come across this in numerous investigations in recent years.

[43] Van't Wout confirmed that there are multiple ways in which email communications may be compromised. Criminal syndicates focus on attempting to induce people through fake or spoofed email addresses into making payments into accounts under the control of the syndicate. In his written statement, he states that he expects the utilisation of technologies available to secure email communication such as Sender Policy Framework (SPF), DomainKeys Identified Mail (DKIM) and Domain-based Message Authentication, Reporting and Conformance protocol (DMARC).

[44] Van't Wout explained that he had prepared a demo and narrative for the purposes of illustrating to the court how easy it was to perpetrate a business

email compromise scam. He also prepared a demo, which illustrated one solution to the problem, being a secure portal for the transmission of sensitive communications to be used in conjunction with two factor authentication. The demo had been agreed to at the joint experts meeting. Mr Van't Wout explained what BEC is, also used a video to demonstrate visually what spoofing of an email looks like. The demo was then played for the court. The video demonstration showed the ease with which an email could be spoofed and altered which included PDF attachments, the inherent insecurity of email, and alternative, safer ways of communicating sensitive information, including using a secure portal in conjunction with two-factor authentication.

[45] Van't Wout also gave evidence as to what technical measures are available to combat BEC, including a video demonstration of a secure portal, and stated that in his view email should not be used for high value business transactions. Van't Wout explained that a secure portal would have been an effective and affordable way of avoiding business email compromise incidents and opined that in his view**,** there was no reason why the defendant could not have used one in 2019. The experts agreed with this contention at the joint experts' meeting (although the defendant's expert Jason Jordaan stated that he had no direct knowledge of the costs of a secure portal in 2019).

[46] Under cross-examination, the defendant's counsel put it to Mr Van**'**t Wout that he had only testified on what was technically possible, and not on what other attorneys and businesses generally did. Van**'**t Wout accepted this, but said that he had seen other conveyancing attorneys using a secure portal. He accepted that information security is in the first place to protect information within an organisation; in the second place to protect information of other

people in the organisations' system and thirdly to protect communications between an organisation and its clients.

[47] The cross-examination also turned to the issue of the secure portal. The defendant's counsel sought to suggest that it would be impractical for everyone transmitting secure information to use a secure portal. Mr Van't Wout explained that this was a risk assessment that the organisation or individual in question would have to make. It was not necessary for all information to be transmitted by way of a secure portal, but only that information which the organisation or individual deemed sensitive. There was a long interaction with counsel for the defendant over the spoofed email sent as part of the demonstration.

[48] The defendant's counsel told Van't Wout that the sending of the spoofed email to the plaintiff's and the defendant's email addresses had failed. This was because the defendant's system recognised that the email had come from an IP address which was not allowed to use the defendant's domain name. Van't Wout explained that the relevant technology was a combination of SPF and DMARC. DMARC was a technology responsible for reporting back that someone was trying to spoof your email address.

[49] Mr Van't Wout also explained that SPF in conjunction with DMARC would have blocked the first fraudulent email. Had DMARC been enabled by the defendant at the time (it was not) it would have alerted the defendant to the fraud attempt. The defendant only used SPF, and not DMARC. MWEB, being the plaintiff's email service provider, did not use SPF at the time. It was put to Van't Wout that had SPF been used by MWEB at the time the fraudulent message would have been blocked or sent to spam because it was from an

unauthorised IP address, and the fraud would have been averted. Van't Wout stated that this depended on how SPF was configured. The defendant's counsel also sought to suggest that the secure portal with two factor authentication solution was an afterthought. Van't Wout correctly pointed out that the idea had been included in his witness statement in paragraphs 9 and 10.

[50] In re-examination, Van't Wout explained how a secure portal with two factor authentication worked, and that such a function was offered as part of LexisNexis' offering. Van't Wout emphasised that email should not be used for high value transactions. On the topic of secure portals, Van't Wout confirmed that the cost estimate he had given was a once-off cost for developing a portal from scratch, which was a small percentage of the defendant's IT security budget. As ENS also pointed out, with which I agree, Mr Van't Wout gave evidence in a satisfactory manner. ENS's criticism being that that he testified about what was technologically possible rather than practice. I deal with that below.

The plaintiff's second expert witness – Mark Heyink

[51] Mr Mark Heyink ("Heyink"), the plaintiff's second expert witness, is an attorney and an expert in information and communications technology law, data protection law, and information security practices, with a particular focus on organisational security safeguards necessary for information governance, management, and security. Mr Heyink's evidence included a description of information security generally, technical and organisational measures to protect information security, and information management systems and governance.

[52] Heyink testified that the risk of business email compromise had been publicised in various advisories and publications for many years, including articles that he wrote, and that it was a well-known risk. On his version, technological safeguards are of little value if the people who use the technology are not sufficiently aware of the risks and of how to mitigate them. In this instance, the defendant's employees were not adequately trained or aware of the risks of BEC.

[53] Since 2018, Heyink authored several articles on behalf of the Law Society of South Africa attempting to create awareness among attorneys on the issue. These articles dealt with the risks of BEC and precautions to be taken. Heyink observed that the defendant's witness statements revealed inadequate awareness among the defendant's staff of BEC. Heyink was referred to the defendant's 'Acceptable Use Policy' that was in place in 2019, and in particular, the sections relating to email and instant messaging usage. Paragraph 10.5 stated: *"No transmission is totally secure and therefore confidential/sensitive information must be password protected. The password must be sent in a separate communication*." He explained that the provision recognised that electronic communications were not secure and it recognised a mechanism of trying to provide security, but which had not been complied with in the present matter.

[54] During cross-examination, the fact that in November 2018, Heyink had sent his bank account details to Mr Aslam Moosajee of the defendant by way of an unprotected/unencrypted MS Word attachment was taken up with him, which he conceded. He also conceded that *"most attorneys send their invoices to their clients by way of pdf attachments to ordinary emails".* Also that his

evidence reflects what he thinks ought to be done and not what actually happens in the market.

Ms Peckham-Kolyvanov

[55] Ms Peckham-Kolyvanov is the IT and Technical Operations Manager at a law firm Miltons Matsemela Attorneys (Miltons). Miltons is a specialist conveyancing firm. She gave evidence of the practice which Miltons adopts in sending bank details to purchasers in a conveyancing transaction. She explained that Miltons had been aware of BEC attacks since 2014, and that she and the senior partner of Miltons asked Korbitec (now known as "*Lexis Nexis*") to offer a solution to combat BEC. LexisNexis introduced products known as LexisTracker and SecureChat, a secure chat portal. Milton's uses these products to communicate bank details and she explained how it works.

[56] According to Ms Peckham-Kolyvanov, the monthly cost of the Secure Chat/Lexis Tracker portal was approximately R1000, which the firm considered reasonable considering the complete protection afforded to all stakeholders against the ever present (and growing) threat of BEC. One of the first steps taken by the firm's administrative staff in a conveyancing transaction was to phone every buyer, seller, and estate agent involved in the transaction, and, *inter alia,* confirm the firm's details and warn all parties about the ever present danger of cyber fraud; how the conveyancing industry is affected; and how the Secure Chat secure portal functions.

[57] Ms Peckham-Kolyvanov stated that she knows of "*many South African law firms which have successfully been using the Secure Chat portal as a part of their Lexis Convey subscription*" but was only able to name a few firms. These

were Greyvensteins Incorporated, ESI Attorneys, Minde Shapiro & Smith and Velile Tinto. The defendant's counsel noted that the defendant's attorneys had contacted the firms mentioned by Peckham-Kolyvanov and that only ESI Attorneys used the secure portal as described by Peckham-Kolyvanov. With the exception of the disagreement over which other firms used a secure portal, Peckham-Kolyvanov's evidence remains, on the main, uncontradicted. As ENS conceded, Ms Peckham-Kolyvanov gave evidence in a satisfactory manner.

The plaintiff's third factual witness –Mr Denoon Sampson

[58] Mr Sampson is an attorney and conveyancer. He practices under the name of Denoon Sampson Ndlovu Inc which employs 4 conveyancers and around 30 employees. Mr Sampson gave evidence on an article which he wrote in August 2019, dealing with BEC and what steps payors should take to avoid BEC scams. The article was prompted by the prevalence of BEC and similar frauds at the time. The article was aimed at attorneys, and so the references to "payor" and "payee" were to attorneys when making or receiving payments respectively. He says that he deals with the practice of his firm, as it developed from 2014 onwards.

[59] Sampson agreed with the advice contained in the England and Wales Conveyancing Association's Cyber Fraud and Fraud Protocols[3] which *inter alia* provide the following "Practice Guidance": Firstly, *"Where possible use a secure portal for all communication-most case management systems will have or support a secure portal*". Second, "*Bear in mind that encrypted email will not protect against a recipient's email account being hacked which means that*

[3] Exhibit 21, 032-474 to 479 (especially paragraph 3 "Change of Banking Details" first three bullet points 032-476).

they could receive email from a fraudster". Third, "*avoid sending or receiving bank details by email*." Sampson also explained the process his firm followed to ensure that bank account details were correctly and safely conveyed to payors and explained how the system had evolved and how the system sometimes needed to be adapted in individual cases. In his witness statement at para 15, Mr Sampson stated that:

> *"About eight years ago we averted a BEC attempt involving a R5 million payment which was due to be paid to our trust account by the purchaser for the balance of the purchase price. The firm had been instructed by the seller to attend to the transfer of his property. Upon receipt of this new instruction I telephoned the purchaser to introduce myself and also to give her the correct trust account bank details over the phone. She made a note of the correct Standard Bank trust account number. About three weeks later my secretary emailed the buyer the Standard Bank trust account details, calling for payment of the balance of the purchase price. However, that email was intercepted and altered to reflect a fraudulent Absa account. Fortunately, the purchaser remembered that I had told her that she was to only pay into our Standard Bank Trust Account, and she immediately telephoned my secretary to query the different banks and account numbers. My secretary immediately realised that there had been an interception and an impersonation of her original email resulting in the insertion of the fraudster's bank account details. Fortunately, the buyer was alerted to the fraud, because I had originally given her the bank account details by telephone. The money was never lost."*

[60] Sampson was cross-examined on the incident described above in paragraph 15 of his witness statement. The defendant's counsel noted that Sampson had forgotten many aspects of the story. Sampson explained that it had happened about 8 years ago and that he had made a diligent search to find more details.

The defendant's counsel suggested that there was no way that the defendant could verify the story. The defendant's counsel also put it to Sampson that his story had been completely fabricated for the purposes of the plaintiff's case. Sampson strenuously denied this.

[61] In cross examination, the defendant's counsel referred Sampson to emails sent by his firm to the defendant with his firm's bank details. Sampson explained that these emails were between law firms, which used email addresses which were more secure than laypersons' email addresses. In addition, conveyancing secretaries often did not want to use their personal devices in transactions and this made it difficult to avoid email when dealing with other law firms.

[62] Sampson confirmed in re-examination that the defendant's attorneys had not bothered to contact his secretary to verify the facts alleged in para 15 of his statement despite her details being made available to them before he was cross-examined and accused of fabrication. In this regard, the Court was referred to the relevant emails establishing the following facts: On 23 February 2022 (about one week before the trial resumed), the defendant'**s** attorney pertinently asked for further particulars about paragraph 15 of Sampson's statement, which contains the evidence Sampson was accused in cross-examination of fabricating**,** including "*the name, address and telephone number of …(the) secretary as mentioned".* On 24 February 2022 plaintiff's attorney replied to Mr Hiepner's request for particulars, stating *inter alia* that:

"the secretary referred to in paragraph 15 is Alice Leisching, who remains employed by Denoon Sampson Ndlovu Inc."

[63] Sampson explained that there was no subsequent request made at any point by Mr Hiepner (defendant's attorney) to interview Ms Leisching, in that regard. He was explicit in his witness statement and evidence that his article was aimed at attorneys and estate agents, and not third party laypersons, and that his firm believed it owed a duty of care to anybody planning to pay money into its account.

The defendant's first factual witness – Eftyhia Maninakis

[64] Ms Maninakis is a conveyancing secretary employed by ENS. She reports to Mr Carrim. Her evidence dealt with her interactions with Ms Hawarden over the period 20 August 2019 to 28 August 2019. In brief, her evidence in chief was that she had addressed emails to Ms Hawarden and that she spoke to Ms Hawarden on 21 August 2019 and 22 August 2019. Paragraph 17 of her written statement, which she confirmed, reads as follows:

"After I spoke to Mr Carrim, I called Ms Hawarden to see if she required any further assistance from me. She was still at Standard Bank and informed me that Mr Carrim had provided her with the information she had requested from him on the interest rates. She informed me that if she was to transfer the amount into ENS' trust account she would want the amount invested with a bank which would provide her with the highest interest rate. She advised that her banker was still trying to establish the process required to issue the guarantees, the time frame involved and the cost of same. She was still undecided and advised that she might be transferring the money into the ENS trust account as it might be the easier option. I told her that it was entirely up to her and asked whether she had taken to her bank my email with the letter

setting out the ENS bank account details. She confirmed that she had both and would correspond with me once she had finalised the matter with her bank."

[65] Under cross examination, Ms Maninakis accepted that she did not know that pdf documents could be manipulated until the incident of Ms Hawarden regarding this matter. She accepted that Ms Hawarden would be relying on the information emailed to her in the event that she decided to transfer the outstanding money into the defendant's bank account. She accepted that Ms Hawarden relied on her for the information, which she emailed, but maintained that Ms Hawarden was in "*professional hands*". She knew that a deposit by Mrs Hawarden into ENS' trust account was one of the two possibilities. Ms Maninakis also knew that if the plaintiff went the cash route, she would transfer the money by way of an electronic transfer. This was part of the reason she had asked the plaintiff if she had the letter with the defendant's bank account details in her possession.

[66] Ms Maninakis explained that she did not send the mandate letter (with fraud warnings) to Ms Hawarden because she did not know at that stage that Ms Hawarden was going to go the deposit route. She also explained that she thought that Ms Hawarden was in the "*safe hands*" of her bank. She did not know at the time that a PDF was not secure and could be manipulated. Ms Maninakis acknowledged that it was no longer her belief that a PDF was secure, and that she had learned this as a result of the incident involving Mrs Hawarden. Ms Maninakis conceded that she only learned of BEC as a result of the incident involving the plaintiff. Following the incident involving Mrs Hawarden, the defendant had started including BEC warnings in its emails.

[67] Ms Maninakis also accepted as a representative of ENS that she owed Mrs Hawarden a duty of care, to be careful in the way that she dealt with the plaintiff and interacted with her on the business front. ENS had included a new warning on its communications as a result of the incident involving the plaintiff, which urged recipients to telephonically verify bank account details. Ms Maninakis was constrained to concede that she had no understanding of how to use the FNB fraud prevention system attached to the email before being removed fraudulently, which was used by the defendant, nor would she know how to explain the system to Ms Hawarden. In any event the electronic stamp on the FNB letter sent to the plaintiff had expired, and it was the defendant's responsibility to the ensure that it was valid.

[68] Ms Maninakis did not know about the defendant's Acceptable Use Policy in August 2019. Although she contended that it was premature to send the plaintiff the investment mandate before she knew if the plaintiff was going to make a direct deposit, she conceded that it was not premature to send the plaintiff the BEC warnings contained in the investment mandate. Ms Maninakis accepted that the warnings were useless if not brought to the attention of the plaintiff before the payment was made. Ms Maninakis also accepted that it would have been a simple precaution to ask the plaintiff to read the bank account details to her on the call.

[69] In re-examination, Ms Maninakis said that she knew it was a possibility that the plaintiff would go the cash route, but in that event she thought that the plaintiff's bank would help her with the payment and that banks were experts in making such transactions. She added that it would not have been any more difficult for the plaintiff or her bank to ask Ms Maninakis to confirm the bank account details as the other way around.

The defendant's second factual witness – Arshaad Carrim

[70] Mr Carrim is a senior associate employed by ENS. He was the conveyancer responsible for the transfer of the property from the seller to Ms Hawarden. His evidence in chief dealt with a conversation which he had with Ms Hawarden on 22 August 2019 whilst she was at the bank. His conversation with her was limited to the issue of interest rates.

[71] During cross-examination, Mr Carrim stated that he could not recall whether he attended training or induction from ENS about matters of cyber security, that he was aware of BEC at the time he spoke to Ms Hawarden, and that he was aware that ENS' practice was to send bank details by email in pdf format. The plaintiff's counsel asked if, in hindsight, Mr Carrim thought it would have been prudent to confirm the defendant's bank details telephonically. Mr Carrim countered that at the time Mrs Hawarden had not decided how to pay the balance of the purchase price.

[72] The plaintiff's counsel then asked Mr Carrim whether**,** in the event the court found that it was a likely step she would have taken or that she was possibly or probably going to pay the defendant directly, it would have been prudent to confirm the defendant's bank details. Mr Carrim said that it would have been, but added that plaintiff's bank could also have advised her on confirming the defendant's bank details. Significantly, Mr Carrim acknowledged that the fraud warnings in the investment mandate were pointless if provided to the recipient after the payment was made.

The defendant's third factual witness – Jaco Van Zyl

[73] Mr Van Zyl is a Systems Architect and head of the IT Infrastructure team at ENS. He testified in his evidence in chief that this position entails dealing

with IT infrastructure. He gave evidence in general on the defendant's information security policies. He was referred specifically to paragraph 10.5 of ENS's Acceptable Use policy which provided as follows: "*No transmission is totally secure and therefore confidential/sensitive information must be password protected. The password must be sent in a separate communication*." He was asked if this applied or should apply to banking details. Van Zyl replied that this depended on whether or not banking details had been classified as sensitive or confidential, and that Ms Jane Naude would be able to answer whether or not this was so.

[74] Van Zyl was then taken through the ENS' Ntrust report. He said that it was commissioned in order to gauge how mature the defendant's information security roadmap was. It was commissioned on around 13 August 2019, before the incident before the incident involving Ms Hawarden. The report was rendered towards the end of September or early October 2019. According to Van Zyl, none of the concerns raised in the Ntrust report "*in any way affected the incident of Ms Hawarden's loss of her R5.5 million*." He confirmed that ENS did have SPF enabled on its systems to ensure that people do not use ensafrica.com to transact or send messages to unsuspecting people and pretend to be someone from ENSafrica.

[75] Under cross-examination however, Van Zyl conceded that email was an inherently dangerous form of communication for sensitive business information if the relevant precautions were not taken. The defendant's Information Security Policy was only approved after the Ntrust report was finalised, but had been applied and adopted in practice from 15 November 2018. Also, the Acceptable Use Policy, including paragraph 10.5, was in place

at the time that the incident occurred. Van Zyl was not aware of the Law Society's warnings of the dangers of business email compromise. He was constrained to concede that if it was found that the defendant's banking details were financially sensitive information, then the clause in this case had not been adhered to. When asked what the defendant had done to avoid a repeat of the incident, Van Zyl stated that he had been instructed not to make any technical changes for as long as this case is pending. He confirmed that the nature of the email sending the defendant's bank account details was confidential.

[76] Having been referred to the advice contained in the England and Wales Conveyancing Association's Fraud and Cyber-Fraud Protocol, Van Zyl agreed that a secure portal would stop this kind of fraud, although he was not aware of the solution at the time. He agreed that secure portals were available in South Africa in 2019, having heard other evidence in the case. He also agreed that it was sound advice to avoid sending or receiving banking details by email.

[77] Van Zyl agreed that if there was a reasonable and practical precaution, which attorneys/conveyancers could take against cyber-hacking; they should take such precautions. He did not mention the plaintiff's incident to Ntrust because it was confidential and he did not know if he was allowed to share the information because it was an ongoing investigation. Van Zyl agreed that if someone was about to pay the defendant on the strength of emailed bank account details, it would be prudent to warn him or her of the dangers before the payment was made and this was the case in point; had the plaintiff been asked to read back the account details, it would have helped.

The defendant's fourth factual witness – Jane Naude

[78] Ms Naudé is the Chief Financial Officer of ENS. Her witness statement dealt with ENS' actions in dealing with the risk of fraud. She explained the generation of the FNB fraud warning letter. Naude said she had reviewed emails and invoices sent by large South African and international law firms in 2019. She said that her review confirmed that most of them did not have any warnings about fraud and those that did, did not warn against the type of fraud that occurred in this instance. She attached a table setting out the information extracted from the emails and invoices reviewed. She also undertook a survey of what other law firms did in relation to their email communications, and when sending out invoices. She said that the outcome of the survey was that "*overwhelmingly there were not many of these firms that had a specific note around the changing of the bank detail at this date*". She added that she was not aware of these firms using more secure methods to communicate bank account details.

[79] Ms Naude did a second survey of communications in which banking details were sent to the defendant. Ms Naudé's conclusions following the surveys was that ENS receive about 5,000 invoices a month from different categories of creditors, which are received by email without any additional protections like password protections. She said that generally the defendant's creditors sent their invoices attached to an email, with no special protective measures. She said that creditors left it to the defendant to verify their banking details. The purpose of the survey according to Naude, was to determine what other firms were doing in relation to how they were sending out their tax invoices for payment, how they were sending out their bank details and also if they had any warnings about fraud on those emails or invoices

[80] Under cross-examination, Ms Naude made the following concessions. Naude did not know if the defendant had a security policy, nor did she know in 2019. She could not recall if the mandatory training and induction process included training on BEC in 2019, and said that the issue fell outside her area. When referred to the defendant's insurance proposal form (Exhibit 13) and the response indicating that the defendant's security and privacy policy did not include mandatory training for all employees, Naude stated that she did not complete the form on her own and the IT team would have answered IT-related questions and this question in particular. Naude was referred to the declaration at the end of the document and asked if it was correct. She said: "As I have said before, I do not know. The form was completed by various different people, who take responsibility for various different areas, either in the finance space or in the practice space, or in the IT space, in completing this form." She repeated that the firm did have mandatory training, but she did not know if it was in the policy.

[81] Naude was referred to paragraph 10.5 of the insurance proposal form. This posed the question: "Is all sensitive and confidential information that is transmitted within and from your organisation, encrypted using industry grade mechanisms?" and had been ticked "Yes". Naude said that this would be a tick from the IT team and that she did not know if it had been correctly made or not. She emphasised that she had relied on her colleagues to answer the questions in their areas correctly. Naude accepted that the transaction with the plaintiff was confidential, but said that the defendant's bank details were not confidential.

[82] Regarding the bundles of invoices (Exhibits 28 and 29), Naude agreed that it

was fair to say that in most cases the law firms mentioned would be already loaded on the defendant's accounting system and would have already been verified and confirmed. The defendant would not make payment if an invoice came in with details did not match those recorded on the supplier database. The system would only pay to accounts which had previously been verified. She also conceded that on first receiving these bank account details, the defendant would have ensured that they were correct. The plaintiff's counsel asked her to determine overnight how many of the service providers were not pre-registered.

[83] Upon her return on the next day of her testimony, Naude said that 3 out of the 13 law firms in the law firms bundle (Exhibit 28) were not pre-registered on the supplier database. In the case of 5 of the firms, it was the first time that the defendant was paying the firms and the invoices constituted proof of their banking details. In the bundle of other vendors (Exhibit 29), all of the vendors were pre-loaded on the system. Naude accepted that ENS was well aware of the dangers of BEC at the time of the incident. Naude agreed that the rule that had been communicated to Ms Maninakis, being that PDF attachments to emails were secure and could not be manipulated, was completely wrong. She accepted that if the court accepted Ms Maninakis' evidence on this, then the defendant's training was inadequate.

[84] Naude also conceded that out of the 23 emails listed on annexure "JN6" to her witness statement, only 3 related to invoices or payments. Of those, she agreed that all three would probably be pre-registered on the defendant's system. It was put to Naude that her evidence was dishonest, because she had said that the majority of the emails related to invoices and payments,

whereas only three emails in fact related to invoices and payments. Naude stated as follows: "*I can only say that I had muddled up the information based on the length of time that has passed from when we prepared for the trial to the initial trial to now, you know, there have been lots of emails and evidence that have been pulled on different things and I do apologise if my recollection on the, this date in particular was not 100 percent correct*". She denied that she had lied in spite of being reminded by the cross-examiner of her repeated claims that she *personally reviewed the 23 emails.* Her evidence in this regard was clearly unconvincing.

The defendant's fifth factual witness – John Webber

[85] Mr John Webber, an attorney and conveyancer, is employed as a director at Cliffe Dekker Hofmeyr (CDH), in Sandton. In 2019, CDH's real estate department consisted of 104 employees of which 24 were conveyancers and 80 were support staff. His evidence was that in 2019, CDH did not employ any additional protections when communicating their bank details to payors. The bank details would be conveyed by email (as a pdf attachment to an email) and it was the payor's responsibility to verify the banking details.

[86] Under cross examination, the plaintiff's counsel illustrated how simple it was to alter a PDF document. Following the demonstration, and in response to a statement that it is necessary for responsible conveyancers and people who have to convey banking details to clients or third parties to stop the continued use of unprotected and unsafe email and attachments**,** he stated "*I will after seeing this demonstration by you look to more secure means to communicate this information in the future*". Mr Webber was constrained to agree that to administer, oversee and promote electronic transfer of substantial sums of

money without having security measures in place would be irresponsible. He admitted that he had not realised that the manner in which he had done it in the past was as insecure as counsel for the plaintiff have demonstrated it to be.

The defendant's first expert witness – Johan Roux

[87] The first expert witness called by the defendant was Mr Johan Roux ("Roux"), a digital forensics expert. Roux conducted an analysis of the emails sent and received by the plaintiff and Ms Maninakis, and identified which of the emails were fraudulent. He concluded that the perpetrator more than likely had access to the plaintiff's email account. It is common cause that Ms Hawarden's email account was hacked.

[88] Under cross examination, he testified that technologies like DMARC, DKIM and SPF would not have stopped a fraud like that which occurred to the plaintiff, because the fraudsters gained access to the plaintiff's email address and were sending emails from the plaintiff's actual account. He also agreed that sending an unprotected email with banking details was very dangerous, and that this fact was known in 2019, at least to experts. In addition, Roux agreed that a normal reader would not detect that the email sent from emaninakis@ensafirca.com was fraudulent.

The defendant's second expert witness – Jason Jordaan

[89] The defendant's second expert witness, Mr Jason Jordaan, is a principal forensic analyst. He had reviewed the particulars of claim and comment**ed** on the actions of the defendant in light of the state of BEC frauds that were occurring in 2019. On his version, it was reasonable for the plaintiff to state that she would not have been able to immediately notice that the first email

received by her was fraudulent, without examining the email header data, which is not something that the average computer user would do. Jordaan testified that if SPF had been employed by MWEB, the fraud would likely not have happened.

[90] During cross examination, Jordaan said that he now believed that *the defendant knew of the risk of business email compromise*, having listened to the evidence in the case and having been referred to the warnings contained in the investment mandate contrary to what was recorded in the joint expert minute wherein he recorded that he did not know if the defendant knew of the risk. He agreed that the plaintiff appeared not to have been warned of the risk of business email compromise.

[91] With reference to comments made at the joint experts' meeting, Jordaan was also asked if there was more that the defendant could have done to avoid the business email compromise which occurred in this case, given that a PDF is not more secure than a Word document. He was constrained to concede that, had Ms Maninakis called the plaintiff on that day and asked "read me the bank account number, that would be a totally costless and simple precaution that she could have taken and would have prevented the fraud" because she was about to pay the 5.5 million. But, he also testified that in a case such as this one, it possible for the hackers to remove the password protected attachment and replace it with their replacement email.

[92] The experts held a joint experts' meeting on 28 September 2021 and 18 October 2021. At the First joint experts' meeting on 28 September 2021, the experts agreed on the following: To assist the court, a demonstration would be prepared which would demonstrate BEC. It would be good practice for both

sending and receiving servers to implement SPF, DMARC and SKIM. With reference to reference to the email sent from the ensaf**ir**ca email address, Jordaan was content to moderate the following statement: *"Unlike the first email (discussed above), the email address which was visible was clearly different from the previous email address by removing the word "clearly".* Also, Jordaan was content to moderate the statement that the plaintiff *"would have been able to immediately notice that the email was fraudulent, without her examining the email header data by removing the word "immediately".*

[93] It was recorded that if SPF had been implemented by MWEB, the second fraudulent email would not have reached the plaintiff. MWEB also did not make use of DMARC or DKIM. The risk of BEC was well-known before 2019. Email disclaimers are not an absolute prevention mechanism because they can be removed, but they are helpful insofar as they raise awareness of BEC. It was not clear when the interception of emails or the compromise of the plaintiff's email account occurred. It was agreed by joint experts' meeting that, insofar as BEC may have been identified as a risk to the defendant, it should have taken steps to mitigate the risk.

[94] Jordaan agreed with Heyink in principle, that the defendant did not consider BEC specifically as a risk or that appropriate technical and organisational measures were introduced to mitigate the risk of BEC specifically. However, he said that the defendant did have security in place to mitigate IT risks in general. Despite the expectation that payment could be made to its bank account, no warning was provided to the plaintiff by the defendant of the risk of business email compromise, Jordaan disagreed that the defendant had a duty to do so. It was noted that BEC had been around for years, particularly in

the context of conveyancing transactions. The measures proposed by Van't Wout in paragraphs 8-10 of his witness statement were good practice, although Jordaan stated that they were not "*required practice".*

[95] A second joint experts' meeting was held on 15 October 2021, to consider the demonstration and the narrative prepared by Van't Wout. The experts were able to agree that email is insecure (although there was disagreement as to whether it could be said that email is "*notoriously*" insecure). In this case the plaintiff was deceived by cybercriminals making changes to emails and spoofing emails. BEC was a known problem at the time of this incident (August 2019) and even before then. It was agreed that some mitigating technologies were also available at the time (August 2019) in the form of the Sender Policy Framework (SPF); DomainKeys Identified Mail (DKIM); Domain-based Message Authentication, Reporting and Conformance protocol (DMARC) and a few email encryption technologies.

[96] The second joint experts' meeting went on to agree that all these technologies can be implemented and maintained by in-house IT personnel (which were available to the defendant). DMARC, which includes all these technologies, can be completely outsourced for a cost of about R2000 - R8000 per month. Outsourcing also includes many additional security options. It was agreed that, a practical alternative to email which could be used for the secure electronic transmission of sensitive documents (and information) is to install and use a secure portal that requires two factor authentication for a guest to gain access to where the sensitive document/information is stored. Two factor authentication requires a second communication channel by which additional authentication information is sent. There are numerous options for a second

communication channel such as SMS (Short Message Service) or other messaging applications which are received on the recipient's mobile device (cell phone. It was noted that secure portals were available in 2019.

[97] The joint expert meeting further agreed that, had a secure portal been used by the defendant as the means to communicate its banking details to the plaintiff at the time of this incident, there would have been no way for the cyber criminals to tamper with the sensitive letter or documents reflecting the defendant's banking account details.

The law

[98] In order to succeed in a delictual claim, the plaintiff would have to prove the following elements: wrongfulness, causation, fault and harm. [4] To recap, the plaintiff alleges that the defendant had a duty to exercise sufficient care in the conduct of the transaction, to warn the plaintiff of the dangers of BEC, and communicate its bank details in a safe manner. Ms Hawarden blames ENS for her loss because, she says, they should have one more to protect her against the risk of loss of she suffered. She says they should have done so by employing more secure means to communicate with her. The conduct complained of for which she seeks to hold ENS liable is, essentially, their omission to protect her. It is trite that to render someone else liable, his or her conduct must have been wrongful, as the first principle of the law of delict is

---

[4] See: *H L & H Timber Products (Pty) Ltd v Sappi Manufacturing (Pty) Ltd* (281/98) [2000] ZASCA 187; [2000] 4 All SA 545 (A) (29 September 2000) at para 13, where the following was said:

"As with delictual claims in general the essential elements are: a) conduct, initiating wrongfulness, by the defendant; b) fault, in this instance negligence, by the defendant; c) harm suffered by the plaintiff; d) a causal connection between (a) and (c)."

that everyone has to bear their own loss[5].

[99] Our law recognises that there is no general right not to be caused pure economic loss and, unlike loss to person or to property, where pure economic loss results, the conduct is *prima facie* lawful[6]. Liability does not arise unless policy considerations require that the plaintiff be compensated[7]. In *Van Wyk v Lewis*[8] it is said, a person who adheres to the general practice of the profession as a rule is not negligent, for such practice indicates what the profession considers to be reasonable conduct.

[100] Conduct is negligent if the actor does not observe the degree of care which the law of delict requires. The standard of care which the law demands is that which a reasonable person in the position of the defendant would exercise in the same situation. Liability for negligence arises if a *diligens paterfamilias* in the position of the defendant would foresee the reasonable possibility of his conduct injuring another in his person or property and causing him patrimonial loss; and would take reasonable steps to guard against such occurrence; and the defendant failed to take such steps[9].

[101] However, whether a *diligens paterfamilias* in the position of the defendant would take any guarding steps at all and, if so, what steps would be reasonable, must always depend on the particular circumstances of each case. No hard and fast basis can be laid down[10]. The court in *Powell and*

[5] Telematrix v Advertising Standards Authority 2006 (1) SA 461 (SCA) para 12. See also Stewart v Botha 2008 (6) SA 310 (SCA) para 12; Imvula Quality Protection v Lourens 2013 (3) SA 407 (SCA) para 32; South African Hang & Paragliding Association v Bewick 2015 (3) SA 449 (SCA) para 31; Home Talk Developments v Ekurhuleni Metropolitan Municipality 2018 (1) SA 391 (SCA) para 1; Hlumisa Investment Holdings v Kirkinis 2020 (5) SA 419 (SCA) para 59

[6] *Country Cloud Trading CC v MEC, Department of Infrastructure Development* 2015 (1) SA 1 (CC) at para 22.

[7] *Telematrix (Pty) Ltd t/a Matrix Vehicle Tracking v Advertising Standards Authority SA* 2006 (1) SA 461 (SCA) at para 13.

[8] Van Wyk v Lewis - 1924 AD 438 at 457.

[9] *Kruger v Coetzee* 1966 (2) SA 428 (A) at 430

[10] Oppelt v Department of Health, Western Cape 2016 (1) SA 325 (CC) at para 69

Another v Absa Bank Ltd t/a Volkskas Bank[11] concluded as follows*: "It would seem to me to follow that if there is no evidence concerning the standard practice in a specialised field, a court, if it is uncertain whether the defendant's conduct measured up to the standard of skill and diligence required in his profession, would ordinarily hold against the party bearing the onus*."

Discussion

[102] Ms Hawarden contends that ENS's conduct was wrongful in its omissions or failure to warn or advise her in regard to the risks of BEC. She contends that ENS was well-aware of this type of fraud before the fraud in this case took place, which is apparent from the warnings contained in the defendant's investment mandate sent to the plaintiff after the payment took place but before the discovery of the fraud. She also contends that a finding in her favour would only impose such a duty on conveyancers and attorneys, who already owe a duty to third party purchasers on the authority of *Bruwer v Pocock & Bailey Ingelyf* [12] and to the public when dealing with trust funds based on the SCA decision of *Du Preez and Others v Zwiegers* [13]**.** The evidence in this case shows that BEC attacks are rife, especially in the conveyancing industry. The parties' experts agreed that BEC has been around for many years, particularly in the context of the conveyancing industry[14], and that the risk of BEC was well-known before 2019.

[103] In *Bruwer*[15], the court held that, because the attorney held the depositor's money in trust, it owed him a duty to exercise care in the way it disposed of

[11] 1998 (2) SA 807 (SE)
[12] *Bruwer v Pocock & Bailey Ingelyf* 2016 JDR 2129 (WCC).
[13] *Du Preez and Others v Zwiegers* 2008 (4) SA 627 (SCA) at para 21.
[14] First experts' joint minute (28 September 2021 meeting), J15, para 46.
[15] Note 9 above.

the money. In *Du Preez*[16], the plaintiff made an unsolicited deposit in an attorney's trust account. The SCA held that the attorney owed the depositor a duty to exercise reasonable care in dealing with his money and put it thus: *"I find it difficult to see what possible scope there is for the contention that there was no legal duty in this situation. An attorney is under a legal duty to deal with trust account money in such a way that loss is not negligently caused, inter alia, to the depositor."*[17]

[104] It is however, also trite, as ENS contends, that our common law does not generally render people liable in delict for the loss they cause others by omission, that is, by their failure to prevent the loss. In support hereof, reference was made to Professors Neethling, Potgieter and Visser who put it as follows: "*As a general rule, a person does not act wrongfully for the purposes of the law of delict if he omits to prevent harm to another person. Thus, the point of departure is that a person is generally not liable where his omission or omissio — his failure to act positively to prevent loss — factually infringes the interests of others. Omissions are therefore prima facie lawful"*[18]**.**

[105] In *Hawekwa Youth Camp v Byre* [19], the Supreme Court of Appeal reminds us that: "*The principles regarding wrongful omissions have been formulated by this court on a number of occasions in the recent past. These principles proceed from the premise that negligent conduct that manifests itself in the form of a positive act causing physical harm to the property or person of another is prima facia wrongful. By contrast, negligent conduct in the form of an omission is not regarded as prima facie wrongful. Its wrongfulness*

[16] Note 10 above.
[17] Du Preez para 19
[18] Neethling – Potgieter – Visser Law of Delict 7th Ed p58 para 5.2
[19] Hawekwa Youth Camp v Byre 2010 (6) SA 83 (SCA) para 22;

*depends on the existence of a legal duty. The imposition of this legal duty is a matter for judicial determination, involving criteria of public and legal policy consistent with constitutional norms. In the result, a negligent omission causing loss will only be regarded as wrongful and therefore actionable if public or legal policy considerations require that such omission, if negligent, should attract legal liability for the resulting damages**".***

[106] To determine wrongfulness in a case such as this one, which falls into both categories of exception because the plaintiff claims pure economic loss caused by omission, the trite approach as advocated by the SCA in *Minister of Safety and Security v Van Duivenboden*[20] at para 21, since endorsed by the Constitutional Court in *Country Cloud Trading v MEC, Department of Infrastructure Development* [21] being that, "*When determining whether the law should recognise the existence of a legal duty in any particular circumstances what is called for is not an intuitive reaction to a collection of arbitrary factors but rather a balancing against one another of identifiable norms".* In *Country Cloud*, the Constitutional Court recognised the risk of indeterminate liability as the main policy consideration that militates against the recognition of liability for pure economic loss[22]. But, the loss in a case of this nature would always be quantifiable and determinate, as it would be limited to the quantum of the payment paid into the account of a fraudster.

[107] The SCA also cautioned in *Fourway Haulage*[23] that the determination of wrongfulness in claims for pure economic loss is a principled exercise based on considerations of public policy and not on the idiosyncratic views of an

[20] 2002 (6) SA 431 (SCA)
[21] Country Cloud Trading v MEC, Department of Infrastructure Development 2015 (1) SA 1 (CC) at para 26; see also Trustees, Two Oceans Aquarium Trust v Kantey & Templer 2006 (3) SA 138 (SCA) para 10
[22] Above at para 24 and 25.
[23] Fourway Haulage SA v SA National Roads Agency 2009 (2) SA 150 (SCA)

individual judge about what is reasonable and fair. It went on to caution that *"[T]he first policy consideration is the law's concern to avoid the imposition of liability in an indeterminate amount for an indeterminate time to an indeterminate class"*[24]. The judicial determination in this regard culminates in a value judgment, as to what is either acceptable (reasonable) or sufficiently legally-reprehensible (unreasonable) to warrant a delictual remedy[25]. It is recognised that the nature of reasonableness in the wrongfulness inquiry should not be confused with the nature of reasonableness in the negligence inquiry. In the wrongfulness context, the issue is the reasonableness of imposing liability on the defendant for the harm resulting from that conduct[26].

[108] The wrongfulness test is open-ended and flexible[27].The Constitutional Court reminds us aptly that our common law should not "*be trapped within the limitations of the past*"[28]. Accordingly, the common law is supposed to adapt to changing needs, and not be static regardless of the evolving perils of cyber-fraud crimes. Whether a duty of care exists would depend on the facts of the case and the identities of the parties. Such a duty clearly exists between a purchaser in a conveyancing transaction and the conveyancing attorney handling the transaction, but would not exist in many other cases.

[109] ENS criticises the plaintiff for saying that she had never before handled such large sums of money, when in fact she had received or paid various large amounts in May and June 2019. This criticism is unfounded. It completely ignores the plaintiff's explanation that the transactions under scrutiny all

[24] Above at para 23. See also Hlumisa Investment Holdings v Kirkinis 2020 (5) SA 419 (SCA) para 68.
[25] *Trustees, Two Oceans Aquarium Trust v Kantey & Templer (Pty) Ltd* 2006 (3) SA 138 (SCA) at para 12.
[26] *Le Roux and Others v Dey (Freedom of Expression Institute and Restorative Justice Centre as Amici Curiae)* 2011 (3) SA 274 (CC) at para 122.
[27] *Van Eeden v Minister of Safety and Security (Women's Legal Centre Trust, as Amicus Curiae)* 2003 (1) SA 389 (SCA) at para 11.
[28] *Du Plessis v De Klerk* 1996 (3) SA 850 (CC) at para 86.

related to her divorce settlement and related house purchase, which related to the very incident before this Court. The criticism in this regard is accordingly without merit.

[110] Also, ENS criticises the defendant's evidence on the Pam Golding warnings, and says that she attempted to conceal the Pam Golding fraud warnings despite the defendant's request for disclosure of third-party warnings. The plaintiff allowed the defendant to make a full copy of her computer and to search it for relevant evidence, which opportunity the defendant took full advantage thereof. Despite its thorough search of the plaintiff's computer, the defendant obtained the Pam Golding warning under subpoena of Pam Golding. Evidently, therefore, the Pam Golding emails were not on the plaintiff's computer.

[111] The plaintiff said in her witness statement that she could not find some emails and believed that emails were deleted from her mailbox by the fraudsters. There are no valid grounds for accusing the plaintiff of trying to conceal anything in these circumstances. The plaintiff said that she had forgotten about the Pam Golding warning when she responded to the defendant's request for disclosure. I find this to be a satisfactory explanation on a purely collateral issue. The plaintiff's reply under cross-examination on a purely collateral matter is considered final and conclusive. I am satisfied that plaintiff testified satisfactorily and was a good witness. He evidence was not seriously challenged.

[112] ENS contends that, if this court holds ENS liable to Ms Hawarden, it would expose all conveyancers, big and small alike, to claims of the same kind by third parties, with whom they have no relationship, for losses they suffered at

the hands of fraudsters who hacked their own email accounts. ENS contends that the ripple effect thereof would not only extend to all firms of attorneys but indeed to all businesses who send their invoices, with their banking details, to their clients by email, which is a near-universal practice for all firms and indeed all businesses to do so, as supported by Van't Wout's evidence and that of Jordaan.

[113] ENS contends more so, because the near-universal practice in the market is that it is the responsibility of the debtor, who chooses to make an electronic payment, to ensure that it is paid into the right account. ENS submits in this regard that the court should decline to extend liability for pure economic loss in this case because it will, in the words of the Constitutional Court, create "*liability in an indeterminate amount for an indeterminate time to an indeterminate class"*[29]*.*

[114] The vexed question is whether the law provided the plaintiff with adequate means to protect herself in the circumstances of her case. In *Country Cloud* the Constitutional Court said the following, on the topic of vulnerability to risk: *"where a plaintiff has taken, or could have reasonably taken, steps to protect itself from or to avoid loss suffered, this is an important factor counting against a finding of wrongfulness in pure economic loss cases"*[30]. In such circumstances the plaintiff is not 'vulnerable to risk' and, on that basis *"reasoned, there is no pressing need for the law of delict to step in to protect the plaintiff against loss"*[31].

---

[29] Country Cloud note 6 above.
[30] At para 51; see also *Cape Empowerment Trust Ltd v Fisher Hoffman Sithole* 2013 (5) SA 183 (SCA) ([2013] ZASCA 16) (*Cape Empowerment Trust*) para 28; *Delphisure Group Insurance Brokers Cape (Pty) Ltd v Dippenaar and Others* 2010 (5) SA 499 (SCA) ([2010] ZASCA 85) para 25; *Fourway Haulage* above n 10 para 25; and *Two Oceans Aquarium* above n8 paras 23 - 24.)
[31] See also see *AB Ventures Ltd v Siemens* Ltd 2011 (4) SA 614 (SCA) at para 21.

[115] It is further stated importantly that[32],

> "*This is not to suggest that a delictual claim is precluded whenever a party puts herself in a position where there is a risk of harm. Far from it. We expose ourselves to risk, for example, every time we elect to travel on public roads and that would not excuse from liability those who culpably crash into us. But where a transaction involves a substantial and highly foreseeable risk of loss, which a commercially sophisticated and well-advised plaintiff nevertheless accepts because of the promise of significant financial gain inextricably linked to it, there is often no pressing need for the law of delict to intervene."*

[116] The SCA held in *AB Ventures*[33] that, "…*there was no call for the law to be extended when the existing law provided adequate means for the plaintiff to protect itself against loss".*

[117] However, the cases cited by the defendant show sophisticated commercial entities failing to protect themselves, or being unable to protect themselves, through contractual mechanisms as opposed to the plaintiff in this matter who did not have a contract with the defendant, as counsel for the plaintiff also contended. In this matter, as stated, the investment mandate was only sent to the plaintiff after payment was made. It is true that in this case Ms Hawarden had no direct contractual relationship, with ENS but dealt with it directly for conveyancing purposes before the investment mandate was sent.

[118] ENS contends in this case, that the Ms Hawarden could have avoided her loss by asking Ms Maninakis or Mr Carrim to confirm ENS' bank details when she spoke to them while she was at her bank or sought the help of her bank. Ms

[32] At para 61.
[33] Above note.

Hawarden specifically asked the bank to help her make the transfer to ENS.

[119] But as for the various concessions made by Ms Maninakis, they confirmed that her training and awareness in regard to BEC was hopelessly inadequate. That she apparently considered the plaintiff to be in “professional hands” as counsel for the plaintiff pointed out, is irrelevant in a context where Ms Maninakis was not conscious of the relevant dangers and precautions. She did not consider the situation unsafe to begin with, and so would not have conducted herself any differently even if the plaintiff was making the payment without the assistance of her bank. Ms Maninakis was oblivious to the relevant risks at the time. She could not have been “reassured” by the bank’s role, because she did not think knew that the plaintiff was at risk.

[120] In contrast to Ms Maninakis, Mr Carrim by his version knew and understood the risks of BEC. He knew that the defendant had put the plaintiff at risk by emailing its bank details to her, and yet he stayed silent. That he considered the defendant to be in safe hands at her bank as contended, is unsatisfactory in circumstances where he knew that the plaintiff was at risk. Carrim spoke to the plaintiff on the telephone while knowing of all the relevant risks.

[121] As for Naude, it was obviously misleading for Naude to refer this court to 23 redacted emails which, save for 3, had nothing to do with invoices and payments. Her other two surveys proved to be completely irrelevant because they dealt with vendors and law firms that were generally pre-loaded as beneficiaries on the defendant’s system. The evidence of Ms Naude was accordingly unsatisfactory.

[122] ENS owed at least, a general duty of care to a purchaser of property, in this

case Ms Hawarden. ENS, as Ms Hawarden contends, had control over the way in which its bank account details were conveyed to her. It chose to do this by way of an unprotected email attaching its bank account details as a PDF document, which could easily be manipulated as the evidence clearly established. In facilitating the transaction, ENS failed to safely communicate its bank details, using technical safety measures or multi-channel verification (in-person or telephonic confirmation). The legal duty of care owed to the purchaser, arises from the moment the defendant accepted the brief to act as conveyancer in the transaction. There is no reason in principle for only recognizing the duty from the date of payment. It is from the (earlier) moment, when the defendant is appointed as the conveyancer, that the plaintiff depended on the defendant to act professionally. Even if the plaintiff was not at that point a client of the defendant, she was in the care of the defendant. Its duties in this regard included its duty to warn defendant of the known risk of BEC and to take the necessary precautions against it to protect itself.

[123] Ms Hawarden explained adequately why she did not check ENS' bank details or ask the bank to do so. She repeatedly said that the Pam Golding experience was three months before. As indicated above, emphasised that she was going through a difficult time on account of her divorce. She repeatedly stated she trusted ENS, the source of the email and *"assumed they would take care of anything that was not safe*".

[124] It is indeed so that he totality of the evidence shows that it was a near-universal practice for conveyancers, and indeed for other businesses, to send their banking details to others by email but for some exceptions thereto. It does not absolve the defendant of its unsafe behaviour, which it knew at the

time was unsafe and knew to take precautions against. It is not as if the defendant didn't know better. Its own investment mandate is, as the plaintiff contends, wholly destructive of defendant's reliance upon the alleged "near-universal practice".

[125] 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 her version, which I accept and cannot fault, she did not think she needed to seek advice as she was dealing with a law firm whose reputation went before it. She, as indicated, gave credible and consistent evidence that the possibility of BEC did not occur to her and that she trusted the defendant. Under such circumstances, a duty clearly exists between a purchaser in a conveyancing transaction and the conveyancing attorney handling the transaction.

[126] I have no difficulty in finding that the defendant's banking details were financially sensitive information regarding this matter and needed to be treated as such. I have no difficulty in concluding that the risk of BEC was foreseen by ENS. ENS is undoubtedly an experienced conveyancer, which understood the risks inherent in conveyancing transactions. The implications of its own investment mandate confirms its knowledge at the relevant time of the dangers of BEC. This is clear from the warnings contained in its investment mandate and its Acceptable Use Policy, and the numerous concessions to this effect made by its witnesses. In the present case, ENS was, I find, the proximate cause of the loss in that it provided its own bank account details and was responsible for their accuracy and for the safety of their transmission. In doing so ENS acted wrongfully in light of legal convictions of community.

[127] In my view, the plaintiff's case established clearly that sending bank details by

email is inherently dangerous, and so must either be avoided in favour of, for example, a secure portal or it must be accompanied by other precautionary measures like telephonic confirmation or appropriate warnings which are securely communicated. The parties' experts agreed that email is not secure. In this case the parties' experts also agreed that secure portals were available in 2019, and would have averted the fraud. Accordingly, the fact that large firms like CDH and the defendant chose not to use effective technologies and measures that were available and were used by smaller conveyancers does not avail them in making a "common practice" argument, as plaintiff contended.

[128] Password protected email was contemplated by the defendant's own Acceptable Use Policy. The experts agreed that there were other mitigating technologies available in 2019, which could have been implemented by the defendant's in-house IT personnel or which would have been outsourced at a cost R2000 - R8000 per month, which is not an unreasonable amount. The defendant's own expert agreed that there was much more the defendant could have done to avoid the fraud.[34] The precautions that the defendant should have and could have implemented but failed to implement would have prevented the fraud regardless how or why the plaintiff's email was hacked. Although the plaintiff was not a client of the defendant, she was, as stated, still in the care of the defendant and vulnerable to risk.

[129] As for the element of causation, it has by now become well settled that, in the law of delict, causation involves two distinct enquiries. First, there is the enquiry into factual causation which is generally conducted by applying the

[34] Transcript, 034-1496, line 22, to 034-1499, line 15.

'but-for test' as described in *International Shipping Co (Pty) Ltd v Bentley*[35]. The facts that are common cause and as found regarding this matter leave no doubt in my mind that, but for the negligent transmission of it**s** account details and failure to warn Ms Hawarden upfront of the inherent danger of BEC, she would not have suffered the loss. On the second enquiry, under the rubric of legal causation, namely whether the negligent conduct of ENS is linked sufficiently closely or directly to the loss suffered by Ms Hawarden for legal liability to ensue, or whether the loss is too remote, I conclude, on the established facts, that it was not too remote. It was accordingly, reasonably foreseeable under the circumstances, I find, for ENS that Ms Hawarden might suffer loss as she did.

[130] ENS was at fault on the basis of negligent conduct. I am not inclined to agree with submissions made by counsel on behalf of ENS that Ms Hawarden must take responsibility for her failure to protect herself against the known risk of relying on banking details received by email. The defendant was an expert conveyancer and was facilitating and managing the transaction. Under these overall circumstances it not overly burdensome or unreasonable to impose liability on ENS. The risk of loss to Mrs Hawarden was highly foreseeable by ENS. There is no risk of boundless liability as feared by ENS as the loss in this case is claimed by a single plaintiff and is finite in its extent. It is, accordingly, not unlimited or indeterminate.

Conclusion

[131] The interests of the defendant as well as the society demand that a legal duty is recognised in this case. ENS is best placed to understand and prevent

[35] 1990 (1) SA 680 (A) at 700E — G.

BEC. Individuals in society are generally not as well-placed to respond to the ever-evolving threat of cyber-crime, which is sophisticated and technical in nature. As stated in *Estate Van der Byl v Swanepoel*, "*where one of two innocent parties has to suffer a loss arising from the misconduct of a third party it is for the public advantage that the loss should fall…on that one of the two who could most easily have prevented the happening or the recurrence of the mischief*".[36] All facts considered, accordingly, I am persuaded that considerations of legal and public policy require liability in this case. Accordingly, the plaintiff's claim is upheld.

Costs

[132] Ordinarily, costs follow the result. The plaintiff seeks a punitive costs order. Attorney and client costs have frequently been awarded against parties for conduct which is vexatious and an abuse of legal process "*even though there is no intention to be vexatious*". As counsel for Ms Hawarden pointed out, the plaintiff's right to privacy was breached by including numerous documents in the trial bundle, which have no relevance to the issues in the case. It is inexcusable for the defendant to have done so. Nowhere and at no stage was there however an explanation or apology offered to plaintiff by any of defendant's witnesses or representatives for the egregious inclusion in the Trial Bundle of patently irrelevant (but highly personal and sensitive documents pulled from the plaintiff's laptop); or the breach of the specific undertaking not to take copies of these documents; or the subsequent addition thereof to the Trial Bundle.

[133] Aggravating this conduct**,** as was earlier pointed out**,** is the defendant's breach

[36] See *Estate Van der Byl v Swanepoel* 1927 AD 141 at 150.

of the undertaking (given by its attorney of record) on 6 August 2021 per email not to take copies of these documents which were stored on plaintiff's hard-drive which itself was made available to defendant's expert to copy and perform a forensic investigation to determine where the hacking occurred. On 13 October 2021 however, in breach of the undertaking of 6 August 2021, the defendant (represented by its attorney acting on its instructions) blatantly made or received copies of the irrelevant (but, for plaintiff, very personal and highly confidential) documents and to compound matters, added the documents to the trial bundle. This alone warrant**s** a punitive costs order. It is therefore unnecessary to deal with the two other remaining grounds relied upon by Ms Hawarden in relation to the unsatisfactory aspect of Naude's testimony as well as unwarranted criticism of Simpson's evidence in support hereof.

[134] For all the reasons given, the following order is granted:

Order

134.1 The defendant is ordered to pay the sum of R 5 500 000 (five million and five hundred thousand Rands) to the plaintiff;

134.2 The defendant is ordered to pay interest on the aforesaid amount calculated at the prescribed rate of 10,25% (ten comma twenty-five percent) per annum from 21 August 2019 to date of payment;

134.3 The defendant is liable for the costs of suit, including the costs of two counsel one of whom is a senior counsel;

134.4 It is declared that the plaintiff's expert witnesses, Messrs Mark Heyink and Anton van't Wout are necessary witnesses and it is directed that

their qualifying fees and expenses be allowed in full.

134.5 All costs payable by the defendant are to be taxed on the scale as between an attorney and his client.

_____

MUDAU J

[Judge of the High Court]

APPEARANCES

For the Plaintiff: CHJ Badenhorst SC & MD Williams

Instructed by: Werkmans Attorneys

For the Defendant: Wim Trengove SC & Rashad Ismail

Instructed by: Edward Nathan Sonnenbergs Incorporated

Date of Hearing (Virtually): 18,19,20,21 and 22 October 2021.

1, 2, 3, 4, 7 and 8 March 2022 as well as 27 September 2022.

Reserved: 27 September 2022.

Date of Judgment: 16 January 2023.