IN THE HIGH COURT OF SOUTH AFRICA
WESTERN CAPE DIVISION, CAPE TOWN

Case Number: 4725/2024

In the matter between:

Gripper & Company (Pty) Limited Applicant

and

Ganedhi Trading Enterprises CC Respondent

JUDGMENT

JANISCH AJ:

Introduction

1. In this matter, brought on motion, the applicant claimed payment of the sum of R1 635 129.83 arising from the sale and delivery of goods to the respondent. This was made up of a capital sum of R866 725.25 and interest thereon at 2% calculated daily and compounded monthly on any unpaid accounts.

2. The application became opposed and the respondent filed answering papers. The applicant filed replying papers.

3. Acknowledging that, in its answering papers, the respondent had disputed the existence of an agreement to pay interest as claimed, and that this constituted a factual dispute that could not properly be decided on the papers, the applicant abandoned the interest portion of its claim and persists in this application only with the claim for the former amount of R866 725.25, being the sale price for the valves.

4. In accordance with the practice directions of this Court, the applicant filed heads of argument. The respondent failed to file heads of argument, and on 31 October 2024, the respondent's attorneys withdrew as attorneys of record. No new attorneys have come on record for the respondent.

5. At the hearing of the matter, Mr Aminosh Singh, the General Manager of the respondent, appeared before me. He confirmed that it was not the respondent's intention to retain new attorneys or counsel and that he would represent the respondent as best he could. He confirmed that he was duly authorised to do so, which is consistent with the fact that he deposed to the answering affidavit for the respondent. I proceeded to entertain argument on that basis.

6. Mr *Bremridge* appeared on behalf of the applicant and moved for the revised relief.

The facts

7. The applicant and the respondent had been dealing with each other since 2014. Throughout this time, the applicant had received payments from the respondent in a specified Standard Bank account.

8. It is common cause that in October 2021, the applicant had agreed to sell valves to the respondent for the amount of R886 726.25. The due date for

delivery was 29 April 2021. There is no dispute that the valves were duly delivered.

9. Both the invoice issued on 15 April 2021 and the delivery note signed by the respondent on 29 April 2021 contained the long-standing Standard Bank banking details of the applicant.

10. On 23 April 2021, a delayed payment arrangement (as opposed to cash on delivery) was entered into. In terms of this agreement, the respondent became liable to make payment on 27 May 2021.

11. It is further common cause that the respondent did not effect payment into the applicant's Standard Bank account on the due date for payment or at all, and therefore that the applicant has never in fact received payment of the invoiced amount.

12. What did happen was that on or around 24 May 2021, the respondent made payment of the invoiced amount into an Absa Bank account which did not belong to the applicant. In so doing, it was the victim of a sophisticated fraud perpetrated by an unknown third party.

13. What appears to have occurred is that this third party was able to intercept or gain access to the email correspondence between representatives of the applicant and the respondent relating to the purchase and sale of the valves, and more particularly the emails that pertained to the extended payment arrangement. It inserted itself and replied to the respondent on the same e-mail thread, writing in the guise of the applicant's managing director, Mr. Max Hafen, and reflecting the email address max@gripper.co.za. The message was as follows:

> *"I need to update our Absa banking details with you, starting from today 28/04/2021 all payment must be submitted to our Absa Bank account.*

The Standard bank account will no longer be in use, all payment submitted to this account will not be processed.

Please acknowledge the receipt of this email so I can forward the banking details."

14. In later correspondence with the applicant, the respondent stated that it had confirmed receipt of the above email and asked for the banking details, which were allegedly provided from the same email address on the same day (28 April 2021). These emails were, however, not attached to the papers, and the respondent also did not provide them pursuant to a notice in terms of Rule 35(12) filed by the applicant in these proceedings (the notice went unanswered entirely).

15. The respondent had also contended in other correspondence that from 13 to 24 May 2021, it "*received emails from max@griper.co.za, requesting proof of payment*." It apparently requested a bank confirmation letter on 24 May 2021, which was sent on the same day. A copy of an Absa Bank account confirmation letter dated 5 May 2021 was attached to the answering affidavit. However, none of the emails referred to in this paragraph were attached to the affidavit. They were also not provided in response to the Rule 35(12) notice in which the emails from "*max@griper.co.za*" were expressly requested.

16. The reference in the above correspondence to an email address with the domain name "*griper*" as opposed to "*gripper*" was not a typographical error. The respondent commissioned a report from an information technology specialist which was attached to the answering papers, and which referred both to emails from max@gripper.co.za and what is referred to as "*the lookalike email max@griper.co.za*".

17. It therefore appears that even though the original fraudulent email of 28 April 2021 came from what purported to be the correct email address, the follow-up requests and the email containing the bank confirmation letter probably came from a similar, but not identical, address.

18. As stated, the respondent proceeded to make payment into the Absa account on 24 May 2021. Three days later, the applicant sent an email requesting its payment. It was then that it was discovered that the payment had been made to an unauthorised account and that the applicant had not in fact changed its banking details from Standard Bank to Absa Bank.

19. It is common cause that the respondent's representatives did not make telephonic contact with the applicant's representatives to confirm the change of banking details. They were apparently satisfied that the emails received were legitimate, as a result of which they made the payment.

Discussion

20. Although in the absence of heads of argument for the respondent it is not entirely clear what the legal nature and ambit of its defence is, its principal contention (reiterated by Mr Singh at the hearing of the matter) is that the applicant's email system must have been hacked by a third party, for which it (the applicant) was to blame. It put up an expert report to say *inter alia* that there was no record of its own systems being compromised, and that the emails from max@gripper.co.za also reflected the correct IP address. The import of this was that it was negligence on the part of the applicant that allowed the fraud to be perpetrated. The contention on the papers was effectively that the applicant should be estopped from claiming payment of the purchase price because the respondent relied to its detriment on a representation emanating from the applicant that payment should be made into the incorrect bank account.

21. It was also averred that owing to the applicant's "*wrongful and negligent conduct, in failing to secure its IT systems, which resulted in the fraudulent communication being dispatched*", the respondent had suffered damages in the amount of the misdirected purchase price. Although a counter-application along those lines was threated, it never materialised.

22. I should mention that that in its founding papers, the applicant had averred that its email / server security had never been compromised. In reply, it pointed out that there was no record of the alleged fraudulent email on its server – in other words, that the fraud had not been perpetrated out of its own domain.

23. Unfortunately, cases presenting with this or a similar fact pattern are all too common in the current era. Cyber-crime is rampant, and has been for many years. Schemes to divert money legitimately owed to unauthorised bank accounts, without the knowledge of either party, are a common occurrence.

24. Unsurprisingly, when this sort of event has occurred, disputes have arisen as to who should bear the risk of loss. Many of these cases have been litigated. A recent judgment which deals at length with the case law on this topic, and the general principles to be extracted from the cases, is **Mosselbaai Boeredienste (Pty) Limited v OKB Motors CC** 2024 JDR 1348 (FB), a full bench decision of the Free State Division, Bloemfontein, which was handed down on 7 March 2024.

25. Most of the cases referred to in **Mosselbaai Boeredienste** involve a defrauded debtor seeking to escape its obligation to effect proper payment of the purchase price to the creditor on the basis that the creditor was in some way responsible for the erroneous payment being made, e.g. through not adequately securing its own computer systems.

26. The full bench however recognised the general principle in our law that it is the debtor's obligation to "*seek out his creditor*" and that until payment is duly effected, the debtor carries the risk that the payment may be misappropriated or mislaid. The principle was stated in **Mannesman Demag (Pty) Limited v Romatex** 1988 (4) SA 383 (D) at 389 F-390 D. That was in the context of a payment by cheque. The Court recognised that even after a cheque has been delivered, it can be diverted in some way so that the money is never cleared to the account of the creditor. That risk remains with the debtor.

27. After dealing extensively with more recent cases pertaining to electronic payment into an unauthorised account following a fraudulent third party intervention, the Court summed up the import of these cases as follows (in paragraph [58]):

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

28. On the facts of that case, it was held that the debtor acted at its own peril when it made payment without properly verifying the correctness of the bank account details. Had it made a simple telephone call, it would have established that the invoice was fraudulently changed and it would not have made payment into the incorrect bank account. Moreover, the interception of the email was held not to be the proximate cause of the payment into the incorrect account, but the decision to make payment after being wrongly satisfied that the bank account details had been verified.

29. I find the same approach to be applicable to the present facts. Even though – as stated – the respondent put up an expert report which contended that the applicant's system must have been hacked (to which the applicants in reply put up a report that its system was secure), on the above authorities this appears not to be relevant. As a matter of fact, the applicant did not represent to the respondent that it would receive payment in the fraudulent account (a third party did), and the payment was therefore not made in reliance upon any representation made by the applicant. It was not suggested that the applicant

was aware of any of these events and therefore failed to take steps to avoid adverse consequences.

30. The focus of the courts in cases like this is on the fact that it is incumbent on the risk-bearing debtor, in making payment, to ensure that it achieves this. This does not require a great deal of effort – as the Court in **Mosselbaai Boeredienste** recognised, a simple telephone call may well suffice. Moreover, on the present facts there are various reasons to criticise the conduct of the respondent. These include:

30.1. The fact, known to any persons in business and making use of computer-based methods of communication and payment, that cyber crime is rampant and that care must be taken at all times to limit its impact. The respondent could not have been unaware of this.

30.2. The fact that the parties had been doing business for 7 years with payments routinely made into the same Standard Bank account.

30.3. The fact that the amount of the invoice in this case was significant, so much so that it gave rise to a bespoke payment agreement as opposed to the usual cash on delivery.

30.4. The fact that the first fraudulent email referred to a need to "*update our Absa banking details with you,*" suggesting that the Applicant already had provided Absa banking details, when this was not true. The respondent had only ever paid into a Standard Bank account.

30.5. The fact that the Respondent started getting what it describes as "*emails requesting proof of payment*" between 13 and 24 May 2021, when payment was not yet due under the payment arrangement. The respondent has not disclosed how many of these emails were received, but the inference is that the fraudster was putting on sustained pressure to pay what was not yet due. This

should have raised some concerns given what seems to have been a co-operative business relationship.

30.6. The fact that the said emails appear to have come from a different email address ("griper.co.za" and not "gripper.co.za").

31. These factors merely serve to accentuate the impression that the respondent failed to take the sorts of steps that a prudent debtor would have taken to ensure that its payment was effected properly. It was this failure, rather than anything that the applicant did, that was the proximate cause of the payment being made.

32. In the circumstances, I find that the respondent has not put up a competent defence, either in law or in fact, to the applicant's claim for payment of the purchase price which remains due. The applicant is entitled to payment in accordance with the agreement of sale.

33. Mr *Bremridge* asked for an order including interest from the date of commencement of the application. As regards costs, he properly submitted that this was not a matter of extraordinary complexity such as to warrant a order for the costs of counsel on more than the basic scale.

Order

34. In the premises, I make the following order:

"1. The Respondent is ordered to make payment to the Applicant in the amount of R866,726.25, together with interest at the prescribed rate from 11 March 2024 (the date of commencement of the application) to date of final payment.

2. The Respondent is to pay the Applicant's costs on a scale as between party and party, including the costs of counsel on Scale A."

M W JANISCH
Acting Judge of the High Court
Western Cape Division

APPEARANCES:

For the Applicants:	I Bremridge SC Instructed by: Gottschalk Attorneys Inc
For the Respondent:	Mr Singh (General Manager at the Respondent – in person)
Date of hearing:	05 November 2024
Date of judgment:	06 November 2024 (electronically)