CYBERCRIME: DEBTOR TO SEEK OUT HIS CREDITOR

Gripper & Company (Pty) Ltd v Ganedhi Trading Enterprises CC (4725/2024) [2024] ZAWCHC 352 (6 November 2024)

Cybercrime is rampant. Schemes that divert money legitimately owed to one person to unauthorised bank accounts – without the knowledge of either party – are common. So too is the litigation that follows the innocent parties' efforts to determine who should bear the risk of the loss. In this matter, the court confirmed that principles extracted from applicable case law have now crystallised into a recognition in our law that it is the debtor's obligation to 'seek out his creditor'. Until payment is duly effected, the debtor carries the risk that the payment may be misappropriated or mislaid, unless the facts support another outcome.

The judgment can be viewed here.

FACTS

Gripper & Company (Pty) Limited ("Gripper") and Ganedhi Trading Enterprises CC ("Ganedhi") have been dealing with each other since 2014. Throughout this time, Gripper had received payment for goods sold and delivered to Ganedhi into its (Gripper's) Standard Bank account.

This matter relates to a payment for a delivery to Ganedhi of industrial valves in April 2021, the value of which exceeded R860 000. Although Ganedhi had always paid on delivery, it had to make arrangements for an extended payment period in this instance. The parties agreed that payment would be made on 27 May 2021, which Ganedhi duly adhered to. But when Gripper contacted it three days later enquiring when payment would be made, it became apparent that the parties' email correspondence had been hacked and that the funds were paid into a fraudster's account.

Upon further investigation, it appeared that the fraudster - writing under the guise of Gripper's managing director and using an email address almost identical with that of Gripper's managing director - sent an email to Ganedhi and advised that its banking details had changed. The email stated further that whereas Ganedhi had always made payment into Gripper's Standard Bank account, it must now effect payment to Gripper's new account at ABSA. Ganedhi did not doubt the authenticity of the email and after requesting and receiving a bank confirmation letter – communicating via the hacked email address where the fraudster was still acting under the guise of Gripper's managing director - unknowingly made payment into the fraudster's account.

Gripper remained out of pocket and ultimately issued summons against Ganedhi for payment of the debt. Gripper contended that its systems were secure and that the fault lay with Ganedhi, having not exercised reasonable caution by telephonically checking the changed account details with Gripper. Ganedhi's primary defence was that, based on an expert's report that it had obtained, it was Gripper's email system that was hacked and that its negligence allowed the fraud to be perpetrated. Gripper disputed this contention, stating that there was no record of the alleged fraudulent email on its server. It also provided a specialist's report, supporting its allegation that its IT systems were not hacked.

HELD

- Cyber-crime is rampant, and has been for many years. Schemes to divert money - legitimately owed by a debtor to a creditor - to unauthorised bank accounts, without the knowledge of either party, are a common occurrence.
- Unsurprisingly, when this sort of event has occurred, disputes have arisen as to who should bear the risk of loss. In the March 2024 judgment in *Mosselbaai Boeredienste (Pty) Limited v OKB Motors CC*, the court dealt at length with the case law on this topic and the general principles to be extracted from the cases. In

a full bench judgment, the court recognised the general principle in our law, being 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 same approach must be applied to the facts of the present matter. Even though Ganedhi had put up an expert report which contended that it was Gripper's system that must have been hacked (which Gripper denied), the authorities referred to in *Mosselbaai* regard this as irrelevant—the courts should instead focus on the principle 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* recognised, a simple telephone call may well suffice", this court commented.
- In addition, on the facts of the present matter, there were grounds to criticise the conduct of Ganedhi, being that:
    - It is known to all business persons that make use of computer-based methods of communication and payment, that cybercrime is rampant and that care must be taken at all times to limit its impact. Ganedhi could not have been unaware of this.
    - The parties had been doing business for seven years with payments routinely made into the same Standard Bank account.
    - The amount of the invoice was significant, so much so that it gave rise to a bespoke payment agreement as opposed to the usual cash on delivery.
    - The first fraudulent email referred to a need to "update our Absa banking details with you," suggesting that Gripper had already provided Absa banking details, when this was not true.
    - Ganedhi started getting what it described as "emails requesting proof of payment" between 13 and 24 May 2021, when payment was not yet due under the payment arrangement, the inference being that the fraudster was pressurising for payment that was not yet due, which should have raised concerns given what seems to have been a co-operative business relationship.
    - The said emails appeared to have come from a different email address ("griper.co.za" and not "gripper.co.za").
- In these circumstances, the responsibility to confirm payment details, lay with Ganedhi as the debtor.

CONCLUSION

The Court ordered Ganedhi to pay the outstanding amount to Gripper.