WERKSMANS
ATTORNEYS

REGULATORY

A tale of cybersecurity blame, who bears responsibility?

18 December 2024 *5 min read*

Who is responsible for the payment of loss arising from cyber fraud, specifically when an email correspondence is intercepted by a scammer and banking details are changed? The Western Cape High Court ("**Court**") recently had the occasion to consider this question in *Gripper & Company (Pty) Ltd v Ganedhi Trading Enterprises CC* (4725/2024) [2024] ZAWCHC 352 (6 November 2024)

The facts

The parties had a relatively long relationship dealing with each other since 2014 and in October 2021, Ganedhi Trading Enterprises CC ("**Ganedhi**") placed an order to purchase valves from Gripper & Company (Pty) Ltd ("**Gripper**"). The due date for delivery was 29 April 2021 and the valves were duly delivered.

Both the invoice issued on 15 April 2021 and delivery note signed by Ganedhi contained the long-standing Standard Banking details of Gripper.

Ganedhi did not effect payment into Gripper's Standard Bank account on the due date for payment – or at all – and, consequently, Gripper never in fact received payment of the invoiced amount.

What did happen – and unbeknown to Ganedhi – on or around 24 May 2021, Ganedhi made payment of the invoiced amount into an Absa Bank account which did not belong to Gripper, but rather a sophisticated fraudster.

The sophisticated fraudster was able to intercept of gain access to the email correspondence between Ganedhi and Gripper relating to the purchase and sale of the valves, and more particularly the emails that pertained to the payment arrangement. The email from the fraudster gave new banking details and came from "*max@griper.co.za*" as opposed to the correct email address "*max@gripper.co.za*". The fraudster consequently masqueraded as Gripper's managing director, Mr. Max Hafen, and used a nearly identical email address with a minor typographical error by omitting the letter "p" in "gripper".

On 24 May 2021, Ganedhi proceeded to make payment into the Absa Bank account – without contacting Gripper to confirm the change of longstanding banking details – having been apparently satisfied that the emails received were legitimate. Three days later, Gripper sent an email requesting its payment whereafter it was discovered that the payment had been made to an unauthorised account and that Gripper had not in fact changed its banking details from Standard Bank to Absa Bank.

The arguments of the parties

Ganedhi argued that Gripper's system must have been hacked by the fraudster for which Gripper is to blame. To this end, Ganedhi put up an expert report to say, amongst others, that there was no record of its own systems being compromised. The import of this was that it was negligence on the part of Gripper that allowed the fraud to be perpetrated and that Gripper should be estopped from claiming payment of the purchase price because Ganedhi relied to its detriment on a representation emanating from Gripper that payment should be made into the incorrect bank account.

Gripper simply argued that its email/server security had never been compromised and 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.

The findings of the court

The court, as a point of departure, noted that –

"*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.*"

The Court examined principles emanating from South African case law and noted specifically 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 Court referred to the decision of *Mannesman Demag (Pty) Limited v Romatex* 1988 (4) SA 383 where 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; and
- 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.

The Court consequently found that the same approach adopted above is applicable to the present dispute between the parties notwithstanding the parties' assertions that the other's systems were compromised and consequent cause of the fraud. The Court held that it is incumbent on the risk-bearing debtor (in this case, Ganedhi), in making payment, to ensure that it achieves this goal and that this does not require a great deal of effort as "*a simple telephone call may well suffice*".

Ultimately, the Court found in favour of Gribber holding that it is entitled to payment of the purchase price in accordance with the sale agreement.

Comment and conclusion

The judgement of the Court highlights the importance of exercising vigilance when making payment. Debtors must take responsibility and "*seek out their creditor*" when making payment. It would seem that blaming will not work and cyber fraud is not an excuse.

Given the findings of the Court, cybersecurity risk in the context of electronic payments will ultimately fall on the debtor and it is important for debtors to take note of their responsibilities and act accordingly even if this means making an extra telephone call.

"*The only truly secure system is one that is powered off, cast in a block of concrete and sealed in a lead-lined room with armed guards – and even then I have my doubts.*"

Gene Spafford, American Professor and Computer Science Researcher

Ahmore Burger-Smidt

Head of Regulatory

View Profile

Dale Adams