# E-Mail Interception – Who Bears the Consequences?

While enjoying the simplicity and ease of our digital lifestyles, one should be aware of all the fraudulent opportunities that come with this. Electronic transactions and e-mail interception are some of the most notorious scams that we encounter these days, and the court's interpretation of who bears the brunt in these cases is noteworthy.

Cybercrime includes payments made into an incorrect, fraudulent bank account, where the innocent party was induced to make the payment into the fraudster's account instead of the beneficiary's bank account. It is also called "third-party impersonation fraud," more commonly referred to as business email compromise scams, and is usually committed by means of electronic email correspondence.

The courts seem to be applying a common sense approach and placing more of a burden on larger entities and certain industries than on the consumer.

In the recent judgment of *Mosselbaai Boeredienste (Pty) Ltd t/a Mosselbaai Toyota v OKB Motors CC t/a Bultfontein Toyota (A43/2021) [2021] ZAFSHC 286*, fraudsters successfully targeted a motor sale transaction.

Bultfontein Toyota ("the purchaser") bought a vehicle from *Mosselbaai Toyota ("the seller")* and paid the purchase price into an incorrect bank account after the seller's e-mail, attaching its banking details, was intercepted by fraudsters and the banking details changed. The purchaser then paid the purchase price into the fraudster's bank account instead of the seller's account.

The court found that the purchaser was aware of a circular of Toyota SA which had drawn its attention to similar cybercrime activities, but it still failed to verify the seller's banking details, which could easily have been done by means of a phone call, in which event it would have realised that the banking details received were incorrect and fraudulent. The court ordered that the purchaser must repay the purchase price of the vehicle to the seller.

Like in many other recent judgments, the court stressed the importance of consumer-appropriate warnings. If the court found that the business did not give

sufficient warnings to the consumer of the possibility of fraud, the business had to bear the financial consequences.

Members of the public and businesses alike should be extremely vigilant when making payments, particularly banking details received **by email** and must always verify the authenticity of a bank account before payment is made. The verification process relating to bank details received by electronic email correspondence should at least include the following:

- The bank details of the payee are to be verified through a trustworthy verification process offered by all of the major banks.
- The email address of the payee must be objectively verified.
- The payee must be verified telephonically by means of his/her correct telephone number.

Martin Bezuidenhout, Van Velden Duffey Inc