ILLEGAL SIM SWAPS: ARE YOU A VICTIM OF BANK FRAUD?

Category: Commercial Law,Privacy Law, Infosec, and POPIA
written by Manyani Maseko | March 6, 2017

With the advent of modern technology taking the forefront in today's society, more people are inclined to make use of electronic payment systems such as internet banking[1]. Although internet banking does appear to be more convenient, it is not without fault as was experienced by Monica Kruger. During 2016, Kruger, a business woman from George was defrauded of an amount of approximately R2 million pursuant to making use of internet banking due to a fraudulent SIM swap[2].

In Kruger's application to the Gauteng Local Division, Johannesburg, she informed the court that pursuant to being robbed, millions were transferred to a Capitec bank account from her ABSA accounts in 80 deposits of R25,000.00 each. Not only was her money unusually transferred but she received no notifications from her bank about the transfers or the adding of an unknown beneficiary to her account as a result of this illegal SIM swap. In essence, Kruger did not authorise any SIM swap in her name. The irony being that Kruger was unaware of the fraud at the time of its occurrence and merely contacted her network provider, Vodacom, as she was unable to connect her phone to the network. Vodacom thereafter informed her to immediately contact ABSA and request that they freeze all her bank accounts, as they suspected fraud.

On establishing the true gravity of the fraudulent activities, Kruger (in her own personal capacity) and ABSA began the process of conducting investigations inclusive of a full on forensic audit. While Kruger was of the view that fault squarely rested with ABSA and that they should refund her money due to the fraudulent suspicious activities, ABSA had taken the opposite view stating that Kruger must have compromised her account in some way.

Considering Kruger's situation which essentially resulted in the all parties playing the "blame" game, as neither Vodacom nor ABSA were willing to accept responsibility for the misappropriation of Kruger's funds, it is important to be weary of fraud especially during the holidays or festive seasons. There are many ways in which you can protect yourself from fraudulent activities associated with internet banking; however, I have narrowed it down to 4 important considerations, namely:

- *Be very mindful of the password you select!!* Fraudsters engaged with phishing[3] activities have developed ingenious methods to source people's passwords by either guessing them or

creating fake websites where usernames and passwords are entered by unsuspecting individuals. Once these details have been obtained, phishers are capable of doing an array of activities such as: changing your details in order to block you from your account, accessing your personal information, hacking into your other accounts etc. It is therefore advisable for you to come up with creative password patterns which are not easily identifiable and with regards to the security verification questions, these should be unique to each application or website that you use.

- *Don't be an easy target!!* When receiving random or suspicious emails, it is crucial to completely ignored and disposed of such emails. These may be emails informing you of large sums of money being deposited into your account or advising you to change/update your email or emails simply from accounts with weird names and domain names.
- *Report!!* If you suspect any suspicious activities, be sure to report them to the appropriate authorities so that they may be countered sooner rather than later.
- *Just ask!!* If you are unsure of the source of an email Eg an email from SARS, your bank or any other provider you usually engage with, contact them on their Customer Care line to verify the authenticity of the alleged email sent to you.

[1] This is also known as online banking, e-banking or virtual banking.

[2] SIM swap refers to process of exchanging an old, damaged or stolen SIM card with a new SIM card. By doing so, the old SIM card is deleted from a network while the new SIM car is linked to your cell phone number.

[3] This refers to the fraudulent practice of sending emails from purported reputable companies in order to induce individuals to reveal personal information such as passwords, banking details, personal information etc.