THE “NEDBANK BREACH”: WHAT IF THE PROTECTION OF PERSONAL INFORMATION ACT WAS IN FORCE?

Category: Commercial Law,Privacy Law, Infosec, and POPIA,Technology Law
written by Lucien Pierce | March 11, 2020

Nedbank has handled the data breach its direct marketing services supplier – Computer Facilities (Pty) Ltd – suffered last week, reasonably well. This is evident from how they appear to have investigated it, to their frank, factual and informative press release. Apart from some reputational damage and a few million rand in forensics, legal and public relations agency fees, Nedbank should come out relatively unscathed.

Of course, if the Protection of Personal Information Act (“POPIA”) was in force, matters would be a little more serious. As much as the press release appears to direct blame at the service provider (and it certainly appears that the service provider was at fault), the reality is that if POPIA was in force, Nedbank would have almost no escape from civil liability for any damages its clients suffer. POPIA makes someone like Nedbank *strictly liable* even though the breach may have been caused by its service provider. There are only four defences that Nedbank could raise: that the breach was caused by an act of God; its customers consented to the breach; its customers caused the breach; it was not reasonably practical to avoid the breach; or the Information Regulator had granted it permission to allow the breach. It’s not likely that Nedbank can use any of these defences so, if POPIA was fully effective, the only question would be how much Nedbank would pay in damages, not if it would have to.

Civil damages are, of course, not the only financial penalties that Nedbank would be liable for. If the Information Regulator, after investigating, decides that Nedbank has indeed committed an offence, it can decide what administrative fine to levy on Nedbank. This administrative fine may not exceed R10 million. Nedbank would have 30 days to decide whether to pay the fine or elect to be put on trial in court. If Nedbank had to contest the fine, the Information Regulator would then refer the offence to the South African Police Service to commence a criminal prosecution in court.

Why, you may ask, would the Information Regulator prosecute Nedbank and not the service provider (after all, it was the service provider who caused the breach). The reason for this is that POPIA requires a person in Nedbank’s position to ensure that its service providers take appropriate, reasonable technical and organisational measures to prevent breaches of this nature. Nedbank had a duty to ensure that these measures were in place and if the breach happened because it hadn’t done

proper checks, then it becomes responsible for the breach happening. If POPIA comes into force on 1 April 2020, as the Information Regulator hopes, everyone that needs to comply with POPIA will be given one year to get their houses in order, before the fines and prosecutions start. You had best get ready, I’m sure Nedbank will.