THE R300 MILLION JAPANESE SOUTH AFRICAN CREDIT CARD HEIST: THE LEGAL IMPLICATIONS FOR BOTH BANKS AND CUSTOMERS!

Category: Commercial Law,Privacy Law, Infosec, and POPIA
written by Lucien Pierce | May 26, 2016

I AM listening to the Alphaville song Big in Japan as I write this. It has a laid back beat: I can almost visualise the bunch of “hackers” coolly, calmly and collectedly sidling up to hundreds of ATMs across Japan and simultaneously withdrawing wads of cash.

The technique used in the R300m heist involving credit cards issued by Standard Bank is not new. In 2012 a group of hackers across the globe co-ordinated about 7,500 ATM withdrawals using cloned bank cards. They netted about R702m. Also in 2012, the Payments Association of SA saw the bank card details of several hundred thousand customers being compromised. Other recent bank hacks have included a R1.2bn hack at the Bangladesh Bank and the theft of the information of 80-million customers of JPMorgan.

While the Japanese heist details are still sketchy, all banks should be taking this heist very seriously. There are a number of factors that Standard Bank et al (meaning Standard Bank and others for those of you who didn’t have Latin imposed on you), need to consider.

Standard Bank is not alone in having experienced a major data breach. Organisations such as Sony, Lockheed, Citigroup and, the International Monetary Fund all experienced major data breaches in the past few years, seeing them all taking rapid action to counter major reputational damage.

Each of these organisations had to publicise these breaches and had to manage and repair the damage done to their reputations. It isn’t only reputational damage that is suffered, but each most likely suffered some sort of financial loss. Each organisation would certainly have incurred expenditure on public relations, legal advisers and organisational changes designed to mitigate and repair the reputational damage.

Standard Bank will also need to consider the Protection of Personal Information Act (Popi), even though it is not yet fully effective. Popi, once it becomes fully effective, will oblige organisations such as Standard Bank to secure the integrity of personal information in its possession or under its control, by taking appropriate, reasonable technical and organisational measures to prevent the loss of

personal information and unlawful access to personal information. In doing so, it will be compelled to implement generally accepted information security practices and procedures available at the time.

Popi also requires organisations such as Standard Bank to notify customers of the loss or exposure of personal information. Although Popi is not fully effective, Standard Bank should probably follow a prudent approach and, either directly or through some other method such as its website, notify its affected customers of the Japanese credit card hack.

It is important to remember that failing to comply with Popi (once it is fully effective) will make those who fail to do so liable to a fine or imprisonment not exceeding 10-years, or both a fine and imprisonment.

If Standard Bank has branches in other jurisdictions where data protection laws are in place, it may also have to seriously consider whether there is any requirement for it to disclose the credit card hack to data protection and related regulators in those jurisdictions. By way of example, in 2010 the UK Financial Services Authority fined Zurich Insurance £2,27m after Zurich Insurance SA lost a back-up disk containing the information of 46,000 customers.

The King III Code Of Governance Principles for SA, 2009 (the King III code) will certainly apply to Standard Bank. Paragraphs 32 and 33 of chapter five, the governance of information technology, deal crisply with the legal aspects of information technology risk management. They state: “IT legal risk arises from the possession, ownership and operational use of technology that may result in the company becoming a party to legal proceedings. When considering the company’s compliance with applicable laws, rules, codes and standards, the board should ensure that IT related laws, rules, codes and standards are considered. Companies must comply with applicable IT laws and consider adherence to IT rules, codes and standards, guidelines and leading practices.”

A person adjudicating any complaint regarding the credit card hack will simply ask whether Standard Bank or its service providers complied with IT rules, codes and standards, guidelines and leading practices. If they did not, then there may be adverse consequences for the guilty parties. In the Adobe Systems, case, even its indemnity clause, which stated clearly that “despite our efforts, no security controls are 100% effective and Adobe cannot ensure or warrant the security of your personal information”, was not regarded as sufficient to prevent claims by customers from proceeding against it.

Interestingly, when the US retailer Target was hacked, credit card issuing banks also litigated against Target. They based their claim on their projected costs to reissue cards and take action to prevent any further fraud. So, if the hacked credit cards were somehow cloned as a result of a retailer or a service provider of Standard Bank, it may be able to take legal action against them.

In essence Standard Bank and its service providers need to ensure that they have prepared themselves for more stringent data protection laws and regulations. They need to also go a step further by ensuring that in contracting with third party service providers, those third party service providers comply with the requirements of relevant data protection laws, recommendations and codes.

I am going to have Alphaville’s Big in Japan stuck in my head for the rest of the day. I am sure Standard Bank will have its big Japan hack stuck in its head for a little longer than that.

Originally published in the 23 May 2016 online edition of Business Day[/fusion_text]