TransUnion Data Breach - Information Regulators Dissatisfaction

By Sashin Naidoo - Senior Associate at JR Attorneys Inc.

On 18 March 2022 TransUnion, a self-identified "*global information and insights company*"[1] and credit bureau, announced a security compromise of its IT systems through an online hack which has since seen a compromise of approximately 4 terabytes (54 million records) of personal date/information as well as a demand for payment of a ransom to the extent of R220 million.[2]

According to the credit bureau, forensic investigations are already under way with a suspension of access for those of its compromised customers together with consultations with cyber and forensic experts, although this would be of little comfort to those of us whose data and personal information have now been placed in the hands of nefarious individuals.[3]

TransUnion has further undertaken to provide free "*identity protection products*" to all of those effected by the breach and/or security compromise and notify those individuals whose data has been compromised as and when its investigation, in collaboration with the SAPS, unfolds.[4]

On 19 March 2022 our Information Regulator, custodian of the Protection of Information Act, 4 of 2013 ("POPIA"), released a statement to the public informing us that the office of the Regulator had met with the CEO of TransUnion to discuss the mass scale security comprise of credit consumer data. The Regulator stressed the importance of "*the need for affected data subjects to be informed early about any security compromise on their personal information to be able to take the necessary preventative action against wrongful use of their personal information.*"[5]

In recognising the enormity of the impact which the security compromise could have on data subjects should TransUnion fail to apprise all affected data subjects of this security compromise, the Regulator instructed TransUnion to submit specific details to its office regarding the number of affected parties as well as and their plan to notify data subjects in terms of Section 22 of POPIA.[6]

TransUnion was given until the 22nd of March 2022 to provide the following information to the regulator:

- the date that the security compromise occurred;
- the cause of the security compromise;
- details of investigations into the security compromise;
- the extent and materiality of the security compromise;
- interim measures put in place to prevent a recurrence of the security compromise; and
- security measures that TransUnion Credit Bureau has put in place to prevent a recurrence of the security compromise.[7]

This information was to be used by the Information Regulator to assist in assessing and instituting further investigations by the Regulator in the pursuit of its mandate prescribed under POPIA.

Section 22 of POPIA reads as follows:

- *"Where there are reasonable grounds to believe that the personal information of a data subject has been accessed or acquired by any unauthorised person, the **responsible party must notify**—*
    1. *the Regulator; and*
    2. ***subject to subsection (3)**, the data subject, unless the identity of such data subject cannot be established. . .*
- *The notification to a data subject referred to in subsection (1) must be **in writing and communicated to the data subject in at least one of the following ways**:*
    1. *Mailed to the data subject's last known physical or postal address;*
    2. *sent by e-mail to the data subject's last known e-mail address;*
    3. *placed in a prominent position on the website of the responsible party;*
    4. *published in the news media; or*

e) as may be directed by the Regulator.

- *The notification referred to in subsection (1) **must provide sufficient information to allow the data subject to take protective measures against the potential consequences of the compromise**, including—*
    1. *a **description of the possible consequences** of the security compromise;*

b) a description of the measures that the *responsible party intends to take or has taken to address the security compromise;*

c) a recommendation with regard to the measures to be taken by the data subject to mitigate the possible adverse effects of the security

compromise; and

1. *if known to the responsible party, the **identity of the unauthorised person** who may have accessed or acquired the personal information.*

(6) The Regulator may direct a responsible party to publicise, in any manner specified, the fact of any compromise to the integrity or confidentiality of personal information, if the Regulator has reasonable grounds to believe that such publicity would protect a data subject who may be affected by the compromise."[8] [emphasis added]

It is clear from the above-mentioned provisions under POPIA that the Information Regulator has been afforded wide discretionary powers in order to ensure that those who have been affected any compromises in relation to the security of their personal information, entrusted to responsible parties, are adequately notified when such compromises occur.

It is further evident that this notice serves to enable a data subject to mitigate any potential adverse impacts associated with the breach and the unauthorised use of their personal information.

On 25 March 2022 the Information Regulator released a media statement wherein it voiced its discontent with the measures and responses adopted by TransUnion. The Information Regulator. The Regulator took issue, chiefly, with the notification which was submitted by TransUnion as required under Section 22(1) of POPIA.[9]

In accordance with Sections 22(4)(e) and 22(6) the Regulator has now directed TransUnion to provide it with the following outstanding information:

TransUnion was further directed to "*use all radio stations, broadcasting in each official language, publish in all newspapers and drive communication on various social media platforms to provide sufficient notification to data subjects about this security compromises*."[10]

8 Section 22 (1), (4), (5) & (6) of POPIA, No. 4 of 2013.

- Office of the Information Regulator (South Africa). "*MEDIA STATEMENT: THE REGULATOR IS DISSATISFIED WITH TRANSUNION'S RESPONSE, AND IT INITIATES AN ASSESSMENT ON THE SECURITY COMPROMISE*" (25 MARCH 2022).

Interestingly, despite seemingly having the election to use one of the means of communication under Section 22(4) of POPIA, the credit bureau was directed to use all of the methods established thereunder and further directed to use of radio and social media platforms in all official languages as a means by which to affect its notice in terms of Section 22(1) of POPIA.

The reasoning behind this direction is found in the nature of the personal information which has been compromised, the contents of the credit bureau's security compromise notification and the extent and severity of the security compromise.

The Information Regulator undoubtedly considered the fact that the credit bureau holds, and is responsible for, the personal information of everyday South Africans, some of whom may only have access to limited means of communication for the requisite notification to be affected.

The means of communication directed to be utilised by the credit bureau are broad and will surely incur a great expense of time, effort, and money, however, it is clear from the Information Regulators direction that this was not a consideration. It appears that the primary focus is to ensure adequate notification to all data subjects impacted by the security compromise as a main concern.

Section 22 is further silent on whether such directive must consider the ability of the responsible party to give effect to any directive issued by the Regulator or whether such directive must be reasonably practicable.

It would appear then that the Regulator may have acted within the ambit of the powers accorded to it under Section 22 of POPIA, notwithstanding any review of such administrative decision which may find its way to our courts.

This then serves as a caution to all those who process the personal information of data subjects, more specifically those who process "big data". The cost of a security compromise under POPIA may be a harsh cost to bear, but the rights of a date subject remain the key priority of our regulatory authority.

This story has not been finalised and is still unfolding and we await any further action by both the Information Regulator and TransUnion in this regard.

Sashin Naidoo (BA Law, LLB) is a Senior Associate at JR Attorneys Inc.