POPIA Data Subject Notification

1. First Impression Labels ("**we**"/ "**our**") would like to inform our customers, business partners, suppliers and employees ("**data subjects**") that we recently suffered a third party cyber incident affecting some of our IT systems which are hosted on Hirt & Carter Group[1]("**Hirt & Carter**") IT systems, where an unauthorised third party accessed certain of Hirt & Carter systems, deployed malicious software, resulting in a loss of access to some of our data and IT systems.

2. This notice serves as notification, in terms of section 22 of the Protection of Personal Information Act, No. 4 of 2013 ("**POPIA**"), to our data subjects.

3. We have, with Hirt & Carter's assistance, immediately taken the necessary steps to protect our data subjects, to address the cyber incident and to minimise the possible risks and impact on our operations as far as possible. This includes, among other things, engaging cyber security and forensic experts to assist in conducting a comprehensive forensic investigation to determine the scope of the incident and take prompt action to secure the impacted systems, isolating and disconnecting the affected systems from the internet, initiating dark web monitoring to identify any potential data leaks and scanning critical systems before bringing those servers online. Together with Hirt & Carter, we have also implemented additional security measures designed to enhance the security of our networks, systems and data and protect against data loss and any future unauthorised access to our data and systems. Hirt & Carter will continuously improve, evaluate and implement additional available steps to further refine the security of its environment which is utilised for hosting our data and systems.

4. As the investigation is ongoing, at this stage we do not know the extent to which any personal information may have been accessed nor the identity of the perpetrator who may have acquired the data containing personal information. For individuals, the data that may have been accessed includes personal details such as names, email addresses, telephone numbers, physical addresses, gender, race, nationality and ID or passport numbers. For businesses, possible categories of information that may have been accessed include company addresses, VAT and BEE documents, telephone numbers, contracts with us and work products as well as the contact details, and in limited instances, ID numbers of company representatives.

5. We are working diligently to restore full functionality to our systems and data so that all areas of the organisation are fully operational as soon as possible.

6. Out of an abundance of caution, we are notifying all our data subjects of this incident in order to ensure that they are able to take the necessary precautions to avoid any potential adverse consequences from this incident and to be vigilant on alert for any possible scams or fraudulent activity

7. Although there is no evidence that any personal information has or will be misused in this case, we encourage data subjects to safeguard their personal information by following these security measures:

    a. data subjects can register for a free Protective Registration listing with Southern Africa Fraud Prevention Service (SAFPS) to help protect them against the risks of identity compromise

---

[1] The Hirt & Carter group includes all of its subsidiaries, affiliates, business partners, trade divisions, including operators such as Forge Marketing Technologies (Pty) Ltd; Hirt & Carter South Africa (Pty) Ltd ; Hirt & Carter Group (Pty) Ltd; Hirt & Carter Software Solutions (Pty) Ltd; Hive Connect (Pty) Ltd; Quickcut Pre Press Network SA (Pty) Ltd; Shift Promo Logistics (Pty) Ltd; Sku (Pty) Ltd; Paton Tupper (Pty) Ltd; and Mainstreet 505 (Pty) Ltd.

(https://www.safps.org.za/Home/OurServices_ApplyProtectiveRegistration);

b. remain vigilant against any suspected unauthorised use of their personal information;
c. be cautious of any unusual or unsolicited communications that ask for personal information or passwords or refer to a web page asking for personal information, in which case steps should be taken to check the true identity of the requester, as fraudsters often pose as officials from trusted authorities like the police or banks.
d. Change passwords regularly and never share these with anyone else.
e. Avoid clicking on links or downloading attachments from suspicious emails.

8. For further information and assistance, please contact:

Riaan Viviers
Information Officer
popiqueries@fil.co.za