Website Notification

8 July 2024

Data subject notification of a security incident in terms of Section 22 of the Protection of Personal Information Act, 4 of 2013

Dear Valued Hirt & Carter Group Stakeholder

This notice serves to inform you about a matter regarding the security of your personal information, the measures we have taken in response, and to provide suggestions on proactive steps you may consider taking.

Regrettably, Hirt & Carter Group[1] experienced a cyber incident which may have exposed certain 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 address, company VAT and BEE documents, telephone numbers, banking details, contracts with us and work products as well as the contact details, and in limited instances, ID numbers of company representatives.

We have no evidence of any misuse of the information accessed and will continue to monitor the situation. We advise you to remain vigilant and be cautious of any unsolicited communications that ask for your personal information or refer you to a web page asking for personal information.

What happened?
On 05 July 2024, we discovered that an unauthorised third party accessed some Hirt & Carter systems, deployed malicious software and therefore had access to certain data, affecting critical servers. As is common with attacks of this nature, it is not possible to identify the individuals of the group responsible for this malicious conduct.

What steps have we taken?
As soon as we became aware of the incident, we appointed leading external cybersecurity experts and forensics firms to assist our IT teams in conducting a comprehensive forensic investigation to determine the scope of the incident and take prompt action to secure our systems.

Our primary concern has been to mitigate the impact of the incident and to implement measures to minimise business interruption to the extent possible. With the assistance of cybersecurity experts, all affected systems were isolated and disconnected from the internet. Further, dark web monitoring was initiated to identify any potential data leaks. Our cybersecurity experts advised the need for a systematic approach to restore operations, including prioritising of critical systems and ensuring scanning before bringing servers online and continuing with our operations.
We have notified the Information Regulator and will cooperate with all relevant authorities as needed.

To prevent a similar occurrence in future, we are implementing numerous measures designed to enhance the security and provide increased visibility of our network, systems and data. Hirt & Carter is committed to continuous improvement and will continue to evaluate and implement additional available steps to further refine the security of our environment.

What steps can you take?
Although there is no evidence that any information has or will be misused in this case, we encourage our stakeholders to safeguard their personal information by following these security measures:

To mitigate any fraudulent consequences, you can place a fraud alert on your credit report at any of the major credit bureaus.

You can register for a free Protective Registration listing with Southern Africa Fraud Prevention Service (SAFPS) to help protect you against the risks of identity compromise (https://www.safps.org.za/Home/OurServices_ApplyProtectiveRegistration).

Remain vigilant against any suspected unauthorised use of your personal information.
Be cautious of any unsolicited communications that ask for your personal information or refer you to a web page asking for personal information: fraudsters often pose as officials from trusted authorities like the police or banks.

Change your passwords regularly and never share these with anyone else.
Avoid clicking on links or downloading attachments from suspicious emails.

We prioritise the trust and privacy of our stakeholders. We take this incident extremely seriously and have dedicated our resources to mitigating the impact. We are committed to learning from this incident to further enhance our security measures.

If you have any questions or require further assistance, please get in touch with us at popiqueries@hcg.one

Sincerely
Hirt & Carter
Yasteel Kuseeal
Information Officer

[1] The Hirt & Carter Group includes all of its subsidiaries, affiliates, business partners, trade divisions and employees, including Operators such as Forge Marketing Technologies (Pty) Ltd; Hirt & Carter (Pty) Ltd ; Hirt & Carter Group (Pty) Ltd; Hirt & Carter Software Solutions (Pty) Ltd; Quickcut Pre Press Network SA (Pty) Ltd; Shift Promo Logistics (Pty) Ltd; Sku (Pty) Ltd; HCSA Labels (Pty) Ltd; and Paton Tupper (Pty) Ltd.