ᐃᓄᐃᑦ
Air Inuit

NOTICE OF CYBERSECURITY INCIDENT AT FORMER SERVICE PROVIDER - SITA

Air Inuit was notified by a former third-party service provider, SITA Passenger Service System (US) Inc. (**SITA**), that it had experienced a cyber-attack in February 2021 where data was accessed and removed. This incident affected many of its clients around the world, including Air Inuit. SITA has advised that certain Air Inuit client data appears to have been compromised in the attack.

It is important to note that Air Inuit's IT infrastructure was not involved in the cybersecurity incident.

SITA operates passenger processing systems. In the past, we had used SITA to process and manage ticketing information. Once we were advised of the attack, we immediately launched a comprehensive investigation to review the compromised data.

What Information Was Involved

SITA has advised that the following personal information of our clients contained on SITA's servers was copied and removed a result of the cyber-attack::

- For Frequent Flyers, the personal information potentially included: name, address, phone number, gender, email address, and date of birth.

- For Horizon DCS members, the personal information potentially included: name, date of birth, gender and flight information.

- For passengers, the personal information potentially included: name of passenger, credit card number, date of expiry and travel information including the names of those who travelled on the under the same reservation. **It is important to note that CVV/CVC numbers were not provided to SITA and therefore were not exposed in this incident**. SITA has notified the following credit card issuers of the incident: Visa, Mastercard, American Express, Discover/Diners and JCB.

What We Are Doing

While this incident was not directed at Air Inuit, we are nonetheless further strengthening our data security measures and will continuously look to make improvements.

What You Can Do

We encourage you to be vigilant and to mitigate any potential harm by taking the following steps to protect yourself:

- Monitor your financial accounts. If you see anything you do not understand or that looks suspicious, or if you suspect that any fraudulent transactions have taken place on a credit or debit card, you should call your bank.

- Change and create strong passwords for any online accounts, in particular those that use or relate to your national security number.

- Be cautious of any unsolicited communications of whatever form (phone call, email, etc.) that ask for your personal information or refer you to a Web page asking for personal information.

- Avoid clicking on links or downloading attachments from suspicious emails.

- Report an incident to the appropriate authorities if you notice any suspicious activity.

Tips and resources for protecting your identity are available at

https://www.priv.gc.ca/en/privacy-topics/identities/identity-theft/guide_idt/.

For More Information

We sincerely regret any concerns or inconvenience this incident may have caused.

Should you have any concerns or questions, please do not hesitate to contact our dedicated resource by phone at 1-833-820-1419 (Mon-Fri, 9h-4h) or by email at cyber-incident_SITA@airinuit.com. Please leave a message and allow us to call you back if our resource is serving another customer.

Sincerely,

Marie-Noëlle Pronovost
Directrice, Opérations commerciales