IGLOO

May 20, 2022

Dear «Employee_Name_Last_Suffix_First_MI»:

The security and confidentiality of our employees' information is one of Igloo's top priorities. We monitor our network and information technology systems for attacks and intrusions on a continuous basis.

Further to this recent ITI post, we are writing to alert you of an incident that potentially resulted in limited access to certain personal information in our possession.

On May 12, 2022, we learned that an unidentified individual accessed a password protected corporate e-mail account. At this point, it appears that the intruder's primary motivation was fraudulent invoice manipulation: a practice wherein the intruder seeks to divert funds payable to Igloo from a client to the intruder's own account.

We took immediate steps upon learning of this incident. All passwords and other login credentials were changed for the affected e-mail account. All Igloo employees have been requested to change their passwords. We undertook an investigation to identify the full nature of the intrusion and retained a leading cyber-security expert to assist us in our investigation. So far, our investigation suggests that the intrusion was limited to one e-mail account (the "Compromised Account"), and we can advise that the intruder can no longer access the Compromised Account.

During our investigation, we determined that the Compromised Account likely contained the following personal information about some of Igloo's employees:

- Name
- Home Address
- Hire Date
- Bank Account Information
- Social Insurance Number
- Personal E-Mail Address
- Sales Commission Amounts

To our knowledge to date, no other financial, banking or personal information such as PINs or credit card information was contained in the compromised account.

To be clear, there is no evidence indicating that the intruder actually viewed any records containing your personal information, nor is there any evidence indicating that the intruder downloaded or otherwise copied any of your information. Moreover, there is no indication that the intruder specifically targeted you in this incident.

Nonetheless, we take this incident extremely seriously. Accordingly, while there is no evidence suggesting that your information has been compromised, we are informing you so that you may take any protective steps you deem necessary.

As a best practice, we recommend that you monitor your e-mail for messages that seem suspicious, even if they appear to come from someone you know. To this end, please keep the following tips in mind:

- Do not click on links unless you have confirmed they are legitimate.
- Hover over the e-mail address to see and verify the exact e-mail address (rather than just the name used).
- If in doubt, send an independent e-mail (i.e. do not click "reply") to the sender to confirm the contents of the original e-mail.
- Alternatively, call the sender to confirm they sent the e-mail.

In addition, **we are providing you with one year of free credit monitoring services and identity protection services** from TransUnion (for Canadian employees) or from CyberScout (for U.S. employees) as more fully described below.

No payment by you is required. It will only take 5 minutes for you to sign up. No credit card is required. You will need your need your social insurance number (for Canadian employees), date of birth, contact information, and phone number.

Please note that to obtain the benefit of these services, you must activate your code by **September 30, 2022.**

We take the safety and security of your personal information very seriously. We sincerely apologize for any inconvenience and we want you to know that we are here to assist you. Should you have any further questions or concerns regarding this incident, please contact the undersigned.

Sincerely,

Michael Misener
Senior Legal Counsel
mmisener@igloosoftware.com
cell: 519-574-3518

*****

IGLOO

Activation Code: «ACTIVATION_CODE»

We have retained the assistance of CyberScout, a company specializing in fraud assistance and remediation services.

Through CyberScout, we have arranged a **12 month subscription** to Credit Monitoring services*, at no cost to you. CyberScout has been retained to help you with any questions or problems you may encounter, including assisting you with obtaining a credit report and placing fraud alerts.

We encourage you to take advantage of this service and help protect your identity. To activate your service, please visit:

https://www.myidmanager.com

You will be prompted to enter the following activation code:

«Activation_Code»

Please ensure that you redeem your activation code before 7/31/2022 to take advantage of the service.

Upon your completion of the enrollment process, you will have access to the following features:

- Access to a credit report with credit score. A credit report is a snapshot of a consumer's financial history and primary tool leveraged for determining credit-related identity theft or fraud.
- Credit monitoring alerts with email notifications to key changes on a consumer's credit file. In today's virtual world, credit alerts are a powerful tool to protect against identity theft, enable quick action against potentially fraudulent activity, and provide overall confidence to potentially impacted consumers.
- Dark Web Monitoring to provide monitoring of surface, social, deep, and dark websites for potentially exposed personal, identity and financial information in order to help protect consumers against identity theft.
- Identity theft insurance of up to $1,000,000 in coverage to protect against potential damages related to identity theft and fraud
- Assistance with reading and interpreting credit reports for any possible fraud indicators.
- Assistance with answering any questions individuals may have about fraud.

Should you have any questions regarding the CyberScout solution, have difficulty enrolling, or require additional support, please contact CyberScout at 1-800-405-6108 from Monday to Friday 8:00 am – 8:00 pm EST, excluding holidays.

* Services marked with an "*" require an internet connection and e-mail account and may not be available to minors under the age of 18 years of age. Please note that when signing up for monitoring services, you may be asked to verify personal information for your own protection to confirm your identity.