

Gerry Gill
Dolden Wallace Folick LLP
14th Floor—20 Adelaide
Street East
Toronto, ON
Canada/M5C 2T6

08/01/2022

Attorney General Brian Frosh
Office of the Attorney General
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202

Dear Attorney General Frosh:

Pursuant to Md. Code Com Law §14-3501 et seq., I am writing to notify you of a data security incident involving one Maryland resident. I am reporting on behalf of my law firm's client, who experienced the incident. The impacted individual was an employee of the client and has been notified already because the client was acting with all due haste.

The client's name and address are as follows:

- Igloo Inc.
55 King St W, Suite 200
Kitchener, Ontario
Canada/N2G 4W1

The identity of the person responsible for the incident is unknown.

NATURE OF THE INCIDENT

On or about April 14, 2022, an unknown individual accessed a password protected email account via a phishing email. Despite the implementation of multi-factor authentication ("MFA"), the threat actor was able to obtain login credentials. The threat actor used the login credentials at the same time as the employee and was granted access when the employee approved the MFA push notification. The threat actor did not gain access to any portion of the organization network or IT systems besides the single one-email account. Any personal information contained within the email account was limited to employee information. Specifically, the personal information may include:

- First Name
- Last Name
- Date of Birth
- Personal Email Addresses
- Bank Account Information

- Home Address
- Social Security Number/Social Insurance Number

The data was in electronic form. There is no evidence of data exfiltration. Further, and based on the preceding account of how the incident was discovered, it appears the threat actor's primary motivation was invoice manipulation and the diversion of client payments. However, it is possible the threat actor had the opportunity to review information contained within the email account.

Discovery of the incident occurred around May 12, 2022, when Igloo Inc. realized a client had received a request for payment from the threat actor. The threat actor had created a fake domain to impersonate Igloo Inc. and used phishing emails in an attempt to divert the client's funds to the threat actor. Accordingly, it is possible the threat actor could have reviewed or accessed an email which contained personal information about an Igloo Inc. employee to carry out the attempted scam. The incident ended May 12, 2022.

We are not aware of any resulting identity theft, fraud, or financial losses arising from this incident.

NUMBER OF RESIDENTS AFFECTED

Around 170 individuals were possibly affected by the incident. This includes one resident of Maryland. Affected individuals were notified via email on May 20, 2022. A copy of this notice is attached hereto. As soon as possible, Igloo will send a supplemental notification to the affected Maryland resident providing the following additional information as required by statute:

- Contact information for the business making the notification, including the address, telephone number, and toll-free number if one is maintained;
- The toll-free telephone numbers and addresses and web site addresses for the Federal Trade Commission and the Office of the Attorney General; and
- A statement that the individual can obtain information from these sources about the steps one can take to avoid identity theft

STEPS TAKEN IN RELATION TO THE INCIDENT

All affected individuals were notified of the incident and advised to exercise caution regarding responding to emails requesting information. Individuals were also reminded to implement safe practices and preventative strategies regarding email usage. Igloo Inc. also notified its clients in efforts to alert them of possible phishing attempts.

Attempts to further limit the risk of a similar event from reoccurring include the implementation of regular employee training addressing email and data security best practices. Additionally, Igloo Inc. has strengthened existing MFA authentication by incorporating a geographical component to the push notification. Igloo Inc. has also retained a cyber-security expert to provide recommendations for its system and will work to implement such recommendations. Expert recommendations included the continued use of

robust anti-virus software and implementations of a third-party endpoint detection and response (“EDR”) tool on corporate IT systems.

CREDIT MONITORING SERVICES PROVIDED

Igloo Inc. has provided affected individuals with one year of free credit monitoring services and identity protection services from TransUnion (for Canadian employees) or from CyberScout (for U.S. employees). These services are free of charge. The affected individuals have been notified that they have until September 30, 2022, to obtain the benefit of these services.

If you have any questions or need further information do not hesitate to contact me.

Sincerely,

Gerry Gill
Counsel
ggill@dolden.com
416-360-0146



_____, 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 supplement our earlier alert to 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. Law enforcement was not notified.

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 12 months of free credit monitoring services and identity protection services** from or from CyberScout 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 date of birth, contact information, and phone number. Please note that to obtain the benefit of these services, you must activate your code by **July 31, 2022**.

We recommend that you take precautionary measures to protect yourself, such as accessing and monitoring your personal credit reports. Under federal law, you have the right to receive, at your request, a free copy of your credit report every 12 months from each of the three consumer credit reporting companies. A credit report can provide information about those who have received your credit history within a certain period of time. You may request a free credit report online at www.annualcreditreport.com or by telephone at 1-877-322-8228.

You can obtain more information from the following sources concerning the steps to take to avoid identity theft:

- The Federal Trade Commission
600 Pennsylvania Avenue, NW
Washington, DC 20580
Telephone: (202) 326-2222
Website: <https://consumer.ftc.gov/features/identity-theft>
- The Office of the Attorney General for Maryland
Identity Theft Unit
200 St. Paul Place, 25th Floor
Baltimore, MD 21202
Telephone: (410) 576-64921
Website: <https://www.marylandattorneygeneral.gov/>



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

Igloo Inc.
55 King St W, Suite 200
Kitchener, Ontario
Canada/N2G 4W1
mmisener@igloosoftware.com
cell: 519-574-3518



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.