77, rue Industrielle
Stanstead (Québec) J0B 3E0

13th September 2024

Notice of Data Breach Following an Incident of Confidentiality

Dear First Name, Last Name

Granit Design Inc. is writing to inform you about an incident that may have affected the security of your personal information. While there is currently no indication that any identity theft has occurred as a result of this incident, some of your personal information was included on the systems that were impacted, so we want to let you know what happened, what we are doing to address it, and the complimentary identity monitoring services we are offering.

What happened?

Granit Design recently experienced a cybersecurity incident affecting the confidentiality of its employee data (the "Incident"). Upon discovery, Granit Design immediately took steps to secure its network environment and launched an investigation with help from outside cybersecurity and forensic experts. The investigation subsequently determined that an unauthorized third party accessed the server between July 20, 2024, and August 2, 2024, and acquired a subset of its files. The investigation remains ongoing to determine the extent of data that was acquired, but Granit Design is notifying all individuals whose information was contained on the affected systems.

Please note receipt of this notice does not mean that your information was actually part of the subset of the files accessed and/or acquired by the unauthorized third party, but was potentially subject to unauthorized access. **We are not aware of any evidence to date that any personal information associated with the Incident has been used for identity theft.**

Granit Design believes the Incident has been contained, and it continues to monitor its systems for any suspicious activity.

What information was involved?

It is unlikely that we will be able to determine with certainty what personal information was accessed or acquired as a result of this Incident. However, the following types of personal information were located on the systems that were compromised: full name, date of birth, driver's license, social security number, bank account number and routing number, and other

personnel-related information including medical questionnaires. These are general categories of information that were involved in the Incident, and ***not all of the listed categories may specifically pertain to you.***

What we are doing.

As described above, we took steps to secure our systems and launched an investigation immediately after discovering the Incident. To help prevent similar occurrences in the future, we will continue to monitor our systems for any suspicious activity, and we have implemented additional measures designed to enhance the security of our network, systems, and data. We will continue to evaluate ways to further enhance the security of its systems to minimize the likelihood of similar incidents occurring in the future.

As an added precaution and to relieve concerns, we have secured the services of Equifax to provide identity monitoring at no cost to you. Your identity monitoring services are described in more details on the attached Equifax document. Please note, if you wish to subscribe in the program to reduce your risk of harm, you will need to enroll. Your Equifax code can be activated until December 31, 2024, after which it will be expired.

What you can do.

In addition to completing your enrollment with Equifax, we encourage you to remain vigilant against incidents of identity theft and fraud, such as by regularly reviewing your account statements with all of your financial institutions.

Again, at this time, there is no evidence that your information has been misused. However, we encourage you to take full advantage of this service offering. Equifax representatives regularly deal with this type of incident and can answer questions or concerns you may have regarding protection of your personal information. The enclosed resources also provide information about fraud alerts and security freezes.

For more information.

We know you trust us to protect your information when you share it with us, and we want to assure you that we consistently strive to take reasonable measures to do so. If you have additional questions or concerns, please call Isabelle Côté at 819-564-2211#232 or communicate by email at icote@granitdesign.com for assistance or any additional questions you may have. Also, you will need to reference the Equifax code in the attached document when calling or enrolling on online, so please do not discard this letter.

We regret this incident and apologize for any inconvenience or concern that it may cause you.

Sincerely,

Granit Design Inc.
Jonathan Vanasse

IDENTITY THEFT IN BRIEF

If you are advised of a breach of confidentiality of your personal information, the situation must be taken seriously and you must take the appropriate measures to protect yourself. This checklist is a tool to help you respond appropriately when you notice that your personal information is lost or stolen.

Contact the companies or public agencies concerned to decrease the risk of financial or other losses (see details in the section **"STEPS TO TAKE TO PROTECT YOUR PERSONAL INFORMATION")**:
o Credit bureaus;

Advise the public agencies concerned if you believe your identity has been compromised following the loss or theft of certain cards or documents (see details in the section "**DO YOU BELIEVE YOUR IDENTITY IS COMPROMISED? REPORT IT")**:
o Financial institutions;
o Service providers;
o Federal Trade Commission;

o Information associated with any health institute o Driver's License;
o Birth certificate;
o Social Security Number (SSN);
o Passport;
o Citizenship certificate;
o Old age security identity card.

STEPS TO TAKE TO PROTECT YOUR PERSONAL INFORMATION

Credit Bureaus :

- Make sure your credit report is accurate and includes only those activities you authorized. Have your credit report corrected, if necessary.

Fraud alerts:

- In case of loss, place fraud alerts in your credit reports and contact personal information agencies. If you choose to place a fraud alert, we recommend you do this after activating your credit monitoring. You can place a fraud alert at one of the three major credit bureaus by phone and also via Experian's or Equifax's website. A fraud alert tells creditors to follow certain procedures, including contacting you, before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit. The contact information for all three bureaus is as follows:

Credit Bureaus

Equifax Fraud Reporting	Experian Fraud Reporting	TransUnion Fraud Reporting
1-866-349-5191	1-888-397-3742	1-800-680-7289
P.O. Box 105069	P.O. Box 9554	P.O. Box 2000
Atlanta, GA 30348-5069	Allen, TX 75013	Chester, PA 19022-2000
www.equifax.com	www.experian.com	www.transunion.com

It is necessary to contact only ONE of these bureaus and use only ONE of these methods. As soon as one of the three bureaus confirms your fraud alert, the others are notified to place alerts on their records as well. You will receive confirmation letters in the mail and will then be able to order all three credit reports, free of charge, for your review. An initial fraud alert will last for one year.

Please Note: No one is allowed to place a fraud alert on your credit report except you.

Security Freeze:

By placing a security freeze, someone who fraudulently acquires your personal identifying information will not be able to use that information to open new accounts or borrow money in your name. You will need to contact the three national credit reporting bureaus listed above to place the freeze. Keep in mind that when you place the freeze, you will not be able to borrow money, obtain instant credit, or get a new credit card until you temporarily lift or permanently remove the freeze. There is no cost to freeze or unfreeze your credit files.

DO YOU BELIEVE YOUR IDENTITY IS COMPROMISED? REPORT IT

Contact the organizations or companies concerned:
- If you have been notified of the loss or theft of your personal information, contact the organizations and companies and follow the instructions you are given.

- If you have not been notified but you are suspicious, immediately notify the organizations and companies that are keeping your personal Information.
- Generally, the organizations and companies that are important to contact, depending on your situation, are the following:

Financial Institutions:
- Immediately notify the issuing credit or debit card company and financial institutions regarding the theft or loss of the card, as well as any other irregularities on your monthly statement and learn the steps to follow in these circumstances.
- Always have the contact information of these card issuing institutions on hand.

Service Providers:
- If someone attempts to assume or fraudulently assumes your identity, notify the various service companies such as the phone, cable, electricity or gas company.
- Obtain new telephone calling cards and change your password or personal identification numbers.
- Contact your Post office organization if you have the impression someone might be intercepting your mail.

Federal Trade Commission:
The Federal Trade Commission encourages those who discover that their information has been misused to file a complaint with them.

All US Residents: Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW Washington, DC 20580

https://consumer.ftc.gov
1-877-IDTHEFT (438-4338)
TTY: 1-866-653-4261

ID cards:
Contact the organizations, follow their instructions:

o Information associated with any health institute o Driver's License o Birth certificate o Social Security Number (SSN)	o Passport o Citizenship certificate o Old age security identity card

<First Name> <Last Name>
Enter your Activation Code: **<Activation Code>**
Enrollment Deadline: **<Expiration Date>**

Equifax Complete™ Premier

*Note: You must be over age 18 with a credit file to take advantage of the product

Key Features

- Annual access to your 3-bureau credit report and VantageScore[1] credit scores
- Daily access to your Equifax credit report and 1-bureau VantageScore credit score
- 3-bureau credit monitoring[2] with email notifications of key changes to your credit reports
- WebScan notifications[3] when your personal information, such as Social Security Number, credit/debit card or bank account numbers are found on fraudulent Internet trading sites
- Automatic fraud alerts[4], which encourages potential lenders to take extra steps to verify your identity before extending credit, plus blocked inquiry alerts and Equifax credit report lock[5]
- Identity Restoration to help restore your identity should you become a victim of identity theft, and a dedicated Identity Restoration Specialist to work on your behalf
- Up to $1,000,000 of identity theft insurance coverage for certain out of pocket expenses resulting from identity theft[6].
- Lost Wallet Assistance if your wallet is lost or stolen, and one-stop assistance in canceling and reissuing credit, debit and personal identification cards.

Enrollment Instructions

Go to ***www.equifax.com/activate***

Enter your unique Activation Code of **<Activation Code>** then click "Submit"

1. **Register:**
   Complete the form with your contact information and click "Continue".
   If you already have a myEquifax account, click the 'Sign in here' link under the "Let's get started" header. Once you have successfully signed in, you will skip to the Checkout Page in Step 4
2. **Create Account:**
   Enter your email address, create a password, and accept the terms of use.
3. **Verify Identity:**
   To enroll in your product, we will ask you to complete our identity verification process.
4. **Checkout**:
   Upon successful verification of your identity, you will see the Checkout Page.
   Click 'Sign Me Up' to finish enrolling.

You're done!

The confirmation page shows your completed enrollment.
Click "View My Product" to access the product features.

[1] *The credit scores provided are based on the VantageScore® 3.0 model. For three-bureau VantageScore credit scores, data from Equifax®, Experian®, and TransUnion® are used respectively. Any one-bureau VantageScore uses Equifax data. Third parties use many different types of credit scores and are likely to use a different type of credit score to assess your creditworthiness.*

[2] *Credit monitoring from Experian and TransUnion will take several days to begin.*

[3] *WebScan searches for your Social Security Number, up to 5 passport numbers, up to 6 bank account numbers, up to 6 credit/debit card numbers, up to 6 email addresses, and up to 10 medical ID numbers. WebScan searches thousands of Internet sites where consumers' personal information is suspected of being bought and sold, and regularly adds new sites to the list of those it searches. However, the Internet addresses of these suspected Internet trading sites are not published and frequently change, so there is no guarantee that we are able to locate and search every possible Internet site where consumers' personal information is at risk of being traded.*

[4] *The Automatic Fraud Alert feature is made available to consumers by Equifax Information Services LLC and fulfilled on its behalf by Equifax Consumer Services LLC.*

[5] *Locking your Equifax credit report will prevent access to it by certain third parties. Locking your Equifax credit report will not prevent access to your credit report at any other credit reporting agency. Entities that may still have access to your Equifax credit report include: companies like Equifax Global Consumer Solutions, which provide you with access to your credit report or credit score, or monitor your credit report as part of a subscription or similar service; companies that provide you with a copy of your credit report or credit score, upon your request; federal, state and local government agencies and courts in certain circumstances; companies using the information in connection with the underwriting of insurance, or for employment, tenant or background screening purposes; companies that have a current account or relationship with you, and collection agencies acting on behalf of those whom you owe; companies that authenticate a consumer's identity for purposes other than granting credit, or for investigating or preventing actual or potential fraud; and companies that wish to make pre-approved offers of credit or insurance to you. To opt out of such pre-approved offers, visit www.optoutprescreen.com*

[6] *The Identity Theft Insurance benefit is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company, under group or blanket policies issued to Equifax, Inc., or its respective affiliates for the benefit of its Members. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.*