20493

ENVIRONMENTAL STONEWORKS

<<Date>> (Format: Month Day, Year)

<<first_name>> <<middle_name>> <<last_name>> <<suffix>>
<<address_1>>
<<address_2>>
<<city>>, <<state_province>> <<postal_code>>
<<country >>

<<b2b_text_1(SubjectLine)>>

Dear <<first_name>> <<middle_name>> <<last_name>> <<suffix>>,

At Environmental Stoneworks, we take the privacy and security of the information we hold very seriously, and we value the relationship with our current and former employees. We are writing to inform you that we recently identified and addressed a security incident and have learned that the incident may have involved access to some of your information, including your <<b2b_text_2(DataElements)>>. This notice outlines the measures we have taken and provides steps you can take in response.

Please note, we have no evidence that your information has been misused. However, out of an abundance of caution, we have arranged to provide identity monitoring at no cost to you for two years through Kroll, a leader in risk mitigation and response. Kroll's team has extensive experience helping people detect possible misuse of their information when they face an unintentional exposure of confidential data. The identity monitoring services we are making available to you include Credit Monitoring, Fraud Consultation and Identity Theft Restoration. For more information on identity theft prevention and Kroll Identity Monitoring, including instructions on how to activate your complimentary membership, please visit the below website and see the additional information provided with this letter.

Visit **https://enroll.idheadquarters.com** to activate and take advantage of your identity monitoring services.

*You have until **August 27, 2021** to activate your identity monitoring services.*

Membership Number: **<<Member ID>>**

We have established a dedicated call center to help answer any questions you may have about this incident. The call center is available at 1-855-935-6089, Monday through Friday, between 7:00 a.m. and 4:30 p.m. Mountain Time, excluding some U.S. holidays.

We deeply regret that this incident occurred and sincerely apologize for any concern or inconvenience this may cause. To prevent incidents like this form occurring in the future, we have implemented enhanced network monitoring tools and further strengthened our security processes.

Sincerely,

Environmental Stoneworks

KROLL

TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES

You have been provided with access to the following services from Kroll:

Triple Bureau Credit Monitoring

You will receive alerts when there are changes to your credit data at any of the three national credit bureaus—for instance, when a new line of credit is applied for in your name. If you do not recognize the activity, you will have the option to call a Kroll fraud specialist, who will be able to help you determine if it is an indicator of identity theft.

Fraud Consultation

You have unlimited access to consultation with a Kroll fraud specialist. Support includes showing you the most effective ways to protect your identity, explaining your rights and protections under the law, assistance with fraud alerts, and interpreting how personal information is accessed and used, including investigating suspicious activity that could be tied to an identity theft event.

Identity Theft Restoration

If you become a victim of identity theft, an experienced Kroll licensed investigator will work on your behalf to resolve related issues. You will have access to a dedicated investigator who understands your issues and can do most of the work for you. Your investigator will be able to dig deep to uncover the scope of the identity theft, and then work to resolve it.

Kroll's activation website is only compatible with the current version or one version earlier of Chrome, Firefox, Safari and Edge.
To receive credit services, you must be over the age of 18 and have established credit in the U.S., have a Social Security number in your name, and have a U.S. residential address associated with your credit file.

ADDITIONAL STEPS YOU CAN TAKE

We remind you it is always advisable to be vigilant for incidents of fraud or identity theft by reviewing your account statements and free credit reports for any unauthorized activity. You may obtain a copy of your credit report, free of charge, once every 12 months from each of the three nationwide credit reporting companies. To order your annual free credit report, please visit www.annualcreditreport.com or call toll free at 1-877-322-8228. Contact information for the three nationwide credit reporting companies is as follows:

- ***Equifax,*** PO Box 740241, Atlanta, GA 30374, www.equifax.com, 1-800-685-1111
- ***Experian,*** PO Box 2002, Allen, TX 75013, www.experian.com, 1-888-397-3742
- ***TransUnion,*** PO Box 2000, Chester, PA 19016, www.transunion.com, 1-800-916-8800

If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should immediately contact the Federal Trade Commission and/or the Attorney General's office in your state. You can obtain information from these sources about steps an individual can take to avoid identity theft as well as information about fraud alerts and security freezes. You should also contact your local law enforcement authorities and file a police report. Obtain a copy of the police report in case you are asked to provide copies to creditors to correct your records. Contact information for the Federal Trade Commission is as follows:

- ***Federal Trade Commission,*** Consumer Response Center, 600 Pennsylvania Avenue NW, Washington, DC 20580, 1-877-IDTHEFT (438-4338), www.ftc.gov/idtheft

Under Massachusetts law, you have the right to file and obtain a copy of a police report. You also have the right to request a security freeze, as described below. You may contact and obtain information from your state attorney general at:

Office of the Massachusetts Attorney General, One Ashburton Place, Boston, MA 02108, 1-617-727 8400, www.mass.gov/ago/contact-us.html

Fraud Alerts and Credit or Security Freezes:

Fraud Alerts: There are two types of general fraud alerts you can place on your credit report to put your creditors on notice that you may be a victim of fraud—an initial alert and an extended alert. You may ask that an initial fraud alert be placed on your credit report if you suspect you have been, or are about to be, a victim of identity theft. An initial fraud alert stays on your credit report for one year. You may have an extended alert placed on your credit report if you have already been a victim of identity theft with the appropriate documentary proof. An extended fraud alert stays on your credit report for seven years.

To place a fraud alert on your credit reports, contact one of the nationwide credit bureaus. A fraud alert is free. The credit bureau you contact must tell the other two, and all three will place an alert on their versions of your report.

For those in the military who want to protect their credit while deployed, an Active Duty Military Fraud Alert lasts for one year and can be renewed for the length of your deployment. The credit bureaus will also take you off their marketing lists for pre-screened credit card offers for two years, unless you ask them not to.

Credit or Security Freezes: You have the right to put a credit freeze, also known as a security freeze, on your credit file, free of charge. This makes it more difficult for identity thieves to open new accounts in your name because most creditors need to see your credit report before they approve a new account. If they can't see your report, they may not extend the credit.

How do I place a freeze on my credit reports? There is no fee to place or lift a security freeze on your credit reports. Unlike a fraud alert, you must separately place a security freeze on your credit file at each credit reporting company. For information and instructions on how to place a security freeze on your credit reports, contact each of the credit reporting agencies at the addresses below:

- **Experian Security Freeze,** PO Box 9554, Allen, TX 75013, www.experian.com
- **TransUnion Security Freeze,** PO Box 2000, Chester, PA 19016, www.transunion.com
- **Equifax Security Freeze,** PO Box 105788, Atlanta, GA 30348, www.equifax.com

You'll need to supply your name, address, date of birth, Social Security number and other personal information when requesting a freeze. After receiving your freeze request, each credit bureau will provide you with a unique PIN (personal identification number) or password. Keep the PIN or password in a safe place. You will need it if you choose to lift the freeze.

How do I lift a freeze? A freeze remains in place until you ask the credit bureau to temporarily lift it or remove it altogether. If the request is made online or by phone, a credit bureau must lift a freeze within one hour. If the request is made by mail, then the bureau must lift the freeze no later than three business days after receiving your request.

If you opt for a temporary lift because you are applying for credit or a job, and you can find out which credit bureau the business will contact for your file, you can save some time by lifting the freeze only at that particular credit bureau. Otherwise, you need to make the request with all three credit bureaus.

If your medical or health insurance information was identified, we recommend that you review statements you receive from your health insurer or healthcare provider. If you see services you did not receive, please contact your insurer or provider immediately.

Environmental Stoneworks is located at 6300 E. Stapleton Drive South, Denver, CO 80216 and can be reached at (800) 891-5402.

Data Breach Notification Submission

MGL Chapter 93H requires that data breaches be reported to the Office of Consumer Affairs and Business Regulation

Instructions: Please complete the form below to submit a data breach notification to the Office of Consumer Affairs and Business Regulation. Keep a copy of this submission for your own records. Please note a separate notification (https://www.mass.gov/service-details/security-breaches) or follow-up to a previous notification must be sent to the Attorney General's Office.

Are you aware that Massachusetts General Laws Chapter 93H, the Data Breach Notification Law, has changed? Please read our Frequently Asked Questions (https://edit.mass.gov/doc/frequently-asked-questions-about-chp-444-of-the-acts-of-2018) regarding data breach notifications and the changes to M.G.L. Chapter 93H.

If you're mailing your submission, please send to: Office of Consumer Affairs and Business Regulation, 501 Boylston St., Suite 5100, Boston, MA 02116 Attention: Undersecretary Edward A. Palleschi

- **Individual breaches affecting multiple debit/credit card holders of your organization can be reported on a monthly basis.**
- **Please do not include any personally identifiable information for Massachusetts residents in any of the fields.**
- **Please do not submit your notification more than once (send either by email or mail - not both).**

Section I: Organization & Contact Information

Business Name *

Environmental Stoneworks

Is this a follow-up to a previous notification received by our office? *

○ Yes

◉ No

Is the business located in the United States? *

◉ Yes

○ No

Business Address *

6300 E. Stapleton Drive South

Address Line 1

Address Line 2

Denver

City

Colorado

State

80216

ZIP Code

Reporting Company Type *

Manufacturing

Reporting on behalf of another company? *

○ Yes

◉ No

Your Name *

Patrick
First Name

Haggerty
Last Name

Title *

Partner

Contact Address *

312 Walnut Street
Address Line 1

Suite 3200
Address Line 2

Cincinnati
City

Ohio
State

45202
ZIP Code

Telephone Number *

(513) 929-3412

Extension (optional)

Email Address *

phaggerty@bakerlaw.com

Relationship to Org *

Other

Section II: Breach Information

Breach start date *

Nov 30 2020

Breach end date *

Dec 24 2020

Date Breach was Discovered *

04 21 2021

Person responsible for data breach. *

Unknown

Breach Type *

Electronic

Number of Massachusetts Residents Affected *

2

Please give a detailed explanation of how the data breach occurred. *

Please see the attached appendix.

Please select the type of personal information that was included in the breached data. *

	Selection(s)
Financial Account Numbers	☐
Social Security numbers	☑

Driver's License	☐
Credit/Debit Card Number	☐
Medical Records	☐

Please check ALL of the boxes that apply to your breach. *

	Selection(s)
The person(s) with possession of personal information had authorized access	☐
The breach was a result of a malicious/criminal act.	☑
The breach occurred while the data was being transported outside of your premises.	☐
The breach occurred at the location of a third party service provider.	☐
There is a written contract in place with the third-party provider requiring protection of personal information.	☐

Section III: Security Environment

For breaches involving paper: A lock or security mechanism was used to physically protect the data. *

☐ Yes

☐ No

☑ N/A

Physical access to systems containing personal information was restricted to authorized personnel only. *

☑ Yes

☐ No

☐ N/A

Network configuration of breached system *

Internet Access Available

For breaches involving electronic systems, complete the following *

	Selection(s)
Breached data was encrypted.	☐
The key to encrypted data was stolen.	☐
Personal information stored on the breached system was password-protected and/or restricted by user permissions.	☑
N/A	☐

Does your business maintain a Written Information Security Program (WISP)? *

☑ Yes

☐ No

Section IV: Remediation

All Massachusetts residents affected by the breach have been notified of the breach. *

☑ Yes

☐ No

Method(s) used to notify Massachusetts residents affected by the breach (check all that apply): *

☐ E-mail

☑ US Mail

☐ Online posting

☐ TV/Radio publication

☐ Other

Date notices were first sent to Massachusetts residents (MM/DD/YYYY) *

05 / 21 / 2021

All Massachusetts residents affected by the breach have been offered complimentary credit monitoring services. *

☑ Yes

☐ No

If the breach of security includes a Social Security number, Massachusetts law requires your credit monitoring comply with Section 3A of Chapter 93H *

☑ I acknowledge our credit monitoring complies with section 3A of Chapter 93H

☐ Our breach did not include a Social Security number

Law enforcement has been notified of this data breach. *

☑ Yes

☐ No

Please describe how your company responded to the breach. Include what changes were made or may be made to prevent another similar breach from occurring, including updating your WISP. *

Please see the attached appendix.

Any documents pertaining to the data breach including the letter being sent to Massachusetts residents must be submitted in this form or sent via email to data.breaches@mass.gov (mailto:data.breaches@mass.gov)

Do you have any documents that you wish to attach? NOTE: Up to 4 uploads are allowed.

Yes / No *

◉ Yes

◯ No

File 1 Upload (optional)

(File uploads have been disabled for this form.)

File 2 Upload (optional)

(File uploads have been disabled for this form.)

File 3 Upload (optional)

(File uploads have been disabled for this form.)

File - 4 Upload (optional)

(File uploads have been disabled for this form.)

Note, Massachusetts General Laws Chapter 93H, the Data Breach Notification Law, has changed. Please read our Frequently Asked Questions (https://edit.mass.gov/doc/frequently-asked-questions-about-chp-444-of-the-acts-of-2018?_ga=2.64737318.861703026.1554127915-2140933988.1483560620) regarding data breach notifications and the changes to M.G.L. Chapter 93H.

Please review the information you have entered and click on the "Submit Form" button below.

SUBMIT FORM

CONTACT

Office of Consumer Affairs and Business Regulation

Address

501 Boylston St, Suite 5100, Boston, MA 02116

Directions (https://maps.google.com/?q=501+Boylston+St%2C+Suite+5100%2C+Boston%2C+MA+02116)

Phone

Consumer hotline (617) 973-8787 (tel:6179738787)

Open M-F 9:00am-4:30pm.