

Cynthia J. Larose
617 348 1732
cjarose@mintz.com



One Financial Center
Boston, MA 02111
617 542 6000
mintz.com

February 11, 2021

VIA EMAIL – DOJ-CPB@doj.nh.gov

Attorney General Gordon MacDonald
Office of the Attorney General
Consumer Protection Bureau
33 Capitol Street
Concord, NH 03301

RE: Notice of Security Incident

Dear Attorney General MacDonald:

This firm represents Walsh Brothers Construction, Inc. (the “Company”), a construction company located in Boston, Massachusetts. We are contacting your office with regard to a recent data security incident that may have affected personal information belonging to New Hampshire residents.

1. Nature of the security incident.

On January 24, 2021, the Company learned it was the victim of a ransomware attack through which, according to the threat email sent by the apparent intruder, unknown malicious actor(s) gained access to and encrypted the Company’s servers and data. Upon discovery, the servers were brought down and all local computers were also disconnected from the Internet. The Company immediately began an investigation into the intrusion, including engagement of third party consultants, to help the Company contain and resolve the incident. The investigation determined that the malicious intrusion began on or about Wednesday, January 20, 2021, and on that day, it appeared that a large number of files may have been exfiltrated prior to the execution of the ransomware variant. Based on the Company’s review of impacted files and investigation, it appeared that it was possible that certain files containing personal information of employees and former employees may have been exfiltrated by the malicious actor. While the data files were being processed and examined, the Company sent out an email alert on Friday, January 29, 2021, followed by the notice letter attached. The Company has had no indication that the personal information has been used or otherwise disclosed or distributed or made public.

2. Number of New Hampshire residents affected

Approximately 11 residents of New Hampshire may have been affected by this incident. The Company notified the individuals via U.S. mail on February 10, 2021. A sample copy of the notification letter is provided with this correspondence.

3. Steps taken relating to the incident

Passwords of all employees were immediately reset and the Company is implementing additional protections for its Citrix portal, including access management. Law enforcement was notified, but the notices to individuals were not delayed pending any investigation. In addition, the Company is offering identity protection services for 24 months through IDX, as further described in the sample letter.

Please contact the undersigned with any questions or if further information is needed.

Sincerely,

A handwritten signature in black ink, appearing to read 'Cynthia J. Larose'.

Cynthia J. Larose

Attachment

WALSH BROTHERS, INC.

C/O IDX
10300 SW Greenburg Rd., Suite 570
Portland, OR 97223

To Enroll, Please Call:
1-800-939-4170
Or Visit:
<https://app.idx.us/account-creation/protect>
Enrollment Code:
<<XXXXXXXXXX>>

<<First Name>> <<Last Name>>
<<Address1>> <<Address2>>
<<City>>, <<State>> <<Zip>>

February 10, 2021

Dear <<First Name>> <<Last Name>>,

What Happened

Walsh Brothers discovered on January 24, 2021 that it was the victim of a ransomware attack and it appears that a malicious and unknown party had obtained access to certain of our servers, including files containing your personal information. Following the discovery of the issue, we contracted with an outside security consulting company to aid in the triage and investigation of the incident as well as the scope of the intrusion. Based on our current review as described further below, we have no indication that your information has been used inappropriately. We want to provide you with information about the incident and with the attached additional information that you may find helpful.

What Information Was Involved

The information in the files included your name, address, and other contact information, Social Security number, driver's license, and direct deposit banking information.

What We Are Doing

We are working to improve security and implement additional safeguards to protect theft or similar criminal activity in the future. We are implementing additional protections for our Citrix portal and have reset all password of employees. We will continue to closely monitor and take further steps as appropriate to safeguard such information. We have reported the matter to law enforcement and will cooperate in any investigation that may commence. We have not delayed this notice in the interim.

In addition, to comply with applicable state laws, we are offering identity protection services at no cost to you through IDX, the security incident and recovery services expert. IDX identity protection services include: 24 months of credit and CyberScan monitoring, a \$1,000,000 insurance reimbursement policy, and fully managed id theft recovery services. With this protection, IDX will help you resolve issues if your identity is compromised.

What You Can Do

We encourage you to contact IDX with any questions and to enroll in the free identity protection services by calling 1-800-939-4170 or going to <https://app.idx.us/account-creation/protect> and using the Enrollment Code provided above. IDX representatives are available Monday through Friday from 9 am - 9 pm Eastern Time. Please note the deadline to enroll is May 10, 2021 (your Enrollment Code will not work after that date).

210 Commercial Street
Boston, MA 02109

Again, at this time, there is no evidence that your information has been misused. It is a good practice to remain vigilant and closely review and monitor your financial accounts, statements, and other financial information for any evidence of unusual activity, fraudulent charges, or signs of identity theft.

For More Information

You will find detailed instructions for enrollment on the enclosed Additional Information document. Also, you will need to reference the enrollment code at the top of this letter when calling or enrolling online, so please do not discard this letter.

Please call 1-800-939-4170 or go to <https://app.idx.us/account-creation/protect> for assistance or for any additional questions you may have about the IDX services.

If you have questions regarding your information, please contact Darlene Conners at 617-878-4800.

Sincerely,

James M. Brosnan

James M. Brosnan
Walsh Brothers, Incorporated

(Enclosure)



ADDITIONAL INFORMATION

- 1. Website and Enrollment.** Go to <https://app.idx.us/account-creation/protect> and follow the instructions for enrollment using your Enrollment Code provided at the top of the letter.
- 2. Activate the credit monitoring** provided as part of your IDX identity protection membership. The monitoring included in the membership must be activated to be effective. Note: You must have established credit and access to a computer and the internet to use this service. If you need assistance, IDX will be able to assist you.
- 3. Telephone.** Contact IDX at 1-800-939-4170 to gain additional information about this event and speak with knowledgeable representatives about the appropriate steps to take to access the identity protection services.
- 4. Review your credit reports.** It is always a good practice to be vigilant by reviewing account statements and monitoring credit reports. Under federal law, you also are entitled every 12 months to one free copy of your credit report from each of the three major credit reporting companies. To obtain a free annual credit report, go to www.annualcreditreport.com or call 1-877-322-8228. You may wish to stagger your requests so that you receive a free report by one of the three credit bureaus every four months. As a Massachusetts resident, you may obtain one or more additional copies of your credit report free of charge. You must contact each of the credit reporting agencies to obtain such additional report(s).

If you discover any suspicious items and have enrolled in IDX identity protection, notify them immediately by calling 1-800-939-4170 or by logging into the IDX website and filing a request for help.

If you file a request for help or report suspicious activity, you will be contacted by a member of our ID Care team who will help you determine the cause of the suspicious items. In the unlikely event that you fall victim to identity theft as a consequence of this incident, you will be assigned an ID Care Specialist who will work on your behalf to identify, stop and reverse the damage quickly.

5. Filing Police Reports. You should also know that you have the right to file a police report if you ever experience identity fraud. Please note that in order to file a crime report or incident report with law enforcement for identity theft, you will likely need to provide some kind of proof that you have been a victim. A police report is often required to dispute fraudulent items. You can report suspected incidents of identity theft to local law enforcement or to the Attorney General.

6. Place Fraud Alerts with the three credit bureaus. 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
1-866-349-5191
P.O. Box 105069
Atlanta, GA 30348-5069
www.equifax.com

Experian Fraud Reporting
1-888-397-3742
P.O. Box 9554
Allen, TX 75013
www.experian.com

TransUnion Fraud Reporting
1-800-680-7289
P.O. Box 2000
Chester, PA 19022-2000
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.**

7. Security Freeze. You have the right to put a security freeze on your credit file, so that no new credit can be opened in your name without your consent. If you place a security freeze on your credit file, potential creditors and other third parties will not be able to get access to your credit report unless you temporarily lift the freeze. Therefore, using a security freeze may delay your ability to obtain credit. *Unlike a fraud alert, you must separately place a security freeze on your credit file at each credit reporting agency using the contact information provided above.* Federal and state laws prohibit charges for placing, temporarily lifting, or removing a security freeze.

The following information must be included when requesting a security freeze (note that if you are requesting a security freeze for your spouse, this information must be provided for your spouse as well): (1) full name, with middle initial and any suffixes; (2) Social Security number; (3) date of birth; (4) current address and any previous addresses for the past five (5) years; and (5) any applicable incident report or complaint with a law enforcement agency or the Registry of Motor Vehicles. The request must also include a copy of a government-issued identification card and a copy of a recent utility bill or bank or insurance statement. It is essential that each copy be legible, display your name and current mailing address, and the date of issue.

8. You can obtain additional information about the steps you can take to avoid identity theft from the following agencies. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them.

North Carolina Residents: Office of the Attorney General of North Carolina, 9001 Mail Service Center Raleigh, NC 27699-9001, www.ncdoj.gov, Telephone: 1-919-716-6400.

Rhode Island Residents: Office of the Attorney General, 150 South Main Street, Providence, Rhode Island 02903, www.riag.ri.gov, Telephone: 401-274-4400

All US Residents: Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW Washington, DC 20580, www.consumer.gov/idtheft, 1-877-IDTHEFT (438-4338), TTY: 1-866-653-4261.