



September 21, 2020

Via E-Mail (DOJ-CPB@doj.nh.gov)

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

To whom it may concern:

I am writing on behalf of Suffolk Construction Co., Inc. ("Suffolk") to inform you of a security incident potentially affecting fourteen (14) New Hampshire residents.

On September 11, 2020, a Suffolk employee sent an email to other Suffolk employees and employees of Suffolk's subcontractors and the Massachusetts Port Authority. That email was sent with an attachment that mistakenly contained the personal information of Suffolk employees and employees of Suffolk's subcontractors. Suffolk has determined that the personal information of fourteen (14) New Hampshire residents was included within the attachment, including their name and Social Security number.

Immediately after discovering the error, Suffolk undertook an investigation into this incident and has verified that the original source file that was mistakenly attached to the e-mail is secured with restricted access. Suffolk has also removed the e-mail message and attachment from employee inboxes. Suffolk requested confirmation from each recipient that he or she permanently deleted the email, has received confirmation of deletion from most recipients, and is continuing to follow up with recipients with the intention of obtaining confirmation from all of them.

Please note that we have no information indicating that the personal information of New Hampshire residents was actually misused. Out of an abundance of caution, Suffolk will send a security incident notification to each potentially affected New Hampshire resident. Suffolk is also offering two years of Experian's IdentityWorks identity theft protection product to these individuals at no cost to them. IdentityWorks includes credit monitoring,

Suffolk

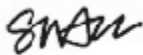
Northeast
65 Allerton Street
Boston, MA 02119

617.445.3500
suffolk.com

identity restoration services, credit monitoring alerts, and identity theft insurance. A copy of the template notification letter is included with this letter.

If you have any questions concerning this matter, please do not hesitate to contact me at 617-517-5223 or SVanDeCarr@suffolk.com.

Sincerely,

A handwritten signature in black ink, appearing to read "SVCarr", is positioned above the typed name.

Sara VanDeCarr
VP, Associate General Counsel & Corporate Compliance Officer
Suffolk Construction Co., Inc.



September 21, 2020

[Name]
[Address]
[City] [State] [Zip Code]

Dear [Name]:

Suffolk Construction Co., Inc. (“Suffolk”), in the ordinary course of its business, collects personal information about employees of its subcontractors. Suffolk is committed to protecting this personal information. Unfortunately, we are writing to inform you of an information security incident that could potentially affect you, and to share with you the steps that Suffolk is taking to address it.

On September 11, 2020, a Suffolk employee sent an email to other Suffolk employees and employees of Suffolk’s subcontractors, and the Massachusetts Port Authority, with an attachment that mistakenly contained your personal information. The attachment included your name and Social Security number. Immediately after discovering the error, Suffolk took steps to confirm that the e-mail and attachment were permanently deleted, and not retained or further disclosed by any of the recipients.

Suffolk has no evidence that your personal information has been misused. We also want to emphasize that the attachment did not contain any of your other sensitive information, such as your driver’s license number, payment card number, or information that would permit access to any financial account.

Nevertheless, out of an abundance of caution, Suffolk is offering you two years of identity protection services at no cost to you through Experian, one of the three nationwide credit bureaus. Your two-year membership in Experian’s IdentityWorksSM product provides identity restoration services, fraud detection tools, and other benefits, which include monitoring your credit file at Experian. Starting today, you can call Experian’s identity restoration agents to assist you to investigate and resolve any incidents of fraud. You may take advantage of this benefit, at any time, until December 31, 2022, by calling Experian at 1-877-890-9332. No enrollment or activation is necessary. The terms and conditions for identity restoration are located at: www.ExperianIDWorks.com/restoration.

While identity restoration is immediately available to you, we also encourage you to activate fraud detection tools available through IdentityWorksSM. This product provides you with identity

Suffolk

Northeast
65 Allerton Street
Boston, MA 02119

617 445 3500
suffolk.com

detection, credit monitoring, and resolution of identity theft. If you wish to enroll in IdentityWorksSM, you will need to do the following:

1. **Visit** the IdentityWorksSM web site: <https://www.experianidworks.com/credit> or call 1-877-890-9332 to enroll and provide Engagement Number **[Number]**.
2. **PROVIDE** your Activation Code: **[Code]**.

Enrollment Deadline: December 31, 2020 (your Activation Code will not work after this date).

If you have any questions concerning IdentityWorksSM or if you prefer to enroll over the phone for delivery of your membership via US mail, please call Experian at 1-877-890-9332. Be prepared to provide Engagement Number [Number] as proof of eligibility for the identity protection product by Experian.

In addition to the offer of IdentityWorksSM, we have included with this letter additional information on steps you can take to protect the security of your personal information. We urge you to review this information carefully.

Suffolk takes seriously both the security of your personal information and this incident. In response to this incident, we have taken appropriate steps to enhance the security for your personal information and to reduce the likelihood of a recurrence.

Suffolk sincerely apologizes for this incident and regrets any inconvenience it may cause you. Should you have any questions or concerns regarding this incident, please do not hesitate to contact me.

Sincerely,

A handwritten signature in black ink, appearing to read 'Seth Williams', with a stylized flourish at the end.

Seth Williams
Project Executive
Suffolk Construction Co., Inc.
SWilliams@suffolk.com
(646) 952-8018

Steps To Protect The Security Of Your Personal Information

By taking the following steps, you can help reduce the risk that your personal information may be misused.

1. Enroll in IdentityWorksSM. You must personally activate identity monitoring for it to be effective. The notice letter contains instructions and information on how to activate your IdentityWorksSM membership. Experian's IdentityWorksSM product will provide the following:

- **Experian credit report at signup:** See what information is associated with your credit file. Daily credit reports are available for online members only.¹
- **Credit Monitoring:** Actively monitors your credit files at Experian for indicators of fraud.
- **Identity Restoration:** Identity restoration specialists are immediately available to help you address credit and non-credit related fraud.
- **Experian IdentityWorksSM ExtendCARE:** You will receive the same high level of identity restoration support even after your IdentityWorksSM membership expires.
- **\$1 Million Identity Theft Insurance²:** Provides coverage for certain costs and unauthorized electronic fund transfers.

Please direct questions about the IdentityWorksSM product to Experian. A credit card is not required for enrollment in IdentityWorksSM. Enrollment in IdentityWorksSM will not affect your credit score. The Terms and Conditions for this offer are located at www.ExperianIDWorks.com/restoration.

2. Review your credit reports. You can receive free credit reports by placing a fraud alert. Under federal law, you also are entitled every 12 months to one free copy of your credit report from each of the three national credit bureaus. 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 from one of the three credit bureaus every four months.

3. Review your account statements. You should carefully review for suspicious activity the statements that you receive from credit card companies, banks, utilities, and other services.

4. Remain vigilant and respond to suspicious activity. If you receive an e-mail or mail alert from Experian, contact an IdentityWorksSM identity resolution agent toll-free at 1-877-890-9332 or visit www.ExperianIDWorks.com/restoration for additional information. You should consider changing your username, passwords, security questions, and security answers to your online accounts. If you

¹ Offline members will be eligible to call for additional reports quarterly after enrolling.

² The Identity Theft Insurance is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

notice suspicious activity on an account statement, report it to your credit card company or service provider and consider closing the account. You should also consider reporting such activity to Suffolk, your local police department, your state's attorney general, and the Federal Trade Commission. If you are a Massachusetts resident, Massachusetts law gives you the right to report this incident to the police in the county where you reside and to receive a police incident report within 24 hours of your report.

5. You have the right to place a "security freeze" on your credit report. A security freeze will prohibit a consumer reporting agency from releasing information in your credit file without your express authorization. The security freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. Please understand that placing a security freeze on your credit file may delay, interfere with, or prevent the timely approval of any subsequent request or application you make for a new loan, mortgage, or any other account involving the extension of credit.

A security freeze does not apply to a person or entity, or its affiliates, or collection agencies acting on behalf of the person or entity, with which you have an existing account that requests information in your credit report for the purposes of reviewing or collecting the account. Reviewing the account includes activities related to account maintenance, monitoring, credit line increases, and account upgrades and enhancements.

To place a security freeze on your credit file, contact the three nationwide credit bureaus, listed below. You will need to provide appropriate proof of your identity to the credit bureau, which will include your name, address, date of birth, Social Security number, and other personal information. 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.

The contact information for all three credit bureaus is as follows:

Equifax	Experian	TransUnion
P.O. Box 105788	P.O. Box 9554	P.O. Box 160
Atlanta, GA 30348	Allen, TX 75013	Woodlyn, PA 19094
1-888-298-0045	1-888-397-3742	1-888-909-8872
www.equifax.com	www.experian.com	www.transunion.com

6. Consider placing a fraud alert with one of the three nationwide credit bureaus. You can place an initial fraud alert by contacting one of the three nationwide credit bureaus listed above. A fraud alert can make it more difficult for someone to get credit in your name because it tells creditors to follow certain procedures to protect you. It also may delay your ability to obtain credit. You may

place a fraud alert in your file by calling just one of the three nationwide credit bureaus listed above. As soon as that bureau processes your fraud alert, it will notify the other two, which then also must place fraud alerts in your file.

An initial fraud alert stays in your file for at least one year. To place this alert, a credit bureau will require you to provide appropriate proof of your identity, which may include your Social Security number. If you are the victim of identity theft, you are entitled to an extended fraud alert, which is a fraud alert lasting 7 years.

An initial fraud alert entitles you to a copy of all the information in your file at each of the three nationwide credit bureaus listed above. These additional disclosures may help you detect signs of fraud, for example, whether fraudulent accounts have been opened in your name or whether someone has reported a change in your address.

7. Additional Information. You may obtain information about fraud alerts and security freezes and additional information about steps you can take to avoid identity theft from the following: Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW, Washington, DC 20580; <http://www.ftc.gov/idtheft/>; (877) IDTHEFT (438-4338).