BOND SCHOENECK & KING

One Lincoln Center | Syracuse, NY 13202-1355 | **bsk.com**

JESSICA COPELAND, ESQ.
jcopeland@bsk.com
C: 716.432.6328

May 26, 2021

VIA ELECTRONIC MAIL AND FIRST CLASS MAIL

Consumer Protection Bureau
Office of the New Hampshire Attorney General
33 Capitol Street
Concord, NH 00301

Re: *Security Incident Notification*

To Whom It May Concern:

We represent Wright Architectural Millwork Corporation (Wright Architectural), located at 115 Industrial Lane, Northampton Massachusetts, 01060. This letter serves as notice to the Office of the Attorney General pursuant to N.H. Rev. Stat. § 359-C:20(I)(b) of a data security incident that may have affected the personal information of one (1) New Hampshire resident.

On or around April 19, 2021, Wright Architectural became aware of a security incident related to a ransomware attack of its computer network and servers, possibly affecting personal data of some of its employees, including one New Hampshire resident. Wright Architectural learned of the incident when one of its administrators could not access email or other network servers. The personal information affected includes name, social security number, date of birth, date of hire and date of termination (if applicable).

As soon as Wright Architectural learned of the data incident, it commenced an investigation with experienced cybersecurity professionals to contain and suspend the intrusion and to work diligently to retrieve and restore access to the Company's data. It has also implemented security and policy changes to protect data moving forward.

Wright Architectural will notify the New Hampshire resident no later than June 2, 2021, and the individual will be offered 18 months of complimentary credit monitoring. A sample copy of the notification letter to the affected individual is included with this correspondence. Should you have any questions or need additional information, please contact me at 716-432-6328 or via email at jcopeland@bsk.com

Very truly yours,

BOND, SCHOENECK & KING, PLLC

Jessica Copeland

[Company Name/Logo]

Notification of Security Breach

[Names
Address
City
State
Zip
Country]

Date

Dear [Name]:

The privacy and security of the personal information we maintain is of the utmost importance to Wright Architectural Millwork Corporation ("Wright Architectural"). We are writing with important information regarding a recent security incident that may have impacted some of your information. We want to provide you with information about the incident, explain the services we are making available to you, and let you know that we continue to take significant measures to protect your information.

What Happened?

On or around April 19, 2021, we became aware of a security incident related to a ransomware attack of our computer network and servers, possibly affecting personal data of some of our employees who are Massachusetts residents. We learned of the incident when one of our administrators could not access email or other network servers.

What Information Was Involved?

We are notifying you that the impacted data contained some of your personal information, specifically name, social security number, date of birth, date of hire and where applicable date of termination from employment.

What Are We Doing?

As soon as we were learned of the data incident, we commenced an investigation. We immediately began working with experienced cybersecurity professionals to contain and suspend the intrusion and to work diligently to retrieve and restore access to the Company's stored data. While we have no indication or evidence that any of the compromised data has been or will be misused, we thought it important to notify you of these incident-related activities.

We are working closely with our outside cybersecurity professionals to ensure that your personal information will be protected. Wright Architectural has implemented several changes that are designed to protect our data, including your personal information, from any subsequent incidents.

What You Can Do?

Wright Architectural is providing you with access to credit monitoring services at no charge. Services are for 18 months from the date of enrollment. If changes occur to your credit file, notification will be sent to you the same day the change or update takes place with the bureau. In order for you to receive the credit monitoring service described above, you must enroll no later than _____, 2021.

This letter also provides other precautionary measures you can take to protect your personal information, including placing a fraud alert and/or free security freeze on your credit files, and/or obtaining a free credit report. Additionally, you should always remain vigilant in reviewing your account statements for fraudulent or irregular activity on a regular basis.

If you have any further questions regarding this incident, please call me at 413 586 3528 EXT 114. I am familiar with this incident and can review with you what you can do to protect against misuse of your information. The response line is available Monday through Thursday, 8am to 4:30pm, Eastern Time.

Sincerely,

Michael D. Buell
President & CEO

– OTHER IMPORTANT INFORMATION –

1. Obtain a Police Report

You have a right to obtain a police report concerning the data incident. To do so, please call your local police station.

2. Placing a Fraud Alert on Your Credit File

Whether or not you choose to use the complimentary 18-month credit monitoring services, we recommend that you place an initial 1-year "fraud alert" on your credit files, at no charge. A fraud alert tells creditors to contact you personally before they open any new accounts. To place a fraud alert, call any one of the three major credit bureaus at the numbers listed below. As soon as one credit bureau confirms your fraud alert, they will notify the others.

Equifax
P.O. Box 105069
Atlanta, GA 30348
www.equifax.com
1-800-525-6285

Experian
P.O. Box 2002
Allen, TX 75013
www.experian.com
1-888-397-3742

TransUnion LLC
P.O. Box 2000
Chester, PA 19016
www.transunion.com
1-800-680-7289

3. Placing a Security Freeze on Your Credit File.

If you are very concerned about becoming a victim of fraud or identity theft, you may request a "security freeze" be placed on your credit file, *at no charge*. A security freeze prohibits, with certain specific exceptions, the consumer reporting agencies from releasing your credit report or any information from it without your express authorization. You may place a security freeze on your credit report by sending a request in writing or by mail, to all three nationwide credit reporting companies. To find out more about how to place a security freeze, you can use the following contact information:

Equifax Security Freeze
P.O. Box 105788
Atlanta, GA 30348
https://www.freeze.equifax.com
1-800-685-1111

Experian Security Freeze
P.O. Box 9554
Allen, TX 75013
http://experian.com/freeze
1-888-397-3742

TransUnion Security Freeze
P.O. Box 2000
Chester, PA 19016
http://www.transunion.com/securityfreeze
1-888-909-8872

In order to place the security freeze, you'll need to supply your name, address, date of birth, Social Security number and other personal information. After receiving your freeze request, each credit monitoring company will send you a confirmation letter containing 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.

If you do place a security freeze *prior* to enrolling in the credit monitoring service as described above, you will need to remove the freeze in order to sign up for the credit monitoring service. After you sign up for the credit monitoring service, you may refreeze your credit file.

4. Obtaining a Free Credit Report.

Under federal law, you are entitled to one free credit report every 12 months from each of the above three major nationwide credit reporting companies. Call **1-877-322-8228** or request your free credit reports online at **www.annualcreditreport.com**. Once you receive your credit reports, review them for discrepancies. Identify any accounts you did not open or inquiries from creditors that you did not authorize. Verify all information is correct. If you have questions or notice incorrect information, contact the credit reporting company.

5. Additional Helpful Resources.

Even if you do not find any suspicious activity on your initial credit reports, the Federal Trade Commission (FTC) recommends that you check your credit reports periodically. Checking your credit report periodically can help you spot problems and address them quickly.

If you find suspicious activity on your credit reports or have reason to believe your information is being misused, call your local law enforcement agency and file a police report. Be sure to obtain a copy of the police report, as many creditors will want the information it contains to absolve you of the fraudulent debts. You may also file a complaint with the FTC by contacting them on the web at www.ftc.gov/idtheft, by phone at 1-877-IDTHEFT (1-877-438-4338), or by mail at Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580. Your complaint will be added to the FTC's Identity Theft Data Clearinghouse, where it will be accessible to law enforcement for their investigations. In addition, you may obtain information from the FTC about fraud alerts and security freezes.

If this notice letter states that your financial account information and/or credit or debit card information was impacted, we recommend that you contact your financial institution(s) to inquire about steps to take to protect your account(s), including whether you should close your account(s) or obtain a new account number(s).

Massachusetts Residents: You may obtain information about preventing identity theft from the Massachusetts Attorney General's Office: https://www.mass.gov/avoiding-identity-theft; Telephone: Consumer Hotline (617) 727-8400; Medicaid Fraud Tip line: (617) 963-2360

New York Residents: You may obtain information about preventing identity theft from the New York Attorney General's Office: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; https://ag.ny.gov/consumer-frauds-bureau/identity-theft; Telephone: 800-771-775 (TDD/TYY Support: 800-788-9898); Medicare Fraud Control Unit Direct Line: 212-417-5397