March 12, 2024

VIA Email
Attorney General John M. Formella
Office of the Attorney General
Consumer Protection & Antitrust Bureau
1 Granite Place South
Concord, NH 03301
DOJ-CPB@doj.nh.gov

Re: Notice of Data Security Incident

Dear Attorney General Formella:

Constangy, Brooks, Smith and Prophete LLP ("Constangy") represents Quaker Window Products, Co. ("Quaker") located in Freeburg, MO in connection with an incident described in greater detail below.

1. **Nature of Incident**

On November 25, 2023, Quaker experienced a network disruption and immediately initiated an investigation of the matter. Quaker engaged cybersecurity experts to assist with the process. The investigation revealed that an unauthorized actor had access to certain files from the Quaker network on or about November 25, 2023. On December 22, 2023, Quaker determined that certain personal data stored in the network environment, including your data, may have been accessible to the unauthorized actor while they were in the network environment. Quaker then took steps to obtain addresses for those individuals whose information was involved.

The potentially affected information varied by individual but may include the following:
.

2. **Number of New Hampshire residents affected**

Quaker notified one (1) New Hampshire residents of the incident via first class U.S. mail on March 12, 2024. A sample copy of the notification letter is included with this correspondence.

3. Steps taken relating to the incident

Upon discovering the issue, Quaker took the steps described above. Quaker also provided notice of the incident to potentially impacted individuals on March 12, 2024 In addition, Quaker is offering affected individuals, whose social security numbers were impacted, complimentary credit monitoring and identity protection services through IDX, A ZeroFox Company, the data breach and recovery services expert. These services include of credit monitoring, identity protection, and fully managed identity theft recovery services. With this protection, IDX will help them resolve issues if their identity is affected.

4. Contact information

If you have any questions or need additional information, please do not hesitate to contact me at

Very truly yours,

Jason Cherry, Esq.

Encl: Sample Consumer Notification Letter

Return to IDX
P.O. Box 989728
West Sacramento, CA 95798-9728

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

March 12, 2024

Subject: Notice of Data <<Variable Text 1: Security Incident/Breach>>

Dear <<First Name>> <<Last Name>>:

We are writing to inform you of an incident recently experienced by Quaker Window Products, Co. ("Quaker") which may have affected the security of some of your personal information. At Quaker, we take the privacy and security of personal information very seriously. Please read this letter carefully as it contains information regarding the incident and steps you can take to help protect your personal information.

What Happened. On November 25, 2023, Quaker experienced a network disruption and immediately initiated an investigation of the matter. We engaged cybersecurity experts to assist with the process. The investigation revealed that an unauthorized actor had access to certain files from the Quaker network on or about November 25, 2023. On December 22, 2023, Quaker determined that certain personal data stored in the network environment, including your data, may have been accessible to the unauthorized actor while they were in the network environment. A notification letter was sent to your address on file. The original notification letter was returned as "undeliverable", so we obtained a new address from our notification vendor.

What Information Was Involved. The impacted information may have included your

What We Are Doing. As soon as we discovered the incident, we took the steps described above and implemented additional security measures to minimize the risk of a similar incident occurring in the future. We have reported this incident to federal law enforcement and will cooperate with any investigative requests. We are further notifying you of this event and advising you about steps you can take to help protect your information.

In addition, we are offering you the opportunity to enroll in free identity protection services through IDX, a data breach and recovery services expert. These services include <<12/24>> months of credit monitoring and CyberScan monitoring, a $1,000,000 insurance reimbursement policy, and fully managed identity theft recovery services. With this protection, IDX will help you resolve issues if your identity is compromised.

What You Can Do. You can follow the recommendations on the following page to help protect your information. You can also enroll in the free services offered to you through IDX identity protection services by calling 1-888-799-4239 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 9:00 a.m. to 9:00 p.m. Eastern Time. You will need to reference the enrollment code in this letter when calling or enrolling online, so please do not discard this letter. Please note the deadline to enroll is .

For More Information: Further information about how to help protect your information appears on the following page. If you need assistance enrolling in the complimentary services being offered to you, please call IDX at 1-888-799-4239 from 9:00 A.M. to 9:00 P.M. Eastern Time, Monday through Friday (excluding holidays). IDX representatives can also answer questions you may have regarding the incident and the protection of your personal information.

We take this event and the security of information in our care seriously. Please accept our sincere apologies and know that we deeply regret any concern or inconvenience that this may cause you.

Sincerely,

Kevin Blansett

Kevin Blansett
Chief Executive Officer
Quaker Window Products, Co.
504 Highway 63 South,
Freeburg, MO 65035
Telephone: 800-347-0438

STEPS YOU CAN TAKE TO HELP PROTECT YOUR INFORMATION

Review Your Account Statements and Notify Law Enforcement of Suspicious Activity: As a precautionary measure, we recommend that you remain vigilant by reviewing your account statements and monitoring free credit reports closely for errors and by taking other steps appropriate to protect accounts, including promptly changing passwords. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained for remediation assistance or contact a remediation service provider. You also should promptly report any fraudulent activity or any suspected incidence of identity theft to proper law enforcement authorities, your state attorney general, and/or the Federal Trade Commission (FTC). 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 Ave, NW, Washington, DC 20580, 1-877-IDTHEFT (438-4338), www.consumer.ftc.gov, www.ftc.gov/idtheft.

Copy of Credit Report: You may obtain a free copy of your credit report from each of the three major credit reporting agencies once every 12 months by visiting http://www.annualcreditreport.com/, calling toll-free 877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. You can print this form at https://www.annualcreditreport.com/cra/requestformfinal.pdf. You also can contact one of the following three national credit reporting agencies:

> *Equifax*, P.O. Box 740241, Atlanta, GA 30374, 1-800-525-6285, www.equifax.com.
> *Experian*, P.O. Box 9532, Allen, TX 75013, 1-888-397-3742, www.experian.com.
> *TransUnion*, P.O. Box 1000, Chester, PA 19016, 1-800-916-8800, www.transunion.com.

Fraud Alerts: There are two kinds of general fraud alerts you can place on your credit report—an initial alert and an extended alert. You may want to consider placing either or both fraud alerts on your credit report. An initial fraud alert is free and will stay on your credit file for at least 90 days. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any accounts in your name. You may have an extended alert placed on your credit report if you have already been a victim of identity theft and provide the appropriate documentary poof. An extended fraud alert is also free and will stay on your credit report for seven years. To place a fraud alert on your credit report, contact any of the three credit reporting agencies identified above. Additional information is available at http://www.annualcreditreport.com. Military members may also place an Active Duty Military Fraud Alert on their credit reports while deployed.

Credit or Security Freezes: Under U.S. law, you have the right to put a credit freeze, also known as a security freeze, on your credit file, for up to one year at no cost. The freeze will prevent new credit from being opened in your name without the use of a PIN number that is issued to you when you initiate the freeze. A security freeze is designed to prevent potential creditors from accessing your credit report without your consent. As a result, using a security freeze may interfere with or delay your ability to obtain credit.

You must separately place a security freeze on your credit file with each credit reporting agency. There is no fee to place or lift a security freeze. For information and instructions on how to place a security freeze, contact any of the credit reporting agencies or the Federal Trade Commission identified above. In order to place a security freeze, you may be required to provide the consumer reporting agency with information that identifies you including your full name, Social Security number, date of birth, current and previous addresses, a copy of your state-issued identification card, and a recent utility bill, bank statement or insurance statement. After receiving your freeze request, each credit bureau will provide you with a unique PIN or password. Keep the PIN or password in a safe place as you will need it if you choose to lift the 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 via phone, a credit bureau must lift the credit freeze within an 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.

IRS Identity Protection PIN: You can obtain an identity protection PIN (IP PIN) from the IRS that prevents someone else from filing a tax return using your Social Security number. The IP PIN is known only to you and the IRS and helps the IRS verify your identity when you file your electronic or paper tax return. You can learn more and obtain your IP PIN here: https://www.irs.gov/identity-theft-fraud-scams/get-an-identity-protection-pin.

You also have certain rights under the Fair Credit Reporting Act (FCRA): These rights include the right to know what is in your file; to dispute incomplete or inaccurate information; to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information. For more information about the FCRA, and your rights pursuant to the FCRA, please visit https://www.consumer.ftc.gov/sites/default/files/articles/pdf/pdf-0096-fair-credit-reporting-act.pdf.

Additional Free Resources: You can obtain information from the consumer reporting agencies, the FTC, or from your respective state attorney general about fraud alerts, security freezes, and steps you can take toward preventing identity theft. You may report suspected identity theft to local law enforcement, including to the FTC or to the attorney general in your state.

Additional Information:

California: The California Attorney General can be reached at: 1300 "I" Street, Sacramento, CA 95814-2919; 800-952-5225; http://oag.ca.gov/

Maryland: The Maryland Attorney General can be reached at: 200 St. Paul Place Baltimore, MD 21202; 888-743-0023; oag@state.md.us or IDTheft@oag.state.md.us; https://www.marylandattorneygeneral.gov/

North Carolina: The North Carolina Attorney General's Office, Consumer Protection Division, can be reached at: 9001 Mail Service Center Raleigh, NC 27699-9001; 877-5-NO-SCAM (Toll-free within North Carolina); 919-716-6000; https://ncdoj.gov/

New York: The New York Attorney General can be reached at: Bureau of Internet and Technology Resources, 28 Liberty Street, New York, NY 10005; 212-416-8433; https://ag.ny.gov/

Rhode Island: The total number of individuals receiving notification of this incident is 0. The Rhode Island Attorney General can be reached at: 150 South Main Street Providence, RI 02903, http://www.riag.ri.gov

Texas: The Texas Attorney General can be reached at: 300 W. 15th Street, Austin, Texas 78701; 800-621-0508; texasattorneygeneral.gov/consumer-protection/