



Lauren Godfrey
322 North Shore Drive,
Building 1B, Suite 200
Pittsburgh, PA 15212
lgodfrey@constangy.com
973.462.9521

May 2, 2024

VIA ONLINE SUBMISSION

Attorney General Aaron Frey
Office of the Attorney General
Consumer Protection Division
Security Breach Notification
111 Sewall Street, 6th Floor
Augusta, ME 04330

Re: Notice of Data Security Incident

Dear Attorney General Frey:

Constangy, Brooks, Smith & Prophete, LLP represents R.J. Grondin & Sons, Inc. (“R.J. Grondin”) in connection with a recent data security incident described in greater detail below.

1. What Happened

On October 26, 2023, R.J. Grondin detected unusual activity associated with one employee’s email account. R.J. Grondin took immediate steps to secure the network and engaged a nationally recognized digital forensics firm to conduct an independent investigation into what happened. The investigation revealed that an unauthorized actor had access to information contained within the employee’s email account from October 12, 2023 until October 19, 2023.

With the assistance of outside data privacy and cybersecurity experts, R.J. Grondin conducted an investigation to identify the individuals whose personal information may have been impacted by this incident and the categories of information potentially involved for each individual. R.J. Grondin recently determined that the impacted email account contained consumers’ personal information. R.J. Grondin completed a comprehensive review of all affected information to identify which individuals were potentially impacted and locate relevant address information to effectuate notification to those whose personal information may have been involved which was completed on April 23, 2024.

Please note that R.J. Grondin has no reason to believe that the consumer’s information has been misused as a result of this incident.

2. What Information Was Involved

The data involved may have included individuals’ name in combination with driver's license or state identification, social security number, and/or account number.

3. Number of Maine Residents Notified

On April 30, 2024, R.J. Grondin notified 719 Maine residents of this data security incident via U.S. First-Class Mail. A sample copy or equivalent of the notification letter sent to potentially impacted individuals is included with this correspondence.

4. Steps Taken Relating to the Incident

As soon as R.J. Grondin discovered the incident, they took the steps described above. R.J. Grondin also performed a thorough review of their systems to investigate the incident and ensure that their systems remain secure. R.J. Grondin implemented additional security measures to protect their digital environment and minimize the likelihood of future incidents.

R.J. Grondin is also providing individuals whose Social Security numbers were potentially affected with access to 12 months of Single Bureau Credit Monitoring/Single Bureau Credit Report/Single Bureau Credit Score services and fraud assistance at no charge provided by IDX.

5. Contact Information

R.J. Grondin remains dedicated to protecting the personal information in its possession. If you have any questions or need additional information, please do not hesitate to contact me.

Best regards,

Lauren D. Godfrey

Lauren Godfrey

CONSTANGY, BROOKS, SMITH &
PROPHETE, LLP

Enclosure: Sample Notification Letter





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

<<FirstName>> <<LastName>>
<<Address1>> <<Address2>>
<<City>>, <<State>> <<Zip Code>>

Enrollment Code: <<XXXXXXXXXX>>

To Enroll, Scan the QR Code Below:

Or Visit:
<https://app.idx.us/account-creation/protect>

April 30, 2024

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

Dear <<FirstName>> <<LastName>>,

R.J. Grondin & Sons, Inc. (“Grondin”) is writing to inform you of a recent data security incident involving your personal information. At Grondin, 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 October 26, 2023, Grondin detected unusual activity associated with one employee’s email account. Grondin took immediate steps to secure the network and engaged a nationally recognized digital forensics firm to conduct an independent investigation into what happened. The investigation revealed that an unauthorized actor likely had access to information contained within the employee’s email account from October 12, 2023 until October 19, 2023. After a thorough review of the information potentially involved in the incident, Grondin determined that your personal information was contained in the account at the time the unauthorized actor likely had access to it. Grondin then worked to obtain contact information to provide you with notification of the incident which we completed on April 23, 2024.

We have no evidence that your information has been misused as a result of the incident.

What information was involved? The data that could have been accessed by the unauthorized party included your name and <<variable text 2>>.

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.

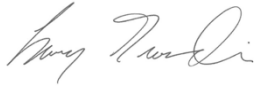
In addition, we are offering you the opportunity to enroll in complimentary identity protection services through IDX, a ZeroFox Company, a data breach and recovery services expert. These services include <<12/24>> months of credit monitoring and CyberScan monitoring, a \$1,000,000 insurance reimbursement 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 IDX’s complimentary identity protection services by scanning the QR code above, going to the link noted above, or calling 1-800-939-4170. When prompted, please provide the unique code above to enroll in the services. The deadline to enroll is July 29, 2024.

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 1-800-939-4170 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,



Larry Grondin
President



R.J. Grondin & Sons, Inc.
11 Bartlett Road
Gorham, ME 04038

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 proof. 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. An Active Duty Military Fraud Alert lasts for one year and can be renewed for the length of your deployment

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:

District of Columbia: The Office of the Attorney General for the District of Columbia can be reached at 400 6th Street, NW, Washington, DC 20001; 202-727-3400; oag@dc.gov; <https://oag.dc.gov/>.

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 2. 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/.

Vermont: The Vermont Attorney General's Office can be reached at: 109 State Street, Montpelier, VT 05609; 802-828-3171; ago.info@vermont.gov; <https://ago.vermont.gov/>.