



150 N. Riverside Plaza, Suite 3000, Chicago, IL 60606 • (312) 819-1900

October 21, 2019

Michael J. Waters

312-463-6212
312-819-1910
mwaters@polsinelli.com

VIA E-MAIL (ATTORNEYGENERAL@DOJ.NH.GOV)
AND FEDERAL EXPRESS

The Honorable Gordon MacDonald
Attorney General of the State of New Hampshire
Office of the Attorney General
33 Capitol Street
Concord, NH 03301

Re: Notification of a Data Security Incident

Dear Madam/Sir:

We represent Cornerstone Benefits, Inc. (“Cornerstone”), in connection with an incident that involved the personal information of two (2) New Hampshire residents and provide this notice on behalf of Cornerstone pursuant to N.H. REV. STAT. ANN. § 359-C:20.

This notice will be supplemented, if necessary, with any new significant facts discovered subsequent to its submission. While Cornerstone is notifying you of this incident, Cornerstone does not waive any rights or defenses relating to the incident or this notice, or the applicability of New Hampshire law on personal jurisdiction.

NATURE OF THE SECURITY BREACH OR UNAUTHORIZED USE OR ACCESS

Cornerstone recently determined that an unauthorized person was able to remotely access an email account of a Cornerstone employee. Upon discovery of the incident, Cornerstone immediately took action, including securing the email account credentials and retaining a leading forensic security firm to investigate and confirm the overall security of its email and computer systems.

On July 23, 2019, Cornerstone learned that the account contained personal information, which Cornerstone was maintaining on behalf of other organizations. These organizations (collectively known as the “Organizations”) include:

- Allen Organ Company
- Perkiomen School

polsinelli.com

Atlanta Boston Chicago Dallas Denver Houston Kansas City Los Angeles Nashville New York Phoenix
St. Louis San Francisco Seattle Washington, D.C. Wilmington
Polsinelli PC, Polsinelli LLP in California

October 21, 2019

Page 2

The personal information that was in the account varied by individual, but may have included an individual's name, address, financial account number and balance, and Social Security number. Cornerstone notified the Organizations of the incident and worked with them to identify the contact information for the impacted individuals.

At this point, Cornerstone is not aware of any fraud or identity theft to any individual as a result of this incident, and cannot confirm if any personal information was actually obtained by an unauthorized party. Nevertheless, because there was an email account compromise and Cornerstone cannot isolate exactly what, if any, information may have been obtained, Cornerstone is notifying all individuals whose personal information could have been accessed. Cornerstone is making these notifications on behalf of the Organizations.

NUMBER OF NEW HAMPSHIRE RESIDENTS AFFECTED

The incident may have impacted two (2) New Hampshire residents. Cornerstone mailed notification letters to impacted individuals on October 18, 2019. The notification letters include an offer for one (1) year of complimentary credit monitoring and identity theft protection. Enclosed is a copy of the notice that is being sent to the impacted residents via first-class United States mail.

STEPS TAKEN RELATING TO THE INCIDENT

Upon learning of the incident, Cornerstone promptly secured the email account to prevent further access. It also retained a leading forensic security firm to investigate and conduct a comprehensive search for any personal information in the impacted email account, and to confirm the security of its email and computer systems. Cornerstone is also providing complimentary identity theft protection services to all individuals whose Social Security or driver's license numbers were contained in the email account. Finally, Cornerstone provided the employee training on phishing and email safety.

CONTACT INFORMATION

Please do not hesitate to contact me if you have any questions or if I can provide you with any further information concerning this matter.

Very truly yours,



Michael J. Waters

Enclosure



*Insight.
Influence.
Integrity.*

<<Date>> (Format: Month Day, Year)

<<first_name>> <<middle_name>> <<last_name>> <<suffix>>
<<address_1>>
<<address_2>>
<<city>>, <<state_province>> <<postal_code>>
<<country >>

Dear <<first_name>> <<middle_name>> <<last_name>> <<suffix>>,

<<b2b_text_1>> The protection and privacy of the personal information entrusted to us is one of our highest priorities. Because of this, we are writing to make you aware of a recent data security incident. We recently discovered that someone accessed the email account of one of our employees without authorization. Upon discovering the incident, we took immediate action to secure the email account to prevent further access. We also retained a leading forensic security firm to investigate and confirm the security of our company's email and computer systems.

At this point, we do not know what, if any, emails in the account may have been viewed, but out of an abundance of caution, we searched the account for any personal information, and are providing you with this notice because some of your information was in the account. On July 23, 2019, we learned that the account contained some of your information. <<b2b_text_2>> Notice was thereafter provided to <<b2b_text_3>, with whom we have been working to prepare this notice to you.

We do not know for certain if any of your personal information was ever viewed or acquired by the unauthorized party, and we are not aware of any instances of identity theft as a result of this incident. However, because we value our relationship with you, we are offering you a complimentary one-year membership of Experian IdentityWorksSM Credit 3B. This product helps detect possible misuse of your personal information and provides you with identity protection services focused on immediate identification and resolution of identity theft. IdentityWorks Credit 3B is completely free to you and enrolling in this program will not hurt your credit score. **For more information on IdentityWorks Credit 3B, including instructions on how to activate your complimentary one-year membership, please see the additional information provided in this letter.**

We take our responsibility to safeguard personal information seriously and apologize for any inconvenience or concern this incident might cause. We are committed to taking steps to help prevent something like this from happening again, including reviewing our technical controls. For further information and assistance, please call 1-877-514-0839 from 9:00 a.m. to 6:30 p.m. ET, Monday through Friday.

Sincerely,

A handwritten signature in black ink, appearing to read "Chris McKinley".

Chris McKinley
Chief Compliance Officer

Activate IdentityWorks Credit 3B

To help protect your identity, we are offering a **complimentary** one-year membership of Experian IdentityWorksSM Credit 3B. This product helps detect possible misuse of your personal information and provides you with superior identity protection support focused on immediate identification and resolution of identity theft.

Activate IdentityWorks Credit 3B Now in Three Easy Steps

1. ENROLL by: <<b2b_text_4 (Date)>> (Your code will not work after this date.)
2. VISIT the **Experian IdentityWorks** website to enroll: <https://www.experianidworks.com/3bcredit>
3. PROVIDE the Activation Code: <<Member ID>>

If you have questions about the product, need assistance with identity restoration or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at 877-288-8057. Be prepared to provide engagement number <<b2b_text_5 (Engagement Number)>> as proof of eligibility for the identity restoration services by Experian.

ADDITIONAL DETAILS REGARDING YOUR 12-MONTH EXPERIAN IDENTITYWORKS CREDIT 3B MEMBERSHIP:

A credit card is **not** required for enrollment in Experian IdentityWorks Credit 3B.

You can contact Experian **immediately without needing to enroll in the product** regarding any fraud issues. Identity Restoration specialists are available to help you address credit and non-credit related fraud.

Once you enroll in Experian IdentityWorks, you will have access to the following additional features:

- **Experian credit report at signup:** See what information is associated with your credit file. Daily credit reports are available for online members only.*
- **Credit Monitoring:** Actively monitors Experian, Equifax and Transunion files for indicators of fraud.
- **Experian IdentityWorks ExtendCARE™:** You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- **\$1 Million Identity Theft Insurance**:** Provides coverage for certain costs and unauthorized electronic fund transfers.

Activate your membership today at <https://www.experianidworks.com/3bcredit> or call 877-288-8057 to register with the activation code above.

What you can do to protect your information: There are additional actions you can consider taking to reduce the chances of identity theft or fraud on your account(s). Please refer to www.ExperianIDWorks.com/restoration for this information. If you have any questions about IdentityWorks, need help understanding something on your credit report or suspect that an item on your credit report may be fraudulent, please contact Experian's customer care team at 877-288-8057.

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

** Identity theft insurance is underwritten by insurance company subsidiaries or affiliates of American International Group, Inc. (AIG). The description herein is a summary and intended for informational purposes only and does not include all terms, conditions and exclusions of the policies described. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

Additional Important Information

As a precautionary measure, we recommend that you remain vigilant to protect against potential fraud and/or identity theft by, among other things, reviewing your account statements and monitoring credit reports closely. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained. You should also promptly report any fraudulent activity or any suspected incidents of identity theft to proper law enforcement authorities, including the police and your state's attorney general, as well as the Federal Trade Commission ("FTC").

You may wish to review the tips provided by the FTC on fraud alerts, security/credit freezes and steps you can take to avoid identity theft. For more information and to contact the FTC, please visit www.ftc.gov/idtheft or call 1-877-ID-THEFT (1-877-438-4338). You may also contact the FTC at: Federal Trade Commission, 600 Pennsylvania Avenue, NW, Washington, DC 20580.

Credit Reports: You may obtain a free copy of your credit report once every 12 months from each of the three national credit reporting agencies by visiting <http://www.annualcreditreport.com>, by calling toll free 1-877-322-8228, 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 a copy of the request form at <https://www.annualcreditreport.com/cra/requestformfinal.pdf>.

Alternatively, you may elect to purchase a copy of your credit report by contacting one of the three national credit reporting agencies. Contact information for the three national credit reporting agencies for the purpose of requesting a copy of your credit report or for general inquiries, including obtaining information about fraud alerts and placing a security freeze on your credit files, is as follows:

Equifax	Experian	TransUnion
1-800-349-9960	1-888-397-3742	1-888-909-8872
www.equifax.com	www.experian.com	www.transunion.com
P.O. Box 105788	P.O. Box 9554	P.O. Box 2000
Atlanta, GA 30348	Allen, TX 75013	Chester, PA 19022

Fraud Alerts: You may want to consider placing a fraud alert on your credit report. An initial fraud alert is free and will stay on your credit file for at least one (1) year. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any new accounts in your name. To place a fraud alert on your credit report, contact any of the three national credit reporting agencies using the contact information listed above. Additional information is available at <http://www.annualcreditreport.com>.

Credit and Security Freezes: You may have the right to place a credit freeze, also known as a security freeze, on your credit file, so that no new credit can be opened in your name without the use of a PIN number that is issued to you when you initiate the freeze. A credit freeze is designed to prevent potential credit grantors from accessing your credit report without your consent. If you place a credit freeze, 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 credit freeze may delay your ability to obtain credit. Unlike a fraud alert, you must separately place a credit freeze on your credit file at each credit reporting company. Since the instructions for how to establish a credit freeze differ from state to state, please contact the three major credit reporting companies using the contact information above.

Individuals interacting with credit reporting agencies have rights under the Fair Credit Reporting Act. We encourage you to review your rights under the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by requesting information in writing from the Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. NW, Washington, DC 20580.

Iowa Residents: Iowa residents can contact the Office of the Attorney general to obtain information about steps to take to avoid identity theft from the Iowa Attorney General's office at: Office of the Attorney General of Iowa, Hoover State Office Building, 1305 E. Walnut Street, Des Moines IA 50319, 515-281-5164.

Maryland Residents: Maryland residents can contact the Office of the Attorney General to obtain information about steps one can take to avoid identity theft from the Maryland Attorney General's office at: Office of the Attorney General, 200 St. Paul Place, Baltimore, MD 21202, (888) 743-0023, www.oag.state.md.us.

North Carolina Residents: North Carolina residents can obtain information about preventing identity theft from the North Carolina Attorney General's Office at: North Carolina Attorney General's Office, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001; 877-5-NO-SCAM (Toll-free within North Carolina); 919-716-6000; www.ncdoj.gov.