



MULLEN
COUGHLIN_{LLC}
ATTORNEYS AT LAW

RECEIVED

JUN 01 2020

CONSUMER PROTECTION

Sian M. Schafle
Office: 267-930-4799
Fax: 267-930-4771
Email: sschafle@mullen.law

1275 Drummers Lane, Suite 302
Wayne, PA 19087

May 28, 2020

INTENDED FOR ADDRESSEE(S) ONLY
VIA U.S. MAIL

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

Re: Notice of Data Event

Dear Sir or Madam:

We represent Visionary Consulting Partners, LLC (“Visionary”), 4031 University Drive, Suite 100, Fairfax, VA 22030, and write to notify your office of an incident that may affect the security of some personal information relating to one (1) New Hampshire resident. This notice will be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, Visionary does not waive any rights or defenses regarding the applicability of New Hampshire law, the applicability of the New Hampshire data event notification statute, or personal jurisdiction.

Nature of the Data Event

Visionary became aware of unusual activity related to an employee email account. Visionary immediately launched an investigation and began working with third-party forensic investigators to determine the nature and scope of the incident. The investigation confirmed that a Visionary employee email account was subject to unauthorized access on separate occasions between January 25, 2019 and March 25, 2019. However, the investigation was unable to determine whether any information was viewed by the unauthorized actor. As a result, with the assistance of third-party forensic investigators, Visionary undertook a comprehensive programmatic and manual review of the email accounts to identify personal information present in the account at the time of the incident. Through this process, it was determined that personal information, as defined by N.H. Rev. Stat. § 359-C:19(IV)(a), may have been accessible, including one or more of the following: name and bank/financial account information. Visionary then reviewed its records to

identify contact information for individuals whose personal information was contained in the email account at the time of the incident.

Notice to New Hampshire Resident

Visionary's review determined that one (1) New Hampshire resident was potentially affected by this incident. On May 28, 2020, Visionary began mailing written notice of this incident in substantially the same form as the letter attached here as *Exhibit A*.

Other Steps Taken and To Be Taken

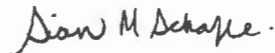
Upon discovering this incident, Visionary moved quickly to investigate and respond to the incident, assess the security of Visionary's systems, reset relevant passwords, and notify potentially affected individuals. While Visionary is unaware of any actual or attempted misuse of the potentially affected information, Visionary is offering complimentary access to credit monitoring and identity restoration services for one (1) year through Experian. Visionary is also working to implement additional training to its employees and is reviewing company policies and procedures relating to data security.

Additionally, Visionary is providing notified individuals with guidance on how to better protect against identity theft and fraud, including advising individuals to report any suspected incidents of identity theft or fraud to their credit card company and/or bank. Visionary is providing individuals with information on how to place a fraud alert and security freeze on one's credit file, the contact details for the national consumer reporting agencies, information on how to obtain a free credit report, a reminder to remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring free credit reports, and encouragement to contact the Federal Trade Commission, their state Attorney General, and law enforcement to report attempted or actual identity theft and fraud.

Contact Information

Should you have any questions regarding this notification or other aspects of the data security event, please contact us at (267) 930-4799.

Very truly yours,



Sian M. Schafle of
MULLEN COUGHLIN LLC

SMS/gcl
Enclosure

EXHIBIT A



<<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>>,

Visionary Consulting Partners, LLC ("Visionary") is writing to notify you of an incident that may affect the security of some of your personal information. We take this incident very seriously, and this letter provides details of the incident, our response, and resources available to you to help protect your information, should you feel it is appropriate to do so.

What Happened? Visionary became aware of unusual activity relating to an employee email account and immediately began an investigation. Working with third-party forensic investigators, we determined that the Visionary email account was subject to unauthorized access on separate occasions between January 25, 2019 and March 25, 2019. While the investigation did not determine that personal information had been viewed by an unauthorized actor, we could not rule out the possibility of such activity. Therefore, in an abundance of caution, Visionary engaged in a comprehensive review of the email account to determine whether sensitive information was present at the time of the incident. Through this process, we determined that the email account contained some personal information. Visionary then began a thorough review of our records to determine to whom the personal information belonged and their contact information for purposes of providing notice of this incident.

What Information Was Involved? Although we are unaware of any actual or attempted misuse of your personal information, we are providing you this notification out of an abundance of caution because your personal information was present in the impacted email account. The investigation confirmed the email account contained information including your <<b2b_text_3 (Impacted Data)>>.

What We Are Doing? Information privacy and security are among our highest priorities. Visionary has strict security measures in place to protect information in our care. Upon learning of this incident, we quickly took steps to confirm the security of our systems, including our employee email accounts. We reset passwords for relevant Visionary email accounts, conducted additional employee training, and reviewed our company policies and procedures relating to data security. We also reported this incident to law enforcement and relevant regulators, where required.

In an abundance of caution, we are also notifying you so that you may take further steps to best protect your personal information, should you feel it is appropriate to do so. We have also arranged to have Experian provide you with credit monitoring and identity restoration services for twelve (12) months at no cost to you, as an added precaution.

What You Can Do. You may review the information contained in the attached "Steps You Can Take to Protect Your Information." You may also enroll to receive the credit monitoring and identity protection services we are making available to you. If you would like to take advantage of these services, you will need to enroll yourself by following the instructions outlined in this letter as we are unable to active them for you.

For More Information. We recognize that you may have questions not addressed in this letter. If you have additional questions, please call our dedicated assistance line at 1-844-923-2641, Monday through Friday, from 8:00 a.m. to 5:30 p.m. Central Time.

Sincerely,

Michael D. Thornton, Sr.

Michael Thornton, Sr.
Chief Operating Officer
Visionary Consulting Partners, LLC

STEPS YOU CAN TAKE TO PROTECT YOUR INFORMATION

Enroll in Credit Monitoring

To help protect your identity, we are offering a complimentary one-year membership of Experian's® IdentityWorksSM. This product provides you with superior identity detection and resolution of identity theft. To activate your membership and start monitoring your personal information please follow the steps below:

- Ensure that you enroll by: <<b2b_text_1 (Date)>> (Your code will not work after this date.)
- Visit the Experian IdentityWorks website to enroll: <https://www.experianidworks.com/3bcredit>
- Provide your 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** by <<b2b_text_1 (Date)>>. Be prepared to provide engagement number <<b2b_text_2 (Engagement #)>> as proof of eligibility for the identity restoration services by Experian.

Monitor Your Accounts

We encourage you to remain vigilant against incidents of identity theft and fraud, to review your account statements, and to monitor your credit reports for suspicious activity. Under U.S. law you are entitled to one free credit report annually from each of the three major credit reporting bureaus. To order your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also contact the three major credit bureaus directly to request a free copy of your credit report.

You have the right to place a "security freeze" on your credit report, which will prohibit a consumer reporting agency from releasing information in your credit report without your express authorization. The security freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, you should be aware that using a security freeze to take control over who gets access to the personal and financial information in your credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, you cannot be charged to place or lift a security freeze on your credit report. Should you wish to place a security freeze, please contact the major consumer reporting agencies listed below:

Experian

P.O. Box 9554
Allen, TX 75013
1-888-397-3742

www.experian.com/freeze/center.html

TransUnion

P.O. Box 160
Woodlyn, PA 19094
1-888-909-8872

www.transunion.com/credit-freeze

Equifax

P.O. Box 105788
Atlanta, GA 30348-5788
1-800-685-1111

www.equifax.com/personal/credit-report-services

In order to request a security freeze, you will need to provide the following information:

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. If you have moved in the past five (5) years, provide the addresses where you have lived over the prior five years;
5. Proof of current address, such as a current utility bill or telephone bill;
6. A legible photocopy of a government-issued identification card (state driver's license or ID card, military identification, etc.);
7. If you are a victim of identity theft, include a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft.

As an alternative to a security freeze, you have the right to place an initial or extended "fraud alert" on your file at no cost. An initial fraud alert is a 1-year alert that is placed on a consumer's credit file. Upon seeing a fraud alert display on a consumer's credit file, a business is required to take steps to verify the consumer's identity before extending new credit. If you are a victim of identity theft, you are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should you wish to place a fraud alert, please contact any one of the agencies listed below:

Experian

P.O. Box 9554
Allen, TX 75013
1-888-397-3742
www.experian.com/fraud/center.html

TransUnion

P.O. Box 2000
Chester, PA 19016
1-800-680-7289
www.transunion.com/fraud-victim-resource/place-fraud-alert

Equifax

P.O. Box 105069
Atlanta, GA 30348
1-888-766-0008
www.equifax.com/personal/credit-report-services

Additional Information

You can further educate yourself regarding identity theft, fraud alerts, security freezes, and the steps you can take to protect yourself by contacting the consumer reporting agencies, the Federal Trade Commission, or your state Attorney General.

The Federal Trade Commission can be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580, www.identitytheft.gov, 1-877-ID-THEFT (1-877-438-4338); TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. You can obtain further information on how to file such a complaint by way of the contact information listed above. You have the right to file a police report if you ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, you will likely need to provide some proof that you have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and your state Attorney General. This notice has not been delayed by law enforcement.

For Maryland residents, the Attorney General can be contacted at 200 St. Paul Place, 16th Floor, Baltimore, MD 21202, 1-410-528-8662, www.oag.state.md.us.

For New Mexico residents, you have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for credit reports to be provided to employers; you may limit "prescreened" offers of credit and insurance you get based on information in your credit report; and you may seek damages from violator. You may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. We encourage you to review your rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

For North Carolina residents, the Attorney General can be contacted at 9001 Mail Service Center, Raleigh, NC 27699-9001, 1-877-566-7226 or 1-919-716-6000, www.ncdoj.gov. You can obtain information from the Attorney General or the Federal Trade Commission about preventing identity theft.

For New York residents, the Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; <https://ag.ny.gov/>.