



MULLEN
COUGHLIN^{LLC}
ATTORNEYS AT LAW

RECEIVED

MAR 02 2021

CONSUMER PROTECTION

M. Alexandra Belton
Office: 267-930-4773
Fax: 267-930-4771
Email: abelton@mullen.law

426 W. Lancaster Avenue, Suite 200
Devon, PA 19333

February 25, 2021

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 Igoe & Company Incorporated (“Igoe”) located at 15090 Avenue of Science, San Diego, CA 92128, and are writing to notify your Office of an incident that may affect the privacy of personal information related to one New Hampshire resident. By providing this notice, Igoe does not waive any rights or defenses regarding the applicability of New Hampshire law or personal jurisdiction.

Nature of the Data Event

Igoe is an employee benefits administrator that provides services to organizations, including the California High Technology Employers Benefit Trust (“Tech Trust”). Igoe is providing notice on behalf of Tech Trust. On March 11, 2020, Igoe learned of unusual activity related to an email account associated with one of its business partners who assists in its COBRA benefit services. Igoe immediately began an investigation, with the assistance of third-party computer forensics specialists, to determine the full nature and scope of the incident. Igoe’s investigation determined that the email account was subject to unauthorized access between February 25, 2020 and March 11, 2020. Although Igoe’s investigation was unable to confirm if specific information within the email account was accessed, Igoe was unable to rule out that possibility. Therefore, Igoe engaged in a comprehensive programmatic and manual review of the entire contents of the email account to determine the type of information contained in the account and to whom the information related. On June 10, 2020, Igoe completed its review and then worked to confirm contact information for potentially impacted individuals and the associated Igoe employer group to whom the individual related. On August 13, 2020, Igoe provided notice of this incident to Tech Trust.

Mullen.law

The type of information in the account included name and Social Security number.

Notice to New Hampshire Resident

On September 25, 2020, Igoe provided written notice of this incident on behalf of Tech Trust to a single New Hampshire resident. Written notice was provided in substantially the same form as the letter attached here as *Exhibit A*. On February 19, 2021, Tech Trust requested that Igoe also provide notice to required state regulators.

Other Steps Taken and To Be Taken

Upon discovering this incident, Igoe moved quickly to investigate and respond and assess the security of Igoe's systems, including its email accounts. Igoe also reviewed existing security policies and implemented additional security measures, including enhancing security training regarding phishing attacks, upgrading its email environment to include additional logging and security features, incorporating conditional access to restrict email account access to internal resources only, automatic enforcement of multi-factor authentication for any exception for the internal conditional access restriction, enabling geo-blocking, and adding warning labels to emails from external sources.

Igoe provided potentially impacted individuals with access to credit monitoring and identity theft protection services for one year through TransUnion. Additionally, Igoe provided potentially impacted 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) 930-4773.

Very truly yours,



M. Alexandra Belton of
MULLEN COUGHLIN LLC

MAB/ara
Enclosure

EXHIBIT A



Return Mail Processing Center
 P.O. Box 6336
 Portland, OR 97228-6336

<<Mail ID>>
 <<Name 1>>
 <<Name 2>>
 <<Address 1>>
 <<Address 2>>
 <<Address 3>>
 <<Address 4>>
 <<Address 5>>
 <<City>><<State>><<Zip>>
 <<Country>>

<<Date>>

Notice of Data Breach

Dear <<Name 1>>:

Igoe Administrative Services (“Igoe”) is an employee benefits administrator that provides services to employers, including <<Variable Data 2>> and writes to notify you of an incident that may affect the privacy of some of your personal information. Igoe takes the protection of your information seriously, and although we have no evidence of actual or attempted misuse of your information, this letter provides details about the incident, our response, and resources available to you to help protect your information from possible misuse, should you feel it is appropriate to do so.

What Happened? On or about March 11, 2020, Igoe was made aware of unusual activity related to an email account associated with one of our business partners who assists in our COBRA benefit services. We immediately began an investigation, with the assistance of third-party computer forensics specialists, to determine the full nature and scope of the incident. Our investigation determined that the email account was subject to unauthorized access between February 25, 2020 and March 11, 2020. Although our investigation was unable to confirm if specific information within the email account was accessed, we were unable to rule out that possibility. Therefore, we engaged in a comprehensive programmatic and manual review of the contents of the email account to determine the type of information contained in the account and to whom the information related. On <<Variable Data 3>>, Igoe provided notice of this incident to its impacted business partners. Although we are unaware of any actual or attempted misuse of your personal information, in an abundance of caution, we are providing you this notice because your information was present in the email account

What Information Was Involved? The information present in the email account at the time of the incident may have included your first and last name and the following: <<Breached Elements>>.

What We Are Doing. Information privacy and security are among our highest priorities. Igoe has strict security measures in place and also requires our business partners to implement rigorous security measures to protect information entrusted to us. Since this incident, we reviewed existing security policies and implemented additional measures to further protect information, including enhanced email security. We are also notifying potentially impacted individuals, including you, so that you may take steps to best protect your information, should you feel it is appropriate to do so. Although we are unaware of any actual or attempted misuse of information as a result of this incident, we arranged to have TransUnion protect your identity for 1 year at no cost to you as an added precaution.

What Can You Do. 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. You may review the information contained in the attached “Steps You Can Take to Help Protect Your Information.” You may also enroll to receive the identity protection services we are making available to you. There is no charge to you for the cost of this service; however, you will need to enroll yourself in this service.

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 855-907-2129 (toll free), Monday through Friday, 6:00 a.m. to 6:00 p.m., PST.

We sincerely regret any inconvenience this incident may cause you. Protecting your information is important to us, and Igoe remains committed to safeguarding the information in our care.

Sincerely,

A handwritten signature in black ink that reads "Laura K. McKinlay". The signature is written in a cursive style with a large, stylized initial "L".

Laura McKinlay
President/CEO
Igoe Administrative Services

Steps You Can Take to Help Protect Your Information

Credit Monitoring and Identity Restoration Services

See last page for instructions.

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
1-800-349-9960
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
1-800-525-6285
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 may be contacted at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202, 1-410-528-8662, www.oag.state.md.us.

For North Carolina residents, the Attorney General may 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/>.

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 violators. 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 Rhode Island residents, the Rhode Island Attorney General may be reached at: 150 South Main Street, Providence, Rhode Island 02903; www.riag.ri.gov; or 1-401-274-4400. Under Rhode Island law, you have the right to obtain any police report filed in regard to this incident. There are approximately 0 Rhode Island residents whose information may have been impacted by this event.

Activation Code: <<Activation Code>>

Complimentary One-Year *myTrueIdentity* Credit Monitoring Service

As a safeguard, we have arranged for you to enroll, at no cost to you, in an online credit monitoring service (*myTrueIdentity*) for one year provided by TransUnion Interactive, a subsidiary of TransUnion,[®] one of the three nationwide credit reporting companies.

How to Enroll: You can sign up online or via U.S. mail delivery

- To enroll in this service, go to the *myTrueIdentity* website at www.MyTrueIdentity.com and, in the space referenced as "Enter Activation Code," enter the 12-letter Activation Code <<Insert Unique 12-letter Activation Code>> and follow the three steps to receive your credit monitoring service online within minutes.
- If you do not have access to the Internet and wish to enroll in a similar offline, paper-based credit monitoring service, via U.S. mail delivery, please call the TransUnion Fraud Response Services toll-free hotline at **1-855-288-5422**. When prompted, enter the six-digit telephone passcode <<Insert static 6-digit Telephone Pass Code>> and follow the steps to enroll in the offline credit monitoring service, add an initial fraud alert to your credit file, or to speak to a TransUnion representative if you believe you may be a victim of identity theft.

You can sign up for the online or offline credit monitoring service anytime between now and <<Enrollment Deadline>>. Due to privacy laws, we cannot register you directly. Please note that credit monitoring services might not be available for individuals who do not have a credit file with TransUnion or an address in the United States (or its territories) and a valid Social Security number. Enrolling in this service will not affect your credit score.

ADDITIONAL DETAILS REGARDING YOUR 12-MONTH COMPLIMENTARY CREDIT MONITORING SERVICE:

- Once you are enrolled, you will be able to obtain one year of unlimited access to your TransUnion credit report and credit score.
- The daily credit monitoring service will notify you if there are any critical changes to your credit file at TransUnion, including fraud alerts, new inquiries, new accounts, new public records, late payments, changes of address, and more.
- The service also includes access to an identity restoration program that provides assistance in the event that your identity is compromised and up to \$1,000,000 in identity theft insurance with no deductible. (Policy limitations and exclusions may apply.)