



MULLEN
COUGHLIN^{LLC}
ATTORNEYS AT LAW

RECEIVED

DEC 16 2019

CONSUMER PROTECTION

Paul T. McGurkin, Jr.
Office: (267) 930-4788
Fax: (267) 930-4771
Email: pmcgurkin@mullen.law

1275 Drummers Lane, Suite 302
Wayne, PA 19087

December 10, 2019

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:

Our office represents Insero & Co., CPAs, LLP (“Insero”) located at 2 State Street, Suite 300, Rochester, NY 14614. Insero provides accounting and auditing services to its many clients. We write on behalf of the Insero clients listed on *Exhibit A* to notify your office of an incident that may affect the security of some personal information relating to four (4) New Hampshire residents who are employees of the various Insero clients listed in Exhibit A. This notice may be supplemented where additional Insero clients request notice be provided on their behalf. By providing this notice, Insero and its clients do 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

On July 18, 2019, Insero identified suspicious activity occurring in an employee’s email account. Insero immediately changed the employee’s password, secured the account, and began an internal investigation into the incident. Insero also engaged a third-party forensic investigation firm to determine the nature and scope of the incident. The forensic investigation revealed that the Insero employee’s email account was subject to unauthorized access from July 16, 2019 to July 18, 2019. The forensic investigation was unable to confirm if personal information was accessed by an unauthorized actor. The investigators were only able to confirm that the personal information was found within an email account subject to unauthorized access. Therefore, the forensic investigators undertook a lengthy programmatic and manual review of all emails and attachments in the email account subject to unauthorized access to determine whether the emails and attachments contained

any sensitive information. This review concluded on August 19, 2019. However, the documentation provided by the investigators did not list the client to whom the individual related. Therefore, an additional manual review of Insero's internal records was conducted so that Insero could provide notice of the incident to the appropriate client. This review was completed on October 21, 2019.

On October 25, 2019, Insero began providing its data owner clients with notice of this incident and offered to provide notice to potentially impacted client employees and applicable state regulators on their behalf. In order to provide notice on behalf of Insero clients, Insero requested that all client employee addresses be provided so that notice letters could be submitted in a timely fashion. The affected email account contained information related to four (4) New Hampshire residents. The information related to these individuals includes their name, Social Security number, and date of birth.

Notice to New Hampshire Residents

On December 11, 2019, Insero will begin mailing written notice of this incident to affected New Hampshire residents in substantially the same form as the letter attached here as *Exhibit B*.¹

Other Steps Taken and To Be Taken

Insero is offering individuals impacted by this incident with access to complimentary credit monitoring and identity restoration services. Additionally, Insero is providing potentially impacted individuals with guidance on how to protect against identity theft and fraud, including 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.

Insero is also taking steps to mitigate the risk that an event like this will occur again in the future by reviewing its policies and procedures and implementing additional safeguards which include:

- Limiting access to email to only users from a Microsoft Outlook client;
- Updating email and network password rules to require 10-characters, uppercase, lowercase, numeric and special character use;
- Activating Microsoft Office 365 logging to track access to email systems; and
- Activating Microsoft Outlook email archiving features to automatically dispose of deleted emails.

In addition to providing notice to your office, Insero is providing notice to other state regulators and the consumer reporting agencies, as required.

¹ Gettysburg College directly notified its affected employees on November 15, 2019.

Consumer Protection Bureau
December 10, 2019
Page 3

Contact Information

Should you have any questions regarding this notification or other aspects of the data security event, please contact us at 267-930-4788.

Very truly yours,

A handwritten signature in black ink, appearing to read "Paul R.", with a long horizontal flourish extending to the right.

Paul T. McGurkin, Jr. of
MULLEN COUGHLIN LLC

PTM/mep
Enclosure

EXHIBIT A

Insero Clients

- Dover Corp.
- Gettysburg College

EXHIBIT B



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>>

RE: Notice of Data Breach

Dear <<Name 1>>

Insero & Co., CPAs, LLP (“Insero”) which provides accounting services to your employer, is writing to inform you of a recent event that may impact the privacy of some of your personal information. We wanted to provide you with information about the event, our response, and steps you may take to better protect against the possibility of identity theft and fraud, should you feel it necessary.

What Happened? Insero recently identified suspicious activity in an employee’s email account. Insero immediately changed the employee’s password and began an internal investigation into the incident. Insero also engaged a third-party forensic investigation firm to determine the nature and scope of the incident. The forensic investigation revealed that the Insero employee’s email account was subject to unauthorized access from July 16, 2019 to July 18, 2019. The forensic investigators then undertook a lengthy programmatic and manual review of all emails and attachments in the email account subject to unauthorized access to determine whether the emails and attachments contained any sensitive information. This review concluded on August 19, 2019. However, the documentation provided by the investigators did not list the Insero client to whom the identified individual related. Therefore, a manual review of Insero’s internal records was conducted so that Insero could provide notice of the incident to the appropriate client and the corresponding individual(s).

On October 21, 2019, Insero completed its work to match potentially affected individuals to their employer. On October 25, 2019 Insero began providing notice of the incident to its clients, including your employer, and requested permission to provide you with notice.

What Information Was Involved? The following information about you was found within the employee’s email account: your name and <<Data Elements>>. The forensic investigation was unable to confirm if the email or attachment with your information was viewed by the unauthorized actor. We were only able to confirm that your information was found within the email account subject to unauthorized access. To date, there is no indication that any of this information has been subject to actual or attempted misuse.

What We Are Doing. We take this incident and the security of personal information on our computer systems seriously. Upon discovery of this incident, we immediately took steps to secure the email account and launched an in-depth investigation with the assistance of a third-party forensic investigation firm to determine the full nature and scope of this incident. As part of our ongoing commitment to the privacy of personal information in our care, we reviewed our existing policies and procedures and implemented additional safeguards to further secure the information in our systems. We are also notifying regulatory authorities, as required by law.

As an added precaution, we are also offering complimentary access to credit monitoring, fraud consultation, and identity theft restoration services through TransUnion. Individuals who wish to receive these services must enroll by following the attached enrollment instructions.

What You Can Do. You can find out more about how to protect against potential identity theft and fraud in the enclosed *Steps You Can Take to Protect Against Identity Theft and Fraud*. There you will also find more information on the credit monitoring services we are offering and how to enroll.

For More Information. We understand that you may have questions about this incident that are not addressed in this letter. If you have additional questions, please call our dedicated assistance line at 833-991-0972, Monday through Friday from 9am to 9pm Eastern Time.

Insero sincerely regrets any inconvenience or concern this incident may have caused you.

Sincerely,

A handwritten signature in black ink, appearing to read "Timothy McLaughlin". The signature is fluid and cursive, with a long horizontal stroke extending to the right.

Timothy McLaughlin
Insero & Co. CPAs, LLP

Steps You Can Take to Protect Against Identity Theft and Fraud

Enroll in Credit Monitoring

While we are unaware of any actual or attempted misuse of your information, in an abundance of caution, we have secured the services of TransUnion to provide Credit Monitoring Services at no cost to you for <<Credit Monitoring>> months.

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.

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
PO Box 9554
Allen, TX 75013
1-888-397-3742
[www.experian.com/freeze/
center.html](http://www.experian.com/freeze/center.html)

TransUnion
P.O. Box 160
Woodlyn, PA 19094
1-888-909-8872
[www.transunion.com/
credit-freeze](http://www.transunion.com/credit-freeze)

Equifax
PO Box 105788
Atlanta, GA 30348-5788
1-800-685-1111
[www.equifax.com/personal/
credit-report-services](http://www.equifax.com/personal/credit-report-services)

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](http://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](http://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](http://www.equifax.com/personal/credit-report-services)

Additional Information

Although we have no reason to believe that your personal information has been used to file fraudulent tax returns, you can contact the IRS at www.irs.gov/Individuals/Identity-Protection for helpful information and guidance on steps you can take to address a fraudulent tax return filed in your name and what to do if you become the victim of such fraud. You can also visit www.irs.gov/uac/Taxpayer-Guide-to-Identity-Theft for more information.

If you identify any fraudulent or suspicious charges on your credit or debit card, you should immediately contact your bank or financial institution. It is also a good practice to remain vigilant of unsolicited communications seeking your credit card or other financial information. Incidents of identity theft should also be reported to your local law enforcement.

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, (410) 528-8662, www.oag.state.md.us.

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 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 Rhode Island Residents, the Rhode Island Attorney General can be reached at: 150 South Main Street, Providence, Rhode Island 02903; www.riag.ri.gov. (401) 274-4400. Under Rhode Island law, you have the right to obtain any police report filed in regard to this incident. There are two Rhode Island residents impacted by this incident.