

July 19, 2016

Blaine C. Kimrey
Shareholder
+1 312 609 7865
bkimrey@vedderprice.com

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

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

**Re: Notification of Cybersecurity Incident Potentially Affecting New Hampshire Resident
Pursuant to N.H. Rev. Stat. § 359-C:20**

Dear Madam/Sir:

We represent IMA[®] (Institute of Management Accountants) in connection with a recent incident that may have impacted the security of certain personal information of one (1) New Hampshire resident. Pursuant to N.H. Rev. Stat. § 359-C:20 IMA is reporting potential unauthorized access to this information.

The investigation of this incident is ongoing, and this notice will be supplemented, if necessary, with any new significant facts discovered after its submission. By providing this notice, IMA does not waive any potential rights or defenses regarding applicability of New Hampshire law or personal jurisdiction in connection with this incident.

Background of the Incident

IMA is a worldwide association of accountants and financial professionals working in business. IMA is headquartered in Montvale, New Jersey, but it provides services to members and customers throughout the United States.

IMA was informed on June 20, 2016, that one of its vendors, Comnet Marketing Group, Inc. ("Comnet"), had been the victim of a potential computer hacker intrusion. An unauthorized user gained administrative access to Comnet's systems on April 23-24, 2016, and issued commands to delete all the data housed on Comnet's servers. That data may have included certain IMA member/customer credit card information that Comnet had collected and stored on behalf of IMA. Comnet did not discover any evidence indicating that the credit card data was accessed or acquired by an unauthorized user or that the unauthorized user intended to steal data. But Comnet says it has been unable to definitively rule out any unauthorized access to or acquisition of data because data potentially relevant to its forensic investigation was deleted by the unauthorized user. Thus, IMA provides this notice out of an abundance of caution.

Upon becoming aware of the potential incident, Comnet immediately launched an investigation to determine whether a security incident had occurred. Specifically, Comnet hired experts to assist in the investigation and response, and has referred this matter to appropriate law enforcement. Consumer credit card information is no longer contained in or accessible via Comnet's systems. Additionally, IMA has terminated its relationship with Comnet, and Comnet no longer serves as a vendor for IMA.

IMA is providing notice to a certain New Hampshire resident that his or her name, postal mailing address, email address, phone number, credit card number, CVV code, and expiration date may have been impacted.

Notice to the New Hampshire Resident

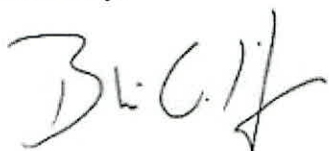
On or about July 20, 2016, IMA is notifying the one (1) potentially affected New Hampshire resident of the incident. Enclosed is a sample of the notification letter that will be sent to the New Hampshire resident via United States first-class mail.

In addition, IMA has established a call center (888-246-3713) that customers can contact between the hours of 9:00 a.m. and 9:00 p.m. Eastern Time to ask questions and to receive further information regarding the incident. IMA has arranged to offer one (1) year of complimentary credit monitoring through Equifax to the affected New Hampshire resident.

Contact Information

Please contact me if you have any questions or if I can provide you with any further information concerning this matter. Thank you.

Sincerely,

A handwritten signature in black ink, appearing to read "B.C. Kimrey", with a stylized flourish at the end.

Blaine C. Kimrey

BCK

cc: IMA



The Association of
Accountants and
Financial Professionals
in Business

Return Mail Processing Center
PO Box 6336
Portland, OR 97228-6336

<<mail id>>
<<FirstName>><<LastName>>
<<Address1>>
<<Address2>>
<<City>><<State>><<Zip>>

<<Date>>

Dear <<Name1>>,

IMA® (Institute of Management Accountants) is committed to the privacy of our members and customers and the security of their information. As part of this commitment, we are providing you this notice regarding an information security incident that could affect you.

What Happened

IMA was informed on June 20, 2016, that one of its vendors, Comnet Marketing Group, Inc. ("Comnet"), had been the victim of an intrusion of its computer systems. An unauthorized user gained administrative access to Comnet's systems on April 23-24, 2016, and issued commands to delete all the data housed on Comnet's servers. That data may have included certain IMA member/customer credit card information that Comnet had collected on behalf of IMA. Comnet did not discover any evidence indicating that the credit card data was accessed or acquired by an unauthorized user or that the unauthorized user intended to steal data. But Comnet has been unable to definitively rule out any unauthorized access to or acquisition of data. Thus, IMA provides this notice out of an abundance of caution.

What Information Was Involved

The information potentially at risk included your name, postal mailing address, email address, phone number, credit card number, CVV code, and expiration date.

What We Are Doing

Investigation. Comnet has referred this matter to appropriate law enforcement, and Comnet's investigation regarding the potential responsible parties is ongoing.

Mitigation. IMA has hired Equifax to provide, at no cost to you, credit monitoring services. The details for opting in to these services are set forth below.

Protection Against Further Harm. No intrusion of IMA's computer systems occurred during this incident and your information is no longer contained in or accessible via Comnet's systems. Additionally, IMA has terminated its relationship with Comnet, and Comnet no longer serves as a vendor for IMA.

What You Can Do

Although we do not have any evidence that your information was accessed or misused as a result of this computer security incident, your information may be at risk. To help protect you, we have partnered with Equifax® to provide its Credit Watch Gold identity theft protection product for one year at no charge to you. A description of this product is provided in the attached material, which also contains instructions about how to enroll (including your personal activation code). If you choose to take advantage of this product, it will provide you with a notification of any changes to your credit information, up to \$25,000 Identity Theft Insurance Coverage and access to your credit report.

You must complete the enrollment process by October 31, 2016. We urge you to consider enrolling in this product, at our expense, and reviewing the Additional Resources enclosed with this letter.

Remain vigilant for any unauthorized use of your credit card information. We suggest that you review your credit card account statements and monitor your credit reports, which you can obtain for free from the three credit reporting agencies listed below. If you feel your credit card information may have been compromised, consider contacting your credit card company and having it cancel your current card and reissue a new card. If you suspect incidents of identity theft, you should notify local law enforcement and/or your state attorney general. We are also contacting the following credit report companies regarding the computer security incident:

Equifax
P.O. Box 105788
Atlanta, GA 30348
(800) 525-6285
www.equifax.com

Experian
P.O. Box 9554
Allen, TX 75013
(888) 397-3742
www.experian.com

TransUnion
Fraud Victim Asst. Div.
P.O. Box 6790
Fullerton, CA 92834
(800) 680-7289
www.transunion.com

For More Information

If you have questions and concerns please contact our toll free number, 888-246-3713 between the hours of 9:00 a.m. and 9:00 p.m. Eastern Time. Additionally, for more information about avoiding identity theft, you can contact the Federal Trade Commission at 600 Pennsylvania Ave. N.W., Washington, D.C. 20580, 1-877-ID-THEFT, consumer.ftc.gov. Residents of Maryland may also obtain information about avoiding identity theft from the Maryland Office of the Attorney General, 200 St. Paul Place, Baltimore, MD 21202, 1-888-743-0023, www.oag.state.md.us. Residents of North Carolina may also obtain information about avoiding identity theft from the North Carolina Attorney General's Office, 9001 Mail Service Center, Raleigh, NC 27699-9001, 1-877-5-NO-SCAM, www.ncdoj.gov.

Sincerely,



Jeff Thomson, CMA, CAE
President and CEO
IMA (Institute of Management Accountants)



Activation Code: <<INSERT Credit Monitoring Code>>

About the Equifax Credit Watch™ Gold identity theft protection product

Equifax Credit Watch will provide you with an “early warning system” to changes to your credit file. Note: You must be over age 18 with a credit file in order to take advantage of the product.

Equifax Credit Watch provides you with the following key features and benefits:

- Comprehensive credit file monitoring and automated alerts of key changes to your **Equifax** credit report
- Wireless alerts and customizable alerts available (available online only)
- Access to your Equifax Credit Report™
- Up to \$25,000 in identity theft insurance with \$0 deductible, at no additional cost to you †
- Live agent Customer Service 7 days a week from 8 a.m. to 3 a.m. to assist you in understanding the content of your Equifax credit information, to provide personalized identity theft victim assistance, and help initiate an investigation of inaccurate information.
- 90 day Fraud Alert placement with automatic renewal functionality* (available online only)

How to Enroll: You can sign up online or over the phone

To sign up online for **online delivery** go to www.myservices.equifax.com/gold

1. Welcome Page: Enter the Activation Code provided at the top of this page in the “Activation Code” box and click the “Submit” button.
2. Register: Complete the form with your contact information (name, gender, home address, date of birth, Social Security Number and telephone number) and click the “Continue” button.
3. Create Account: Complete the form with your email address, create a User Name and Password, check the box to accept the Terms of Use and click the “Continue” button.
4. Verify ID: The system will then ask you up to four security questions to verify your identity. Please answer the questions and click the “Submit Order” button.
5. Order Confirmation: This page shows you your completed enrollment. Please click the “View My Product” button to access the product features.

To sign up for **US Mail delivery**, dial 1-866-937-8432 for access to the Equifax Credit Watch automated enrollment process. Note that all credit reports and alerts will be sent to you via US Mail only.

1. Activation Code: You will be asked to enter your enrollment code as provided at the top of this letter.
2. Customer Information: You will be asked to enter your home telephone number, home address, name, date of birth and Social Security Number.
3. Permissible Purpose: You will be asked to provide Equifax with your permission to access your credit file and to monitor your file. Without your agreement, Equifax cannot process your enrollment.
4. Order Confirmation: Equifax will provide a confirmation number with an explanation that you will receive your Fulfillment Kit via the US Mail (when Equifax is able to verify your identity) or a Customer Care letter with further instructions (if your identity can not be verified using the information provided). Please allow up to 10 business days to receive this information.

Directions for placing a Fraud Alert

A fraud alert is a consumer statement added to your credit report. This statement alerts creditors of possible fraudulent activity within your report as well as requests that they contact you prior to establishing any accounts in your name. Once the fraud alert is added to your credit report, all creditors should contact you prior to establishing any account in your name. To place a fraud alert on your credit file, visit: https://www.alerts.equifax.com/AutoFraud_Online/jsp/fraudAlert.jsp or you may contact the Equifax auto fraud line at 1-877-478-7625, and follow the simple prompts. Once the fraud alert has been placed with Equifax, a notification will be sent to the other two credit reporting agencies, Experian and Trans Union, on your behalf.

† Identity Theft Insurance underwritten by insurance company subsidiaries or affiliates of American International Group, Inc. 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. This product is not intended for minors (under 18 years of age)

* The Automatic Fraud Alert feature made available to consumers by Equifax Information Services LLC and fulfilled on its behalf by Equifax Consumer Services LLC

STATE OF NH
DEPT OF JUSTICE
2016 JUL 20 AM 9:43