

KIRKLAND & ELLIS LLP
AND AFFILIATED PARTNERSHIPS

STATE OF NH
DEPT OF JUSTICE

2016 APR 22 AM 10: 21

655 Fifteenth Street, N.W.
Washington, D.C. 20005

(202) 879-5000

www.kirkland.com

Facsimile:
(202) 879-5200

John A. Eisenberg
To Call Writer Directly:
(202) 879-5902
john.eisenberg@kirkland.com

April 21, 2016

VIA FEDERAL EXPRESS

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

Dear Mr. Attorney General:

I am writing as counsel to Examination Management Services, Inc. ("EMSI") to notify you of an incident that occurred on March 24, 2016, in which employee and former employee W-2 Forms from 2015 were disclosed to an unknown party in response to a "spoofed" email that appeared to come from an authorized internal EMSI email account. According to EMSI's records, it appears that the personal information of 10 New Hampshire residents was included in the disclosed information.

EMSI's investigation into this incident continues, and EMSI is cooperating with law enforcement, including the Federal Bureau of Investigation. In addition, EMSI is reviewing its internal procedures and protocols to help prevent this sort of incident from occurring again.

Because EMSI takes the security of the personal information of its employees and former employees very seriously, it wanted to let affected individuals know about the disclosure as soon as possible. Accordingly, EMSI sent affected individuals a memorandum with initial information by March 30, 2016. EMSI subsequently mailed written notices pursuant to Section 359-C:20 of the Revised Statutes of New Hampshire on April 6, 2016. Copies of the written notice pursuant to the statute and of the initial memorandum are attached hereto. Notice was not delayed because of a law enforcement investigation. To protect affected individuals, EMSI is offering identity protection services from Equifax for 12 months from the date of the notice.

If you have any questions relating to this incident, please do not hesitate to contact me.

Sincerely,



John A. Eisenberg

Enclosures: Memorandum re Potential Disclosure of Personally Identifiable Information
Notice of Data Breach



Memorandum re Potential Disclosure of Personally Identifiable Information

Date: March 28, 2016

This memorandum is to inform you that we believe that your W-2 Form for 2015 may have been disclosed to an unauthorized party on Thursday, March 24, 2016. W-2 Forms contain such information as your full name, address, Social Security Number, and wage and tax information.

Although we have no specific evidence to date that this information has been used improperly, we are concerned that someone could attempt to use it to file a fraudulent tax return on your behalf or to open credit in your name. Because the security of your personal information is a top priority for us, we immediately contacted law enforcement and will cooperate with them as they investigate this crime. In the near future, we will send you a notification letter with additional information. In the meantime, we wanted to let you know the following:

First, if you believe you have been impacted by tax fraud, please follow the steps outlined in the IRS publication entitled Identity Theft Information for Taxpayers, available at <https://www.irs.gov/pub/irs-pdf/p5027.pdf>.

Second, you can contact the IRS for assistance with any questions you may have regarding your tax return at 800-908-4490, Monday-Friday, 7 a.m. – 7 p.m. (in your local time zone; Alaska and Hawaii follow Pacific Time).

Third, to help protect your credit, EMSI has arranged with Equifax Personal Solutions to provide you with a one-year subscription for Equifax Credit Watch™ Gold with 3-in-1 Monitoring Identity Theft Protection Product, at no cost to you. A description of this product and enrollment instructions will be enclosed with our forthcoming notification letter.

Fourth, we encourage you to obtain a copy of your credit report from one of the three major credit reporting agencies (Equifax, Trans Union, and Experian). You should check these credit reports for any unauthorized transactions. By law, you have a right to obtain a free credit report from any of the three consumer reporting agencies each year.

Fifth, you should consider placing a fraud alert or freeze on your credit files with all three of the major credit reporting agencies. You may contact these agencies directly as follows:

Examination Management Services, Inc.

3050 Regent Boulevard, Suite 400. | Irving, TX 75063 | 214-689-3600 | www.emsinet.com

Equifax Credit Information Services, Inc.

P.O. Box 740241
Atlanta, GA 30374
Equifax.com
1-888-766-0008

Experian

P.O. Box 9556
Allen, TX 75013
Experian.com
1-888-397-3742

Trans Union Consumer Relations

P.O. Box 2000
Chester, PA 19022-2000
Transunion.com
1-888-259-6845

We know that this news may be upsetting to you and we apologize for any inconvenience or anxiety this incident might cause. We take very seriously your privacy and the protection of your personally identifiable information. Please know that we are investigating what occurred and are reviewing our internal policies and procedures to help prevent an incident like this from occurring again.

For additional information, former employees should contact Tina Maxwell at 214-689-4297 and current employees should contact their designated human resources representative.

Regards,

Anthony Falisi
General Counsel

Examination Management Services, Inc.

3050 Regent Boulevard, Suite 400. | Irving, TX 75063 | 214-689-3600 | www.emsinet.com

Return mail will be processed by: IBC
PO Box 1122
Charlotte, NC 28201-1122
PO #121998A



10 00002475



3050 Regent Boulevard, Suite 400, Irving, TX, 75063

April 6, 2016

Re: Notice of Data Breach

Dear [REDACTED],

We are writing to supplement the information in our March 28 memorandum to you regarding an incident in which your personal information was disclosed to an unauthorized party.

What Happened

On March 24, 2016, in what is known as a “spoofing” attack, an unknown third party sent us an email from what appeared to be an authorized internal company account requesting employee W-2 forms. Copies of 2015 W-2 forms were sent in response to this email. We began investigating the incident as soon as we became aware of it. We have notified law enforcement and will cooperate with their efforts.

What Information Was Involved

The information in your 2015 W-2 form was disclosed to an unauthorized party. This includes your full name, address, Social Security Number, and wage and tax information. As such, we are concerned that someone may be attempting to use it to file a fraudulent tax return on your behalf or to open credit in your name.

What We Are Doing

Our investigation into this incident continues, and we are cooperating with law enforcement, including the Federal Bureau of Investigation. In addition, we are reviewing our internal procedures and protocols to help prevent this sort of incident from occurring again.

In an effort to provide you with additional protection for your personal credit information, we have arranged with Equifax Personal Solutions to provide you a one-year subscription, at no cost to you, for Equifax Credit Watch™ Gold with 3-in-1 Monitoring Identity Theft Protection Product. A description of this product and enrollment instructions are enclosed as Attachment B. The promotion code to activate the product is located at the top of the enrollment instructions. Please note that this code is valid for 60 days. Your enrollment in this program is completely voluntary, but it can help you protect your credit against unauthorized use of your personal information by others.

What You Can Do

The security of personal information is a top priority for us. In order to help you reduce the risk that your personal information could be misused, we urge you to take the following steps:

- If you believe you have been impacted by tax fraud, please follow the steps outlined in the IRS publication entitled Identity Theft Information for Taxpayers, available at <https://www.irs.gov/pub/irs-pdf/p5027.pdf>. You also may want to fill out the attached IRS form (Identity Theft Affidavit) and return the completed form to the IRS, so that the IRS knows that your W-2 form was disclosed to an unauthorized party. An electronic version of the form is available at <https://www.irs.gov/pub/irs-pdf/fl4039.pdf>.
- Contact the IRS for assistance with any questions you may have regarding your tax return at 800-908-4490, Monday-Friday, 7 a.m. – 7 p.m. (in your local time zone; Alaska and Hawaii follow Pacific Time).
- Activate your subscription for Equifax Credit Watch™ Gold with 3-in-1 Monitoring Identity Theft Protection Product.
- Remain vigilant in reviewing your account statements and 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.



- Obtain a copy of your credit report from one of the three major credit reporting agencies (Equifax, Trans Union, and Experian). You should check these credit reports for any unauthorized transactions. By law, you have the right to obtain a free credit report from any of the three consumer reporting agencies each year.
- Consider placing a fraud alert or a freeze on your credit file to protect against possible identity theft. A fraud alert lets creditors know to contact you before opening any new account, and a freeze generally stops all access to your credit report. To place a fraud alert or a freeze on your credit file or to report identity theft, you can contact the major credit bureaus as follows:

Equifax Credit Information Services, Inc.
P.O. Box 740241
Atlanta, GA 30374
Equifax.com
1-888-766-0008

Experian
P.O. Box 9556
Allen, TX 75013
Experian.com
1-888-397-3742

Trans Union Consumer Relations
P.O. Box 2000
Chester, PA 19022-2000
Transunion.com
1-888-259-6845

- Consider filing a report with your local police department.
- Consider reporting any suspected identity theft to your state attorney general.
- Attachment A includes contact information for the FTC, state-specific disclosures, and other steps you can take to help protect your information.

For More Information

For additional information, please call our designated hotline at 866-221-0155.

Once again, let me apologize for any inconvenience or anxiety this incident might cause and urge you to take the precautions set forth in this letter and its attachment to help prevent, detect, and report any potential misuse of your personal information.

Regards,


Anthony Falisi
General Counsel

Attachment A
Additional Information

STEPS YOU CAN TAKE TO FURTHER PROTECT YOUR INFORMATION

You may wish to visit the website of the U.S. Federal Trade Commission at www.consumer.gov/idtheft or reach the FTC at 1-877-382-4357 or 600 Pennsylvania Avenue, NW, Washington, DC 20580 for further information about how to protect yourself from identity theft. Your state Attorney General may also have advice on preventing identity theft.

We recommend that you remain vigilant by reviewing your account statements and 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 also should promptly report any fraudulent activity or any suspected incidence of identity theft to proper law enforcement authorities, your state Attorney General, and/or the Federal Trade Commission.

To file a complaint with the FTC, go to www.ftc.gov/idtheft or call 1-877-ID-THEFT (877-438-4338). Complaints filed with the FTC will be added to the FTC's Identity Theft Data Clearinghouse, which is a database made available to law enforcement agencies.

Consider reviewing your Social Security statement at www.socialsecurity.gov/myaccount. To block electronic access to your Social Security record, visit https://secure.ssa.gov/acu/IPS_INTR/blockaccess.

SECURITY FREEZES

You may obtain information from the FTC and the credit reporting agencies about security freezes. A security freeze is intended to prevent credit, loans and services from being approved in your name without your consent; however, using a security freeze may delay your ability to obtain credit.

To place a security freeze on your credit report, you need to send a request to each national credit reporting agency by certified mail, overnight mail, or regular stamped mail. The following information must be included when requesting a security freeze (note that if you are requesting a credit report for your spouse, this information must be provided for him/her as well): (1) full name, with middle initial and any suffixes; (2) Social Security number; (3) date of birth; (4) current address and any previous addresses for the past five years; and (5) any applicable incident report or complaint with a law enforcement agency or the Registry of Motor Vehicles. The request must also include a copy of a government-issued identification card and a copy of a recent utility bill or bank or insurance statement. It is essential that each copy be legible, display your name and current mailing address, and the date of issue. The consumer reporting agency may charge a fee to place a freeze or lift or remove a freeze, unless you are a victim of identity theft or the spouse of a victim of identity theft, and you have submitted a valid police report relating to the identity theft incident to the national credit reporting agency. Visit the websites of each consumer reporting agency for more information about placing a freeze, as they may have different requirements depending on the state in which you reside.

ADDITIONAL STATE REQUIREMENTS

California Residents: Your receipt of this notice has not been delayed as the result of any law enforcement investigation activity.

Iowa Residents: Iowa law requires us to advise you to report suspected incidents of identity theft to local law enforcement or the Iowa Attorney General.

Maryland Residents: You may contact the Office of the Maryland Attorney General at 1 (888) 743-0023 by visiting the website <https://www.oag.state.md.us/> or by writing to the Office of the Maryland Attorney General at 200 St. Paul Place, Baltimore, MD 21202. You can obtain information on the steps you can take to avoid identity theft from the FTC and the Office of the Maryland Attorney General.

North Carolina Residents: You may contact the North Carolina Attorney General's Office at 919-716-6400, or by visiting the website <http://www.ncdoj.gov>, or by writing to the Attorney General's Office, 9001 Mail Service Center, Raleigh, NC 27699-9001.

Wyoming Residents: Your receipt of this notice has not been delayed as the result of any law enforcement investigation activity.

Oregon Residents: If you suspect that you are the victim of identity theft, you should contact the Oregon State Attorney General.

Attachment B
Equifax Product Description and Enrollment Instructions

Promotion Code: [REDACTED]
About the Equifax Credit Watch™ Gold with 3-in-1 Monitoring Identity Theft Protection Product

Equifax Credit Watch will provide you with an “early warning system” to changes to your credit file and help you to understand the content of your credit file at the three major credit-reporting agencies. 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:

- o Comprehensive credit file monitoring and automated alerts of key changes to your **Equifax, Experian, and TransUnion** credit reports
- o Wireless alerts and customizable alerts available (available online only)
- o One 3-in-1 Credit Report and access to your Equifax Credit Report™
- o Up to \$1 million in identity theft insurance 1 with \$0 deductible, at no additional cost to you
- o 24 by 7 live agent Customer Service to assist you in understanding the content of your Equifax credit information, to provide personalized identity theft victim assistance and in initiating an investigation of inaccurate information.
- o 90 day Fraud Alert 2 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/tri

Welcome Page: Enter the Activation Code provided at the top of this page in the “Activation Code” box and click the “Submit” button.

- o 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.
- o 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.
- o 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.
- o 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.

- o Activation Code: You will be asked to enter your enrollment code as provided at the top of this letter.
- o Customer Information: You will be asked to enter your home telephone number, home address, name, date of birth and Social Security Number.
- o 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.
- o 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: www.fraudalerts.equifax.com 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.

1 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)

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