American College of
Emergency Physicians®

P.O. Box 619911
Irving, TX 75038

IMPORTANT INFORMATION
PLEASE READ CAREFULLY

July 22, 2016

[redacted]

Dear [redacted],

The privacy and security of your personal information is of utmost importance to American College of Emergency Physicians ("ACEP") and we take significant measures to protect it. I am writing to provide you with important information about a recent incident with a third party vendor involving some of your personal information. We want to provide you with information regarding the incident, explain the services we are making available to help safeguard you against identity fraud, and let you know that we continue to take significant measures to protect your information.

ACEP utilizes a third party vendor, ComNet Marketing Group, Inc. ("ComNet"), as part of its membership renewal process. In particular, ComNet contacts ACEP members for payment of membership renewal. You may recall that you were contacted by ComNet and renewed your membership over the phone with them. On June 23, 2016 ACEP was notified by ComNet that On April 23, 2016, certain ComNet files were affected by ransomware malware. The data was restored, and while that investigation was ongoing, on April 24, 2016, ComNet suffered a failure of the NetApp appliance – the storage system that housed sensitive data collected by ComNet on ACEP's behalf. ComNet subsequently learned that an unauthorized user gained administrative access to ComNet's NetApp storage appliance and issued commands to delete all of the NetApp storage volumes. ComNet has not discovered any evidence indicating that your data was accessed or acquired by an unauthorized user or that the unauthorized user intended to steal data. However, ComNet is unable to definitively rule out any unauthorized access or acquisition of your data. Upon learning of the incident, ACEP immediately commenced a full investigation. As part of our investigation, we have been working very closely with external cybersecurity professionals who regularly investigate and analyze these types of incidents.

We have devoted considerable resources to identify exactly whose information may be at risk and contacting the potentially affected individuals. Based on what ComNet has reported to ACEP, it appears that your personal information, including, your full name, address, and credit card or debit card, or other payment information you used to renew your membership, may have been accessed by an unauthorized third party as a result of the intrusion.

To date, we are not aware of any reports of identity fraud or other harmful activity resulting from this incident, or that any personal information has actually been accessed or misused. Out of an abundance of caution, we wanted to make you aware of the incident, explain the services we are making available to help safeguard you against identity fraud, and suggest steps you should take as well.

Enclosed in this letter you will find information on enrolling in a 12-month membership of Equifax Credit Watch™ Silver, that we are providing at no cost to you, along with other precautionary measures you can take

RECEIVED
AUG 17 2016

to protect your personal information, including placing a Fraud Alert, placing a Security Freeze, and/or obtaining a free credit report. Additionally, you should always remain vigilant in reviewing your financial account statements for fraudulent or irregular activity on a regular basis.

On behalf of American College of Emergency Physicians, please accept our sincere apologies that this incident occurred. We continually evaluate and modify our practices to enhance the security and privacy of your information.

If you have any further questions regarding this incident, please contact the Membership Department at [redacted] Monday through Friday, 8:00 am to 5:00 p.m. Central Time.

Sincerely,

[redacted]

[redacted]
American College of Emergency Physicians

RECEIVED
AUG 17 2016
OFFICE OF CONSUMER PROTECTION

– ADDITIONAL PRIVACY SAFEGUARDS INFORMATION –

1. Enrolling in Complimentary 12-Month Credit Monitoring.

Activation Code: [redacted]

Protecting your personal information is important to American College of Emergency Physicians. In response to this incident and as a precautionary measure, we have arranged with Equifax Personal Solutions to help you protect your identity and your credit information for one year, at no cost to you.

Equifax Credit Watch™ Silver will provide you with an "early warning system" to changes to your credit file and help you to understand the content of your Equifax credit file. The key features and benefits are listed below.

Equifax Credit Watch provides you with the following benefits:

- Comprehensive credit file monitoring of your Equifax credit report with daily notification of key changes to your credit file.
- Wireless alerts and customizable alerts available
- One copy of your Equifax Credit Report™
- $25,000 in identity theft insurance with $0 deductible, at no additional cost to you †
- 24 by 7 live agent Customer Service to assist you in understanding the content of your Equifax credit information, to provide personalize identity theft victim assistance and in initiating an investigation of inaccurate information.
- 90 day Fraud Alert placement with automatic renewal functionality *

To sign up online for online delivery go to [redacted]

1. Welcome Page: Enter the Activation Code provided at the top of your letter 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.

You must sign up for this credit monitoring before **October 14, 2016**. You will not be able to enroll after this date.

† 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

RECEIVED
AUG 17 2016
OFFICE OF CONSUMER PROTECTION

2. **Placing a Fraud Alert.**

Whether or not you choose to use the complimentary 12 month credit monitoring services, we recommend that you place an initial 90-day "Fraud Alert" on your credit files, at no charge. A fraud alert tells creditors to contact you personally before they open any new accounts. To place a fraud alert, call any one of the three major credit bureaus at the numbers listed below. As soon as one credit bureau confirms your fraud alert, they will notify the others.

Equifax	**Experian**	**TransUnion**
P.O. Box 105069	P.O. Box 2002	P.O. Box 2000
Atlanta, GA 30348	Allen, TX 75013	Chester, PA 19022
www.equifax.com	www.experian.com	www.transunion.com
1-800-525-6285	1-888-397-3742	1-800-680-7289

3. **Consider Placing a Security Freeze on Your Credit File.**

If you are very concerned about becoming a victim of fraud or identity theft, you may request a "Security Freeze" be placed on your credit file. A security freeze prohibits, with certain specific exceptions, the consumer reporting agencies from releasing your credit report or any information from it without your express authorization. You may place a security freeze on your credit report by sending a request in writing, by mail, to all three nationwide credit reporting companies. To find out more on how to place a security freeze, you can use the following contact information:

Equifax Security Freeze	**Experian Security Freeze**	**TransUnion Security Freeze**
PO Box 105788	PO Box 9554	P.O. Box 2000
Atlanta, GA 30348	Allen, TX 75013	Chester, PA 19022
https://www.freeze.equifax.com	http://experian.com/freeze	http://www.transunion.com/securityfreeze
1-800-685-1111	1-888-397-3742	1-800-680-7289

4. **Obtaining a Free Credit Report.**

Under federal law, you are entitled to one free credit report every 12 months from each of the above three major nationwide credit reporting companies. Call **1-877-322-8228** or request your free credit reports online at **www.annualcreditreport.com**. Once you receive your credit reports, review them for discrepancies. Identify any accounts you did not open or inquiries from creditors that you did not authorize. Verify all information is correct. If you have questions or notice incorrect information, contact the credit reporting company.

5. **Additional Helpful Resources.**

Even if you do not find any suspicious activity on your initial credit reports, the Federal Trade Commission (FTC) recommends that you check your credit reports periodically. Checking your credit report periodically can help you spot problems and address them quickly.

If you find suspicious activity on your credit reports or have reason to believe your information is being misused, call your local law enforcement agency and file a police report. Be sure to obtain a copy of the police report, as many creditors will want the information it contains to absolve you of the fraudulent debts. You may also file a complaint with the FTC by contacting them on the web at www.ftc.gov/idtheft, by phone at 1-877-IDTHEFT (1-877-438-4338), or by mail at Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580. Your complaint will be added to the FTC's Identity Theft Data Clearinghouse, where it will be accessible to law enforcement for their investigations. In addition, you may obtain information from the FTC about fraud alerts and security freezes.

RECEIVED
AUG 17 2016
OFFICE OF CONSUMER PROTECTION

If you live in ***Iowa***, you may also report suspected incidents of identity theft to local law enforcement or the Iowa Attorney General:

Office of the Iowa Attorney General
Consumer Protection Division
1305 East Walnut Street
Des Moines, IA 50319
(515) 281-5164
1-888-777-4590
Fax: (515) 281-6771
www.iowaattorneygeneral.gov

If you live in ***Maryland***, in addition to the FTC, the Maryland Office of the Attorney General can also be contacted to obtain information on the steps you can take to avoid identity theft:

Office of the Attorney General
Consumer Protection Division
200 St. Paul Place
Baltimore, MD 21202
1-888-743-0023
www.oag.state.md.us

If you live in ***North Carolina***, in addition to the FTC, the North Carolina Office of the Attorney General can also be contacted to obtain information on the steps you can take to prevent identity theft:

North Carolina Department of Justice
Office of the Attorney General
9001 Mail Service Center
Raleigh, NC 27699-9001
1-877-566-7226
www.ncdoj.com

6. Reporting Identity Fraud to the IRS.

If you believe that you are a victim of identity fraud AND it is affecting your federal tax records (or may affect them at some time in the future), such as your attempt to file your federal tax returns electronically was rejected or if you received a notice from the IRS indicating someone was otherwise using your Social Security number, it is recommended that you do the following:

- Contact your tax preparer, if you have one.
- File an Identity Theft Affidavit (Form 14039) with the IRS. The form can be downloaded at: https://www.irs.gov/pub/irs-pdf/f14039.pdf
- Call the IRS at (800) 908-4490, ext. 245 to report the situation. The unit office is open Monday through Friday from 7 am to 7 pm.
- Report the situation to your local police department.

Additional information regarding preventing tax related identity theft can be found at http://www.irs.gov/uac/Identity-Protection.

RECEIVED
AUG 17 2016
OFFICE OF CONSUMER PROTECTION

7. **Reporting Identity Fraud to the Social Security Administration.**

If you believe that you are a victim of identity fraud AND it is affecting your Social Security account or records, you may contact the Social Security Administration at 1-800-772-1213 or visit https://secure.ssa.gov/acu/IPS_INTR/blockaccess. You also may review earnings posted to your record on your Social Security Statement on www.socialsecurity.gov/myaccount.

- The Social Security Administration has published Identity Theft and Your Social Security Number at: https://www.ssa.gov/pubs/EN-05-10064.pdf.

RECEIVED
AUG 17 2016
OFFICE OF CONSUMER PROTECTION