WHITEFORD, TAYLOR & PRESTON L.L.P.

SEVEN SAINT PAUL STREET
BALTIMORE, MARYLAND 21202-1636
MAIN TELEPHONE (410) 347-8700
FACSIMILE (410) 752-7092

BALTIMORE, MD
BETHANY BEACH, DE*
BETHESDA, MD
COLUMBIA, MD
DEARBORN, MI
FALLS CHURCH, VA
LEXINGTON, KY
PITTSBURGH, PA
ROANOKE, VA
TOWSON, MD
WASHINGTON, DC
WILMINGTON, DE*

WWW.WTPLAW.COM
(800) 987-8705

S. KEITH MOULSDALE
DIRECT LINE (410) 347-8721
DIRECT FAX (410) 223-3721
kmoulsdale@wtplaw.com

December 29, 2016

Attorney General Joseph Foster
NH Department of Justice
33 Capitol Street
Concord, NH 03301

Dear Attorney General Foster:

Our law firm represents the American Pharmacists Association ("APhA"), a tax exempt entity under Section 501(c)(6) of the Internal Revenue Code, which is a national professional society of pharmacists, scientists, students, technicians, and others interested in advancing the profession. Pursuant to N.H. Rev. Stat. § 359-C:20, APhA hereby notifies you that Comnet Marketing Group, Inc. ("Comnet"), an APhA vendor, experienced a data security breach involving ransomware malware and unauthorized access on or about April 23-24, 2016 that may have involved the personal information of two New Hampshire residents.

Comnet processed membership renewals on behalf of APhA, and collected the name, credit card number, CVV code, and credit card expiration date for APhA members who opted to renew their membership. Upon discovering the breach, Comnet conducted a forensic investigation and alerted the FBI to this incident.

Comnet, however, terminated its business operations shortly after this incident. While it continued its forensic investigation following the termination of its business operations, the termination of its operations made it difficult for APhA to obtain information required to determine the extent of the breach. For this reason, APhA retained an independent forensic investigator to also look into this matter.

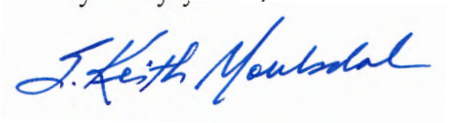
There is no evidence that personal information was accessed or acquired by the intruder, and Comnet's legal counsel have informed us that they are not aware of any individual having been a victim of identity theft as a result of this incident. Comnet has also advised us that all APhA member data on the Comnet system was deleted as part of the breach, along with data potentially relevant to a forensic investigation. As a

result, the forensic investigators were unable to definitively rule out unauthorized access to or acquisition of APhA member personal information.

While there is no evidence that the personal information of any New Hampshire resident was accessed or acquired as a result of the breach, we have opted to send notice to all New Hampshire residents who may have been impacted by this incident out of an abundance of caution. Notice was sent to the last known postal address we have on file for each of these residents on December 29, 2016; a copy of the form of such notice is attached. APhA has also offered to provide free credit monitoring services for these individuals through AllClear ID for a period of twelve months. In addition to providing affected members with access to credit monitoring services, we have increased scrutiny of our vendors with respect to data security, and adopted an enhanced data security education and training plan. Finally, since Comnet has ceased operations, it no longer serves as a vendor for APhA.

Please feel free to contact me by phone at 410-347-8421 or by email at kmoulsdale@wtplaw.com if you have any questions.

Very truly yours,



S. Keith Moulsdale

SKM:slp

Enclosure: Resident Notification Letter

2225110.1

American Pharmacists Association®

Improving medication use. Advancing patient care.

APhA

December 29, 2016

[Resident Name]
[Address]
[City, State, Zip Code]

Dear *[Resident Name]*:

We are writing to notify you that the data storage system belonging to one of our third party vendors, Comnet Marketing Group ("Comnet"), was affected by ransomware malware and accessed without authorization. The affected Comnet system was used to store credit card information of certain American Pharmacists Association ("APhA") members. While there is no evidence that your information was actually accessed or acquired by the unauthorized intruder, as a precaution, APhA is notifying you of this incident and providing you with information regarding precautionary measures you may wish to take. We sincerely apologize for any inconvenience this incident may cause, and thank you for your understanding and cooperation.

What Happened?

On or about April 23-24, 2016, all files on Comnet's data storage system were encrypted by ransomware. We understand that Comnet learned of the incident on or shortly after these dates. Although Comnet was able to decrypt those files, shortly after doing so, all files on the system were deleted by an unauthorized third party. Comnet was unable to recover those files.

What Information Was Involved?

The affected Comnet system stored credit card information collected by Comnet on behalf of various customers, including APhA, between April 18, 2015 and April 28, 2016. The APhA member-related information stored on that Comnet system and potentially at risk of having been accessed includes your name, mailing address, email address, phone number, credit card number, CVV code, and expiration date.

What are we Doing?

Comnet conducted a forensic investigation, alerted the FBI, and advised us that there is no evidence that credit card data was accessed or acquired by the intruder or

that any individual has been a victim of identity theft as a result of this incident. APhA also conducted its own investigation. But, because the intruder deleted all of its files, Comnet was prevented from being able to definitively rule out unauthorized access to or acquisition of personally identifiable information of APhA members.

Comnet is no longer in business, and no longer has access to APhA member data. In an effort to protect our members from potential harm, however, APhA will provide credit monitoring services for affected APhA members through AllClear ID for a period of twelve months. This service will be provided free of charge to affected APhA members. Information regarding this service and instructions on how to enroll are provided with this letter.

In addition to providing affected members with access to credit monitoring services, we have increased scrutiny of our vendors with respect to data security, and adopted an enhanced data security education and training plan.

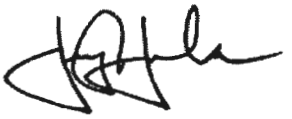
What Can You Do?

In addition to enrolling in the free credit monitoring service referenced above, we encourage you to review the enclosed information on how to protect against misuse of your personal information. The enclosed information also includes additional information for residents of certain states. Please carefully review the attachments to see if additional information may apply to you.

For More Information.

We apologize for any inconvenience this incident may cause. If you have any questions about the information in this letter, please feel free to contact the undersigned at the following number on weekdays between the hours of 9 am and 5 pm ET: 1- (202) 429-7545.

Sincerely,



Joseph J. Janela, CPA
Senior Vice-President & Chief
Financial Officer

2225087.2

UNAUTHORIZED ACCESS NOTIFICATION

Q: Why am I receiving this notification?

You are receiving this notification because of recent unauthorized access to Comnet's computer systems that contained certain personal information of certain APhA members.

Q: What type of information is at risk?

The APhA member-related information stored on that Comnet system and potentially at risk of having been accessed includes your name, mailing address, email address, phone number, credit card number, CVV code, and expiration date.

Q: Will APhA help me protect myself against the possibility that my information is misused?

As an added precaution, we have arranged to have AllClear ID protect your identity for 12 months at no cost to you. The following identity protection services start on the date of this notice and you can use them at any time during the next 12 months.

AllClear Identity Repair: This service is automatically available to you with no enrollment required. If a problem arises, simply call 1-877-676-0379 and a dedicated investigator will help recover financial losses, restore your credit and make sure your identity is returned to its proper condition.

AllClear Credit Monitoring: This service offers additional layers of protection including credit monitoring and a $1 million identity theft insurance policy. To use this service, you will need to provide your personal information to AllClear ID. You may sign up online at enroll.allclearid.com or by phone by calling 1-877-676-0379 using the following redemption code: 1447476993.

Please note: Additional steps may be required by you in order to activate your phone alerts and monitoring options.

Q: Is there anything I can do to protect myself against the possibility that my information was accessed?

Yes. APhA recommends that you remain vigilant over the next twelve to twenty-four months for incidents of fraud and identity theft, including by: (a) immediately reporting any suspicious activity or incidents (including suspected identity theft) to your credit card company as well as to the Attorney General for your state, the Federal Trade Commission ("FTC"), and local or other applicable law enforcement agencies; (b) reviewing credit card and other account statements; and (c) obtaining

and monitoring free credit reports for unexplained, suspicious or unauthorized activity.

You may obtain a copy of your credit report once per year, free of charge, whether or not you suspect any unauthorized activity on your account, by contacting each of the nationwide consumer credit reporting agencies identified below, or by visiting www.annualcreditreport.com. You may obtain information about additional protections, such as fraud alerts and security freezes, from each of the three credit reporting agencies shown below.

Equifax	**Experian**	**TransUnion**
(888) 766-0008	**(888) 397-3742**	**(800) 680-7289**
P.O. Box 740256	P.O. Box 2104	P.O. Box 6790
Atlanta, GA 30374	Allen, TX 75013	Fullerton, CA 92834
www.equifax.com	www.experian.com	www.transunion.com

The FTC recommends that you check your credit reports periodically to help you spot problems and address them quickly. If a report shows accounts you did not open, inquiries from creditors that you did not initiate, personal information, such as a home address, that is inaccurate, or other information you do not understand, contact one of the credit reporting agencies immediately. In addition, if you find suspicious activity on your credit reports or have reason to believe your personal information is being misused, authorities generally recommend that you take two additional steps: First, call your local law enforcement agency and file a police report and get a copy of the police report because many creditors want the information it contains to absolve you of any fraudulent charges. Second, file a complaint with the FTC, which will be added to the FTC's Identity Theft Data Clearinghouse, where it will be accessible to law enforcement agencies for their investigations.

You can file a complaint or obtain additional information about preventing identity theft from the Federal Trade Commission:

Federal Trade Commission
600 Pennsylvania Avenue, NW
Washington, DC 20580
www.consumer.gov/idtheft
Toll free: (877) 438-4338

Q: How do I request a security freeze?

Following is general information about how to request a security freeze from the three credit reporting agencies. While we believe this information is accurate, you should contact each agency for the most accurate and up-to-date information.

A security freeze prohibits a credit reporting agency from releasing any information from a consumer's credit report without written authorization. However, please be aware that placing a security freeze on your credit report may delay, interfere with, or prevent the timely approval of any requests you make for new loans, credit mortgages, employment, housing or other services. In some states, if you have been a victim of identity theft, and you provide the credit reporting agency with a valid police report, the agency cannot charge you to place, lift or remove a security freeze. In all other cases, a credit reporting agency may charge you up to $10.00 each to place, temporarily lift, or permanently remove a security freeze.

To place a security freeze on your credit report, you must send a written request to **each** of the three major consumer reporting agencies: Equifax (www.equifax.com); Experian (www.experian.com); and TransUnion (www.transunion.com) by regular, certified or overnight mail at the addresses below:

Equifax Security Freeze	**Experian Security Freeze**	**TransUnion Security Freeze & Fraud Victim Assistance Dept.**
P.O. Box 105788	P.O. Box 9554	P.O. Box 6790
Atlanta, GA 30348	Allen, TX 75013	Fullerton, CA 92834
https://www.freeze.equifax.com	www.experian.com/freeze	https://freeze.transunion.com

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;
8. If you are not a victim of identity theft, include payment by check, money order, or credit card (Visa, MasterCard, American Express or Discover only). Do not send cash through the mail.

The credit reporting agencies have three (3) business days after receiving your request to place a security freeze on your credit report. The credit agencies must

also send written confirmation to you within five (5) business days and provide you with a unique personal identification number (PIN) or password, or both, that can be used by you to authorize the removal or lifting of the security freeze.

To lift the security freeze in order to allow a specific entity or individual access to your credit report, you must call or send a written request to the credit reporting agencies by mail and include proper identification (name, address, and social security number) **and** the PIN number or password provided to you when you placed the security freeze as well as the identities of those entities or individuals you would like to receive your credit report or the specific period of time you want the credit report available. The credit reporting agencies have three (3) business days after receiving your request to lift the security freeze for those identified entities or for the specified period of time.

To remove the security freeze, you must send a written request to each of the three credit bureaus by mail and include proper identification (name, address, and social security number) **and** the PIN number or password provided to you when you placed the security freeze. The credit bureaus have three (3) business days after receiving your request to remove the security freeze.

Q: Are there federal or state resources that can assist me in protecting my identity?

Yes. APhA recommends that you utilize these resources to protect yourself from the possibility of fraud and identity theft.

The FTC can provide you with additional information about steps you can take to avoid identity theft and may be contacted at:

Federal Trade Commission
Consumer Response Center
600 Pennsylvania Avenue, NW
Washington, DC 20580
Toll free: (877) 438-4338
www.ftc.gov/idtheft

For Maryland residents, in addition to the FTC, the Maryland Office of the Attorney General can provide you with additional information about steps you can take to avoid identity theft and may be contacted at:

Maryland Office of the Attorney General
Consumer Protection Division
200 Saint Paul Place
Baltimore, Maryland 21202
Toll free: (888) 743-0023

www.oag.state.md.us/idtheft/

For Massachusetts residents, please note that you have the right to obtain a police report.

For North Carolina residents, in addition to the FTC, the North Carolina Attorney General's Office can provide you with additional information about steps you can take to avoid identity theft and may be contacted at:

North Carolina Attorney General Roy Cooper
9001 Mail Service Center
Raleigh, NC 27699-9001
(919) 716-6400
www.ncdoj.com

For Rhode Island residents, please note that you have the right to file or obtain a police report. Also, in addition to the FTC, the Rhode Island Attorney General's Office can provide you with additional information about steps you can take to avoid identity theft and may be contacted at:

Office of the Attorney General
150 South Main Street
Providence, Rhode Island 02903
(401) 274-4400
http://www.riag.ri.gov/ConsumerProtection/About.php#

Q: Who can I contact at APhA for additional information?

To answer any question or address any concerns you may have, please contact our Senior Vice-President & Chief Financial Officer – Joseph Janela - by any of the following methods:

email: jjanela@aphanet.org
phone: 1- (202) 429-7545
mail: American Pharmacists Association
2215 Constitution Avenue, NW
Washington, DC 20037-2985