

[PENN STATE ALUMNI ASSOCIATION LETTERHEAD]

<Mail Name>
<Address 1>
<Address 2>
<Address 3>

**Re: IMPORTANT NOTICE
Computer Server Security Breach with Vendor for Penn State Alumni Association
Your Credit Card(s) Ending in [XXXX]**

Dear <Salutation>:

The Penn State Alumni Association (PSAA) recently learned that one of its contractors, ComNet Marketing Group, Inc. (ComNet), experienced a security breach of the computer server that stored PSAA members' credit card information.

What Happened?

ComNet's computer server deletion occurred around April 24, 2016. Upon learning of the incident, ComNet launched a forensic investigation and determined that an unauthorized user had gained administrative access and issued commands to delete files containing PSAA members' personal information from its computer server. ComNet did not initially notify PSAA until June 21, 2016, and even then, it did not provide specific details to us sufficient to provide this notification to you until July 11, 2016. We are continuing to follow up with ComNet to obtain additional information.

We are informing you of this incident at this point because we believe your credit card data was stored on ComNet's deleted computer server. ComNet has advised PSAA that the membership data it collected, including your credit card information, has been destroyed and that it has no evidence that your credit card data was accessed or acquired by the unauthorized user. We are, however, notifying our alumni who were potentially affected as a precaution so that you can, if you deem appropriate, take additional steps to protect yourself and your information.

What Information Was Involved?

The information stored on the computer server included customer demographic data, such as name, address, and phone number, and credit card information, including card number, CVV codes and expiration dates.

What We Are Doing:

PSAA requires Payment Card Industry Data Security Standard (PCI DSS) compliance from all of our business partners who handle our members' credit card information. We take this incident very seriously and we are committed to preventing incidents such as these in the future. PSAA is no longer doing business with ComNet.

What You Can Do:

We also want to make you aware of certain precautionary measures that you might consider taking. These measures are good practices regardless of this incident and even if you have not identified any suspicious activity related to your credit card and other accounts which may have your confidential personal information.

You should carefully check all credit cards and other financial account information that you receive. If you detect any unauthorized or suspicious activity in any of these accounts, you should contact your credit card company or other account issuer immediately.

We recommend that you place a fraud alert on your credit files. A fraud alert requires potential creditors to use what the law refers to as “reasonable policies and procedures” to verify your identity before issuing credit in your name. A fraud alert typically lasts for 90 days and may be initiated by you without cost to you. You can place a 90 day fraud alert through any of the reporting agencies listed below.

Equifax

800.525.6285
P.O. Box 740241
Atlanta, GA 30374
www.equifax.com

Experian

888.397.3742
P.O. Box 9532
Allen, TX 75013
www.experian.com

TransUnion

800.680.7289
Fraud Victim Assistance Division
P.O. Box 6790
Fullerton, CA 92834
www.transunion.com

We also recommend that you obtain a free credit report from one of the three credit bureaus; Experian, Equifax, or TransUnion. You can do so at: www.annualcreditreport.com. Following such review, you should promptly report any suspicious activity to the proper law enforcement authorities including local law enforcement, your state’s attorney general, and/or the Federal Trade Commission at www.ftc.gov.

Other important tips to protect yourself:

- Visit <http://www.experian.com/credit-advice/topic-fraud-and-identity-theft.html> for general information regarding protecting your identity.
- The Federal Trade Commission (600 Pennsylvania Avenue, NW, Washington, D.C. 20580) has an identity theft hotline: 877-438-4338; TTY: 1-866-653-4261. They also provide information online at www.ftc.gov/idtheft.
- Many State Attorney General Offices additionally provide information about protecting your identity on their websites.

Free Credit Monitoring:

To help detect any possible misuse of your personal information, we are offering you access to a complimentary one-year membership to Experian’s® ProtectMyID® Elite. Experian is the largest credit bureau in the United States, and the ProtectMyID Elite Service helps detect possible misuse of your personal information, provides you with superior identity protection support that is focused on immediate identification and resolution of identity theft, and provides free fraud resolution and identity protection for one year. Please note you must activate this membership by **October 31, 2016**, which will then continue for **12** full months from your enrollment date.

