kUSC.org
CLASSICAL | fm 91.5

P.O. Box 7913
Los Angeles, CA
90007-0913
telephone
213-225-7400
facsimile
213-225-7410
e-mail
kusc@kusc.org

July 7, 2016

Acct#
[name]
[address]
City State Zip

Re: Notice of Data Breach

Dear [Name]:

What Happened?

KUSC recently learned that one of its contractors, Comnet Marketing Group ("Comnet"), was affected by ransomware malware, which ultimately resulted in deletion of its storage system that housed customer credit card information. KUSC engaged Comnet to assist with performing certain telemarking activities, and in the course of those activities, Comnet obtained credit card information from a relatively small number of KUSC donors.

The system deletion occurred around April 24, 2016. Upon learning of the incident, Comnet launched a forensic investigation and determined that an unauthorized user gained administrative access and issued commands to delete the system. Comnet did not initially notify KUSC until June 21, 2016, but did not provide specific details sufficient to provide this notification until June 28, 2016.

We are informing you of this incident because your credit card data was stored in Comnet's deleted system. Comnet has advised that all KUSC data, including your cardholder information, has been destroyed and has no evidence that credit card data was accessed or acquired by the unauthorized user; however, we are notifying our members who were potentially affected as a precaution.

What Information Was Involved?

The information stored on the system 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:

KUSC is taking this incident very seriously and is committed to preventing future such events. As an example, KUSC no longer is doing business with Comnet.

What You Can Do:

We also want to make you aware of certain precautionary measures that you might consider. These measures are good practices regardless of this incident and even if you have not identified any suspicious activity related to your accounts.

You should carefully check all credit card 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 lasts for 90 days. 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 credit report from one of the three credit bureaus; Experian, Equifax or TransUnion. You can do so at: www.annualcreditreport.com. Following such reviews, 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 ("FTC") at www.ftc.gov.

For More Information

We apologize for any inconvenience or concern that this notification may cause. As an important KUSC donor, we want to ensure that we do all that we can to maintain your trust and confidence. KUSC takes these matters very seriously and we will do all that we can to prevent future such incidents.

If you have any further questions, please call me directly at 213.225.7534.

Sincerely,

Minnie Prince

Minnie Prince
Development Director