Jonathan D. Lee, Esq. *Principal*

Direct Voice: (202) 756-1304 Mobile: (202) 257-8435 Fax: (202) 403-3372
jonathan@jdleeconsulting.com

Mr. William Appleton, Esq. Senior Vice President/General Counsel The E.W. Scripps Company 312 Walnut Street 2800 Scripps Center Cincinnati, OH 45202

April 30, 2013

JD Lee Consulting, LLC, 1776 I St., NW, Suite 900 Washington, DC 20006

Re: *Cease and Desist/Mitigation of Harm/Preservation of Evidence Request* Dear Mr. Appleton:

I am writing in my role as counsel for two telecommunications carriers, TerraCom, Inc. ("TerraCom") and YourTel America, Inc. ("YourTel") (collectively, the "Companies"). TerraCom and YourTel are separate companies, but have some common shareholders and share some key management employees.

TerraCom and YourTel request your immediate assistance in mitigating the damage from a prolonged pattern of accessing and downloading of certain confidential data belonging to the Companies and stored on the servers of their contractor, Call

Centers India, Inc. d/b/a Vcare Corporation ("Vcare"). TerraCom and YourTel are still in the process of conducting an investigation, but they have already confirmed that the intrusions and downloading were initiated from computers with IP addresses associated with the "Scripps Howard News Service" and "EW Scripps Company" (collectively, "Scripps"). One of the Scripps IP addresses is from a Cincinnati location: 216.196.131.38. The other Scripps IP address is from a Maryland location: 216.55.38.126

The person or persons using the Scripps IP addresses (the "Scripps Hackers") have engaged in numerous violations of the Computer Fraud and Abuse Act, 18 U.S.C. § 1030, by gaining unauthorized access into confidential computer files maintained for the Companies by Vcare, and by digitally transferring the information in these folders to Scripps. I request that you take immediate steps to identify the Scripps Hackers, cause

them to cease their activities described in this letter, and assist the Companies in mitigating the damage from the Scripps Hackers' activities.

My clients' immediate concern is in fulfilling their own obligations under state data breach notification laws, as well as complying with any other applicable federal or state regulatory requirements. The illegally accessed data contains personal information of thousands of individuals in over 20 states.

In order to determine accurately the legal obligations created by the Scripps Hackers' unauthorized access to this data, the Companies need to know whether the Scripps Hackers made any further disclosure, distribution or use of the data, or if the data was simply accessed and stored in the course of a journalistic effort. To that end, I am also requesting that after determining the identity of the Scripps Hackers you determine as soon as possible what they have done with the Companies' data that they digitally transferred to Scripps' IP addresses. This information is crucial to the

Companies, as without it they have great difficulty determining the likelihood of harm (including ID theft) to affected individuals and thus the Companies' reporting obligations under various states' data breach notification laws.

Background

On Friday, April 26, 2013, Dale Schmick, COO of TerraCom and YourTel, received an email from Scripps employee Isaac Wolf requesting an "on-camera" interview with Mr. Schmick. A copy of the email is attached to this letter. In the email, Mr. Wolf stated that

in the course of conducting google [sic] searches on TerraCom, [he] stumbled across numerous completed Lifeline applications from TerraCom and YourTel which are posted freely online. Many of these applications include full Social Security numbers, dates of birth and other identifying details.

Mr. Wolf's email was copied to two other Scripps employees, James Osman and Lawan Hamilton.

The applications referred to in the email were applications for voice telephone service under the Federal Communications Commission ("FCC") Lifeline Program, which offers subsidized service to qualifying low income customers. Any applicant must demonstrate eligibility for a Lifeline subsidy by providing a Social Security number and other information, such as income information or evidence of participation in a qualifying federal program such as the Supplemental Nutritional Assistance Program. This information is considered to be confidential and subject to protection under most states' laws.

The Companies have contracted with Vcare to perform many aspects of their customer relationship management. Vcare maintains customer data, provides back office services, as well as data analytics. Vcare also collects information provided by

applicants for Lifeline service and uses this information to help the Companies determine eligibility and provide Lifeline services.

Upon receiving Mr. Wolf's email on April 26, Mr. Schmick forwarded it to Vcare, which immediately provided additional security on all servers on which the Companies' Lifeline

applicant data was stored. At the same time, Vcare initiated an intensive investigation of its system and server access logs to determine whether there had been any unauthorized access to the data.

Vcare's Ongoing Investigation

Vcare has informed the Companies that it has confirmed that between March 24 and April 26 the Scripps Hackers accessed directories on Vcare's servers that contained all of the Lifeline applications processed by Vcare since April 2012, when it became the Companies' third party data processor. Vcare states that it does not maintain its server access logs for more than 30 days, so it cannot be sure when the Scripps Hackers' activities began.

Much of the Scripps Hackers' activity was automated. After March 25, they began using the "Wget" program to search for and download the Companies' confidential data. On April 4th, the Scripps Hackers expanded their activity and attempted to hack into additional Vcare servers and directories providing greater access, which would have allowed them to assume employee status, add users, create customer applications and assign inventory. They were denied access on each attempt. On the same day, however, the Scripps Hackers gained access to other server directories that contained documents demonstrating proof of address, proof of enrollment in public assistance programs, or proof of income ("Proof Files"). Beginning on April 5th, the Scripps Hackers

digitally transferred (or downloaded) over 120,000 Proof Files. In total, the Scripps Hackers downloaded at least 19,000 applications and 127,000 Proof Files over the March 24-April 26 period.

Vcare has informed the Companies that, so far as it can determine, the Scripps Hackers were the only persons that have sought and gained access without authorization to the Companies' confidential data stored by Vcare.

Request for Assistance in Determining the Effect of the Unauthorized Access

We are still evaluating the likelihood of future harm to the applicants whose data was accessed and downloaded by the Scripps Hackers. If the purpose of the hacking was journalistic and the Scripps Hackers have not made and do not intend to make any further disclosure of the hacked data, then any financial or other risk for those applicants would be minimal and notification of the breach may not be necessary under the laws of about half of the states involved. However, the downloading of more than 120,000 files over a period of several weeks may not be consistent with a solely journalistic intent.

It is this uncertainty that leads me to request that you take immediate steps to determine the identity and the intentions of the Scripps Hackers. I believe that expedited action is in both the Companies' and Scripps' best interests, since it may minimize the need for and costs of many state breach notifications. Because the Scripps Hackers have put the Companies in the position of having to incur the costs of potentially complying with more than 20 state data breach notification laws, the Companies are likely to look to Scripps to reimburse them for those costs.

Preservation of Evidence

The actions of the Scripps Hackers have already resulted in damages and loss to TerraCom and YourTel. At this point, it is not possible for the Companies to know the extent of the losses, particularly the costs of any breach notifications that the Scripps Hackers' actions will ultimately cause to Vcare and to them.

TerraCom and YourTel reserve the right to pursue all available civil remedies under state and federal statutes. Given that civil litigation is highly likely, please consider this letter as notice to preserve any potentially relevant evidence that is in the possession or control of Scripps (or its employees and agents), regardless of the media format in which the evidence exists. Scripps is on notice to preserve all evidence related to any research or reportorial inquiry into the events addressed in this letter, TerraCom, YourTel, Vcare, or the FCC's Lifeline program. In particular, this notice applies to all documents, phone records, and computer records of Isaac Wolf, James Osman and Lawan Hamilton, and any other Scripps employees working with them.

Thank you in advance for your cooperation in resolving these issues. If you would like to discuss this further, please contact me at 202-257-8435. If I have not heard from you, I will contact you no later than 4 p.m. EDT, Wednesday, May 1st, so that my clients may notify state law enforcement and regulators as to when they will be able to provide any required notice to applicants whose data has been compromised.

Sincerely,

Jonathan D. Lee Principal