Nelson Mullins

Nelson Mullins Riley & Scarborough LLP
Attorneys and Counselors at Law
Atlantic Station / 201 17th Street, NW / Suite 1700 / Atlanta, GA 30363
Tel: 404.322.6000 Fax: 404.322.6033
www.nelsonmullins.com

February 16, 2012

VIA FEDERAL EXPRESS & FACSIMILE

Attorney General Michael A. Delaney
Office of the Attorney General
Attn: Security Breach Notification
NH Department of Justice
33 Capitol Street
Concord, NH 03301
Fax: 603-271-2110

Re: Data Breach Notification

Dear Attorney General Delaney:

We write to inform you of a recent data security incident on behalf of our client, Horry Telephone Cooperative, Inc. ("HTC"). HTC was informed that between February 1, 2012 and February 3, 2012 unauthorized attempts were made to illegally transfer funds from an HTC bank account. These efforts were averted because of established security measures and at no time were HTC internal databases accessed. However, it was discovered that the intruder had limited ability to view automated payment records being processed by a third party vendor. Those records included ONLY the following information about HTC customers:

1. The name on the customer's bank account used for automated payments to HTC;
2. The bank routing number used for automated payments to HTC;
3. The customer's bank account number used for automated payments to HTC; and
4. The customer's HTC account number.

To help clarify, the information that was potentially viewed is similar to, but less than, the information that is on a written check.

HTC has determined that the breach of security described above may have affected the names and financial account numbers of 8 residents in your state. Our client is providing written notification by U.S. first class mail to all affected residents to the last home address our client has on record, and a sample notification letter is enclosed.

In addition to contacting all affected customers, HTC has notified the appropriate law enforcement organizations, financial institutions, and related software providers and vendors to make them aware of this incident. To reduce the chances of such an event happening again, HTC has worked with its anti-virus software vendor, Symantec, to insure that Symantec has added the Win32Zbot signature to its software package which was the virus or malware associated with this attack. These updates have been deployed to all of the computers on HTC's internal network. Furthermore, HTC is in the process of adding another layer of security middleware that conducts deep packet analysis of encrypted files sent to the HTC network. Also, HTC has also implemented a user awareness program in order to educate and provide additional training on security to our employees. Lastly, HTC continues to review its policies and procedures to reduce the risk of a future incident of this nature.

Very truly yours,

Jon Neiditz

cc: Horry Telephone Cooperative, Inc.
Enclosures

February 13, 2012

Dear _____

The HTC information security program is always monitoring, preventing, and detecting security threats similar to those seen on news reports. Cyber criminals use sophisticated viruses to attack some of the most secure systems in the world. We have learned that between February 1st and February 3rd unauthorized attempts were made to illegally transfer funds from an HTC bank account. These efforts were averted because of established security measures and at no time were HTC internal databases accessed. However, it was discovered that the intruder had limited ability to view automated payment records being processed by a third party vendor. Those records included ONLY the following information:

The name on the bank account used for your automated payments to HTC
(same information found on any printed check)
The bank routing number used for your automated payments to HTC
(same information found on any printed check)
The bank account number used for your automated payments to HTC
(same information found on any printed check)
Your HTC account number

To help clarify, the information that was potentially viewed is similar to, but less than, the information that is on a written check.

The records that might have been accessed **DID NOT** include sensitive information such as your social security number, your address, credit card data, or any other information.

In addition to contacting you, HTC has notified the appropriate law enforcement organizations, financial institutions, and related software providers and vendors to make them aware of this incident. It is possible that you may receive an additional notification from your bank.

Our main concern is that the intruder may attempt to use this information to create a fraudulent demand draft on your account. Because of this possibility, **it is recommended to contact your bank from where your HTC draft payment is made to discuss available options that may help to prevent or identify any fraudulent activity. We also encourage you to closely monitor this account for any unauthorized activity**. HTC is committed to ensuring that all customer information is kept secure and private and takes this incident very seriously. We continue to review our policies and procedures to reduce the risk of a future incident of this nature.

Should you have any questions, please do not hesitate to connect with our office anytime Monday – Friday during the hours of 8:00 AM and 5:00 PM at 843-369-8530 or toll free at 1-855-260-2537. In addition please find the enclosed security/fraud protection practices for your reference.

M. O'Neal Miller, Jr.
Chief Financial Officer

Commonly Used Practices to help Protect your Identity

1. Verify Bank Policies. Review your bank's policies and procedures regarding reporting suspicious or fraudulent activity.

2. Review your credit reports. Remain vigilant by reviewing all account statements and monitoring credit reports. You can receive free credit reports by placing fraud alerts and through your credit monitoring. Under federal law, you also are entitled every 12 months to one free copy of your credit report from each of the three major credit reporting companies. To obtain a free annual credit report, go to www.annualcreditreport.com or call 1-877-322-8228. You may wish to stagger your requests so that you receive a free report by one of the three credit bureaus every four months.

You should also know that you have the right to file a police report if you ever experience identity fraud. Please note that in order to file a crime report or incident report with law enforcement for identity theft, you will likely need to provide some kind of proof that you have been a victim. A police report is often required to dispute fraudulent items. You can report suspected incidents of identity theft to local law enforcement or to the Attorney General.

3. Place Fraud Alerts with the three credit bureaus. You can place a fraud alert at one of the three major credit bureaus by phone and also via Experian's website. A fraud alert tells creditors to follow certain procedures, including contacting you, before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit. The contact information for all three bureaus is as follows:

Credit Bureaus

Equifax Fraud Reporting
1-800-525-6285
P.O. Box 740241
Atlanta, GA 30374-0241
www.equifax.com

Experian Fraud Reporting
1-888-397-3742
P.O. Box 9532
Allen, TX 75013
www.experian.com

TransUnion Fraud Reporting
1-800-680-7289
Fraud Victim Assistance Division
P.O. Box 6790
Fullerton, CA 92834-6790
www.transunion.com

It is necessary to contact only ONE of these bureaus and use only ONE of these methods. As soon as one of the three bureaus confirms your fraud alert, the others are notified to place alerts on their records as well. You will receive confirmation letters in the mail and will then be able to order all three credit reports, free of charge, for your review.

4. Security Freeze: By placing a freeze, someone who fraudulently acquires your personal identifying information will not be able to use that information to open new accounts or borrow money in your name. You will need to contact the three national credit reporting bureaus listed above in writing to place the freeze. Keep in mind that when you place the freeze, you will not be able to borrow money, obtain instant credit, or get a new credit card until you temporarily lift or permanently remove the freeze. The cost of placing the freeze is no more than $10 for each credit reporting bureau for a total of $30. However, if you are a victim of identity theft and have filed a report with your local law enforcement agency or submitted an ID Complaint Form with the Federal Trade Commission, there is no charge to place the freeze.

5. You can obtain additional information about the steps you can take to avoid identity theft from the following:

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

For North Carolina Residents:
Office of the Attorney General of North Carolina
9001 Mail Service Center
Raleigh, NC 27699-9001
www.ncdoj.com/
Telephone: 1-919-716-6400

For all other US Residents:
Identity Theft Clearinghouse
Federal Trade Commission
600 Pennsylvania Avenue, NW
Washington, DC 20580
www.consumer.gov/idtheft
1-877-IDTHEFT (438-4338)
TDD: 1-202-326-2502