

September 24, 2007

Kelly A. Ayotte, Esq.
Attorney General
New Hampshire Department of Justice
33 Capitol Street
Concord, NH 03301

Dear Attorney General Ayotte,

We are writing to inform you of a recent security incident that we discovered on September 12, 2007.

The Nature Conservancy is a 501(c)(3) non-profit conservation organization whose mission is to preserve the plants, animals and natural communities that represent the diversity of life on Earth by protecting the lands and waters they need to survive. The Conservancy is headquartered in Arlington, Virginia and has approximately 3,500 employees throughout the 50 United States and in 29 countries outside the U.S.

On September 12, 2007, we discovered that we have been the victims of a hacking incident in which unauthorized individuals compromised the security of one of our computers. We took immediate steps to secure the computer to prevent further unauthorized access. Unfortunately, the computer contained Human Resources related information. We are currently cooperating with the F.B.I. to investigate the incident and determine the personal information that was accessed or acquired. The database included names, home addresses, Social Security numbers and possibly financial account numbers. While we do not know for sure whether the information was accessed or acquired, we have given notice to potentially affected individuals so that they can take action to protect themselves.

Through our internal investigation following the incident, we have determined that personal information regarding approximately 3,500 individuals may have been affected by the breach including 29 individuals residing in New Hampshire. Potentially affected individuals were notified on September 21, 2007; copy attached.

Please contact me at (970) 221-2939 if you have questions.

Very Truly Yours,

Katherine Runnels / by cas

Katherine W. Runnels
Senior Attorney
The Nature Conservancy

CC: Philip Tabas, General Counsel
Attachment (notice letter to employees)

From: Jean-Louis Ecochard [jecochar@TNC.ORG]
Sent: Friday, September 21, 2007 6:59 PM
To: All TNC Staff
Subject: URGENT: Personal Data Security Incident (on behalf of Steve Howell)
Importance: High

This message is to inform you of a recent and potentially serious data security incident that may involve the theft of Conservancy employees' personal information.

The Nature Conservancy has been the victim of a criminal hacking incident in which unauthorized individuals illegally gained access to a Conservancy computer containing Human Resources data. The data accessed included the names, home addresses, Social Security numbers and financial account numbers of some Conservancy employees on the U.S. payroll. We're working very hard to learn as much as we can about the content of the data that was compromised and will keep you informed.

At this time, we do not believe that international employees are affected by this; however, we will continue to investigate and be in contact with you as we learn more. We will also be working to notify former employees whose information may have been included in the accessed data.

This incident has been reported to the U.S. Federal Bureau of Investigation, and we will contact other law enforcement agencies as appropriate.

We are committed to making sure each affected employee has the support needed to monitor his/her credit and knows how to respond if problems are identified. To assist you, we are in the process of finalizing an agreement whereby we will provide you with credit monitoring for one year at no cost to you. As early next week as possible, we will send you information on the details of the service and how to register for it, along with other information concerning this incident and resources available to you. In the meantime, I urge you to consider taking the following steps:

- Contact the fraud department of one of the three major credit reporting agencies (TransUnion - 800-680-7289; Equifax - 888-766-0008; and Experian - 888-397-3742). You have the right to ask the agencies to place a "fraud alert" in your file. A fraud alert can make it more difficult for someone to get credit in one's name because it tells creditors to follow certain procedures to protect you. It also may delay one's ability to obtain credit. Individuals may place a fraud alert in one's file by calling just one of the three nationwide credit reporting agencies. As soon as that agency processes your fraud alert, it will notify the other two credit reporting agencies, which then must also place fraud alerts in your file.
- Watch for any unusual activity on your credit card accounts or suspicious items on your bills. Report suspicious activity to card issuers.

9/24/2007

- Review information provided by the Federal Trade Commission on what do to if your personal information has been compromised at <http://www.ftc.gov/bcp/edu/microsites/idtheft/>.

Please know that we are taking this matter very seriously. We regret that this all too common crime has affected you and so many of our colleagues. Watch for more information early next week.

Sincerely,

Steve Howell

STATE OF NH
DEPT OF JUSTICE
07 SEP 27 AM 10:59