

February 24, 2011

Attorney General of New Hampshire
State House Annex
33 Capitol Street
Concord, NH 03301

Dear Sir or Madam:

We represent the IEEE, 445 Hoes Lane, Piscataway, New Jersey. In mid December 2010, IEEE became aware of intrusions into its database. IEEE immediately engaged a team of forensic investigators to determine the source and scope of these intrusions. On or about February 10, 2011, the investigators concluded that a file containing customer credit card information had been deleted on or about November 17, 2010. Based on this conclusion it appears that an unauthorized person may have obtained access to credit card numbers and the associated names, expiration dates and security numbers for approximately 828 cardholders. There is approximately one resident of New Hampshire whose data was accessed. The IEEE has notified the Federal Bureau of Investigation of this data breach.

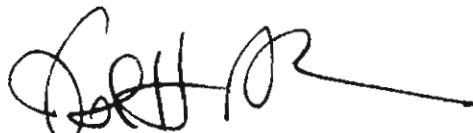
Although we have no proof that any of this credit card information was removed from IEEE's database or copied or that anyone to date has used any of this credit card information to make fraudulent charges, we are, out of an abundance of caution, notifying all 828 cardholders of this unauthorized access and providing residents of your state with the attached notification letter. This is a draft and minor changes may be made prior to it being sent out in the next couple of days.

As you can see, the letter advises the cardholders of this potential breach of their credit card information, the steps they should take to avoid credit card fraud and offers them a free service to monitor their credit over the next year.

During the period of forensic evaluation, which began in December 2010, the forensic investigators found certain vulnerabilities in the system and immediately corrected them to avoid a recurrence of future intrusions.

Please feel free to call me if you have any questions.

Very truly yours,



Nathaniel H. Akerman

February __, 2011

[Address]

Important Notice Regarding Your Personal Information

Re: [type of credit card]

Dear _____:

IEEE is writing to inform you that a company database which contained your credit card information was accessed by a third party through a sophisticated network intrusion and may have been viewed by the third party. Your credit card information was entered into the IEEE database when you registered for an IEEE conference. The information accessed included your name, credit card number, expiration date and your card identification number. We have notified law appropriate law enforcement authorities and are closely monitoring and assisting with the investigation.

We have no proof that your credit card information was removed from our system. We are, however, concerned about the possible misuse of your credit card, and out of an abundance of caution we are writing so that you may take steps to protect yourself from fraud and identity theft. In light of this situation, we encourage you to review your credit card statements for any unauthorized activity. You should contact your credit and bank card issuers as soon as possible to review your accounts for unauthorized charges or transactions.

If there are unauthorized charges or if you otherwise believe that your card number has been taken by an unauthorized person, you should inform your card issuer on the phone and in writing that the charges were not authorized by you. Regardless of whether you currently have any unauthorized charges, the prudent course of action would be to request that your current card account be closed and a new card be issued in your name.

As a further precaution, you may wish to place a fraud alert on your credit file. Specific information about protecting your credit lines and financial information is enclosed with this letter. ***Please review it closely.*** We also recommend that you review the identity theft materials posted for consumers on the Federal Trade Commission's (the "FTC's") Web site,

<http://www.ftc.gov/bcp/edu/microsites/idtheft/>, and in particular, the posted copy of the FTC's booklet, *"Take Charge: Fighting Back Against Identity Theft."*

In an effort to protect you as a result of the recent potential release of your information, IEEE would like to offer you a one year subscription to LifeLock. LifeLock is a company that specializes in identity theft protection services. To obtain details and/or enroll with LifeLock, all you have to do is call [REDACTED] or visit the website at www.lifelock.com to enroll. Use promotion code [REDACTED] when prompted. LifeLock's specialized team of telephone representatives are available 24 hours a day, seven days a week to answer any questions you may have regarding the incident. As soon as you complete the enrollment process, your coverage will begin.

We regret the occurrence of this incident and any inconvenience it may have caused you. We value our relationship with you and want to work through this matter with you.

Sincerely,

Steps to take to protect your credit and identity

Should you ever believe your identity has been stolen or that you are at risk of having your identity stolen, you can follow the Federal Trade Commission's ("FTC's") guidelines on protecting yourself against identity theft. The FTC works for the consumer to prevent fraudulent, deceptive, and unfair business practices in the marketplace and to provide information to help consumers spot, stop and avoid them.

First, you should contact your credit and bank card issuers as soon as possible to review your accounts for unauthorized charges or transactions. If there are unauthorized charges or if you otherwise believe that your card number has been taken by an unauthorized person, you should inform your card issuer on the phone and in writing that the charges were not authorized by you, and you should request that your current card account be closed and a new card issued in your name.

You may wish to consider placing a fraud alert on your credit file. A fraud alert tells creditors to contact you before they open any new accounts or change your existing credit accounts. Because creditors seek additional verification from you when a fraud alert is in place on your credit file, one effect of the fraud alert is that it slows the processing time for opening new accounts and making changes on your existing accounts.

To place a fraud alert on your credit file, call any one of the three major credit bureaus. As soon as one credit bureau processes your fraud alert, it will notify the other credit bureaus on your behalf to place fraud alerts. All three credit reports will be sent to you, free of charge, for your review.

Equifax
1-800-525-6285

Experian
1-888-397-3742

TransUnionCorp
1-800-680-7289

You may also have right under applicable state law to request a "security freeze" on your credit report. A security freeze will prohibit a credit reporting agency from releasing any information in your credit report without your express authorization.

Even if you do not initially find any suspicious activity on your card accounts, credit reports and/or bank statements, the FTC recommends that you check your credit reports, card charges and financial statements regularly. Victim information sometimes is held for use or shared among a group of thieves at different times. Checking your credit reports, card charges and financial statements periodically can help you spot problems and address them quickly. Once a year you can obtain a free credit report by calling 1- 877-322-8228 or going online to www.annualcreditreport.com.

If you find suspicious activity on your accounts or have reason to believe that your personal information is being misused, it may be necessary for you to file a police report and obtain a copy of that police report. Many creditors require the information the police report contains to absolve you of the fraudulent debts.

You may also want to file a complaint with the FTC, which will be logged into its database of identity theft cases used by law enforcement agencies for investigations. To get free information or file a complaint with the FTC, you may call the FTC at 1-877-438-4338, or use the complaint form at <https://www.ftccomplaintassistant.gov/>.

If you are a resident of Maryland, you may also contact the Maryland Attorney General's Office at 410-576-6491.