January 30, 2009

Attorney General Kelly A. Ayotte
New Hampshire Attorney General's Office
33 Capitol Street
Concord, NH 03301
Telephone: (603) 271-3658
Fax: (603) 271-2110

Re: Security Breach Notification

Dear Attorney General Ayotte:

Pursuant to the New Hampshire Right to Privacy Act, § 359-C:20 *et seq*, I am hereby notifying you of a data security incident involving three New Hampshire residents. ETS has provided notice on January 30, 2009 to these individuals through written notice, a copy of which is attached for your reference.

If you require any additional information or if you should have any further questions regarding this notification, please do not hesitate to contact me at:

[redacted]

Email: [redacted]
Telephone: [redacted]
Fax: [redacted]

Sincerely,

Cynthia Raiton

Educational Testing Service
Rosedale Road
Princeton, NJ 08541
phone: (609) 921-9000
fax (609) 734-5410
web www.ets.org

ETS CONFIDENTIAL – NH LETTER

[Date]

[Individual Name]
[Home Address]

This letter is to notify you of a potential compromise of your personal information, including your name and social security number. We collected this information from you as part of our record keeping relating to your role as a reader for ETS.

Overnight on December 15, 2008, a laptop went missing from the desk of an employee at the offices of Educational Testing Service (ETS). The laptop had been locked into its docking station. On December 16, the fact that the laptop was missing was reported to ETS IT Security and ETS corporate security. IT Security examined the hard drive backup for the laptop and discovered that some personally identifiable Information (PII) about you was present on the hard drive of the missing laptop, including your name and social security number.

We have contacted local law enforcement authorities regarding this incident. We have no reason to believe that the laptop was taken because of the PII on its hard drive. As there is a potential that it could be accessed, we recommend that you take precautionary measures, including the actions further detailed in Exhibit A attached to this letter. ETS is making efforts to recover the missing hardware.

ETS is taking steps to prevent a recurrence of this incident. First, ETS has enhanced its physical security measures at all offices. Second, ETS has begun deploying comprehensive military-grade encryption to all of its laptops; this project is scheduled for completion in the second quarter of 2009. In addition, all ETS computers, including laptops, can be accessed only via enforced strong passwords which must be changed regularly.

To help you detect the possible misuse of your personal information, ETS is paying to provide you with a one year membership in Experian's Triple Advantage^{SM} Premium credit monitoring product at no cost to you. Triple Advantage^{SM} Premium will monitor your credit reports at the three national credit reporting companies: Experian®, Equifax® and TransUnion® and notify you of key changes. Triple Advantage^{SM} Premium is a tool that will help you identify potentially fraudulent use of your information. Your Triple Advantage^{SM} Premium membership will be paid for the first year. If you wish to continue your membership beyond the end of the first year, you will need to contact Experian to make arrangements, including paying any costs, for any extended period.

You have ninety (90) days from the date of this letter to activate this membership, which will then continue for twelve (12) full months. We encourage you to activate your credit monitoring membership as soon as possible.

Your complimentary 12-month **Triple Advantage℠ Premium** membership includes:

- Triple Advantage Premium monitors your credit reports every day so you don't have to
- Email alerts when key changes are detected so you can act quickly
- A free three bureau credit report and score
- If you become a victim of fraud or identity theft, our Fraud Resolution Team will assist you with the recovery process, every step of the way
- $25,000 in identity theft insurance provided by Virginia Surety Company, Inc. with no deductible*

*Due to New York state law restrictions, identity theft insurance coverage cannot be offered to residents of New York. All other benefits of Triple Advantage Premium are available to residents of New York.

The web site to enroll in Triple Advantage℠ Premium and your individual activation code are both listed below. To sign up, please visit the web site and enter your individual activation code. Please keep in mind that once activated, the code cannot be re-used for another enrollment. The web site will guide you through the process of enrolling in Triple Advantage℠ Premium.

Triple Advantage Premium Web Site: [**insert**]
Your Activation Code: **[insert Activation Code]**

If you wish to enroll over the phone for delivery of your membership via US mail, please call _____.

We apologize for any inconvenience and concern that this situation may cause. Should you have any questions regarding this notice, including questions regarding your particular record, please do not hesitate to contact a PASS representative, by phone at 1-800-301-7286, or by mail at Educational Testing Service, PASS, 225 Phillips Boulevard, Ewing, NJ 08628.

Sincerely,

EDUCATIONAL TESTING SERVICE

EXHIBIT A

IDENTITY THEFT PREVENTION INFORMATION

FTC: You may take steps to protect yourself against potential misuse of data that has been the subject of a data security incident. The Federal Trade Commission discusses several steps, including obtaining and reviewing your credit report, filing a "fraud alert" and requesting a "credit freeze". The most current and detailed information is available online (for answers to the questions below, see http://www.ftc.gov/bcp/edu/microsites/idtheft/consumers/defend.html), but if you are not able to access the linked material, you may also contact the FTC by mail at Federal Trade Commission, CRC-240, Washington, D.C. 20580, or by toll-free number, 1-877-FTC-HELP (382-4357) or 1-877-ID-THEFT (438-4338).

1. What are the steps I should take if I'm a victim of identity theft?
2. What is a fraud alert?
3. What is a credit freeze?
4. Should I apply for a new Social Security number?
5. What is an identity theft report?
6. What do I do if the police only take reports about identity theft over the Internet or telephone?
7. What do I do if the local police won't take a report?
8. How do I prove that I'm an identity theft victim?

Fraud Alert: A fraud alert tells creditors to take reasonable steps to verify your identity, including calling you before opening new accounts or changing your existing accounts. A fraud alert may be placed or removed at no cost to you. An initial fraud alert stays active for 90 days. To request a fraud alert, you will need to contact one of the following credit reporting agencies (see the FTC materials for further details). The credit reporting agency is required to notify the other two credit reporting agencies, who will also place a fraud alert on your credit file. You will then receive letters from all of them with instructions on how to obtain a free copy of your credit report from each.

Experian: 1-888-397-3742; www.experian.com; P.O. Box 9532, Allen, TX 75013
Equifax: 1-800-525-6285; www.equifax.com; P.O. Box 740241, Atlanta, GA 30374-0241
TransUnion: 1-800-680-7289; www.transunion.com; Fraud Victim Assistance Division, P.O. Box 6790, Fullerton, CA 92834-6790.

If you observe evidence of attempts to open fraudulent accounts and you have a copy of a police report reporting that you are experiencing identity theft, then you may also request a 7-year fraud alert. Be aware that placing a fraud alert does not always prevent new accounts from being opened or prevent a takeover of your existing accounts, so you should monitor any alerts sent to you by the credit monitoring services. Also, be aware that a company may not be able to immediately extend credit to you if your identity can not be verified at the time you are applying for credit. You should consider providing a mobile telephone number when placing any fraud alert if you have one.

Monitor Credit Reports and Accounts: When you receive your credit reports, you should look them over carefully and consider taking the steps recommended by the FTC. For example, look for accounts you did not open. Additionally, look for inquiries from creditors that you did not initiate. And finally, look for personal information that you do not recognize. Also, you should monitor your accounts for suspicious activity. If you see anything you do not understand, call the credit reporting agency or provider of your account at the telephone number on the credit report or account statements. If you do find suspicious activity on your credit reports, you may call your local police or sheriff's office and may be able to file a police report of identity theft and obtain a copy of the police report. Potentially, you may need to give copies of the police report to creditors to clear up your records. You may also make a report to the FTC.