

North Carolina Security Breach Reporting Form Pursuant to the Identity Theft Protection Act of 2005

Name of Business Owning or Licensing Information Affected by the
 Breach: Heinemann-Raintree
 Address: 1 North LaSalle, Suite 1800
Chicago IL 60602
 Telephone: 312 324 5200
 Fax: 312 324 5201
 Email: WWW.HeinemannRaintree.com

PLEASE SUBMIT FORM TO:
 Consumer Protection Division
 NC Attorney General's Office
 9001 Mail Service Center
 Raleigh, NC 27699-9001
 Telephone: (919) 716-6000
 Toll Free in NC: (877) 566-7226
 FAX: (919) 716-6050

Date Security Breach Reporting Form submitted: 8/8/08, (letter sent 7/15/08)
 Date the Security Breach was discovered: 4/29/08
 Estimated number of affected individuals: 1,940
 Estimated number of NC residents affected: 34

Name of business maintaining or possessing information that was the subject of the Security Breach, if the business that experienced the Security Breach is not the same entity as the business reporting the Security Breach (pursuant to N.C.G.S. § 75-65(b)): Pearson Education, Inc.

Describe the circumstances surrounding the Security Breach and state whether the information breached was in electronic or paper format: An unauthorized third party was able to penetrate the database that contained product information used by the Heinemann-Raintree websites.

Regarding electronic information breached, state whether the information breached or potentially breached was password protected or encrypted in some manner. No. If so, please describe the security measures protecting the information: _____

Describe any measures taken to prevent a similar Security Breach from occurring in the future: The websites were temporarily taken down, and programming changes and other security measures were implemented to protect the sites from future third party attacks.

Date affected NC residents were/will be notified: 7/14/08

If there has been any delay in notifying affected NC residents, describe the circumstances surrounding the delay pursuant to N.C.G.S. § 75-65(a) and (c): N/A

If the delay was pursuant to a request from law enforcement pursuant to N.C.G.S. § 75-65(c), please include the written request or the contemporaneous memorandum.

How NC residents were/will be notified?
 (pursuant to N.C.G.S. § 75-65(e))

- written notice
- electronic notice (email)
- telephone notice
- substitute notice

Please attach copy of the notice if in written form or a copy of any scripted notice if in telephonic form.

Signature: [Signature] Date: 8/8/08

Contact Person, Title: George Costello Sr., Vice President

Address: Pearson Education, Inc.

(if different from above) One Lake St. Upper Saddle River NJ 07458

Telephone: 201 236 3433 Fax: 201 818 8749 Email: george.costello@pearsoned.com

July 11, 2008



Dear Heinemann-Raintree Customer:

Heinemann-Raintree, publishers of PreK-Secondary nonfiction books for the library and classroom, maintains websites where customers can learn about and purchase our products. We have learned of a breach of the security of those websites, and wanted to inform you about it because your credit card data may have been compromised.

We recently learned that in January 2007, an unauthorized person was able to obtain access to the database that contains the product information used by the Heinemann-Raintree websites. This gave the person the ability to view information appearing on the websites, including information provided by our customers to buy Heinemann-Raintree products on the sites. As a result, this person may have been able to view our customers' names, billing and shipping addresses, payment methods, and credit-card numbers (if the customers paid with credit cards).

When we learned of this unauthorized access, we immediately discontinued operation of the websites, on a temporary basis, and corrected the problem that was allowing the unauthorized access. The websites are now up and running, and are safe and secure. They can be reached at www.heinemannraintree.com, www.heinemannlibrary.com, and www.heinemannclassroom.com.

As a result of this unauthorized access, it is possible that your credit card information could be misused, although at this time we have seen no evidence that this has occurred.

We have notified our credit card processor of this incident. We also recommend that you contact your credit card issuer to advise them of this incident and to arrange for a new credit card. Here are some other things you can do to monitor and protect your credit file, or if you think your credit card information has been misused:

Fraud Alert. You can place a fraud alert on your credit file. By doing so, you let creditors know to watch for suspicious activity in your accounts, such as someone trying to open a credit card account in your name.

To place a fraud alert, you only need to call one of the following three major credit reporting agencies, because each agency will alert the other two. Your phone call will take you to an automated phone system. Be sure to listen carefully to the selections and indicate that you are at risk for credit fraud.

Equifax

(888) 766-0008
Consumer Fraud Division
P.O. Box 740256
Atlanta, GA 30374
<http://www.equifax.com>

Experian

(888) 397-3742
Credit Fraud Center
P.O. Box 1017
Allen, TX 75013
<http://www.experian.com>

TransUnion

(800) 680-7289
Fraud Victim Assistance
Department
P.O. Box 6790
Fullerton, CA 92834
<http://www.tuc.com>

Soon after you place a fraud alert, you will receive credit reports by mail, and at no charge, from all three credit reporting agencies. In the credit report:

- Check your personal information, including home address, Social Security number, and other information, for accuracy.
- Look for actions that you did not authorize, such as charges that you did not make, accounts that you did not open, or inquiries from creditors that you did not initiate.

If you find anything in the credit report that looks wrong or that you do not understand, call the credit agency at the telephone number listed on your credit report, and close accounts that have been tampered with or established fraudulently.

Please note that, by law, you are entitled to one free credit report from each of the three credit bureaus once every 12 months, whether or not you decide to place a fraud alert on your credit file. It is a good idea to periodically obtain these reports, and confirm the activity in your credit file. Checking in this way can help you spot problems and address them quickly. We suggest that you remain vigilant about monitoring your credit accounts for at least the next 24 months.

File a Police Report. If you find suspicious activity on your credit reports or have reason to believe your information is being misused, call your local police department and file a police report. Obtain a copy of the report, because many creditors want the information it contains to absolve you of the fraudulent debts.

File a Complaint with the Federal Trade Commission ("FTC") or your state's Attorney General. You should also report any suspected identity theft to the FTC at www.ftc.gov/idtheft or at 1-877-ID-THEFT (877-438-4338) and to your state's attorney general. If you notify the FTC, your complaint will be added to the FTC's Identity Theft Data Clearinghouse, where it will be accessible to law enforcers for their investigations.

Please know that we greatly regret that this incident occurred, and we have taken steps to correct the problem. We are fully committed to protecting the privacy and confidentiality of our customers' personal information. If you have any questions about this incident, about this letter, or about other issues raised here, please call the Heinemann-Raintree Customer Service Center at (888) 454-2279. We thank you for your understanding, and for being a Heinemann-Raintree customer.

Very truly yours,

Graham Shaw
President