GOODWIN

David S. Kantrowitz
617.570.1254
DKantrowitz@goodwinprocter.com

Goodwin Procter LLP
100 Northern Avenue
Boston, MA 02210

goodwinlaw.com
+1 617 570 1000

November 22, 2016

STATE OF NH
DEPT OF JUSTICE
2016 NOV 28 PM 1:31

VIA CERTIFIED MAIL

Attorney General's Office
NH Department of Justice
33 Capitol Street
Concord, NH 03301

Re: Notice of Data Security Incident

Dear Sir/Madam:

We write on behalf of Educents Inc. ("Educents") to inform you that Educents was recently the victim of a cyber-intrusion. Specifically, between September 26, 2016 and October 18, 2016, an unauthorized person may have gained access to credit card numbers and other information that certain Educents customers entered during the Educents checkout process. Educents learned of the incident on October 18, 2016. Educents provided notice by first-class mail to the three affected New Hampshire residents whose personal information could have been accessed on November 16, 2016. We have enclosed a copy of that notice with this letter.

Educents has locked down its systems and removed the malware that was responsible for the issue. Educents is also conducting an internal review of its systems to help further protect against similar attacks in the future.

By providing this notice, Educents does not waive any rights or defenses regarding the applicability of New Hampshire law, personal jurisdiction, or the applicability of the New Hampshire data incident notification statute. Please contact me if you have any questions.

Best regards,

David S. Kantrowitz

Enclosure

November 16, 2016

«firstname» «lastname»
«street»
«City», «State» «postcode»

Notice of Data Breach

Dear «firstname»,

As you know, we recently informed you by email that an unauthorized person may have accessed your credit card number, along with any other information you entered in the Educents checkout process (such as name and address), between September 26, 2016 and October 18, 2016. We are sending this letter to provide additional information about the incident as well as resources you can use to monitor your personal information and protect against identity theft and fraud.

What Happened?

Between September 26, 2016 and October 18, 2016, an unauthorized person potentially gained access to your credit card number, along with any other information you entered in the Educents checkout process. Educents learned of the incident on October 18, 2016.

What Information Was Involved?

The potentially-affected information includes any information that you entered during the Educents checkout process, including your credit card number and expiration date (and card verification value, the three digits code on the back of your card), as well as potentially your name, mailing address, and email address.

What We are Doing

After becoming aware of the incident, we took immediate action to lock down our systems and remove the malware that was responsible for the issue. We also are conducting an internal review of our systems to help further protect against similar attacks in the future.

What You Can Do

Although we have no evidence that your credit card number has been used in an unauthorized manner, for your security we strongly recommend that you immediately contact your credit or debit card company or bank to request a new card number. You should also always be vigilant for incidents of fraud and identity theft, including by regularly viewing your account statements and monitoring your free credit reports.

For more information on how you can help protect yourself, please review the enclosed *Steps You Can Take to Protect Yourself From Identity Theft.*

For More Information

We take data security and your privacy very seriously. If you have any further questions or concerns about this incident, feel free to call our dedicated hotline at +1 866-431-3829.
Or email us at customers@educents.com

Sincerely,

The Educents Team

Steps You Can Take to Protect Yourself From Identity Theft

1. ***Review your account statements and credit reports and notify law enforcement and Educents of suspicious activity.***

Even if you do not feel the need to register for a credit monitoring service, as a precautionary measure, we recommend that you regularly review statements from your bank, credit card, and other accounts and periodically obtain your credit report from one or more of the national credit reporting companies. You may obtain a free copy of your credit report online at www.annualcreditreport.com, by calling toll-free 1.877.322.8228, or by mailing an Annual Credit Report Request Form (available at www.annualcreditreport.com) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. You may also purchase a copy of your credit report by contacting one or more of the three national credit reporting agencies:

Equifax
P.O. Box 740241
Atlanta, GA 30374
www.equifax.com
1.888.766.0008

Experian
P.O. Box 9532
Allen, TX 75013
www.experian.com
1.888.397.3742

TransUnion
P.O. Box 2000
Chester, PA 19022-2000
www.transunion.com
1.800.680.7289

When you receive your credit reports, look them over carefully. Look for accounts that you did not open and/or inquiries from creditors that you did not initiate. Also check to see if your personal information on the credit report is accurate. If you see anything you do not understand, call the credit reporting agency at the telephone number on the report.

We recommend that you remain vigilant in your review of your account statements and credit reports. You should promptly report any suspicious activity or suspected identity theft to us and to the proper law enforcement authorities, including local law enforcement, your state's attorney general, and/or the Federal Trade Commission. A copy of a police report may be required by creditors to clear up your records.

2. ***Consider placing a fraud alert or a security freeze on your credit files.***

Fraud Alerts: There are two types of fraud alerts that you can place on your credit report to put your creditors on notice that you may be a victim of fraud: an initial alert and an extended alert. You may request that an initial fraud alert be placed on your credit report if you suspect you have been, or are about to be, a victim of identity theft. An initial fraud alert stays on your credit report for at least 90 days. You may have an extended alert placed on your credit report if you have already been a victim of identity theft with the appropriate documentary proof. An extended fraud alert stays on your credit report for seven years. You can place a fraud alert on your credit report by calling the toll-free fraud number of any of the three national credit reporting agencies listed above.

Security Freezes: You may have the right to put a security freeze, also known as a credit freeze, on your credit file, so that no new credit can be opened in your name without the use of a PIN number that is issued to you when you initiate a freeze. A security freeze is designed to prevent potential credit grantors from accessing your credit report without your consent. If you place a security freeze, potential creditors and other third parties will not be able to get access to your credit report unless you temporarily lift the freeze. Security freeze laws vary from state to state.

Keep in mind that when you place the freeze, you may not be able to borrow money, obtain instant credit, or get a new credit card until you temporarily lift or permanently remove the freeze. In addition, you may incur fees to place, lift and/or remove a credit freeze. The cost of placing, temporarily lifting, and removing a security freeze also varies by state, generally $5 to $20 per action at each credit reporting company. *Unlike a fraud alert, you must separately place a security freeze on your credit file at each credit reporting*

company. Since the instructions for how to establish a credit freeze differ from state to state, please contact the three major credit reporting companies at the numbers above to find out more information.

3. Learn more about how to protect yourself from identity theft.

You may wish to review the Federal Trade Commission's guidance on how consumers can protect themselves against identity theft. For more information:

Federal Trade Commission
600 Pennsylvania Avenue NW
Washington, DC 20580
www.ftc.gov/idtheft
1.877.ID.THEFT (1.877.438.4338)

For residents of Maryland: You may also obtain information about preventing and avoiding identity theft from the Maryland Office of the Attorney General:

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

For residents of North Carolina: You may also obtain information about preventing and avoiding identity theft from the North Carolina Attorney General's Office:

North Carolina Attorney General's Office
Consumer Protection Division
9001 Mail Service Center
Raleigh, NC 27699-9001
1-877-5-NO-SCAM
www.ncdoj.gov