



Andrew B. Epstein
+1 720 566 4203
aepstein@cooley.com

VIA CERTIFIED MAIL RETURN RECEIPT REQUESTED

December 11, 2019

Office of the Attorney General
State of New Hampshire
Attn: Security Breach Notification
33 Capitol Street
Concord, NH 03301

RECEIVED
DEC 16 2019
CONSUMER PROTECTION

Re: Legal Notice of Potential Data Incident

Dear Sir or Madam:

I write on behalf of my client, Web Courseworks Ltd. ("WCW"), to inform you of a potential data incident involving the personal information of approximately five New Hampshire residents that are customers of the American Association of Nurse Anesthetists ("AANA"). WCW is a service provider to AANA with respect to the AANA e-commerce website that experienced the potential incident. WCW will notify the potentially affected individuals and outline some steps that each may take to help to protect his/her personal information.

WCW hosts AANA's e-commerce website. WCW notified AANA of a potential data incident due to an unauthorized individual gaining access to AANA's e-commerce website and inserting a malicious script designed to capture payment card information entered into the checkout page. Specifically, the malicious script may have affected the following types of information entered on the website between May 23, 2019 and October 3, 2019: name, billing address, credit card type, credit card number, credit card verification value or credit card expiration date. Please note, at this time, WCW has no evidence that the code actually captured any personal information.

WCW takes the privacy of personal information seriously. Promptly after discovering the script, WCW removed the malicious code and engaged an outside forensic investigation firm to assist with investigating and remediating this potential incident. To help prevent something like this from happening in the future, WCW is continuing to enhance security controls and monitor its systems to detect and prevent unauthorized access.

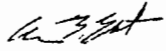
On approximately December 12, 2019, WCW will notify the potentially affected individuals via written letter with information about the incident, the types of information affected, and contact information where he/she may obtain additional information. A copy of the template notice being sent to potentially affected residents is enclosed for your reference.

WCW's investigation of this matter remains ongoing at this time, and we will provide further updates to your office if needed. If you have questions or need further information regarding this potential incident, please contact me at +1 (720) 566-4203 or aepstein@cooley.com.

Cooley

Office of the Attorney General
December 11, 2019
Page Two

Sincerely,



Andrew B. Epstein

ABE:ABE



Return Mail Processing Center
P.O. Box 6336
Portland, OR 97228-6336

<<Mail ID>>
<<Name 1>>
<<Name 2>>
<<Address 1>>
<<Address 2>>
<<Address 3>>
<<Address 4>> <<Date>>
<<Address 5>>
<<City>><<State>><<Zip>>
<<Country>>

Dear <<Name 1>><<Name 2>>:

Web Courseworks Ltd. (“WCW”) recently became aware of a potential information security incident that may affect the personal information of certain customers of the American Association of Nurse Anesthetists (“AANA”). WCW is providing this notice to inform you of the incident and to call your attention to some steps you can take to help protect yourself.

What Happened

WCW is a third-party service provider of learning management system products and services to AANA. AANA has the relationship to the individuals potentially affected by this incident. To our knowledge, an unauthorized individual — not associated with WCW or AANA — modified a piece of computer code used on a WCW-hosted website that services AANA customers. This modified computer code was designed to capture payment card data and limited other information entered on certain pages on the website. The modified code was active on the website between May 23, 2019, and October 3, 2019.

What Information Was Involved

We believe that the incident may have affected limited personal information, such as first name, last name, billing address, credit card type, credit card number, credit card verification value or credit card expiration date. Please note, at this time, we have no evidence that the code actually captured any personal information.

What WCW Is Doing

Upon learning of this potential incident, WCW promptly launched an investigation and remediated the issue by removing the modified code that was designed to capture information on AANA’s website. WCW also engaged a leading cybersecurity investigation firm to assist with its investigation, and is continuing to review and enhance the company’s security measures to help prevent something like this from happening again in the future. WCW also contacted law enforcement and will cooperate with any investigation of this incident.

What You Can Do

We want to make you aware of steps you can take to help guard against fraud or identity theft. Carefully check your credit reports for accounts you did not open or for inquiries from creditors you did not initiate. If you see anything you do not understand, call the credit agency immediately. If you find any suspicious activity on your credit reports, call your local police or sheriff’s office, and file a police report for identity theft and get a copy of the report. You may need to give copies of the police report to creditors to clear up your records.

You may choose to notify your bank to see if there are any additional protections available to help to prevent someone from accessing your account or initiating transactions without your permission. As a general practice, you can regularly monitor your accounts for unusual activity or any transactions you do not recognize. If you find anything unusual, contact your bank immediately.

You may also carefully review credit and debit card account statements as soon as possible in order to determine if there are any discrepancies or unusual activity listed. We urge you to remain vigilant and continue to monitor statements for any unusual activity going forward. If you see anything you do not recognize, you should immediately notify the issuer of the credit or debit card as well as the proper law enforcement authorities, including local law enforcement, your state's attorney general, and/or the Federal Trade Commission ("FTC"). In instances of payment card fraud, it is important to note that cardholders are typically not responsible for any fraudulent activity that is reported in a timely fashion.

Other Important Information

We have included the "Information about Identity Theft Protection" reference guide below, which describes additional steps that you may take to help protect yourself, including recommendations by the FTC regarding identity theft protection and details on placing a fraud alert or a security freeze on your credit file.

For More Information

For more information about this potential incident, or if you have questions or concerns, you may contact our call center at 833-947-1401 between the hours of 9am – 9pm Eastern time, Monday through Friday excluding holidays. We sincerely regret any concern this incident may cause.

Sincerely,

A handwritten signature in black ink that reads "Scott Hinkelman". The signature is written in a cursive, slightly slanted style.

Scott Hinkelman
Chief Operating Officer, WCW

INFORMATION ABOUT IDENTITY THEFT PROTECTION

Review Accounts and Credit Reports: You can regularly review statements from your 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 listed at the bottom of this page.

You should remain vigilant with respect to reviewing your account statements and credit reports, and you should promptly report any suspicious activity or suspected identity theft to the proper law enforcement authorities, including local law enforcement, your state's attorney general, and/or the Federal Trade Commission ("FTC"). You may contact the FTC or your state's regulatory authority to obtain additional information about avoiding and protection against identity theft: Federal Trade Commission, Consumer Response Center 600 Pennsylvania Avenue, NW, Washington, DC 20580, 1-877-IDTHEFT (438-4338), www.ftc.gov/idtheft.

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.marylandattorneygeneral.gov.

For residents of New York: You may also obtain information about preventing and avoiding identity theft from the New York Attorney General's Office: Office of the Attorney General, The Capitol, Albany, NY 12224-0341, 1-800-771-7755, <https://ag.ny.gov/internet/privacy-and-identity-theft>.

For residents of North Carolina: You may also obtain information about preventing and avoiding identity theft from 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.

For residents of Rhode Island: You may also obtain information about preventing and avoiding identity theft from the Rhode Island Office of the Attorney General: Rhode Island Office of the Attorney General, Consumer Protection Unit, 150 South Main Street, Providence, RI 02903, 401-274-4400, <http://www.riag.ri.gov>. Approximately two (2) Rhode Island residents were potentially affected by this incident.

Security Freezes and Fraud Alerts: You have a right to place a security freeze on your credit report, which will prohibit a consumer reporting agency from releasing information in your credit report without your express authorization. The security freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, you should be aware that using a security freeze to take control over who gets access to the personal and financial information in your credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit.

A security freeze does not apply to a person or entity, or its affiliates, or collection agencies acting on behalf of the person or entity, with which you have an existing account that requests information in your credit report for the purposes of reviewing or collecting the account. Reviewing the account includes activities related to account maintenance, monitoring, credit line increases, and account upgrades and enhancements. Please contact the three major credit reporting companies as specified below to find out more information about placing a security freeze on your credit report.

As an alternative to a security freeze, you have the right to place an initial or extended fraud alert on your credit file at no cost. An initial fraud alert is a 1-year alert that is placed on a consumer's credit file. Upon seeing a fraud alert display on a consumer's credit file, a business is required to take steps to verify the consumer's identity before extending new credit. If you are a victim of identity theft, you are entitled to an extended fraud alert, which is a fraud alert lasting 7 years. You can place a fraud alert on your credit report by contacting any of the three national credit reporting agencies at the addresses or toll-free numbers listed below.

Additional Information for New Mexico Residents: The federal Fair Credit Reporting Act (FCRA) promotes the accuracy, fairness, and privacy of information in the files of consumer reporting agencies. Here is a summary of your major rights under the FCRA:

- You have the right to be told if information in your file has been used against you;
- You have the right to receive a copy of your credit report and the right to ask for a credit score;
- You have the right to dispute inaccurate, incomplete, or unverifiable information;
- You have the right to have outdated negative information removed from your credit file;
- You have the right to limit access to your credit file;
- You have the right to limit “prescreened” offers of credit and insurance you get based on information in your credit report;
- You have the right to seek damages from violators; and
- You have the right to place a security freeze on your credit report.

New Mexico consumers have the right to obtain a security freeze or submit a declaration of removal. You may obtain a security freeze on your credit report to protect your privacy and ensure that credit is not granted in your name without your knowledge. You may submit a declaration of removal to remove information placed in your credit report as a result of being a victim of identity theft. You have a right to place a security freeze on your credit report or submit a declaration of removal pursuant to the Fair Credit Reporting and Identity Security Act.

The security freeze will prohibit a consumer reporting agency from releasing any information in your credit report without your express authorization or approval. The security freeze is designed to prevent credit, loans and services from being approved in your name without your consent. When you place a security freeze on your credit report, you will be provided with a personal identification number, password or similar device to use if you choose to remove the freeze on your credit report or to temporarily authorize the release of your credit report to a specific party or parties or for a specific period of time after the freeze is in place. To remove the freeze or to provide authorization for the temporary release of your credit report, you must contact the consumer reporting agency and may need to provide the following:

- (1) The unique personal identification number, password or similar device provided by the consumer reporting agency;
- (2) proper identification to verify your identity;
- (3) information regarding the third party or parties who are to receive the credit report or the period of time for which the credit report may be released to users of the credit report; and
- (4) payment of a fee, if applicable.

A consumer reporting agency that receives a request from a consumer to temporarily lift a freeze on a credit report shall comply with the request no later than three business days after receiving the request. As of September 1, 2008, a consumer reporting agency shall comply with the request within fifteen minutes of receiving the request by a secure electronic method or by telephone.

A security freeze does not apply in all circumstances, such as when you have an existing account relationship and a copy of your credit report is requested by your existing creditor or its agents for certain types of account review, collection, fraud control or similar activities; for use in setting or adjusting an insurance rate or claim or insurance underwriting; for certain governmental purposes; and for purposes of prescreening as defined in the federal Fair Credit Reporting Act.

If you are actively seeking a new credit, loan, utility, telephone or insurance account, you should understand that the procedures involved in lifting a security freeze may slow your own applications for credit. You should plan ahead and lift a freeze, either completely if you are shopping around or specifically for a certain creditor, with enough advance notice before you apply for new credit for the lifting to take effect. You should contact a consumer reporting agency and request it to lift the freeze at least three business days before applying. As of September 1, 2008, if you contact a consumer reporting agency by a secure electronic method or by telephone, the consumer reporting agency should lift the freeze within fifteen minutes. You have a right to bring a civil action against a consumer reporting agency that violates your rights under the Fair Credit Reporting and Identity Security Act.

For more information, including information about additional rights, you can visit <https://www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf>, <https://www.consumerfinance.gov/learnmore/>, or write to: Consumer Financial Protection Bureau, 1700 G Street N.W., Washington, DC 20552.

You can obtain more information about fraud alerts and credit freezes by contacting the FTC or one of the national credit reporting agencies listed below.

National Credit Reporting Agencies' Contact Information

Equifax
(www.equifax.com)
General Contact:
P.O. Box 740241
Atlanta, GA 30374
800-685-1111
Fraud Alerts and Security Freezes:
P.O. Box 740256
Atlanta, GA 30374

Experian
(www.experian.com)
General Contact:
P.O. Box 2002
Allen, TX 75013
888-397-3742
Fraud Alerts and Security Freezes:
P.O. Box 9556
Allen, TX 75013

TransUnion
(www.transunion.com)
**General Contact, Fraud Alerts
and Security Freezes:**
P.O. Box 2000
Chester, PA 19022
888-909-8872