
919 North Market Street, 11th Floor
Wilmington, DE 19801-3034
TEL 302.252.4465
FAX 302.252.4466
www.ballardspahr.com

Edward J. McAndrew
Tel: 302.252.4451
Fax: 302.252.4466
McAndrewE@ballardspahr.com

March 13, 2018

Via E-mail (attorneygeneral@doj.nh.gov)

The Honorable Joseph Foster
Office of the Attorney General
33 Capitol Street
Concord, NH 03301

Re: Security Incident Notification

Dear Attorney General Foster:

We are providing notice on behalf of CNU Online Holdings, LLC and its subsidiaries, collectively d/b/a NetCredit ("NetCredit"), to the New Hampshire Office of the Attorney General, pursuant to N.H. REV. STAT. ANN. § 359-C:20, about an incident potentially involving three (3) New Hampshire residents.

Beginning on or about February 20, 2018, NetCredit's security team discovered that an unauthorized party gained access to a small percentage of NetCredit accounts by using a valid email address and password to log in to each affected account. Based on NetCredit's investigation, it does not believe that its system was breached or that the unauthorized party obtained account holder email addresses or passwords from NetCredit.

Once the unauthorized party gained access to a NetCredit account using valid login credentials, the unauthorized party may have viewed the account holder's name, telephone number, physical address, last four digits of their bank account number, NetCredit account number, last four digits of their Social Security number, and basic employment and income information.

Once NetCredit became aware of the incident, it restricted access to the online accounts that it believes were affected by disabling the current passwords and requiring account holders to reset their passwords. NetCredit has also disabled the ability to change an account holder's email address and bank account information through the online account and is requiring account holders to call NetCredit directly and provide specific proof of identity before any changes to the email addresses or bank account information on an account can be made. In addition, NetCredit is continuing to monitor these accounts for suspicious activity.

On March 8, 2018, NetCredit sent emails to the New Hampshire account holders whose accounts may have been involved in this incident to explain the situation. Please find attached a copy of the notification letter to the account holders for your reference.

The Honorable Joseph Foster
March 13, 2018
Page 2

If you should have any questions or if we can provide further assistance to the New Hampshire residents affected by this incident, please feel free to contact me at (302) 252-4451 or mcandrew@ballardspahr.com.

Respectfully submitted,



Edward J. McAndrew

EJM/pm
Attachment

March __, 2018

[FName] [LName]
[Address1]
[Address 2]
[City], [State] [Zip]

Re: Notice of Data Security Incident

Dear [FName]:

We recently became aware that an unauthorized party utilized the email address and password associated with your NetCredit account to access your account. We want to provide you with information on the situation, including what happened, the steps we have taken, the ways you can reach us for further help or to answer questions, and the steps you may take to protect yourself against identity theft and fraud.

WHAT HAPPENED? On February 20, 2018, our security team discovered that an unauthorized party used valid email addresses and passwords to log in to a small percentage of NetCredit accounts. Based on our investigation, we do not believe that the unauthorized party obtained account holder email addresses or passwords from us or that our security systems were breached. In some instances, after gaining access to an account using the login credentials, the unauthorized party changed some of the personal information in the account, such as the email address and bank account information associated with the account.

WHAT INFORMATION WAS INVOLVED? Access to an account could have enabled the unauthorized party to view the account holder's name, telephone number, physical address, last four digits of their bank account number, NetCredit account number, last four digits of their Social Security number, and basic employment and income information.

WHAT WE ARE DOING. Once we became aware of the incident, we took steps to block the unauthorized party and restricted access to the online accounts that we believe were affected. Due to these security precautions, you will not be able to access your account using your current password and will need to change your password. In addition, we are continuing to monitor your account for suspicious activity.

WHAT YOU CAN DO. In order to regain access to your online account, you will need to change your password by going to www.netcredit.com/signin, clicking on the "Forgot password?" link, and following the instructions there. You can also call us at (877) 392-2014 to have a password reset link sent to you. We also encourage you to review the enclosed information on how to ensure the security of your information with us, as well as how to protect yourself against identity theft or fraud.

FOR MORE INFORMATION. We very much appreciate your business and the opportunity to serve you. We take very seriously the trust you have placed in us by choosing us as a financial partner, and the security of the personal information that our account holders entrust into our care is one of our highest priorities. Our team is here and ready to help. You can reach us at (877) 392-2014 or support@netcredit.com.

Sincerely,

Jason Such
Senior Manager - Head of Servicing, Net Credit

ADDITIONAL STEPS YOU CAN TAKE TO PREVENT IDENTITY THEFT AND FRAUD

You may take action directly to further protect against possible identity theft or other financial loss. We encourage you to be vigilant against incidents of identity theft by reviewing your account statements regularly and monitoring your credit reports for suspicious activity. Under U.S. law, you are entitled to one free credit report annually from each of the three major credit reporting agencies. To order your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also contact the three major credit reporting agencies directly to request a free copy of your credit report.

At no charge, you can also have these credit reporting agencies place a "fraud alert" on your file that alerts creditors to take additional steps to verify your identity prior to granting credit in your name. Note, however, that because it tells creditors to follow certain procedures to protect you, it may also delay your ability to obtain credit while your identity is verified. As soon as one credit reporting agency confirms your fraud alert, the others are notified to place fraud alerts on your file. Should you wish to place a fraud alert, or should you have any questions regarding your credit report, please contact any one of the credit reporting agencies listed below.

Equifax Information Services LLC
P.O. Box 105069
Atlanta, GA 30348
866-349-5191
<https://www.alerts.equifax.com/AutoFraudOnline/jsp/fraudAlert.jsp>

Experian
P.O. Box 9554
Allen, TX 75013
888-397-3742
<https://www.experian.com/ncaconline/fraudalert>

TransUnion Fraud Victim Assistance
P.O. Box 2000
Chester, PA 19016
888-909-8872
<https://fraud.transunion.com/fa/fraudAlert/landingPage.jsp>

In addition to a fraud alert, consumers may place a security freeze on their credit reports. A security freeze prohibits a credit reporting agency from releasing any information from a consumer's credit report without the consumer's written authorization. However, please be advised that placing a security freeze on your credit report may delay, interfere with, or prevent the timely approval of any requests you make for new loans, credit mortgages, employment, housing, or other services.

If you have been a victim of identity theft, and you provide the credit reporting agencies with a valid police report, it cannot charge you to place, lift, or remove a security freeze. In all other cases, a credit reporting agency may charge you a fee to place, temporarily lift, or permanently remove a security freeze. You will need to place a security freeze separately with each of the three major credit reporting agencies listed above if you wish to place the freeze on all of your credit files.

To find out more on how to place a security freeze, you can contact the credit reporting agencies using the information below:

Equifax Security Freeze
P.O. Box 105788
Atlanta, GA 30348
800-685-1111
https://www.freeze.equifax.com/Freeze/jsp/SFF_PersonalIDInfo.jsp

Experian Security Freeze
P.O. Box 9554
Allen, TX 75013
888-397-3742
<https://www.experian.com/freeze/center.html>

TransUnion LLC
P.O. Box 2000
Chester, PA 19016
888-909-8872
<https://freeze.transunion.com/sf/securityFreeze/landingPage.jsp>

You can further educate yourself regarding identity theft, fraud alerts, and the steps you can take to protect yourself, by contacting the Federal Trade Commission or your state Attorney General. The Federal Trade Commission can be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580, www.ftc.gov/idtheft/, 1-877-ID-THEFT (1-877-438-4338); TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a

complaint with them. You can obtain further information on how to file such a complaint by way of the contact information listed above. Instances of known or suspected identity theft should also be reported to law enforcement, including your state Attorney General.

For Iowa residents, the Attorney General can be contacted at Hoover State Office Building, 1305 E. Walnut St., Des Moines, IA 50319, 1-888-777-4590, www.iowaattorneygeneral.gov.

For Maryland residents, the Attorney General can be contacted at 200 St. Paul Place, Baltimore, MD 21202, 1-888-743-0023, www.marylandattorneygeneral.gov.

For North Carolina residents, the Attorney General can be contacted at 9001 Mail Service Center, Raleigh, NC 27699, 919-716-6400, www.ncdoj.gov.

For Oregon residents, the Attorney General can be contacted at Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301, 1-877-877-9392, www.doj.state.or.us/.

For Rhode Island residents, the Attorney General can be contacted at Office of the Attorney General, 150 South Main Street, Providence, Rhode Island 02903, 401-274-4400, www.riag.ri.gov.

For all other residents, information on how to contact your state attorney general may be found at www.naag.org/naag/attorneys-general/vhos-my-ag.php.