



MULLEN  
COUGHLIN<sub>LLC</sub>  
ATTORNEYS AT LAW

RECEIVED

APR 29 2019

CONSUMER PROTECTION

Edward J. Finn  
Office: 267-930-4776  
Fax: 267-930-4771  
Email: [efinn@mullen.law](mailto:efinn@mullen.law)

1275 Drummers Lane, Suite 302  
Wayne, PA 19087

April 25, 2019

**VIA U.S. MAIL**

Attorney General Gordon J. MacDonald  
Office of the New Hampshire Attorney General  
Attn: Security Breach Notification  
33 Capitol Street  
Concord, NH 03301

**Re: Notice of Data Security Incident**

Dear Attorney General MacDonald:

We represent North 40 Outfitters ("North 40") headquartered at 5109 Alaska Trail, P.O. Box 6430, Great Falls, Montana, 59406, and are writing to supplement the notification provided to your office on February 14, 2019. By providing this notice, North 40 does not waive any rights or defenses.

**Additional Facts Regarding the Data Event**

On or about November 8, 2018, as a result of increased monitoring and enhanced security controls, North 40 identified suspicious activity regarding its online payment processing platform. North 40 immediately launched an investigation with the assistance of a third-party forensic firm to determine the nature and scope of the activity. The earlier findings of the investigation determined that customer credit and debit card information for transactions that occurred on North 40's ecommerce website between February 2, 2018 and November 20, 2018 may have been subject to unauthorized access and/or acquisition. North 40 successfully blocked further unauthorized access to customer card information and provided notice of the incident to the affected individuals and your office on February 14, 2019. Through the investigation of a Payment Card Industry Forensic Investigator ("PFI"), it was determined that the bad actor returned after the initial window of compromise. The PFI investigation concluded on March 26, 2019, concluding that it was possible that customer credit and debit card information for transactions that occurred on North 40's website between December 17, 2018 and January 22, 2019 may also have been subject to unauthorized access and/or acquisition. The investigation found an intruder introduced a program on North 40's webserver that may have caused customers to download a script which may have captured their card data when entered into the checkout page. This incident only affected transactions made on North 40's e-commerce website. No transactions made in North 40's retail stores were affected.

Attorney General MacDonald  
April 25, 2019  
Page 2

The information that could have been subject to unauthorized access includes customer names, credit or debit card numbers, card expiration date, and card security number or CVV. Certain customers' North 40 user account names and passwords may also have been affected.

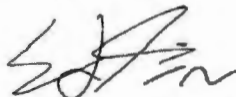
#### **Notice to Hew Hampshire Residents**

On or about April 25, 2019, North 40 provided written notice of this incident to all potentially affected individuals, which includes eleven (11) Hew Hampshire residents, which includes all individuals who used a card during the second window of compromise and whose information may have been exposed. Written notice is being provided in substantially the same form as the letter attached hereto as *Exhibit A*.

#### **Contact Information**

Should you have any questions regarding this notification or other aspects of the data security event, please contact us at 267-930-4776.

Very truly yours,



Edward J. Finn of  
MULLEN COUGHLIN LLC

EJF:ANM

# **EXHIBIT A**



CSWW, Inc.

[NAME]

[ADDRESS]

[CITY], [STATE] [ZIP CODE]

[DATE]

**Re: Notice of Data Breach**

Dear [NAME]:

North 40 Outfitters (“North 40”) recently discovered that customer credit and debit card data may have been compromised on our website, and that this incident may have affected the security of your personal information. This incident affected only our website, and not our North 40 retail locations. We take this incident very seriously and are providing you with information and access to resources so that you can protect your personal information, should you feel it is appropriate to do so.

**What Happened?** On or about November 8, 2018, as a result of advanced platform monitoring and security controls, North 40 identified suspicious activity regarding our online payment processing platform. North 40 immediately launched an investigation with the assistance of a third-party forensic firm to determine the nature and scope of the activity. On or about March 26, 2019, the forensic investigators finished their investigation and concluded that it was possible that customer credit and debit card information for transactions that occurred on North 40’s website between December 17, 2018, and January 22, 2019 may have been subject to unauthorized access and/or acquisition. The investigation found an intruder introduced a program on our webserver that may have caused your computer to download a script which may have captured your card data when entered into the checkout page. While the investigation was unable to definitively confirm whether card data was accessed or taken, North 40 is notifying you in an abundance of caution because we have confirmed that your credit or debit card was used for a transaction on our website during the relevant time period, and your information may be affected.

**What Information Was Involved?** The information potentially affected includes your name, credit or debit card number, expiration date, and card security code number or CVV. Your North 40 account username and password may also have been affected.

**What We Are Doing.** We take the security of personal information in our care very seriously. We have security measures in place to help protect the data on our systems and are working to implement additional safeguards and training to further protect the privacy and security of information in our care. This incident has been reported to your credit card company, and we will be reporting this incident to certain state regulators, Attorneys General and law enforcement.

**What You Can Do.** Please review the enclosed “Steps You Can Take to Prevent Identity Theft and Fraud.” We advise you to report any suspected incidents of identity theft to your credit card company and/or bank, as well as your local law enforcement or the Attorney General. If you have a North 40 online account, you should promptly change your password, security question and/or answer, and take appropriate steps to protect any other online accounts that have the same user name or email address and password, security question, and/or answer.

**For More Information.** We understand that you may have questions about this incident that are not addressed in this letter. If you have additional questions, or need assistance please call our dedicated assistance line at [Call Center Number], Monday through Friday 7:00 am to 4:30 pm MST.



CSWW, Inc.

North 40 takes the privacy and security of the personal information in our care seriously. We regret any concern this situation has caused you.

Sincerely,

Curtis L. Wike  
Vice President





CSWW, Inc.

## STEPS YOU CAN TAKE TO PREVENT IDENTITY THEFT AND FRAUD

We advise you to remain vigilant by reviewing all account statements and monitoring free credit reports.

### Monitor Your Accounts.

*Credit Reports.* We encourage you to remain vigilant against incidents of identity theft and fraud, to review your account statements, and to monitor your credit reports and explanation of benefits forms for suspicious activity. Under U.S. law, you are entitled to one free credit report annually from each of the major credit reporting bureaus. To order your free credit report, visit [www.annualcreditreport.com](http://www.annualcreditreport.com) or call, toll-free, 1-877-322-8228. You may also contact the major credit bureaus listed below to request a free copy of your credit report.

*Fraud Alerts.* At no charge, you can also have these credit bureaus 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 the agency verifies your identity. As soon as one credit bureau 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 agencies listed below.

Security Freeze. You have the 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. Pursuant to federal law, you cannot be charged to place or lift a security freeze on your credit report. Should you wish to place a security freeze, please contact the major consumer reporting agencies listed below:

|   |   |   |
|---|---|---|
| <b>Experian</b><br>PO Box 9554<br>Allen, TX 75013<br>1-888-397-3742<br><a href="http://www.experian.com/freeze/center.html">www.experian.com/freeze/center.html</a> | <b>TransUnion</b><br>P.O. Box 2000<br>Chester, PA 19016<br>1-888-909-8872<br><a href="http://www.transunion.com/credit-freeze">www.transunion.com/credit-freeze</a> | <b>Equifax</b><br>PO Box 105788<br>Atlanta, GA 30348-5788<br>1-800-685-1111<br><a href="http://www.equifax.com/personal/credit-report-services">www.equifax.com/personal/credit-report-services</a> |
|---|---|---|

In order to request a security freeze, you will need to supply the following information:

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. If you have moved in the past five (5) years, provide the addresses where you have lived over the prior five years;
5. Proof of current address, such as a current utility bill or telephone bill;
6. A legible photocopy of a government-issued identification card (state driver’s license or ID card, military identification, etc.);



CSWW, Inc.

7. If you are a victim of identity theft, include a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft.

To remove the security freeze, you must send a written request to each of the three credit bureaus by mail and include proper identification (name, address, and social security number) and the PIN number or password provided to you when you placed the security freeze. The credit bureaus have three (3) business days after receiving your request to remove the security freeze.

**Additional Information.** You can further educate yourself regarding identity theft, security freezes, fraud alerts, and the steps you can take to protect yourself against identity theft and fraud by contacting the Federal Trade Commission or your state Attorney General. ***For Maryland residents,*** the Attorney General can be contacted by mail at 200 St. Paul Place, Baltimore, MD, 21202; toll-free at 1-888-743-0023; by phone at (410) 576-6300; consumer hotline (410) 528-8662; and online at [www.marylandattorneygeneral.gov](http://www.marylandattorneygeneral.gov). ***For New Mexico residents,*** you have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for credit reports to be provided to employers; you may limit "prescreened" offers of credit and insurance you get based on information in your credit report; and you may seek damages from violator. You may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. We encourage you to review your rights pursuant to the Fair Credit Reporting Act by visiting [www.consumerfinance.gov/f/201504\\_cfpb\\_summary\\_your-rights-under-fcra.pdf](http://www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf), or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. Instances of known or suspected identity theft should also be reported to law enforcement. ***For North Carolina Residents:*** The North Carolina Attorney General can be contacted by mail at 9001 Mail Service Center, Raleigh, NC 27699-9001; toll-free at 1-877-566-7226; by phone at 1-919-716-6400, and online at [www.ncdoj.gov](http://www.ncdoj.gov). ***The Federal Trade Commission*** can be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580; [www.identitytheft.gov](http://www.identitytheft.gov); 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261. The Federal Trade Commission encourages those who discover that their information has been misused to file a complaint with them. Instances of known or suspected identity theft should be reported to law enforcement, the Federal Trade Commission, and your state Attorney General. This notice has not been delayed as a result of a law enforcement investigation. ***For Rhode Island Residents:*** The Rhode Island Attorney General can be reached at: 150 South Main Street, Providence, Rhode Island 02903, [www.riag.ri.gov](http://www.riag.ri.gov), 1-401-247-4400. Under Rhode Island law, you have the right to obtain any police report filed in regard to this incident. There are approximately two (2) Rhode Island residents impacted by this incident.