



MULLEN
COUGHLIN^{LLC}
ATTORNEYS AT LAW

Edward J. Finn
Office: 267-930-4776
Fax: 267-930-4771
Email: efinn@mullen.law

1275 Drummers Lane, Suite 302
Wayne, PA 19087

February 23, 2018

VIA U.S. MAIL & E-MAIL

Office of the Attorney General
1125 Washington Street SE
PO Box 40100
Olympia, WA 98504-0100
E-Mail: securitybreach@atg.wa.gov

Re: Notice of Data Security Incident

Dear Sir or Madam:

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 our preliminary notice to your office of an incident that may affect the security of personal information relating to 2,671 Washington residents. By providing this notice, North 40 does not waive any rights or defenses.

Nature of the Data Event

On or about January 10, 2018, North 40 was alerted by its card processor that certain credit and debit cards used on its e-commerce site may have been subject to unauthorized use. North 40 immediately launched an investigation to determine the nature and scope of the incident. On or about January 29, 2018, North 40 discovered that customer credit and debit card information for transactions that occurred on its e-commerce website between January 20, 2017 and January 29, 2018 were at risk of unauthorized access and/or acquisition. This incident only affected transactions made on North 40’s e-commerce website. No transactions made in North 40’s retail stores were affected.

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. It is unknown how many cards were actually acquired, but because cards were at risk during that time period, notice was provided to all potentially affected individuals out of an abundance of caution.

Notice to Washington Residents

On or about February 23, 2018, North 40 provided written notice of this incident to all affected individuals, which includes 2,671 Washington residents. Written notice is being provided in substantially the same form as the letter attached here as *Exhibit A*.

Other Steps Taken and To Be Taken

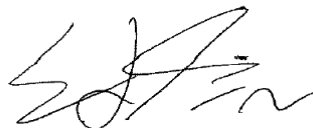
Upon discovering the event, North 40 moved quickly to investigate the incident, minimize risk to the information, and to provide the affected individuals with notice of this incident. North 40 is working to implement additional safeguards and training to its employees, and continues to monitor its e-commerce environment to guard against suspicious activity.

Additionally, North 40 is providing all impacted individuals with guidance on how to better protect against identity theft and fraud, including advising individuals to report any suspected incidents of identity theft or fraud to their credit card company and/or bank. North 40 is also providing individuals with information on how to place a fraud alert and security freeze on one's credit file, information on protecting against tax fraud, the contact details for the national consumer reporting agencies, information on how to obtain a free credit report, a reminder to remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring free credit reports, and encouragement to contact the Federal Trade Commission, their state Attorney General, and law enforcement to report attempted or actual identity theft and fraud. North 40 has reported this incident to the credit card companies. North 40 is also providing written notice of this incident to other state regulators as necessary.

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:ncl

cc: Office of the Attorney General
Consumer Protection Division
800 5th Ave., Suite 2000
Seattle, WA 98104-3188
E-Mail: securitybreach@atg.wa.gov

EXHIBIT A



CSWW, Inc.

Return Mail Processing Center
PO Box 6336
Portland, OR 97228-6336

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

<<Date>>

Re: Notice of Data Breach

Dear <<Name1>>:

North 40 Outfitters (“North 40”) is writing to inform you that we have recently experienced a data privacy incident involving the unauthorized access to customer credit and debit card data from our e-commerce website. This incident has affected the security of some of your personal information. 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.

While we have implemented additional security measures to address this issue, if you have a North 40 online account, we encourage you to 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.

Please Note: This incident only affected transactions made on our e-commerce website. Transactions made in our retail stores were not affected.

What Happened? On or about January 10, 2018, North 40 was alerted that certain credit and debit cards used on its e-commerce site may have been subject to unauthorized access. North 40 immediately launched an investigation to determine the nature and scope of the incident. On or about January 29, 2018, North 40 discovered that customer credit and debit card information for transactions that occurred on its e-commerce website between January 20, 2017 and January 29, 2018 was subject to unauthorized access and/or acquisition. North 40 is notifying you because we have confirmed that your credit or debit card was used for a transaction on our e-commerce 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 user name 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 protect the data on our systems and we are working to implement additional safeguards and training to our employees to safeguard 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 and Attorneys General and law enforcement.

What You Can Do. Please review the enclosed “Steps You Can Take to Prevent Identity Theft and Fraud.” In addition, 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.



CSWW, Inc.

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 888-732-2151.

Again, North 40 takes the privacy and security of the personal information in our care seriously. We sincerely apologize for this incident, and regret any concern or inconvenience this has caused you.

Sincerely,

Curtis L. Wike
Vice President

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 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 may also place a security freeze on your credit reports. A security freeze prohibits a credit bureau 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 bureau with a valid police report, it cannot charge you to place, lift, or remove a security freeze. In all other cases, a credit bureau 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 major credit bureaus listed below if you wish to place a freeze on all of your credit files. In order to request a security freeze, you will need to supply your full name, address, date of birth, Social Security number, current address, all addresses for up to five previous years, email address, a copy of your state identification card or driver’s license, and a copy of a utility bill, bank or insurance statement, or other statement proving current residence. If you are the victim of identity theft, include a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft. Fees vary based on where you live, but commonly range from \$3 to \$15. To find out more on how to place a security freeze, obtain a credit report, or fraud alert, you can use the following contact information:

Equifax
P.O. Box 105069
Atlanta, GA 30348
800-525-6285
www.equifax.com

Experian
P.O. Box 2002
Allen, TX 75013
888-397-3742
www.experian.com

TransUnion
P.O. Box 2000
Chester, PA 19106
800-680-7289
www.transunion.com



CSWW, Inc.

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. **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 violators. 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, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580. **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. *The Federal Trade Commission* can be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580; 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.