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

1275 Drummers Lane, Suite 302
Wayne, PA 19087

February 14, 2019

VIA EMAIL

Office of the Attorney General
1125 Washington Street SE
PO Box 40100
Olympia, WA 98504-0100
Email: 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 provide notice to your office of an incident that may affect the security of personal information relating to certain Washington residents. This notice may be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, North 40 does not waive any rights or defenses regarding the applicability of Washington law, the applicability of the Washington data incident notification statute, or personal jurisdiction.

Nature of 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. On or about December 14, 2018, the forensic investigation determined that customer credit and debit card information for transactions that occurred on North 40's e-commerce website between February 2, 2018 and November 20, 2018 may have been subject to unauthorized access and/or acquisition. North 40 provided notice to individuals whose credit and debit cards were used on their e-commerce website during the relevant period. 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.

Notice to Washington Residents

On or about February 14, 2019, North 40 provided written notice of this incident to all potentially affected individuals, including two thousand six hundred thirty-two (2,632) Washington residents, which includes all individuals who used a card during the 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***.

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 and the consumer reporting agencies, as required.

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.

<<Date>> (Format: Month Day, Year)

<<FirstName>> <<MiddleName>> <<LastName>> <<NameSuffix>>
<<Address1>>
<<Address2>>
<<City>>, <<State>> <<Zip>>

Re: Notice of Data Breach

Dear <<FirstName>> <<LastName>>,

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 December 14, 2018, the forensic investigation determined that customer credit and debit card information for transactions that occurred on North 40's website between February 2, 2018, and November 20, 2018 may have been 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 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 1-833-228-5728, Monday through Friday 7:00 am to 4:30 pm MST.

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

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 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:

Experian
PO Box 9554
Allen, TX 75013
1-888-397-3742
www.experian.com/freeze/center.html

TransUnion
P.O. Box 2000
Chester, PA 19016
1-888-909-8872
www.transunion.com/credit-freeze

Equifax
PO Box 105788
Atlanta, GA 30348-5788
1-800-685-1111
www.equifax.com/personal/credit-report-services

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.);
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. **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, 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. 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. **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, 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 twenty (20) Rhode Island residents impacted by this incident.