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

1275 Drummers Lane, Suite 302
Wayne, PA 19087

April 25, 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 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.

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 April 25, 2019, North 40 provided written notice of this incident to all potentially affected individuals, which include three hundred and fifteen (315) Washington 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