



Brian Craig
2112 Pennsylvania Avenue NW, Suite 500
Washington, D.C. 20037
Brian.Craig@lewisbrisbois.com
Direct: 202.926.2904

September 4, 2020

VIA ELECTRONIC SUBMISSION

Attorney General Gordon MacDonald
Office of the Attorney General
Consumer Protection Bureau
33 Capitol Street
Concord, NH 03301
DOJ-CPB@doj.nh.gov

Re: Notification of Data Security Incident

To Whom It May Concern:

Lewis Brisbois Bisgaard & Smith LLP represents Noveske Rifleworks, LLC (“Noveske”) in connection with the data security incident described in greater detail below. The privacy and security of all information within Noveske’s possession is extremely important to Noveske. Thus, in addition to providing notification of this incident to potentially impacted individuals, Noveske has taken steps to help prevent similar incidents in the future.

1. Nature of the security incident.

On May 13, 2020, Noveske learned of unusual activity within its email environment. Noveske then took immediate steps to secure its email system and engaged an independent digital forensics firm to conduct an investigation. As a result, Noveske learned that certain employee email accounts had been accessed without authorization. Noveske then engaged a document review vendor to assist in reviewing the contents of the relevant accounts believed to contain personal information. As a result of this review, Noveske learned on August 21, 2020 that the personal information of certain New Hampshire residents may have been accessed without authorization as a result of this incident. Noveske then worked diligently to identify up-to-date address information and to provide notification to potentially impacted individuals. The information impacted in connection with this incident may have included individuals’ names as well as individuals’ Social Security numbers and payment information.

2. Number of New Hampshire residents.

Noveske notified one (1) New Hampshire resident(s) of this data security incident by letter sent via first class U.S. mail on September 4, 2020. A sample copy of the notification letter sent to the affected individuals is included with this correspondence.

3. Steps taken relating to the incident.

September 4, 2020

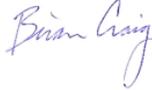
Page 2

As set forth in the enclosed letter, Noveske has taken steps in response to this incident to help prevent similar incidents from occurring in the future. Those steps have included, among other things, working with leading cybersecurity experts to enhance the security of its digital environment and reporting the incident to law enforcement. Furthermore, out of an abundance of caution, Noveske is also providing complimentary credit monitoring and identity theft restoration services to each letter recipient through ID Experts, a data breach and recovery services expert.

4. Contact information.

Noveske remains dedicated to the protection of all personal information within its control. If you have any questions or need additional information relating to this incident, please do not hesitate to contact me at Brian.Craig@lewisbrisbois.com. Please include Alexis Kirkman, Alexis.Kirkman@lewisbrisbois.com, on all correspondence pertaining to this matter as well.

Sincerely,



Brian Craig of
LEWIS BRISBOIS BISGAARD & SMITH LLP

Encl.: Sample Consumer Notification Letter



Noveske Rifleworks, LLC
 C/O ID Experts
 10300 SW Greenburg Rd., Suite 570
 Portland, Oregon 97223

To Enroll, Please Call:
 1-800-939-4170
 Or Visit:
<https://app.myidcare.com/account-creation/protect>
 Enrollment Code: <<Code>>

<<First Name>> <<Last Name>>
 <<Address1>> <<Address2>>
 <<City>>, <<State>> <<Zip Code>>

September 4, 2020

Re: Notice of Data Breach

Dear <<First Name>> <<Last Name>>:

I am writing to inform you of a data security incident experienced by Noveske Rifleworks, LLC (“Noveske”) that may have affected your personal information. The privacy and security of your personal information is extremely important to Noveske. That is why I am writing to inform you of this incident, to offer you complimentary credit monitoring and identity theft restoration services, and to provide you with information relating to steps that can be taken to help protect your personal information.

What Happened? On May 13, 2020, Noveske learned of unusual activity within its email environment. Upon discovering this activity, Noveske immediately took steps to secure all Noveske email accounts and launched an investigation. As part of that investigation, Noveske engaged an independent digital forensics firm to determine what happened and whether any information was accessed or acquired without authorization as a result. As a result of this engagement, the digital forensics firm reported to Noveske that the email accounts of certain Noveske employees had been accessed without authorization. Following a review of the contents of the relevant email accounts, Noveske learned on August 21, 2020 that some of your personal information was contained therein which may have been accessed without authorization as a result of this incident. Noveske then worked diligently to identify up-to-date address information in order to provide notification to potentially impacted individuals.

Please note that this incident was limited to potential unauthorized access to information transmitted via email and did not affect any other Noveske information systems, including its core payroll and tax payment systems. Please also note that **Noveske also has no evidence to suggest that your information has been misused in connection with this incident.** but is nonetheless notifying you out of an abundance of caution.

What Information Was Involved? The information impacted in connection with this incident may have included your name, address, date of birth, online credentials, driver’s license number or other state identification number, payment card information, financial account number, or routing number. Your Social Security number was not impacted in connection with this incident.

What Are We Doing? As soon as Noveske discovered this incident, Novseke took the measures described above. In addition, because Noveske takes the security of all information within its possession very seriously, Noveske notified law enforcement of this incident and took steps to enhance the security of its email system in order to minimize the likelihood of similar incidents occurring in the future. Noveske is also providing you with information about steps that you can take to help protect your personal information and is offering you complimentary MyIDCare™ services through ID Experts®, the data breach and recovery services expert. MyIDCare™ services include << twelve (12) / twenty-four (24) >> months of credit monitoring, dark web monitoring, a \$1,000,000 identity fraud loss reimbursement policy, and fully managed identity theft recovery services. With this protection, ID Experts® will help you to resolve issues if your identity is compromised.

What Can You Do? Please follow the recommendations on the following page to help protect your personal information. Please also contact ID Experts® to enroll in the complimentary MyIDCare™ services being offered to you by calling 1-800-939-4170 or by going to <https://app.myidcare.com/account-creation/protect> and using the Enrollment Code provided above. Please note that the deadline to enroll is December 4, 2020.

For More Information: Further information about how to protect your personal information appears on the following page. If you have questions or need assistance, please call ID Experts® at 1-800-939-4170, Monday through Friday from 9 a.m. until 9 p.m. Eastern Standard Time (excluding holidays). ID Experts® representatives are fully versed on this incident and can answer any questions you may have regarding the protection of your personal information.

We take your trust in us and this matter very seriously and we apologize for any worry or inconvenience that this incident may cause you.

Sincerely,

A handwritten signature in black ink that reads "Deborah Brown". The signature is written in a cursive, flowing style.

Deborah Brown
Controller
Noveske Rifleworks, LLC

STEPS YOU CAN TAKE TO HELP FURTHER PROTECT YOUR INFORMATION

Review Your Account Statements and Notify Law Enforcement of Suspicious Activity: As a precautionary measure, we recommend that you remain vigilant by reviewing your account statements and credit reports closely. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained. You also should promptly report any fraudulent activity or any suspected incidence of identity theft to proper law enforcement authorities, your state attorney general, and/or the Federal Trade Commission (FTC).

Copy of Credit Report: You may obtain a free copy of your credit report from each of the three major credit reporting agencies once every 12 months by visiting <http://www.annualcreditreport.com/>, calling toll-free 877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. You can print this form at <https://www.annualcreditreport.com/cra/requestformfinal.pdf>. You also can contact one of the following three national credit reporting agencies:

TransUnion P.O. Box 1000 Chester, PA 19016 1-800-916-8800 www.transunion.com	Experian P.O. Box 9532 Allen, TX 75013 1-888-397-3742 www.experian.com	Equifax P.O. Box 105851 Atlanta, GA 30348 1-800-525-6285 www.equifax.com	Free Annual Report P.O. Box 105281 Atlanta, GA 30348 1-877-322-8228 annualcreditreport.com
---	---	--	---

Fraud Alert: You may want to consider placing a fraud alert on your credit report. An initial fraud alert is free and will stay on your credit file for at least 90 days. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any accounts in your name. To place a fraud alert on your credit report, contact any of the three credit reporting agencies identified above. Additional information is available at <http://www.annualcreditreport.com>.

Security Freeze: You have the right to put a security freeze on your credit file. This will prevent new credit from being opened in your name without the use of a PIN number that is issued to you when you initiate the freeze. A security freeze is designed to prevent potential creditors from accessing your credit report without your consent. As a result, using a security freeze may interfere with or delay your ability to obtain credit. You must separately place a security freeze on your credit file with each credit reporting agency. There is no charge to place, lift or remove the security freeze. In order to place a security freeze, you may be required to provide the consumer reporting agency with information that identifies you including your full name, Social Security number, date of birth, current and previous addresses, a copy of your state-issued identification card, and a recent utility bill, bank statement or insurance statement.

Additional Free Resources: You can obtain information from the consumer reporting agencies, the FTC or from your respective state Attorney General about steps you can take toward preventing identity theft. You may report suspected identity theft to local law enforcement, including to the FTC or to the Attorney General in your state. Residents of Maryland, North Carolina, Rhode Island, and Washington, D.C. can obtain more information from their Attorneys General using the contact information below.

Federal Trade Commission 600 Pennsylvania Ave, NW Washington, DC 20580 consumer.ftc.gov, and www.ftc.gov/idtheft 1-877-438-4338	Maryland Attorney General 200 St. Paul Place Baltimore, MD 21202 https://oag.state.md.us 1-888-743-0023	North Carolina Attorney General 9001 Mail Service Center Raleigh, NC 27699 https://ncdoj.gov 1-877-566-7226	Rhode Island Attorney General 150 South Main Street Providence, RI 02903 http://www.riag.ri.gov 401-274-4400	Washington D.C. Attorney General 441 4th Street, NW Washington, DC 20001 https://oag.dc.gov/ 202-727-3400
--	--	---	--	---

You also have certain rights under the Fair Credit Reporting Act (FCRA), including: to know what is in your file; to dispute incomplete or inaccurate information; to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information, as well as others. For more information about the FCRA, and your rights pursuant to the FCRA, please visit http://files.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf.



MyIDCare™ Enrollment

Website and Enrollment. Please visit <https://app.myidcare.com/account-creation/protect> and follow the instructions for enrollment using your Enrollment Code included with this letter.

Activate the monitoring provided as part of your MyIDCare™ membership. The monitoring included in the membership must be activated to be effective. Note: You must have established credit and access to a computer and the internet to use this service. If you need assistance, MyIDCare™ will be able to assist you.

Telephone. Contact MyIDCare™ at 1-800-939-4170 to speak with knowledgeable representatives about the appropriate steps to take to protect your credit identity.

This MyIDCare™ enrollment will include one-year enrollment into:

SINGLE BUREAU CREDIT MONITORING - Monitoring of credit bureau for changes to the member's credit file such as new credit inquires, new accounts opened, delinquent payments, improvements in the member's credit report, bankruptcies, court judgments and tax liens, new addresses, new employers, and other activities that affect the member's credit record.

CYBERSCAN™ MONITORING - Dark Web monitoring of underground websites, chat rooms, and malware, 24/7, to identify trading or selling of personal information like SSNs, bank accounts, email addresses, medical ID numbers, driver's license numbers, passport numbers, credit and debit cards, phone numbers, and other unique identifiers.

IDENTITY THEFT INSURANCE - Identity theft insurance will reimburse members for expenses associated with restoring their identity should they become a victim of identity theft. If a member's identity is compromised, the policy provides coverage for up to \$1,000,000, with no deductible, from an A.M. Best "A-rated" carrier. Coverage is subject to the terms, limits, and/or exclusions of the policy.

FULLY-MANAGED IDENTITY RECOVERY - ID Experts' fully-managed recovery service provides restoration for identity theft issues such as (but not limited to): account creation, criminal identity theft, medical identity theft, account takeover, rental application, tax fraud, benefits fraud, and utility creation. This service includes a complete triage process for affected individuals who report suspicious activity, a personally assigned IDCare Specialist to fully manage restoration of each case, and expert guidance for those with questions about identity theft and protective measures.