LEWIS BRISBOIS BISGAARD & SMITH LLP

Elizabeth R. Dill
550 E. Swedesford Road, Suite 270
Wayne, Pennsylvania 19087
Elizabeth.Dill@lewisbrisbois.com
Direct: 215.977.4080

August 5, 2020

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

Re: Notification of Data Security Incident

Dear Attorney General MacDonald:

We represent GWB, LLC, d/b/a Grand Western ("Grand Western") in connection with a data security incident which is described in greater detail below. Grand Western takes the protection of all sensitive information within its possession very seriously and is taking steps to prevent similar incidents from occurring in the future.

1. **Nature of the security incident.**

Grand Western learned of suspicious activity occurring on the e-commerce web platform for its online store, grandwesternsteaks.com. Upon discovering this activity, Grand Western took immediate steps to further secure its system and conducted a thorough internal investigation to determine the scope of the issue. Grand Western also engaged a nationally-recognized digital forensics firm to conduct an independent investigation into what happened and whether any customer payment card information had been accessed or acquired without authorization. On June 22, 2020, the investigation identified the individuals who made purchases on Grand Western's online store whose names, payment card numbers, expiration dates and security codes may have been exposed during the potential windows of compromise. Grand Western then worked diligently to identify up-to-date address information in order to notify all potentially impacted individuals. On July 13, 2020, Grand Western identified three (3) New Hampshire residents within the potentially affected population.

2. Number of New Hampshire residents affected.

Grand Western sent notification letters on July 30, 2020 to the three (3) affected New Hampshire residents regarding this data security incident via first-class U.S. mail. A sample copy of the notification letter is included with this letter.

3. Steps taken relating to the incident.

Grand Western has taken steps in response to this incident to prevent similar incidents from occurring in the future. Those steps have included working with leading cybersecurity experts to enhance the security of its e-commerce platform. Additionally, Grand Western promptly notified the payment card brands and the Federal Bureau of Investigation in an effort to prevent fraud associated with this incident. Grand Western is also offering identity protection services through ID Experts, which will help individuals resolve issues if their identity is compromised due to this incident.

4. Contact information.

Grand Western remains dedicated to protecting the personal information in its possession. If you have any questions or need additional information, please do not hesitate to contact me at (215) 977-4080 or via email at Elizabeth.Dill@lewisbrisbois.com.

Regards,

Elizabeth R. Dill of
LEWIS BRISBOIS BISGAARD & SMITH LLP

Enclosure: Sample Notification Letter
ERD:ALW

Grand Western

C/O ID Experts
10300 SW Greenburg Rd. Suite 570
Portland, OR 97223

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

July 30, 2020

Re: Notification of Data Security Incident

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

GWB, LLC d/b/a Grand Western is writing to notify you of a data security incident relating to your purchase through our online store, grandwesternsteaks.com, which may have involved your payment card information. At Grand Western, we take the privacy and security of your information very seriously. We are writing to both inform you of the incident, and to advise you about certain steps you can take to protect your information.

What Happened? We learned of suspicious activity occurring in Grand Western's online store. Upon discovering this activity, we took immediate steps to further secure our system and customer information. We also engaged a nationally-recognized digital forensics firm to conduct an independent investigation into what happened and determine whether any customer payment card information had been accessed or acquired without authorization.

What Information was Involved? After an extensive forensics investigation and diligent review of the customer information that was potentially affected, we determined on June 22, 2020 that this incident may have involved payment card information of certain customers who purchased products through our online store between February 25, 2020 and May 13, 2020. The affected information includes names, card numbers, expiration dates, and security codes.

What Are We Doing? As soon as we discovered the incident, we took the steps discussed above. In addition, we reported the matter to the payment card brands and the Federal Bureau of Investigation to protect your information and prevent fraudulent activity. In order to prevent similar incidents from occurring in the future, we have implemented additional measures to enhance the security of our e-commerce platform. We are also providing you with information about steps you can take to protect your personal information. As an added precaution, we are offering, at no cost to you, MyIDCare Identity Protection Services through ID Experts.® With this protection, MyIDCare will help you resolve issues if your identity is compromised.

What You Can Do. You can follow the recommendations included with this letter to protect your personal information. We recommend that you review your current and past credit and debit card account statements for discrepancies or unusual activity. If you see anything that you do not understand or that looks suspicious, or if you suspect that any fraudulent transactions have taken place, you should call the bank that issued the credit or debit card immediately. In addition, you can contact ID Experts' Certified Recovery Advocates at 1-800-939-4170, who will work on your behalf to help resolve these issues. ID Experts' Certified Recovery Advocates are available Monday through Friday from 9 am - 8 pm Eastern Time.

<u>For More Information</u>: If you have any questions or need assistance, we encourage you to contact our dedicated call center at 1-800-939-4170 between 9 am - 8 pm Eastern Time.

We take this matter very seriously. Please accept our apologies for any concern or inconvenience this may cause you.

Sincerely,

The Grand Western Team

GRAND WESTERN STEAKS

240 SW 32nd Street
Fort Lauderdale, Florida 33315

STEPS YOU CAN TAKE TO 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 and review 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 should also 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 (the "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 also contact one of the following three national credit reporting agencies:

Equifax	**Experian**	**TransUnion**	**Free Annual Report**
P.O. Box 105851	P.O. Box 9532	P.O. Box 1000	P.O. Box 105281
Atlanta, GA 30348	Allen, TX 75013	Chester, PA 19016	Atlanta, GA 30348
1-800-525-6285	1-888-397-3742	1-800-916-8800	1-877-322-8228
www.equifax.com	www.experian.com	www.transunion.com	www.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 one year. 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. 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 the following states can obtain more information from their Attorney General using the contact information below.

California Residents: Visit the California Office of Privacy Protection (http://www.ca.gov/Privacy) for additional information on protection against identity theft.

Kentucky Residents: Office of the Attorney General of Kentucky, 700 Capitol Avenue, Suite 118 Frankfort, Kentucky 40601**,** www.ag.ky.gov, Telephone: 1-502-696-5300.

Maryland Residents: Office of the Attorney General of Maryland**,** Consumer Protection Division 200 St. Paul Place Baltimore, MD 21202**,** www.oag.state.md.us/Consumer, Telephone: 1-888-743-0023.

North Carolina Residents: Office of the Attorney General of North Carolina**,** 9001 Mail Service Center
Raleigh, NC 27699-9001, www.ncdoj.gov, Telephone: 1-919-716-6400.

Oregon Residents: Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, www.doj.state.or.us/, Telephone: 877-877-9392

Rhode Island Residents: Office of the Attorney General, 150 South Main Street, Providence, Rhode Island 02903, www.riag.ri.gov, Telephone: 401-274-4400

All US Residents: Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW Washington, DC 20580, www.consumer.gov/idtheft, 1-877-IDTHEFT (438-4338), TTY: 1-866-653-4261.

You also have certain rights under the Fair Credit Reporting Act (FCRA): These rights include knowing what is in your file; disputing incomplete or inaccurate information; and requiring consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information. For more information about the FCRA, please visit https://www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf.