



LEWIS BRISBOIS BISGAARD & SMITH LLP

Sean B. Hoar  
888 SW Fifth Ave., Suite 9000  
Portland, OR 97204  
Sean.Hoar@lewisbrisbois.com  
Direct: 971.712.2795

December 16, 2021

**VIA ELECTRONIC MAIL**

Attorney General Tom Miller  
Consumer Protection Division  
Security Breach Notifications  
Office of the Attorney General of Iowa  
1305 E. Walnut Street  
Des Moines, Iowa 50319-0106  
Email: [consumer@ag.iowa.gov](mailto:consumer@ag.iowa.gov)

Re: **Notification of Data Security Incident**

Dear Attorney General Miller:

Lewis Brisbois Bisgaard & Smith LLP (“Lewis Brisbois”) represents Tennis Warehouse, LLC (“Tennis Warehouse”) regarding a data security incident referenced below. The purpose of this letter is to notify you of the incident pursuant to Iowa Code §715C.2.

**Nature of the Security Incident.** On October 15, 2021, Tennis Warehouse became aware of a potential data security incident. We immediately began an internal investigation and engaged an independent computer forensics firm to determine whether any personal information was affected in the incident. On November 6, 2021, the investigation determined that payment card information was obtained without authorization on October 1, 2021. On November 29, 2021, the affected persons were identified after a thorough search of digital evidence.

**Type of Information and Number of Iowa Residents Affected.** As referenced above, the incident involved payment card information. On December 16, 2021, Tennis Warehouse began notifying 2,932 potentially affected payment card holders who are residents of Iowa via first class U.S. mail or email. A sample copy of the notification letter is included with this correspondence.

**Measures Taken in Response to Incident.** Upon becoming aware of the incident, Tennis Warehouse took the measures referenced above. We also reported the incident to the payment card brands in an attempt to prevent fraudulent activity on the affected accounts. We also reported the incident to law enforcement and have worked closely with the digital forensics firm to enhance the security of our sites to facilitate safe and secure transactions.

**Contact Information.** Tennis Warehouse remains dedicated to protecting personal information in its control. If you have any questions or need additional information, please contact Sean Hoar at 971.712.2795

Attorney General Tom Miller  
December 16, 2021  
Page 2

or via email at [Sean.Hoar@lewisbrisbois.com](mailto:Sean.Hoar@lewisbrisbois.com) or Laura Funk at 972.942.5696 or via email at [Laura.Funk@lewisbrisbois.com](mailto:Laura.Funk@lewisbrisbois.com).

Sincerely,



Sean B. Hoar of  
LEWIS BRISBOIS BISGAARD & SMITH LLP

CC: Laura Funk, Partner  
Lewis Brisbois Bisgaard & Smith LLP

Enclosure: Sample Consumer Notification Letter

<<Variable Logo>>

P.O Box 989728  
West Sacramento, CA 95798-9728

<<First Name>> <<Last Name>>

<<Address1>>

<<Address2>>

<<City>>, <<State>> <<Zip>>

December 16, 2021

**Re:** <<Variable Header>>

Dear <<First Name>> <<Last Name>>,

This letter is to provide you with information about a data security incident that may have affected your payment card information. The privacy and security of your personal information is extremely important to us as we very much appreciate your business and your confidence in us. We are sending this letter to notify you of the incident, to provide you with information about the nature of the incident, and the steps you can now take to protect your personal information.

**What Happened.** On October 15, 2021, <<Entity>> Warehouse, LLC (“<<Entity>> Warehouse”) we became aware of a potential data security incident. We immediately began an internal investigation and engaged an independent computer forensics firm to determine whether any personal information was affected in the incident. The investigation has been extensive, requiring the analysis of a substantial amount of digital evidence. On November 6, 2021, the investigation determined that payment card information was obtained without authorization on October 1, 2021. On November 29, 2021, the investigation determined that your payment card information may have been affected during the incident.

**What Information Was Involved.** The incident may have involved payment card information, including your name, address, payment card number <<Last 4 Digits>> , expiration date, and payment card security code.

**What We Are Doing.** We took the measures referenced above, and reported the incident to the payment card brands in an attempt to prevent fraudulent activity on the affected accounts. We also reported the incident to law enforcement and will provide whatever cooperation is necessary to hold the perpetrators accountable. We have also worked closely with the digital forensics firm to enhance the security of our sites to facilitate safe and secure transactions.

**What You Can Do.** Receiving this letter does not mean that you are the victim of identity theft. We strongly recommend, however, that you take the steps referenced on the following page to protect your personal information.

**For More Information.** If you have questions or need assistance, please never hesitate to call (833) 381-2293, Monday through Friday from 9 a.m. to 9 p.m. Eastern Time.

We sincerely apologize for this incident. We value you, your personal information, and your continued business.

Sincerely,



Mark Sczbecki

Co-Owner

<<Entity>> Warehouse, LLC

1295 Bluegrass Lakes Parkway  
Alpharetta, Georgia 30004

## Steps You Can Take to Protect Your Personal 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 payment card account statements. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company that issued the payment card or with whom 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 1-877-322-8228, 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 also can contact one of the following three national credit reporting agencies:

**Equifax**

P.O. Box 105851  
Atlanta, GA 30348  
1-800-525-6285  
[www.equifax.com](http://www.equifax.com)

**Experian**

P.O. Box 9532  
Allen, TX 75013  
1-888-397-3742  
[www.experian.com](http://www.experian.com)

**TransUnion**

P.O. Box 1000  
Chester, PA 19016  
1-800-916-8800  
[www.transunion.com](http://www.transunion.com)

**Fraud Alert:** Although the theft of payment card information should not affect access to credit, as a normal preventive practice, 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 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 for up to one year at no cost. 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 fraud alerts, security freezes, and 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.

**Federal Trade Commission**

600 Pennsylvania Ave, NW  
Washington, DC 20580  
consumer.ftc.gov, and  
[www.ftc.gov/idtheft](http://www.ftc.gov/idtheft)  
1-877-438-4338

**Maryland Attorney General**

200 St. Paul Place  
Baltimore, MD 21202  
[oag.state.md.us](http://oag.state.md.us)  
1-888-743-0023

**New York Attorney General**

Bureau of Internet and Technology  
Resources  
28 Liberty Street  
New York, NY 10005  
1-212-416-8433

**North Carolina Attorney General**

9001 Mail Service Center  
Raleigh, NC 27699  
[ncdoj.gov](http://ncdoj.gov)  
1-877-566-7226

**Rhode Island Attorney General**

150 South Main Street  
Providence, RI 02903  
<http://www.riag.ri.gov>  
1-401-274-4400

**Washington D.C. Attorney  
General**

441 4th Street, NW  
Washington, DC 20001  
[oag.dc.gov](http://oag.dc.gov)  
1-202-727-3400

**You also have certain rights under the Fair Credit Reporting Act (FCRA):** These rights include 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 other rights. For more information about the FCRA, and your rights pursuant to the FCRA, please visit <https://www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf>.

