



MULLEN
COUGHLIN^{LLC}
ATTORNEYS AT LAW

Rebecca J. Jones
Office: (267) 930-4839
Fax: (267) 930-4771
Email: rjones@mullen.law

426 W. Lancaster Avenue, Suite 200
Devon, PA 19333

March 23, 2022

INTENDED FOR ADDRESSEE(S) ONLY

VIA E-MAIL

Office of the Attorney General
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202
E-mail: idtheft@oag.state.md.us

Re: Notice of Data Event

Dear Sir or Madam:

We represent Leerburg Enterprises, Inc. ("Leerburg") located at 406 Technology Drive West, Menomonie, Wisconsin 54751, and are writing to notify your office of an incident that may affect the security of some personal information relating to three hundred forty-four (344) Maryland residents. This notice may be supplemented with new significant facts learned subsequent to its submission. By providing this notice, Leerburg does not waive any rights or defenses regarding the applicability of Maryland law, the applicability of the Maryland data event notification statute, or personal jurisdiction.

Nature of the Data Event

On March 4, 2021, Leerburg was notified that certain credit and debit cards used on its e-commerce website may have been subject to unauthorized access, and immediately began working to remedy the issue. Leerburg subsequently commenced an investigation with the assistance of payment card industry-accredited computer forensic specialists, to determine the nature and scope of the activity. This investigation was concluded on January 13, 2022. Additionally, Leerburg commenced an extensive review of the payment card transactions made through its website during the relevant time period. As a result of the investigation, Leerburg determined that certain Leerburg customer payment card information for transactions that occurred on its e-commerce website between September 8, 2020 and November 24, 2021 was subject to unauthorized access and/or acquisition. Leerburg is notifying individuals who conducted credit or debit card transactions on its e-commerce website during the relevant time period. Once made aware of the issue, Leerburg remediated the issue that allowed the unauthorized access and/or acquisition to occur, and implemented additional security enhancements to help prevent an incident from occurring in the future. There have been no further issues reported since the problem was remediated.

The information that could have been subject to unauthorized access includes name, credit or debit card number, expiration date, and security code number or CVV code.

Notice to Maryland Residents

On or about March 23, 2022, Leerburg provided notice of this incident to all affected individuals, which includes approximately three hundred forty-four (344) Maryland residents. Written notice is being provided via mail, and email where permitted, in substantially the same form as the letter attached here as ***Exhibit A***.

Other Steps Taken and To Be Taken

Upon discovering the event, Leerburg worked diligently to investigate and respond to the incident, assess the security of Leerburg's systems, and notify potentially affected individuals. Leerburg is also working to implement additional data security safeguards.

Leerburg is providing 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. Leerburg is providing individuals with information on how to place a fraud alert and security freeze on one's credit file, 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.

Contact Information

Should you have any questions regarding this notification or other aspects of the data security event, please contact us at (267) 930-4839.

Very truly yours,

A handwritten signature in black ink, appearing to read "Rebecca Jones", written over a light gray rectangular background.

Rebecca J. Jones of
MULLEN COUGHLIN LLC

RJJ/lhw
Enclosure

EXHIBIT A

Leerburg Enterprises, Inc.
P.O. Box 1907
Suwanee, GA 30024

<<Name 1>> <<Name 2>>
<<Address 1>>
<<Address 2>>
<<City>>, <<State>> <<Zip>>
<<Country>>

March 23, 2022

Notice of <<Variable Data 1>>

Dear <<Name 1>> <<Name 2>>:

Leerburg Enterprises, Inc. ("Leerburg") is contacting you to notify you of an incident that affects some of your payment card information used on our e-commerce website. We take the security of personal information in our care seriously and are providing you with this notice to make you aware of the incident, the steps we are taking in response, and steps you may take to help protect your personal information, should you feel it is appropriate to do so.

What Happened?

On March 4, 2021, we were notified that certain credit and debit cards used on our e-commerce website may have been subject to unauthorized access, and immediately began working to remedy the issue. We subsequently commenced an investigation with the assistance of payment card industry-accredited computer forensic specialists to determine the nature and scope of the activity. This investigation was concluded on January 13, 2022. As a result of the investigation, we determined that certain Leerburg customer payment card information for transactions that occurred on our e-commerce website between September 8, 2020 and November 24, 2021 was subject to unauthorized access and/or acquisition. Leerburg is notifying you because we have confirmed that your credit or debit card was used for a transaction on our e-commerce website during the relevant time period, and your information may be affected.

Once made aware of the issue, we remediated the issue that allowed the unauthorized access and/or acquisition to occur and implemented additional security enhancements to help prevent an incident from occurring in the future. There have been no further issues reported since the problem was remediated. Additionally, we commenced an extensive review of the payment card transactions made through our website during the relevant time period.

What Information Was Involved?

The information that was affected includes your name, credit or debit card number, expiration date, and security code number or CVV code.

What We Are Doing.

We take this incident and the security of personal information entrusted to us very seriously. Upon learning of this incident, we worked diligently to identify and remediate the issue. Leerburg has security measures in place to protect the information in our care, and we are working to implement additional safeguards moving forward. We have been in contact with the credit card brands about this issue, and we will be reporting this incident to certain state regulators and Attorneys General as required.

What You Can Do.

Leerburg encourages you to remain vigilant against incidents of potential fraud and/or misuse of your information, and to review the enclosed *Steps You Can Take to Protect Personal Information*. In addition, we encourage you to report any suspected incidents of identity theft to local law enforcement or your state Attorney General.

For More Information.

If you have questions that are not answered by this letter, you may call our dedicated assistance line at 1-833-774-2189, available Monday through Friday, from 8:00 a.m. to 8:00 p.m., Central Time. Additionally, you can write to us at Leerburg Enterprises, Inc., 406 Technology Drive West, Menomonie, Wisconsin 54751.

We sincerely apologize for this incident, and regret any inconvenience this incident may cause you. Leerburg takes the protection of the personal information within our care seriously and we remain committed to safeguarding your information.

Sincerely,

Leerburg Enterprises, Inc.

STEPS YOU CAN TAKE TO PROTECT PERSONAL INFORMATION

Monitor Your Accounts

We advise you to remain vigilant by reviewing all account statements and monitoring free credit reports for suspicious activity and to detect errors over the next 12 to 24 months. If you discover or suspect fraudulent activity involving your credit or debit card, we encourage you to contact the issuing bank. The number to call for assistance is usually on the back of the card.

Under U.S. law, a consumer is entitled to one free credit report annually from each of the three major credit reporting bureaus, Equifax, Experian, and TransUnion. To order your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also directly contact the three major credit reporting bureaus listed below to request a free copy of your credit report.

Consumers have the right to place an initial or extended “fraud alert” on a credit file at no cost. An initial fraud alert is a 1-year alert that is placed on a consumer’s credit file. Upon seeing a fraud alert display on a consumer’s credit file, a business is required to take steps to verify the consumer’s identity before extending new credit. If you are a victim of identity theft, you are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should you wish to place a fraud alert, please contact any one of the three major credit reporting bureaus listed below.

As an alternative to a fraud alert, consumers have the right to place a “credit freeze” on a credit report, which will prohibit a credit bureau from releasing information in the credit report without the consumer’s express authorization. The credit 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 credit 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 credit freeze on your credit report. To request a security freeze, you will need to provide the following information:

1. Full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. Addresses for the prior two to 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, etc.); and
7. A copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft if you are a victim of identity theft.

Should you wish to place a credit freeze, please contact the three major credit reporting bureaus listed below:

Equifax	Experian	TransUnion
https://www.equifax.com/personal/credit-report-services/	https://www.experian.com/help/	https://www.transunion.com/credit-help
1-888-298-0045	1-888-397-3742	1-833-395-6938
Equifax Fraud Alert, P.O. Box 105069 Atlanta, GA 30348-5069	Experian Fraud Alert, P.O. Box 9554, Allen, TX 75013	TransUnion Fraud Alert, P.O. Box 2000, Chester, PA 19016
Equifax Credit Freeze, P.O. Box 105788 Atlanta, GA 30348-5788	Experian Credit Freeze, P.O. Box 9554, Allen, TX 75013	TransUnion Credit Freeze, P.O. Box 160, Woodlyn, PA 19094

Additional Information

You may further educate yourself regarding identity theft, fraud alerts, credit freezes, and the steps you can take to protect your personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or your state Attorney General. The Federal Trade Commission may 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 also encourages those who discover that their information has been misused to file a complaint with them.

You can obtain further information on how to file such a complaint by way of the contact information listed above. You have the right to file a police report if you ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, you will likely need to provide some proof that you have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and your state Attorney General. This notice has not been delayed by law enforcement.

For District of Columbia residents, the District of Columbia Attorney General may be contacted at: 400 6th Street, NW, Washington, DC 20001; 202-727-3400; and oag@dc.gov.

For Maryland residents, the Maryland Attorney General may be contacted at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-410-528-8662 or 1-888-743-0023; and www.oag.state.md.us.

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 bureaus 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.

For New York residents, the New York Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; or <https://ag.ny.gov/>.

For North Carolina residents, the North Carolina Attorney General may be contacted at: 9001 Mail Service Center, Raleigh, NC 27699-9001; 1-877-566-7226 or 1-919-716-6000; and www.ncdoj.gov.

For Rhode Island residents, the Rhode Island Attorney General may be reached at: 150 South Main Street, Providence, RI 02903; www.riag.ri.gov; and 1-401-274-4400. Under Rhode Island law, you have the right to obtain any police report filed in regard to this incident. There are <<#>> Rhode Island residents impacted by this incident.