



[DATE]

Name

Address

City State Zip

RE: Notice of Data Breach

Dear [Recipient Name]:

Runnings is writing regarding a recent data security incident that may impact certain payment card information used by you to make purchases on our website. Please note that this incident only affects customers who made online purchases and not those who made in store purchases. We wanted to provide you with information about this incident, our response and steps you can take to prevent fraud, should you feel it necessary to do so.

**What Happened?** On Monday, February 13, 2017, we were notified by Aptos, the company that hosts our e-commerce platform, that it had discovered potential unauthorized access to the platform. Aptos informed us that an intruder placed malware on the website that allowed access to customers' payment card data when making purchases. After discovering the issue, Aptos retained a third party forensic investigator and notified law enforcement. Runnings believes that both of these investigations are ongoing. Aptos' investigation to date indicates that the period of intrusion was February through December 2016 and affects cards used to make online purchases during and prior to those dates. We are informing you of this incident as you made at least one purchase on our website during this time period. Aptos discovered the issue in November but informed us that law enforcement requested that Aptos not inform its clients about the issue while the law enforcement investigation was under way.

**What Information Was Involved?** While its investigation is ongoing, Aptos has told us that it believes that certain payment information of customers of Runnings and 39 other vendors that use its platform were subject to unauthorized access from February through December 2016. The data elements potentially subject to unauthorized access include your: name, address, phone number, email address and credit and/or debit card information.

**What We Are Doing.** Runnings and Aptos take the security of your personal information very seriously. Aptos has removed the malware that led to the vulnerability and implemented additional security measures to reduce the likelihood of a similar incident from happening in the future. We are providing notice of this incident to those who may be impacted so that they can take steps to prevent against possible fraud, should they feel it is

necessary to do so. We will also work with Aptos to notify certain state regulators and the credit reporting agencies about this incident.

**What You Can Do.** You can stay vigilant by reviewing your credit card statements for any suspicious charges. You can also review the enclosed *Steps You Can Take to Protect Against Identity Theft and Fraud* which includes guidance on steps you can take to better protect against the possibility of fraud and identify theft.

**For More Information.** If you have questions or concerns that are not addressed in this notice letter, you may call [name] at XXX-XXX-XXXX Monday through Friday, X:00 a.m. to X:00 p.m. E.S.T. Please do not contact your local store with questions. This call center is better equipped to address all questions regarding the incident.

We take the privacy of your personal information seriously. We sincerely regret any inconvenience or concern this incident has caused you.

Sincerely,

*Terry Kriz*

Terry Kriz

Director of IT and Security

## Steps You Can Take to Protect Against Identity Theft and Fraud

We encourage you to remain vigilant against incidents of identity theft and fraud, to review your account statements, and to monitor your credit reports for suspicious activity. Under U.S. law you are entitled to one free credit report annually from each of the three major credit reporting bureaus. To order your free credit report, visit [www.annualcreditreport.com](http://www.annualcreditreport.com) or call, toll-free, 1-877-322-8228. You may also contact the three major credit bureaus directly to request a free copy of your credit report.

At no charge, you can also have these credit bureaus place a "fraud alert" on your file that alerts creditors to take additional steps to verify your identity prior to granting credit in your name. Note, however, that because it tells creditors to follow certain procedures to protect you, it may also delay your ability to obtain credit while the agency verifies your identity. As soon as one credit bureau confirms your fraud alert, the others are notified to place fraud alerts on your file. Should you wish to place a fraud alert, or should you have any questions regarding your credit report, please contact any one of the agencies listed below.

Equifax  
P.O. Box 105069  
Atlanta, GA 30348  
800-525-6285  
[www.equifax.com](http://www.equifax.com)

Experian  
P.O. Box 2002  
Allen, TX 75013  
888-397-3742  
[www.experian.com](http://www.experian.com)

TransUnion  
P.O. Box 2000  
Chester, PA 19022-2000  
800-680-7289  
[www.transunion.com](http://www.transunion.com)

You may also place a security freeze on your credit reports. A security freeze prohibits a credit bureau from releasing any information from a consumer's credit report without the consumer's written authorization. However, please be advised that placing a security freeze on your credit report may delay, interfere with, or prevent the timely approval of any requests you make for new loans, credit mortgages, employment, housing, or other services. If you have been a victim of identity theft, and you provide the credit bureau with a valid police report, it cannot charge you to place, list or remove a security freeze. In all other cases, a credit bureau may charge you a fee to place, temporarily lift, or permanently remove a security freeze. You will need to place a security freeze separately with each of the three major credit bureaus listed above if you wish to place a freeze on all of your credit files. To find out more on how to place a security freeze, you can use the following contact information:

Equifax Security Freeze  
P.O. Box 105788  
Atlanta, GA 30348  
1-800-685-1111  
(NY residents please call  
1-800-349-9960)  
<https://www.freeze.equifax.com>

Experian Security Freeze  
P.O. Box 9554  
Allen, TX 75013  
1-888-397-3742  
[www.experian.com/freeze/center.html](http://www.experian.com/freeze/center.html)

TransUnion  
P.O. Box 2000  
Chester, PA 19022-2000  
1-888-909-8872  
[www.transunion.com/credit-freeze](http://www.transunion.com/credit-freeze)

You can further educate yourself regarding identity theft, fraud alerts, and the steps you can take to protect yourself, by contacting the Federal Trade Commission or your state Attorney General. The Federal Trade Commission can be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580, [www.identitytheft.gov](http://www.identitytheft.gov), 1-877-ID-THEFT (1-877-438-4338); TTY: 1-866-653-4261. **For Maryland residents**, the Attorney General can be reached at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-888-743-0023; and [www.oag.state.md.us](http://www.oag.state.md.us). **For North Carolina residents**, the Attorney General can be contacted by mail at 9001 Mail Service Center, Raleigh, NC 27699-9001; toll-free at 1-877-566-7226; by phone at 1-919-716-6400; and online at [www.ncdoj.gov](http://www.ncdoj.gov). **For Rhode Island Residents:** The Rhode Island Attorney General may be contacted at: Rhode Island Attorney General's Office, 150 South Main St., Providence, RI 02903. <http://www.riag.ri.gov>. Approximately 4 Rhode Island residents may have been affected by this incident. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. Instances of known or suspected identity theft should also be reported to law enforcement. This notice has not been delayed by law enforcement.