

July 29, 2016

Oregon Department of Justice  
Consumer Protection  
1162 Court Street NE  
Salem, OR 97301-4096  
(503)0378-4400

Dear Customer,

We value your business and respect the privacy of your information. As a precautionary measure, we are writing to let you know about a potential data security incident that may involve your information. Our online sales platform may have been attacked by an Internet hacker and the security of certain information that was transmitted to us in connection with online sales during a short period of time may have been compromised.

You may have read about similar data security breaches in the news recently. Unfortunately, we are the latest victims in this trend. Although we had taken measures that we believe were commercially reasonable under the circumstances, we may have been subject to a sophisticated cyber-attack that appears to have potentially penetrated our defenses. Malicious code may have been placed on our system and based upon our investigation, appears to have intercepted customer information that was transmitted during purchase transactions from May 3<sup>rd</sup>, 2016 until July 10<sup>th</sup>, 2016.

The data that may have been accessed included credit card numbers and corresponding credit card expiration dates, email addresses, delivery and billing addresses. We do not have access to birthdates or Social Security Numbers so these categories of information were not at risk. Information transmitted during in-store sales in our retail store locations are not at risk from this incident.

We first began to suspect that we could have been the victim of a cyber-attack made against our system on or about July 6<sup>th</sup>, 2016 when some of our customers mentioned experiencing unauthorized transactions on their credit card or debit card accounts. We promptly commenced an investigation of the relevant facts, and around July 7<sup>th</sup> 2016, we concluded that it was likely that our system had been penetrated by a cyber-attack. We continued investigating to determine the nature and scope of the attack and involved experienced third party professionals to assist us.

We have notified the Raleigh Police Department, the appropriate state authorities in almost every state, the federal authorities, and the three national credit reporting bureaus (Experian, Equifax and TransUnion) of these events. We are committed to cooperating with law enforcement as they investigate this incident. In addition, we have involved a third party professional information technology firm to analyze our system and implement additional measures and monitoring software improvements to our security so that we are no longer vulnerable to this type of cyber-attack. Additionally, we have implemented a "saved credit card" feature at Jerry's online website using the latest token encryption technology. We are now confident that our system is no longer vulnerable to this particular type of cyber-attack.

We place a high priority on our relationship with you. Your trust is very important to us and we take our responsibility to protect your data very seriously. We are providing the following information to you to help you avoid potential financial loss in connection with this incident. We encourage you to take the following steps to protect yourself:

- Although passwords were not part of the cyber-attack, as best practices, we still encourage you to Login to your [www.jerrysartarama.com](http://www.jerrysartarama.com) account and change your password.
- If you use the same password with any other website, *especially* for online banking or other sensitive services, please change it immediately. (As a general rule, it is not prudent to use the same password for multiple online accounts.)
- Carefully review your account statements for the card(s) you used to purchase items from us during the time period described above, and report any suspicious charges to your card issuer promptly upon receipt.
- Consider proactively contacting your card issuer and changing your card number.

If you discover any suspicious or unusual activity on your accounts or suspect fraud, report it immediately to your financial institution(s). In addition, you may contact the Federal Trade Commission ("FTC"), your state officials, or local law enforcement to report incidents of credit or debit card fraud or identity theft or to learn about steps you can take to protect yourself from identity theft. Contact information for the Federal Trade Commission is as follows: **Federal Trade Commission**, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580. You may also call 1- (877) 438-4338 or visit [www.consumer.gov/idtheft](http://www.consumer.gov/idtheft). Reports filed with the FTC will be added to the FTC's Identity Theft Data Clearinghouse, which is a database made available to law enforcement agencies.

Contact information for certain state officials is included with this letter. Additional rights that residents of certain states may have are also included with this letter. **Please read the attached document, or call the credit bureaus, to determine if your state provides additional rights or resources to you.**

You are also entitled to a **free copy of your credit report** every 12 months from each of the three nationwide credit reporting agencies. You may learn more about this by going to [www.AnnualCreditReport.com](http://www.AnnualCreditReport.com) or by calling (877) 322-8228 or writing to Annual Credit Report Request Services, P.O. Box 105281, Atlanta, GA 30348. You may contact these credit reporting agencies individually to request more information at:

**Equifax**  
(800) 525-6285  
P.O. Box 740256  
Atlanta, GA 30374-0241  
[www.equifax.com](http://www.equifax.com)

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

**TransUnion**  
(800) 680-7289  
P.O. Box 105281  
Atlanta, GA 30348-5281  
[www.transunion.com](http://www.transunion.com)

You may want to consider proactively 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 with your identity and requests that the creditor contact you prior to opening any new credit accounts in your name. To place a fraud alert on your credit report, contact any one of the three national credit reporting agencies identified above.

Residents of some states have the right to put a security "**freeze**" on their credit files. This prevents any new credit from being opened without the use of a PIN that is issued when the freeze is put into place. Please see the attached to determine if your state's laws give you the right to place a security freeze on your credit file. A security freeze must be requested with each credit reporting agency separately. (The credit reporting agencies may charge a fee of up to \$5 to place, lift or remove a security freeze, depending upon the state of residence.) Generally, 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.

If you have questions about this incident or would like more information about how to protect yourself, you may call our representatives at 1-888-283-6748 toll-free weekdays between 6:00 A.M. and 6:00 P.M. Pacific. We have arranged for assistance to be provided to you at this telephone number.

We are extremely sorry for the inconvenience that this has caused; we know that your time and the security of your information are important. Like you, some of our employees made purchases online through our store during this period, and we understand your feelings in the aftermath of this cyber-attack. We hope that we can restore the confidence that our customers have put in our company over the past 49 years. Thank you for your patience and understanding.

Sincerely,

Michael Marchetta  
Director of Marketing Operations  
Jerry's Artarama

## State-Specific Information

### Hawaii Residents

Hawaii residents should remain vigilant by reviewing all account statement and monitoring free credit reports.

### Maryland Residents

Maryland residents may also wish to review information provided by the Maryland Attorney General on how to avoid identity theft at <http://www.oag.state.md.us/idtheft>, or by sending a letter to Office of the Attorney General, Identity Theft Unit, 200 St. Paul Place, 16th Floor, Baltimore, MD 21202, sending an email message to [idtheft@oag.statemd.us](mailto:idtheft@oag.statemd.us), or calling 410-576-6491 (toll free at 888-743-0023).

### North Carolina Residents

North Carolina Department of Justice  
Consumer Protection Division  
9001 Mail Service Center  
Raleigh, NC 27699-9001  
(877) 566-7226  
<http://www.ncdoj.com/consumer.aspx>

#### North Carolina Consumers Have the Right to Obtain a Security Freeze.

You have a right to place a "security freeze" on your credit report pursuant to North Carolina law. The security freeze will prohibit a consumer reporting agency from releasing any information in your credit report without your express authorization. A security freeze can be requested in writing by first-class mail, by telephone, or electronically. You also may request a freeze by visiting the following Web sites or calling the following telephone numbers:

#### Experian

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

#### TransUnion

TransUnion Protected Consumer Freeze  
P.O. Box 380  
Woodlyn, PA 19094  
<https://freeze.transunion.com>  
1-800-916-8800

#### Equifax

Equifax Security Freeze  
P.O. Box 105788  
Atlanta, Georgia 30348  
<https://www.freeze.equifax.com>  
1-800-685-1111

The security 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 security freeze to take control over who gains 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 new loans, credit, mortgage, insurance, rental housing, employment, investment, license, cellular phone, utilities, digital signature, Internet credit card transactions, or other services, including an extension of credit at point of sale. The freeze will be placed within three business days if you request it by mail, or within 24 hours if you request it by telephone or electronically. When you place a security freeze on your credit report, within three business days, you will be sent a personal identification number or a password to use when you want to remove the security freeze, temporarily lift it, or lift it with respect to a particular third party. A freeze does not apply when you have an existing account relationship and a copy of your report is requested by your existing creditor or its agents or affiliates for certain types of account review, collection, fraud control, or similar activities. You should plan ahead and lift a freeze if you are actively seeking credit or services as a security freeze may slow your applications, as mentioned above. You can remove a freeze, temporarily lift a freeze, or lift a freeze with respect to a particular third party by contacting the consumer reporting agency and providing all of the following:

- (1) Your personal identification number or password,
- (2) Proper identification to verify your identity, and
- (3) Proper information regarding the period of time you want your report available to users of the credit report, or the third party with respect to which you want to lift the freeze.

A consumer reporting agency that receives a request from you to temporarily lift a freeze or to lift a freeze with respect to a particular third party on a credit report shall comply with the request no later than three business days after receiving the request by mail and no later than 15 minutes after receiving a request by telephone or electronically. A consumer reporting agency may charge you up to three dollars (\$3.00) to institute a freeze if your request is made by telephone or by mail. A consumer reporting agency may not charge you any amount to freeze, remove a freeze, temporarily lift a freeze, or lift a freeze with respect to a particular third party, if any of the following are true:

- (1) Your request is made electronically.
- (2) You are over the age of 62.
- (3) You are the victim of identity theft and have submitted a copy of a valid investigative or incident report or complaint with a law enforcement agency about the unlawful use of your identifying information by another person, or you are the spouse of such a person.

You have a right to bring a civil action against someone who violates your rights under the credit reporting laws. The action can be brought against a consumer reporting agency or a user of your credit report.