Dear Customer:

Burnt Ridge Nursery and Orchards, Inc. ("Burnt Ridge") recently became aware of a data security incident involving the presence of malware on the servers of one of our third-party vendors. This vendor provides the shopping cart and payment processing functionality for various companies' e-commerce sites, including ours. The vendor has confirmed that the malware was removed and additional steps were taken to block the unauthorized activity.

We are reaching out at our earliest opportunity as our customers are a top priority, and we take the protection of your information very seriously.

Below is additional information about what happened, what the vendor did in response, and what steps you can take to further protect your information.

What Happened? In early February 2022, the vendor identified malware on one of its servers that hosts multiple ecommerce websites. The vendor quickly commenced an investigation and removed malware found on the server that hosts Burnt Ridge's official website https://www.burntridgenursery.com/. The vendor also retained data security experts to conduct a thorough investigation of the incident's nature and scope and assist in the vendor's containment and remediation efforts. The vendor has informed us that the payment card information of individuals who used a card on our site between 9/18/2020 and 2/3/2022 may have been acquired by an unauthorized party. Orders placed over the phone, by mail, or in person were not affected. Based on our own investigation of our sales records within this timeframe, we believe that you may have been one of the impacted customers. This notice is not delayed as a result of a law enforcement investigation.

What Information Was Involved? The malware was designed to capture certain payment card information, including cardholder name, payment card number, security code and expiration date.

What We Are Doing: As indicated above, after becoming aware of the issue, the vendor took immediate steps to identify and remove the malware and block further unauthorized activity. The vendor promptly launched an extensive investigation with the assistance of data security experts to determine the timeframes of exposure for each of the vendor's affected customers and to identify impacted cardholders. The vendor also notified federal law enforcement authorities and has been coordinating with the payment card companies in an effort to protect affected cardholders.

What You Can Do: Please consider the following recommendations:

Review Your Account Statements. We encourage you to remain vigilant by reviewing your account statements. If you believe there is an unauthorized charge on your card, please contact your financial institution or card issuer immediately. Federal law and the payment card brands' policies provide that cardholders have limited liability for unauthorized charges reported in a timely manner. Please contact your card brand or issuing bank for more information about the policy that applies to you.

Order a Credit Report. You are entitled under U.S. law to one free credit report annually from each of the three nationwide consumer reporting agencies. To order your free credit report, visit www.annualcreditreport.com or call toll-free at 1-877-322-8228.

Review the Reference Guide: The Reference Guide below provides additional recommendations on the protection of personal information.

For More Information: If you have any questions about this data security incident, please email us at mail@burntridgenursery.com or call us at 360-985-2873, Monday through Friday, 9:00 to 4:00 pst.

We hope this information is useful to you, and we sincerely regret any inconvenience or concern this may cause our customers.

Sincerely,

Michael Dolan Carolyn Cerling-Dolan

President Vice president

Burnt Ridge Nursery and Orchards, Inc.

432 Burnt Ridge Rd.

Onalaska WA 98570

Reference Guide

We encourage affected customers to consider taking the following steps:

Order A Free Credit Report. To order your free credit report, visit www.annualcreditreport.com, call toll-free at 1-877-322-8228, or complete the Annual Credit Report Request Form on the U.S. Federal Trade Commission's (" FTC' ") website at www.consumer.ftc.gov and mail it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. The three nationwide consumer reporting agencies provide free annual credit reports only through the website, toll-free number or request form. When you receive your credit report, review it carefully. Look for accounts you did not open. Look in the "inquiries" section for names of creditors from whom you have not requested credit. Some companies bill under names other than their store or commercial names. The consumer reporting agency will be able to tell you when that is the case. Look in the "personal information" section for any inaccuracies in your information (such as home address and Social Security number). If you see anything you do not understand, contact the consumer reporting agency. Errors in this information may be a warning sign of possible identity theft. You should notify the consumer reporting agencies of any inaccuracies in your report, whether due to error or fraud, as soon as possible so the information can be investigated and, if found to be in error, corrected. If there are accounts or charges you did not authorize, immediately notify the appropriate consumer reporting agency in writing. If the information cannot be explained, then you will need to call the creditors involved. Information that cannot be explained also should be reported to your local police or sheriff's office because it may signal criminal activity.

Report Incidents. If you detect any unauthorized transactions in a financial account, promptly notify your payment card company or financial institution. If you detect any incident of identity theft or fraud,

promptly report the incident to law enforcement, the FTC and your state Attorney General. You can contact the FTC to learn more about how to protect yourself from becoming a victim of identity theft and how to repair identity theft: Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW Washington DC 20580, 1-877-IDTheft (438-4338), www.ftc.gov/idtheft/. If you believe your identity has been stolen, the FTC recommends that you take these steps: • Close the accounts that you have confirmed or believe have been tampered with or opened fraudulently. For streamlined checklists and sample letters to help guide you through the recovery process, please visit https://www.identitytheft.gov/. • File a local police report. Obtain a copy of the police report and submit it to your creditors and any others that may require proof of the identity theft crime.

Consider Placing a Fraud Alert on Your Credit File. To protect yourself from possible identity theft, consider placing a fraud alert on your credit file. A fraud alert helps protect you against the possibility of an identity thief opening new credit accounts in your name. When a merchant checks the credit history of someone applying for credit, the merchant gets a notice that the applicant may be the victim of identity theft. The alert notifies the merchant to take steps to verify the identity of the applicant. You can place a fraud alert on your credit report by calling any one of the three largest nationwide consumer reporting agencies; the toll free numbers for each of these agencies are provided here for your convenience. You will reach an automated telephone system that allows you to flag your file with a fraud alert at all three consumer reporting agencies. For more information on fraud alerts, you also may contact the FTC as described above. Equifax Information Services LLC, P.O. Box 740241, Atlanta, GA 30374, 1-800-525-6285, www.equifax.com ; Experian Inc., P.O. Box 9554, Allen, TX 75013, 1-888-397-3742, www.experian.com ; TransUnion LLC, P.O. Box 2000, Chester, PA 19016, 1-800-680-7289, www.transunion.com

Consider Placing a Security Freeze on Your Credit File. You may wish to place a "security freeze" (also known as a "credit freeze") on your credit file. A security freeze is designed to prevent potential creditors from accessing your credit file at the consumer reporting agencies without your consent. Unlike a fraud alert, you must place a security freeze on your credit file at each consumer reporting agency individually. There is no charge to place or lift a security freeze. For more information on security freezes, you may contact the three nationwide consumer reporting agencies or the FTC as described above. As the instructions for establishing a security freeze differ from state to state, please contact the three nationwide consumer reporting agencies to find out more information. The consumer reporting agencies may require proper identification prior to honoring your request. For example, you may be asked to provide: • Your full name with middle initial and generation (such as Jr., Sr., II, III) • Your Social Security number • Your date of birth • Addresses where you have lived over the past five years • A legible copy of a government-issued identification card (such as a state driver's license or military ID card) • Proof of your current residential address (such as a current utility bill or account statement)

For Iowa Residents. You may contact law enforcement or the Iowa Attorney General's Office to report suspected incidents of identity theft. This office can be reached at: Office of the Attorney General of Iowa Hoover State Office Building 1305 E. Walnut Street Des Moines, IA 50319 (515) 281-5164 www.iowaattorneygeneral.gov

For Maryland Residents. You can obtain information from the Maryland Office of the Attorney General about steps you can take to avoid identity theft. You may contact the Maryland Attorney General at: Maryland Office of the Attorney General Consumer Protection Division 200 St. Paul Place Baltimore, MD 21202 (888) 743-0023 (toll-free in Maryland) (410) 576-6300 www.marylandattorneygeneral.gov

For New Mexico Residents. You have rights under the federal Fair Credit Reporting Act ("FCRA"). These include, among others, the right to know what is in your file; to dispute incomplete or inaccurate information; and to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information. For more information about the FCRA, please visit https://www.ftc.gov/legal-library/browse/statutes/fair-credit-reporting-ach

For New York Residents. You can obtain information from the New York State Office of the Attorney General about how to protect yourself from identity theft and tips on how to protect your privacy online. You can contact the New York State Office of the Attorney General at: Office of the Attorney General, Albany, NY 12224-0341, 1-800-771-7755 (toll-free) or 1-800-788-9898 (TDD/TTY toll-free line), https://ag.ny.gov/ or Bureau of Internet and Technology (BIT) of the New York Attorney General's Office, 28 Liberty Street, New York, NY 10005, (212) 416-8433, https://ag.ny.gov/internet/resource-center

For North Carolina Residents. You can obtain information from the North Carolina Attorney General's Office about preventing identity theft. You can contact the North Carolina Attorney General at: North Carolina Attorney General's Office, 9001 Mail Service Center, Raleigh, NC, 27699-9001, (877) 566-7226 (toll-free in North Carolina) or (919) 716-6400 www.ncdog.gov

For Oregon Residents. We encourage you to report suspected identity theft to the Oregon Attorney General at: Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, (877) 877-9392 (toll-free in Oregon) or (503) 378-4400 www.doj.state.or.us

For Rhode Island Residents. You may obtain information about preventing and avoiding identity theft from the Rhode Island Office of the Attorney General at: Rhode Island Office of the Attorney General, Consumer Protection Unit, 150 South Main Street Providence, RI 02903, (401)-274-4400, www.riag.ri.gov . You have the right to obtain a police report and request a security freeze as described above. The consumer reporting agencies may require that you provide certain personal information (such as your name, Social Security number, date of birth, and address) and proper identification (such as a copy of a government-issued ID card and a bill or statement) prior to honoring your request for a security freeze on your account.

For Washington, D.C. Residents. You may obtain information about preventing and avoiding identity theft from the Office of the Attorney General for the District of Columbia at: Office of the Attorney General for the District of Columbia, 400 6th Street NW, Washington, D.C. 20001, (202)-727-3400, www.oag.dc.gov