

THEISEN SUPPLY INC.

Return Mail Processing Center
P.O. Box 6336
Portland, OR 97228-6336

<<Mail ID>>
<<Name1>>
<<Address1>>
<<Address2>>
<<City>> <<State>> <<Zip>>

<<Date>>

RE: Notice of Data Breach

Dear <<Name1>>:

Theisen's Inc., ("Theisen's"), is writing regarding a recent data security incident on our e-commerce website that may impact the demographic and payment card information you used on our site. 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 February 8, 2017, we received information from Aptos, the company that hosts and manages our e-commerce site, that customer information stored in their system had been compromised by malicious software injected into the Aptos system sometime in February, 2016. This malicious software allowed the attacker to capture sensitive customer information prior to encryption as well as decrypt historical credit card information stored on the site. Upon learning of this incident, we immediately began an investigation to identify what happened and what information may be impacted. Aptos has been working with the FBI and the U.S. Department of Justice since they discovered the intrusion and have only recently received permission from the FBI to notify us about this incident. **Please note that this incident affects only transactions made on our e-commerce website, and does not affect any purchases made in our retail stores.**

What Information Was Involved? Aptos is reporting that customer demographic and credit/debit card information entered on our e-commerce site between February 2016 and December 2016 was accessed by an unknown actor. In addition to payment information entered between February and December, 2016, the intruder also had access to historical payment card information stored by Aptos. The information accessed includes the cardholder's name, address, telephone number, email address, card number, card type and expiration date. While the card number and other card data was encrypted, Aptos reports that the bad actor was able to decrypt the card data.

What We Are Doing. We take this incident, and information security, very seriously at Theisen's. We are diligently investigating this incident, and we are currently taking steps to obtain additional information from Aptos. We are also working to ensure that Aptos is taking all steps necessary to protect our customer information. Additionally, we are providing written notice of this incident to those who may be impacted so that they can take steps to prevent possible fraud. Certain state regulators are also being notified 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.

As an added precaution, we have arranged to have Experian to provide you with CSID Protector services, including CyberAgent[®] Internet Surveillance and Identity Theft Insurance, for 12 months at no cost to you. The following identity protection services start on the date of this notice, and you can use them at any time during the next 12 months. The cost of this service will be paid for by Theisen's. It is incumbent upon you to enroll in these services, as we are not able to act on your behalf to enroll you in identity monitoring.

CSID Protector includes:

- CyberAgent®: CSID's Internet surveillance technology scours websites, chat rooms and bulletin boards 24/7 to identify trading or selling of your personal information on the Dark Web.
- Identity Theft Insurance: You are eligible for reimbursement for certain expenses in the event that your identity is compromised with a \$1,000,000 insurance policy that has been issued to CSID.
- Identity Restoration: Work with a certified identity theft restoration specialist, who will work on your behalf to restore your identity and let you get on with your life

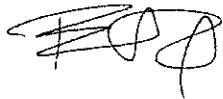
You can sign up for these services by doing the following:

- Visit <https://www.csid.com/csiddlyprotector> to complete a secure sign up process and answer some questions to confirm your identity.
- Submit your PIN Code: <<Code>>. This PIN Code can only be used once and cannot be transferred to another individual.
- Activate your CSID Protector coverage no later than March 2, 2018.

Additionally, Identity Restoration services are available to you as of March 3, 2017, with no further action required. If you are a victim of fraud, simply call CSID at (877) 926-1113 no later than March 2, 2018, and a dedicated Identity Theft Restoration agent will help you restore your identity. Please provide the PIN Code in this letter as proof of eligibility. The Engagement number for this matter is DB00570.

For More Information. We sincerely regret any inconvenience or concern this incident may have caused you. If you have questions or concerns that are not addressed in this notice letter, you may call the dedicated assistance line we've established regarding this incident. You may call the assistance line at 844-774-7461, Monday through Friday, 9:00 a.m. to 9:00 p.m. E.S.T (excluding U.S. holidays).

Sincerely,



Brannon Dixon
President, Theisen's, Inc.

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 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

Experian
P.O. Box 2002
Allen, TX 75013
888-397-3742
www.experian.com

TransUnion
P.O. Box 2000
Chester, PA 19022-2000
800-680-7289
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

TransUnion
P.O. Box 2000
Chester, PA 19022
1-888-909-8872
www.transunion.com

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. **For North Carolina residents**, the Attorney General can be contacted at 9001 Mail Service Center, Raleigh, NC 27699-9001, 1-919-716-6400, www.ncdoj.gov. **For Maryland residents**, the Attorney General can be contacted at 200 St. Paul Place, 16th Floor, Baltimore, MD 21202, 1-888-743-0023, www.oag.state.md.us. **For Rhode Island residents**, Attorney General can be contacted at (401) 274-4400, <http://www.riag.ri.gov>, or 150 South Main Street, Providence, RI 02903. Approximately 6 Rhode Island residents may be impacted by this incident. The Federal Trade Commission can be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580, www.identitytheft.gov, 1-877-ID-THEFT (1-877-438-4338); 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 crime report or incident report with law enforcement for identity theft, you will likely need to provide some kind of proof that they have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement.