

16866

From: Identity Guard notification@services.identityguard.com
Subject: Test - Notice of Data Security Incident
Date: April 24, 2020 at 3:39 PM
To: Evan Lefever ELefever@auracompany.com



You're receiving this email as a test email. Some contents may not display or behave properly.



Dear %%FIRST NAME%% %%LAST NAME%%,

BACKGROUND:

We value your business and respect the privacy of your information, which is why, as a precautionary measure, we are writing to let you know about a data security incident that may have involved your personal information.

Affected information may have included data (including first name, last name, mailing address, shipping address, credit card number, credit card type, credit card security code, email address, and account information) that was entered while creating an account or placing an order.

Pacific Press values your privacy and deeply regrets that this incident occurred. We have conducted a thorough review of the potentially affected website and we have implemented additional security measures designed to prevent a recurrence of such an attack and to protect the privacy of our valued customer's personal data.

We are also working closely with major credit card suppliers and law enforcement to ensure the incident is properly addressed.

Please review the attachment to this letter (Steps You Can Take to Further Protect Your Information) for further information on steps you can take to protect your information and how to receive free credit monitoring services for one year.

COMPLIMENTARY SERVICE OFFER: At our expense, Pacific Press would like to offer you a free one year subscription to Identity Guard[®] Total, a credit monitoring and identity theft protection service. Identity Guard Total provides essential monitoring and protection of not only credit data, but also monitors the Dark Web and alerts you if your Social Security number, credit cards, and bank account numbers are found in unsecure online locations. This program is provided by Intersections Inc., a leading provider of consumer and corporate identity risk management services.

IDENTITY GUARD[®] TOTAL features include:

- Dark Web Monitoring
- IBM Watson[®] Artificial Intelligence
- High Risk Transaction Alerts
- US Based Identity Theft Recovery Assistance
- 3-Bureau Credit Monitoring
- \$1 Million Identity Theft Insurance*
- Account Access via Mobile App
- Anti-Phishing App
- PC Protection Tools

If you wish to take advantage of this monitoring service, you must enroll by July 24, 2020.

*Identity Theft Insurance underwritten by insurance company subsidiaries or affiliates of American International Group, Inc. The description herein is a summary and intended for informational purposes only and does not include all terms, conditions and exclusions of the policies described. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

ENROLLMENT PROCEDURE: To activate this coverage please visit the Web site listed below and enter the activation code. The activation code is required for enrollment and can only be used one time by the individual addressed.

Web Site: app.identityguard.com/activate/pacificpress
Activation Code: %%ACTIVATION CODE%%

In order to enroll, you will need to provide the following personal information:

- Mailing Address
- Social Security Number
- E-mail Address
- Phone Number
- Date of Birth
- Activation Code

This service is complimentary; no method of payment will be collected during enrollment and there is no need to cancel. We apologize for any inconvenience and urge you to enroll today. If you have any further questions regarding this incident, please call us at 1-888-416-0042, Monday – Friday 8am - 11pm (EST).

Sincerely,



Dale E. Galusha
President

Steps You Can Take to Further Protect Your Information

• Review Your Account Statements and Notify Law Enforcement of Suspicious Activity

As a precautionary measure, we recommend that you remain vigilant by reviewing your account statements and credit reports closely. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained. You also should promptly report any fraudulent activity or any suspected incidence of identity theft to proper law enforcement authorities, including your state attorney general and the Federal Trade Commission (FTC).

To file a complaint with the FTC, go to IdentityTheft.gov or call 1-877-ID-THEFT (877-438-4338). Complaints 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.

• Obtain and Monitor Your Credit Report

We recommend that you obtain a free copy of your credit report from each of the three major credit reporting agencies once every 12 months by visiting <http://www.annualcreditreport.com>, calling toll-free 877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. You can access the request form at <https://www.annualcreditreport.com/requestReport/requestForm.action>. Or you can elect to purchase a copy of your credit report by contacting one of the three national credit reporting agencies. Contact information for the three national credit reporting agencies for the purpose of requesting a copy of your credit report or for general inquiries is provided below:

Equifax
(866) 349-5191

Experian
(888) 397-3742

TransUnion
(800) 888-4213

www.equifax.com
P.O. Box 740241
Atlanta, GA 30374

www.experian.com
P.O. Box 4500
Allen, TX 75013

www.transunion.com
2 Baldwin Place
P.O. Box 1000
Chester, PA 19016

• **Consider Placing a Fraud Alert on Your Credit Report**

You may want to consider 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 within your report and requests that the creditor contact you prior to establishing any accounts in your name. To place a fraud alert on your credit report, contact any of the three credit reporting agencies identified above. Additional information is available at <http://www.annualcreditreport.com>.

• **Take Advantage of Additional Free Resources on Identity Theft**

We recommend that you review the tips provided by the Federal Trade Commission's Consumer Information website, a valuable resource with some helpful tips on how to protect your information. Additional information is available at <https://www.consumer.ftc.gov/topics/privacy-identity-online-security>.

For more information, please visit IdentityTheft.gov or call 1-877-ID-THEFT (877-438-4338). [A copy of Identity Theft – A Recovery Plan, a comprehensive guide from the FTC to help you guard against and deal with identity theft, is enclosed/can be found on the FTC's website at https://www.consumer.ftc.gov/articles/pdf-0009_identitytheft_a_recovery_plan.pdf.]

• **Security Freeze**

In some US states, you have the right to put a security freeze on your credit file. A security freeze (also known as a credit freeze) makes it harder for someone to open a new account in your name. It is designed to prevent potential creditors from accessing your credit report without your consent. As a result, using a security freeze may interfere with or delay your ability to apply for a new credit card, wireless phone, or any service that requires a credit check. You must separately place a security freeze on your credit file with each credit reporting agency. 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. There is no charge to request a security freeze or to remove a security freeze.

This email was sent to elefever@auracompany.com because it contains important information about your account. If you have previously unsubscribed from Identity Guard® marketing alerts, you will no longer receive special offers but you will continue to receive emails concerning your account. If you believe you received this email in error, please forward it to our customer care team at customer care@identityguard.com.

We will never ask you for your personal information in an email. We respect your privacy. If you no longer wish to receive messages from Identity Guard®, you may unsubscribe at any time.
© 2020 Intersections Inc. d/b/a Aura, P.O. Box 222546 Chantilly, VA 20153-2546.

STATEMENT OF CONFIDENTIALITY

The information contained in this electronic message, and any attachments to this message, are intended for the exclusive use of the intended recipients and may contain confidential and privileged information. Any unauthorized review, use, disclosure or distribution of this email message or its attachments is prohibited. If you are not the intended recipient, please notify Aura at security@auracompany.com, and then destroy all copies of this message and any attachments.