USI UNDERSTAND. SERVICE. INNOVATE.

USI Insurance Services
200 Summit Lake Drive
Suite 350
Valhalla , NY 10595
www.usi.biz
Phone: 914.749.8500
Fax: 610.537.4500

May 19, 2016

VIA EMAIL

Office of the Attorney General
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202
Idtheft@oag.state.md.us

Re: Notice of Data Breach

Dear Administrator Karberg:

Pursuant to Md. Code, Com. Law § 14-3501 et seq., we are writing to inform you that USI, Inc. is providing notice to certain Maryland residents regarding the inadvertent disclosure of W2 Forms of USI Insurance Services, LLC's employees.

I. Nature of the Data Breach

USI Insurance Services is a wholly-owned subsidiary of USI, Inc. A former USI Insurance Services employee (the "Employee") recently requested a copy of his W2 Form from a USI payroll representative. On April 28, 2016, the payroll representative mistakenly emailed to the Employee an attachment containing the W2 Forms of other USI Insurance Services employees.

The Employee notified USI when he received the incorrect attachment and, upon notice, we launched an investigation to determine the scope of the incident. We confirmed with the Employee that he did not share the attachment with anyone else or otherwise use the information contained in it, and that he deleted the attachment.

The W2 Forms contain a variety of information including, for example, names, Social Security numbers and employee tax information. Based on our investigation, we have no evidence to date that any personal information has been misused.

II. Number of Maryland Residents Affected

Based on our investigation, we have identified 46 Maryland residents affected by the incident.

III. Steps We Have Taken or Plan to Take Relating to the Incident

First, upon discovery of the incident, we launched an investigation and interviewed the Employee that received the W2 Forms – see the explanation contained in Section I (Nature of the Data Breach) of this notice for additional information.

Second, we have terminated the USI payroll representative responsible for the inadvertent disclosure.

Third, on May 20, 2016, we are sending notice (via first class mail) to the state residents that have been impacted by the incident. A sample of the notification letter is enclosed.

Fourth, we have partnered with AllClear ID to help protect the affected individuals from identity theft. Specifically, we have purchased for those individuals 12 months of AllClear ID's "AllClear SECURE" and "AllClear PRO" which include both credit monitoring services and a variety of ancillary support services, such as identity repair and identity theft insurance. AllClear ID is also staffing a toll-free call center to answer questions about the incident, as explained in the enclosed sample notification letter.

Finally, we are introducing new measures to prevent an incident like this from occurring again. Specifically, the payroll team has modified its procedures, USI has ceased distributing W2 Forms to employees via email (either upon request or otherwise) and will be implementing an upgraded online payroll system to better facilitate employee retrieval of W2 Forms via a secure portal.

IV. Recently Submitted Notice

On May 12, 2016, USI provided your office with a similar notice involving a data breach that occurred on April 19, 2016 (the "April 19 Breach"). Please note that (1) the current incident was attributable to the same USI payroll representative (who has since been terminated) that caused the April 19 Breach, and (2) the current incident took place before any of the remediation measures described in Section III (Steps We Have Taken or Plan to Take Relating to the Incident) were implemented.

Although the April 19 Breach was attributable to the same USI payroll representative, the April 19 Breach involved a different employee population. Moreover, based on our internal investigation, we have determined that (1) neither the terminated employee nor any other USI payroll team member has made any other similarly unauthorized disclosures, and (2) the remediation steps set out in Section III should prevent the reoccurrence of a similar incident.

Please contact me if you have any questions or would like additional information.

Sincerely,

Terry L. Burston
Vice President
Assistant General Counsel & Chief Compliance Officer
USI, Inc.
200 Summit Lake Drive, Suite 350, Valhalla, NY 10595
Direct: 914-749-8541 | Cell: 551-587-0514| Email: terry.burston@usi.biz

Enclosure
#46233211_v2

Processing Center • P.O. BOX 141578 • Austin, TX 78714

00004
ACD1234
01796
JOHN Q. SAMPLE
1234 MAIN STREET
ANYTOWN US 12345-6789

May 20, 2016

Dear John Sample:

I am writing to notify you about a data security incident. Specifically, a former USI Insurance Services LLC employee (referred to below as the "Employee") recently requested a copy of his W2 Form from a USI payroll representative. On April 28, 2016, the payroll representative mistakenly emailed to the Employee an attachment containing the W2 Forms of other USI Insurance Services employees.

The Employee notified us when he received the incorrect attachment and, upon notice, we launched an investigation to determine the scope of the incident. We confirmed with the Employee that he did not share the attachment with anyone else or otherwise use the information contained in it, and that he deleted the attachment.

You are receiving this notice because your W2 Form was included in the attachment. As you know, your W2 Form includes, among other information, your name, Social Security number and employee tax information. I would like to emphasize that, to date, we have no evidence that your information has been misused. Nevertheless, as a precautionary measure, we have arranged to have AllClear ID provide the following services to you for 12 months, all at no cost to you.

- AllClear SECURE: The team at AllClear ID is ready and standing by if you need identity repair assistance. This service is automatically available to you with no enrollment required. If a problem arises, simply call 1-855-284-7629 and a dedicated investigator will help recover financial losses, restore your credit and make sure your identity is returned to its proper condition.

- AllClear PRO: This service offers additional layers of protection including credit monitoring and a $1 million identity theft insurance policy. To use the PRO service, you will need to provide your personal information to AllClear ID. You may sign up online at enroll.allclearid.com or by phone by calling 1-855-284-7629 using the following redemption code: Redemption Code. Please note that additional steps may be required by you in order to activate your phone alerts and monitoring options.

The above identity protection services start on the date of this notice, and you can use them at any time during the next 12 months.

Experts recommend, as a general consumer protection measure, that you periodically review your credit report and account statements, even if you do not initially find suspicious activity. We have

also included with this letter an explanation of additional steps you may consider taking to further protect yourself. Moreover, you should not provide personal information to others unless you are certain of the requester's identity and, as always, you should remain vigilant for incidents of fraud and identity theft.

We take our responsibility to protect your privacy very seriously. We regret that this incident occurred, and have taken several steps to prevent future incidents of this nature. Specifically, the payroll team modified its procedures, USI has ceased distributing W2 Forms to employees via email (either upon request or otherwise) and USI will be implementing an upgraded online payroll system to better facilitate employee retrieval of W2 Forms via a secure portal.

If you have any questions, please do not hesitate to contact us, toll-free, at 1-855-284-7629 on Monday through Saturday from 8:00 a.m. to 8:00 p.m., Central Standard Time.

Sincerely,

Kim Van Orman

Kim Van Orman
SVP and Chief Human Resources Officer, USI Inc.
200 Summit Lake Drive, Suite 350
Valhalla, NY 10595
P: (914) 749-8558

IDENTITY THEFT PRECAUTIONS

Free Credit Report

The Fair Credit Reporting Act requires each of the three nationwide consumer reporting agencies (Equifax, Experian and TransUnion) to provide you annually, upon request, with a free copy of your credit report. Obtaining a copy of your credit report from each agency on an annual basis, and reviewing it for suspicious activity, can help you spot problems and address them quickly. You can request your free credit report online at www.annualcreditreport.com or by phone at 1-877-322-8228. You can also request your free credit report by completing the request form available at www.annualcreditreport.com, and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281.

Fraud Alert

As a precaution against identity theft, you can consider placing a fraud alert on your credit file. A "fraud alert" tells creditors to contact you before opening a new account or changing an existing account. A fraud alert also lets your creditors know to watch for unusual or suspicious activity. To place a fraud alert, call any one of the three major consumer reporting agencies listed below. An initial fraud alert remains effective for ninety days, and is free of charge. If you wish, you can renew the fraud alert at the expiration of this initial period. As soon as one credit agency confirms your fraud alert, the others are notified to place fraud alerts on your file.

Equifax
Equifax Information Services LLC
P.O. Box 105069
Atlanta, GA 30348-5069
Toll-free: 800-525-6285
www.fraudalerts.equifax.com

TransUnion
Fraud Victim Assistance Department
P.O. Box 6790
Fullerton, CA 92834
Toll-free: 800-680-7289
www.transunion.com

Experian
P.O. Box 9532
Allen, TX 75013
Toll-free: 888-397-3742
www.experian.com/fraud/center.html

The consumer reporting agencies can also provide you information about security freezes.

Further Information

You may obtain additional information about identity theft (including a security freeze) by contacting the above or the Federal Trade Commission (FTC) using the contact information below. In addition, certain state laws advise you to report suspected incidents of identity theft to local law enforcement or to your Attorney General's office.

Federal Trade Commission
Consumer Response Center
600 Pennsylvania Avenue, NW
Washington, DC 20580
1-877-IDTHEFT (438-4338)
www.ftc.gov/idtheft

Maryland Office of the Attorney General
200 St. Paul Place
Baltimore, MD 21202
1-888-743-0023
www.oag.state.md.us

02-03-4

AllClear Secure Terms of Use

If you become a victim of fraud using your personal information without authorization, AllClear ID will help recover your financial losses and restore your identity. Benefits include:

- 12 months of coverage with no enrollment required;
- No cost to you – ever. AllClear Secure is paid for by the participating Company.

Services Provided
If you suspect identity theft, simply call AllClear ID to file a claim. AllClear ID will provide appropriate and necessary remediation services ("Services") to help restore the compromised accounts and your identity to the state prior to the incident of fraud. Services are determined at the sole discretion of AllClear ID and are subject to the terms and conditions found on the AllClear ID website. AllClear Secure is not an insurance policy, and AllClear ID will not make payments or reimbursements to you for any financial loss, liabilities or expenses you incur.

Coverage Period
Service is automatically available to you with no enrollment required for 12 months from the date of the breach incident notification you received from Company (the "Coverage Period"). Fraud events that occurred prior to your Coverage Period are not covered by AllClear Secure services.

Eligibility Requirements
To be eligible for Services under AllClear Secure coverage, you must fully comply, without limitations, with your obligations under the terms herein, you must be a citizen or legal resident eighteen (18) years of age or older and have a valid U.S. Social Security number. Minors under eighteen (18) years of age may be eligible, but must be sponsored by a parent or guardian. The Services cover only you and your personal financial and medical accounts that are directly associated with your valid U.S. Social Security number, including but not limited to credit card, bank, or other financial accounts and/or medical accounts.

How to File a Claim
If you become a victim of fraud covered by the AllClear Secure services (an "Event"), you must:

- notify AllClear ID by calling 1.855.434.8077 to report the fraud prior to expiration of your Coverage Period;
- provide proof of eligibility for AllClear Secure by providing the redemption code on the notification letter you received from the sponsor Company;
- fully cooperate and be truthful with AllClear ID about the Event and agree to execute any documents AllClear ID may reasonably require; and
- fully cooperate with AllClear ID in any remediation process, including, but not limited to, providing AllClear ID with copies of all available investigation files or reports from any institution, including, but not limited to, credit institutions or law enforcement agencies, relating to the alleged theft.

Coverage Under AllClear Secure Does Not Apply to the Following:
Any expense, damage or loss:

- due to
  - any transactions on your financial accounts made by authorized users, even if acting without your knowledge, or
  - any act of theft, deceit, collusion, dishonesty or criminal act by you or any person acting in concert with you, or by any of your authorized representatives, whether acting alone or in collusion with you or others (collectively, your "Misrepresentation");
- incurred by you from an Event that did not occur during your coverage period; or
- in connection with an Event that you fail to report to AllClear ID prior to the expiration of your AllClear Secure coverage period.

Other Exclusions:

- AllClear ID will not pay or be obligated for any costs or expenses other than as described herein, including without limitation, fees of any service providers not retained by AllClear ID. AllClear ID reserves the right to investigate any asserted claim to determine its validity.
- AllClear ID is not an insurance company, and AllClear Secure is not an insurance policy; AllClear ID will not make payments or reimbursements to you for any loss or liability you may incur.
- AllClear ID is not a credit repair organization, is not a credit counseling service, and does not promise to help you improve your credit history or rating beyond resolving incidents of fraud.
- AllClear ID reserves the right to reasonably investigate any asserted claim to determine its validity. All recipients of Secure coverage are expected to protect their personal information in a reasonable way at all times. Accordingly, recipients will not deliberately or recklessly disclose or publish their Social Security number or any other personal information to those who would reasonably be expected to improperly use or disclose that Personal Information.

Opt-out Policy
If for any reason you wish to have your information removed from the eligibility database for AllClear Secure, please contact AllClear ID:

E-mail	Mail	Phone
support@allclearid.com	AllClear ID, Inc. 823 Congress Avenue Suite 300 Austin, Texas 78701	1.855.434.8077