

May 16, 2019

E6530-L01-0123456 0001 00000001 *****OEL
SAMPLE A SAMPLE



APT 123
123 ANY ST
ANYTOWN, US 12345-6789



Notice of Data Breach

Dear Sample A Sample:

Delta Health Systems (“DHS”) is a third party administrator that was previously contracted to provide administrative services on behalf of the health plan sponsored by your employer, Turlock Irrigation District (“TID”). On April 18, 2019, TID notified us that your personal information was publically accessible through a link to our website. This incident occurred despite the fact that our website security requires login credentials to access that information.

What Happened

A TID billing statement containing your personal information was inadvertently made available on the internet for an unknown period of time that ended on April 18, 2019. Upon learning that the statement was publically accessible, the DHS Information Technology team (“IT”) immediately removed the document from our website. Thereafter, we launched an investigation, which subsequently revealed that this incident was caused by a configuration error made by a third party website developer. More specifically, the developer applied two conflicting permissions to the billing statement link, one allowing general access and the other restricting access to the document. This conflict resulted in the billing statement, and your personal information, being publically accessible via the internet.

What Information Was Involved?

We have determined that the following information about you was accessed: first and last name, employer name and address, DHS identification number and Social Security Number (“SSN”). The information that was accessed did not include credit card information or bank account numbers.

What we are Doing

This issue was corrected on April 18, 2019 when DHS IT reconfigured our website permissions and deleted the billing statement from our website. As an extra precaution, we also contacted Yahoo to ensure that the “cached” information was removed from their search engine, so as to prevent the link from continuing to display your information after the billing statement was deleted; Yahoo was the only search engine through which this document could be accessed.

DHS is also in the process of enhancing our analytics tools and login security to ensure that we can better track access to sensitive documents and ensure that access is restricted to authorized users. Finally, we are building a new website that will not utilize the incorrectly configured software that ultimately led to the compromise of your personal information.

0123456



To help protect your identity, we are also offering a complimentary one-year membership of Experian's® IdentityWorksSM. This product provides you with superior identity detection and resolution of identity theft. To activate your membership and start monitoring your personal information please follow the steps below:

- Ensure that you **enroll by: 8/31/2019** (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll: WWW.WEBSITE.COM
- Provide your **activation code: ABCDEFGHI**

If you have questions about the product, need assistance with identity restoration or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at 888-292-0073 by **8/31/2019**. Be prepared to provide engagement number **ENGAGEMENT** as proof of eligibility for the identity restoration services by Experian.

ADDITIONAL DETAILS REGARDING YOUR 12-MONTH EXPERIAN IDENTITYWORKS MEMBERSHIP:

A credit card is **not** required for enrollment in Experian IdentityWorks.

You can contact Experian **immediately** regarding any fraud issues, and have access to the following features once you enroll in Experian IdentityWorks:

- ◆ **Experian credit report at signup:** See what information is associated with your credit file. Daily credit reports are available for online members only.*
- ◆ **Credit Monitoring:** Actively monitors Experian, Equifax and Transunion files for indicators of fraud.
- ◆ **Internet Surveillance:** Technology searches the web, chat rooms & bulletin boards 24/7 to identify trading or selling of your personal information on the Dark Web.
- ◆ **Identity Restoration:** Identity Restoration specialists are immediately available to help you address credit and non-credit related fraud.
- ◆ **Experian IdentityWorks ExtendCARETM:** You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- ◆ **Up to \$1 Million Identity Theft Insurance^{**}:** Provides coverage for certain costs and unauthorized electronic fund transfers.

If you believe there was fraudulent use of your information and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent at 888-292-0073. If, after discussing your situation with an agent, it is determined that Identity Restoration support is needed, then an Experian Identity Restoration agent is available to work with you to investigate and resolve each incident of fraud that occurred (including, as appropriate, helping you with contacting credit grantors to dispute charges and close accounts; assisting you in placing a freeze on your credit file with the three major credit bureaus; and assisting you with contacting government agencies to help restore your identity to its proper condition).

Please note that this Identity Restoration support is available to you for one year from the date of this letter and does not require any action on your part at this time. The Terms and Conditions for this offer are located at www.ExperianIDWorks.com/restoration. You will also find self-help tips and information about identity protection at this site.

What You Can Do

The information that was accessed did not contain your credit card information or bank account numbers. However, we encourage you to remain vigilant by reviewing account statements and monitoring free credit reports. You may also obtain information from the FTC and the credit reporting agencies about fraud alerts and security freezes.

Equifax
PO BOX 740241
ATLANTA GA 30374-0241
1-800-685-1111
equifax.com

Experian,
PO BOX 9532
ALLEN TX 75013
1-888-397-3742
experian.com

TransUnion
PO BOX 6790
FULLERTON CA 92834-6790
1-800-916-8800
transunion.com

You may also place a 90-Day Fraud Alert on your Credit File. An **initial 90-day security alert** indicates to anyone requesting your credit file that you suspect you are a victim of fraud. When you or someone else attempts to open a credit account in your name, increase the credit limit on an existing account, or obtain a new card on an existing account, the lender should take steps to verify that you have authorized the request. If the creditor cannot verify this, the request should not be satisfied. You may contact one of the credit reporting companies above for assistance.

If you are very concerned about becoming a victim of fraud or identity theft, a security freeze might be right for you. Placing a freeze on your credit report will prevent lenders and others from accessing your credit report in connection with any new credit application, which will prevent them from extending credit. A security freeze generally does not apply to circumstances in which 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. With a security freeze in place, you will be required to take special steps when you wish to apply for any type of credit. This process is also completed through each of the credit reporting agencies.

Visit www.annualcreditreport.com or call 1-877-322-8228. Once you receive your credit reports, review them for discrepancies. Identify any accounts you did not open or inquiries from creditors that you did not authorize. Verify all information is correct. If you have questions or notice incorrect information, contact the credit reporting company.

Take steps such as: carrying only essential documents with you; being aware of whom you are sharing your personal information with; and shredding receipts, statements, and other sensitive information. Remain vigilant by reviewing account statements and monitoring credit reports.

Carefully review your credit reports and bank, credit card and other account statements. Be proactive and create alerts on credit cards and bank accounts to notify you of activity. If you discover unauthorized or suspicious activity on your credit report or by any other means, file an identity theft report with your local police and contact a credit reporting company.

Contact your healthcare provider if bills do not arrive when expected, and review your Explanation of Benefit forms to check for irregularities or suspicious activity. You can also contact your health insurance company to notify them of possible medical identity theft or ask for a new account number.

You may also file a complaint with the FTC at www.ftc.gov/idtheft or at 1-877-ID-THEFT (877-438-4338).

For More Information

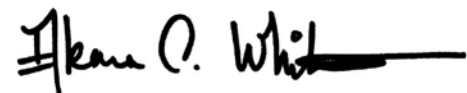
You may visit <http://www.experian.com/credit-advice/topic-fraud-and-identity-theft.html> for general information regarding protecting your identity. You can also contact The Federal Trade Commission at their identity theft hotline: 1-877-438-4338; TTY: 1-866-653-4261. They also provide information online at www.ftc.gov/idtheft. You can also obtain information about steps to avoid identity theft from any of the above credit reporting agencies or the Attorney General.

0123456



DHS sincerely apologizes for this incident and we regret any inconvenience it may cause you. If you need any additional information or wish to contact us with questions, please contact us at 888-292-0073.

Sincerely,

A handwritten signature in black ink that reads "Akara C. Whiten" followed by a horizontal line.

Akara C. Whiten, JD, CIPP
Director of Compliance and Privacy Officer
Delta Health Systems