

Source: <http://www.health.utah.gov/databreach/>, June 6, 2012



Personal Health Information Breach

Frequently Asked Questions

Office of the Data Security Ombudsman

On Tuesday, May 15, 2012 Governor Gary R. Herbert announced the appointment of Sheila Walsh-McDonald as the Data Security Ombudsman. The ombudsman and her staff will work directly with victims of the personal health information data breach. They will focus on providing individual case management, credit and identity theft counseling, and community outreach.

You can reach the Office of the Data Security Ombudsman directly via e-mail at ombudsman@utah.gov or by calling the toll-free hotline at 1-855-238-3339, a representative will collect your contact information and the Ombudsman's Office will return your call directly.

To read more about Gov. Herbert's announcement of the Office of the Data Security Ombudsman, [click here](#).

Recent Updates

The Utah Department of Health has sent letters to all individuals who had their Social Security number stolen during the breach and whose addresses the department was able to obtain. These letters include instructions on how to take advantage of one year of free credit monitoring services. If you received one of these letters, we strongly encourage you to activate the credit monitoring service.

If you haven't received a letter, but want to find out if your Social Security number was stolen, you can call our toll-free hotline at 1-855-238-3339. Please be aware that in order to check if your number was stolen you will need to provide it to the hotline.

A substantial amount of people who have no history with either the Medicaid or CHIP programs had their personal information stolen off the server. This is because health care providers often submit personal information on patients to the state in order to check their status as possible Medicaid recipients. It appears some health care providers conduct these inquiries on patients who are privately insured, as well as on patients who they believe may be on Medicaid.

Health care providers conduct these inquiries with an expectation that the state keep these data secure.

The Utah Departments of Technology Services and Health take full responsibility for not ensuring the security of these data, and are deeply sorry for the distress the breach has caused.

Information Resources

Child Identity Protection

<https://cip.utah.gov>

The Utah Attorney General's Child Identity Protection (CIP) program helps prevent identity thieves from using the personal identifying information of Utah children in the issuance of credit. CIP provides Utah parents/guardians with a secure process to enroll a child's information with a national credit reporting company (TransUnion). Upon receipt of an enrolled child's information via CIP, TransUnion will take certain proprietary fraud prevention steps, including but not limited to the entry

of portions of that information into its High Risk Fraud database. Such information will remain in the High Risk Fraud database until the child's 17th birthday, at which time it will be removed.

Adults (those older than 17 years of age) seeking protection against identity theft may add a **fraud alert** or **security freeze** to their credit files by contacting the three national credit reporting companies.

Fraud Alert

You can add a fraud alert message to your credit report to help protect your credit information. Fraud alert messages notify potential credit grantors to verify your identification before extending credit in your name in case someone is using your information without your consent. We recommend that you review a copy of your personal credit report. If you believe that information in your credit report is inaccurate due to identity theft or fraud, call the phone number on your report for assistance from a representative specially trained in consumer credit fraud.

To monitor your credit, you may get one free copy of your credit file every 12 months from each of the nationwide credit reporting agencies. For your free credit report, call one of the nation's three credit bureaus:

- **TransUnion**
<http://www.transunion.com>, 1-800-888-4213
- **Experian**
<http://www.experian.com>, 1-866-200-6020
- **Equifax**
<http://www.equifax.com>, 1-800-685-1111

Credit Freeze

A Credit Freeze simply means that new credit accounts will not be approved and your credit file cannot be accessed by anyone without your approval. Even if thieves have all of your personal identifying information, they still won't be allowed to get credit in your name.

You can **freeze your credit lines** by contacting the nation's three credit bureaus. By freezing your credit, anytime you apply for a mortgage, car loan, credit card, department store account, or any other type of credit, you will have to confirm your identity and unlock your credit report.

To freeze your credit, contact one of the nation's three credit bureaus:

- **TransUnion**
<https://freeze.transunion.com>
1-888-909-8872
- **Experian**
<http://www.experian.com>
1-866-200-6020
- **Equifax**
<https://www.freeze.equifax.com>
1-800-685-1111

Personal Identity Theft

The Utah Attorney General's Office sponsors the Identity Theft Reporting Information System to assist victims of identity theft. For more information and resources related to **protecting and monitoring your personal identity**, visit <http://idtheft.utah.gov>.

Previous News Releases

Monday, April 9, 2012

Friday, April 6, 2012

Wednesday, April 4, 2012



County: Select County

City: Select City

Submit Query

Reset

[Home](#) | [Contact Us](#) | [A-Z List](#) | [About Us](#) | [Use Disclaimer](#) | [Privacy Policy](#)

[Utah.gov Home](#) | [Utah.gov Terms of Use](#) | [Utah.gov Privacy Policy](#) | [Utah.gov Accessibility Policy](#) | [Translate Utah.gov](#)

Copyright © 2012 State of Utah - All rights reserved.



Frequently Asked Questions

Q: What happened?

A: On March 10, 2012 computer hackers illegally gained access to a Utah Department of Technology Services (DTS) computer server that stores Medicaid and CHIP claims data. The thieves began removing data from the server on March 30, 2012. DTS detected the activity on April 2, 2012 and immediately shut down the server. As its investigation proceeded, DTS discovered data from eligibility inquiries (inquiries sent from health care providers to determine if patients are enrolled in Medicaid) was also stored on the server. This additional data included information from individuals who may not be Medicaid or CHIP clients.

The breach occurred due to an error on the server at the password authentication level, allowing the hacker to circumvent the security system. DTS has processes in place to ensure the state's data is secured, but this particular server was not configured according to normal procedure.

Q: How do I get in touch with the Data Security Ombudsman?

A: Governor Gary Herbert announced the creation of the Ombudsman's Office to provide a higher level of assistance to victims of the data breach. The ombudsman and her staff will focus on individual case management, credit and identity theft counseling, and community outreach. You can reach the Ombudsman via e-mail at ombudsman@utah.gov or by dialing the toll-free hotline 1-855-238-3339, hotline operators will take your name and number and the Ombudsman's Office will return your call.

Q: I am not a Medicaid or CHIP client, but I received a letter stating my Social Security number was stolen. Why?

A: You have probably visited a health care provider in the past several months, and your provider, or their billing entity, submitted your SSN to us in a transaction called a Medicaid Eligibility Inquiry. Some health care providers submit information to the UDOH on all their clients to determine which ones are enrolled in Medicaid. Even though you have no history with the program, this is how your personal information was compromised during the breach.

We understand this is unsettling news and apologize for the stress it has caused. The letter you received outlines steps to take in order to protect your personal credit file and we strongly encourage you to take those steps.

Q: Who had their information stored on the server?

A: Medicaid and CHIP recipients and their health care providers had information stored on the server. Other victims include people whose information was sent to the state by a health care provider in a transaction called a Medicaid Eligibility Inquiry to determine their status as possible Medicaid recipients. These victims are likely to be people who have visited a health care provider in the past four months. Some may be Medicaid or CHIP recipients; others are individuals whose health care providers were unsure as to their status as Medicaid recipients.

Q: I do not live in Utah, have never been to Utah, or received health care in Utah, why did I receive a letter?

A: Some of the compromised information included in the data breach was random 9-digit numbers that were not attached to any other verifying or sensitive information (e.g. DOB, name, address). However, those nine digits coincidentally matched up to your Social Security number. We are sorry for the worry this has caused, but wanted you to be aware so that you can be proactive in protecting your personal information. For extra precaution, we recommend that you activate the free credit monitoring service provided by Experian detailed in the letter you received.

Q: How do I sign up for credit monitoring and identity theft insurance?

A: If your Social Security number was stolen, you will receive a letter with instructions on how to receive one year of free credit monitoring services from Experian, a global leader in the credit monitoring field. This service includes daily credit monitoring, alerts of key changes to credit files, and identity theft insurance. The identity theft insurance provides \$1 million of coverage to adults and \$2 million of coverage to households. The policy covers certain costs associated with identity theft, such as fraudulent electronic fund transfers, lost wages, legal fees, and other costs. When you enroll in the credit monitoring service you are automatically enrolled in the insurance plan.

We strongly encourage you to activate this service.

There are a number of other steps you can take to protect yourself from identity theft, including freezing your credit and placing a fraud alert on your personal credit file. You must initiate these activities on your own with each of the nation's three credit bureaus. For information on how to do this, visit <http://idtheft.utah.gov>.

Q: I received a letter with an activation code for credit monitoring but I threw the letter away or lost it. How do I get a new code?

A: Call our toll free hotline at 1-855-238-3339; you will be prompted to enter #2 to speak to a customer service representative. Once you are on the line with a representative let them know of your situation. They will collect your name and phone number and pass it along to the Utah Department of Health. The health department will then work with Experian to issue you a new activation code.

Q: I called the hotline and confirmed my Social Security number was compromised but I have not received a letter with an activation code for credit monitoring. What should I do?

A: Call our toll free hotline at 1-855-238-3339; you will be prompted to enter #2 to speak to a customer service representative. Once you are on the line with a representative let them know of your situation. They will collect your name and phone number and pass it along to the Utah Department of Health. The health department will then work with Experian to issue you an activation code.

Q: I received a letter stating my Social Security number was compromised. A few days later I received a follow-up letter stating my Social Security number *wasn't* compromised. Which letter is accurate?

A: Some individuals may have received two letters; the first indicating their SSN had been compromised, the second indicating it hadn't. This is because your information appeared in two different areas of the breached server. The second letter you received stating your SSN had not been compromised was sent in error and you should disregard it. Your original letter contained instructions on how to activate a free credit-monitoring service. If you have not done so already, we strongly encourage you to activate that service.

Q: I received a letter but would like to verify its authenticity.

A: There are several markings on the letter you can use to confirm its authenticity. Such as:

Return Address:

Bureau of Managed Health Care **OR** Utah Department of Health
PO Box 143108
SLC, UT 84114-3108

Top right-hand:

State of Utah (with State Seal above)
Gary R. Herbert, Governor

Salutation:

Sincerely,
Utah Department of Health
Division of Medicaid and Health Financing

This letter was issued by the State of Utah, Department of Health to alert you to a data breach which included your personal identifying information. We understand this is unsettling news and apologize for the stress it has caused. The letter you received outlines steps to take in order to protect your personal credit file and we strongly encourage you to take those steps.

Q: What kind of information was on the server?

A: Claims payment and eligibility inquiries contain sensitive, personal health information from individuals and health care providers. Such information could include Social Security numbers, names, dates of birth, addresses, diagnosis codes, national provider identification numbers, provider taxpayer identification numbers, and billing codes.

Personal financial information, such as bank account numbers or credit card numbers, ARE NOT stored on this server and would NOT have been compromised during this attack.

Q: How many victims are there?

A: The most sensitive information stored on the server was individual's Social Security numbers (SSNs). Approximately 280,000 people had their SSNs stolen off the server. Other less sensitive information, such as names, dates of birth, and addresses was also store on the server. As many as 500,000 additional individuals may have had this type of information compromised.

Q: Can you tell me if my Social Security number was stolen?

A. We have compiled a list of all the Social Security numbers that were compromised. You may call the data breach hotline (**1-855-238-3339**) to find if your Social Security number was compromised.

In addition, a letter will be mailed to each individual whose Social Security number was taken. The letter will also provide information on how to take advantage of free credit-monitoring services for one year and other resources available to protect your credit.

In the meantime, you can visit www.health.utah.gov/databreach for contact information on how to monitor your credit, including how to place a fraud alert or credit freeze on your file.

Q: Was any of my personal information on the server, and how will I know if it was stolen?

A: If you are a victim in this case, you will be receiving a letter from the Utah Department of Health (UDOH). UDOH has already notified the majority of people whose SSNs were compromised during the attack. If your SSN was accessed, the letter will also provide information on how to take advantage of free credit monitoring services for one year.

Possible victims should be aware that nobody from DTS or UDOH will be contacting them and asking for information over the phone or via e-mail regarding this incident. Scammers may attempt to reach victims in this manner. We strongly recommend that people do not provide private information in response to telephone or e-mail contacts they have not initiated.

Q: How is information stored and how were the hackers able to access it?

A: DTS servers have multi-layered security systems that include many controls, including: perimeter security, network security, identity management, application security, and data security. In this particular incident, a configuration error occurred at the password authentication level, allowing the hacker to circumvent the security system. DTS has processes in place to ensure the state's data is secured, but this particular server was not configured according to normal procedure.

Q: What is being done to ensure other information is secure?

A: At the direction of Governor Gary Herbert, the state has hired an independent, nationally recognized auditor to conduct a full-scale review of all its data storage and data security systems. If there are additional weaknesses, this audit will expose them and the state will take immediate action to remedy those weaknesses.

DTS has also implemented new processes to ensure this type of breach will not happen again. Additional steps are being implemented to improve security controls related to the implementation of computer hardware and software, as well as increased network monitoring and intrusion detection capabilities.

Q: If people have additional questions regarding this issue, what should they do?

A: Please visit <http://www.health.utah.gov/databreach>, which is the principal source for information about the incident.