[redacted]

Office of the Attorney General

Attn: Security Breach Notification

On behalf of Cigna Medicare, I am writing to inform you about an incident in which personal information relating to three (3) Maryland residents whose information was involved in an unauthorized access to a third party.

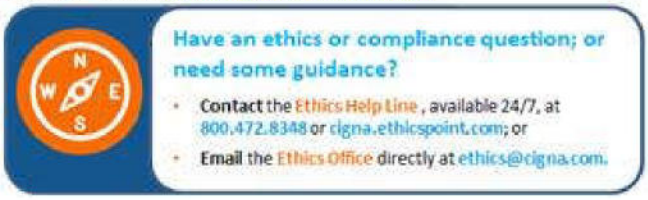
Specifically, Solutran, a vendor Cigna uses for a prepaid discount card and healthy food services, notified us on February 15, 2023 that there had been unauthorized access to some of its member web portals. This occurred when a bad actor logged into accounts after obtaining credentials from another public breach (i.e. credential stuffing). The following information is viewable in the portal: member name, date of birth, address, phone number, transaction activity and prepared card number/security code. Social Security numbers and medical diagnosis/treatment information are not stored in the portal.

In response to the incident, Cigna confirmed Solutran initiated password resets and enhanced security controls to address this issue. Additional logging and monitoring is under development for further security enhancements. Members will all receive a new prepaid card.

We will notify the three (3) Maryland residents of this incident. (A copy of that notice is attached)

Please do not hesitate to contact me at KCKellogg@express-scripts.com or 314-684-5143 if you have any questions.

Chris Kellogg
Privacy
Express Scripts | One Express Way | St. Louis, MO 63121
t 314-684-5143 | ckellogg@express-scripts.com



Optum Financial™

Optum Privacy Office
11000 Optum Circle
Eden Prairie, MN 55344
1-888-839-7948

[Date]

[Name]
[Street Address]
[City, State, ZIP]

NOTICE OF DATA BREACH

Dear [Member/Patient Full Name]:

We are writing to inform you that your [name of portal] web account was accessed by an unknown third party. Unfortunately, it appears that personal information identifying you may have been exposed.

What Happened

On February 15, 2023, Solutran, part of Optum Financial Services (OFS), became aware of unauthorized access to some of its member web portals and immediately launched an investigation. On February 19, 2023, Solutran confirmed that your [name of portal] account had been accessed by this unauthorized third party using your login credentials. Our investigation revealed that the suspicious activity began on or around January 13, 2023, and has now been effectively remediated and contained.

What Information Was Involved

- Member's first and last name
- Client's name
- Date of Birth
- Mailing Address
- Phone number
- Transaction activity
- Prepaid card number and security code.

No Social Security number, driver's license number, medical diagnosis or treatment information was involved. In addition, there is no evidence that your login credentials were accessed or obtained from any Solutran systems.

Although your information may have been accessed, we believe the intent was to use the monetary benefits available on the account, which would have been limited to only the dollars on the prepaid card. If any fraudulent activity is identified on a member account, Solutran will make impacted members financially whole.

We deeply regret this incident and any inconvenience or concern that it may cause.

What We Are Doing

Appropriate corrective action has been taken in response to the incident, including but not limited to forced password reset and enhanced security controls. Security control enhancements stopped the suspicious activity on March 9, 2023. Additional logging and monitoring is under

development and further security control enhancements are planned, including a new user identity management system.

You should have received an email with a password reset link and instructions. Additionally, we will cancel your current prepaid member card and a new card will be mailed to you on or before [date]. If you have not received an email with a password reset link or a new card by then, please contact us at [Solutran will provide phone number].

What You Can Do

We recommend that if you use the same username and password combination on [name of portal] as well as any external site(s), you change your password on those external sites to a password you have not previously used.

We do not think that the information disclosed was sufficient to steal your identity or impact your credit. However, as a precaution to protect against misuse of your personal information, you may want to order copies of your credit reports from each of the three national credit reporting agencies to check for any inaccurate information, particularly medical services or medical bills that you do not recognize. If you notice any suspicious activity, contact the credit reporting agencies using the contact information provided on the report or as listed below:

Equifax Information Services LLC	Experian	TransUnion LLC
P.O. Box 105069	P.O. Box 9554	P.O. Box 2000
Atlanta, GA 30348-5069	Allen, TX 75013	Chester, PA 19016
800-525-6285	888-397-3742	800-680-7289
www.equifax.com	www.experian.com	www.transunion.com

For More Information

Solutran and OFS take this matter seriously and are committed to protecting the privacy and security of your personal information. If you have any questions regarding this notice or have any further concerns, please feel free to call [phone number], Monday through Friday, [time] – [time] [time zone].

Sincerely,

Signature

Name
Title
Company