From: IDTheft
Sent: Friday, September 6, 2024 9:59 AM
To: IDTheft
Subject: RE: [Confidential] Maryland Attorney General
Attachments: Member Notice.pdf

Follow Up Flag: Follow up
Flag Status: Flagged

Categories: Data breach

From: Deike, Marcia
Sent: Thursday, September 5, 2024 3:27 PM
To: IDTheft <IDTheft@oag.state.md.us>
Subject: RE: [Confidential] Maryland Attorney General

Good afternoon,

Attached please find the Cybersecurity event report submitted 8/28/2024 of

Content of report included:
To: Maryland Office of the Attorney General
We are writing to notify you of a Cybersecurity Event. Relevant information regarding the event is below.

Date of Cybersecurity Event	July 31, 2024
How the information was exposed, lost, stolen, or breached, including the specific roles and responsibilities of any third-party service providers.	The event resulted from a system error during an update to our document delivery system. As a result of the error, some documents were inadvertently posted to an incorrect members' online account with USAA. No third-party service providers were responsible for or involved in the system error. USAA was unable to confirm whether the incorrectly posted information was ultimately accessed by the incorrect recipient, but was able to determine that the incorrect recipient was logged into their online account at the time the incorrectly posted information was available.
How the cybersecurity event was discovered.	On April 30, 2024, USAA became aware of a system error that occurred during a routine update to our document delivery system. The error was reported to USAA's Enterprise Privacy Office on May 6 for investigation and assessment, which concluded on July 31, 2024.
Identity of source of the cybersecurity event	Internal system error
Whether any lost, stolen, or breached information has been recovered and if so, how this was done.	n/a

Whether the licensee has filed a police report or has notified any regulatory, government, or law enforcement agencies and, if so, when the notification was provided.	USAA has not engaged law enforcement. Beginning on August 2, 2024, USAA began notifying relevant regulatory and government authorities.
A description of the specific types of information acquired without authorization. Specific types of information mean particular data elements including, for example, types of medical information, types of financial information, or types of information allowing identification of the consumer.	USAA was unable to confirm whether the incorrectly posted information was ultimately accessed by the incorrect recipient, but was able to determine that the incorrect recipient was logged into their online account at the time the incorrectly posted information was available. The personal information inadvertently disclosed varied by individual and may have included internal business and member facing documents that including the following: name, address, email address, date of birth, Social Security number, driver's license number, passport number, vehicle identification number, loan number, health information and property and casualty insurance information.
Period during which the information system was compromised by the cybersecurity event	No information system was compromised by the event.
The number of total consumers in this state affected by the cybersecurity event.	1008 Maryland residents. The notification to Maryland residents is attached.
Investigation of cybersecurity event, results of internal review, remediation steps and privacy policy.	Upon learning of the error, USAA promptly took corrective steps to remove the inadvertently posted documents, investigate the event, and ensure that any inadvertently delivered documents were subsequently delivered to the correct member. We have also undertaken additional measures to prevent the error from occurring in the future, including reviewing, and enhancing our IT change management processes. Impacted residents will be notified by August 30, 2024, and offered a free two-year membership of Experian's IdentityWorks credit monitoring product.
The name of a contact person who is both familiar with the cybersecurity event and authorized to act for the licensee.	Jeff Kennedy Chief Privacy Officer 9800 Fredericksburg Rd San Antonio, Texas 78288 Phone: 706-464-1618 Email address: jeff.kennedy@usaa.com

If you have any questions about the incident, please do not hesitate to contact me at the phone or email address below.

Sincerely,

Jeff Kennedy
Chief Privacy Officer
USAA
706-464-1618 / jeff.kennedy@usaa.com

Note: Submitted by Marcia Deike on behalf of Jeff Kennedy.
787921

United Services Automobile Association
9800 Fredericksburg Road
San Antonio, TX 78288

NOTICE OF DATA INCIDENT

[redacted]

August 27, 2024

Dear [redacted],

NOTICE OF DATA INCIDENT

USAA takes the protection of our members' personal information very seriously, so we are writing to tell you about an incident that may have involved your personal information.

What Happened
On April 30, 2024, we became aware of a system error that occurred during a routine update to our document delivery system. As a result of the error, some documents for members with property and casualty insurance products through USAA were inadvertently posted to another member's online account. Upon learning of the error, USAA promptly took corrective steps to remove the inadvertently posted documents and commenced an investigation of the incident. Based on our investigation, which concluded on July 31, 2024, we determined that some of your personal information may have been inadvertently disclosed to another USAA member.

Although we have no indication of any fraud or identity theft resulting from this incident, we are sending you this notice to provide you with information about the incident, what we are doing and steps you can take to help protect your personal information.

What Information Was Involved
The personal information inadvertently disclosed varied by individual, but may have included the following: name, address, email address, date of birth, Social Security number, driver's license number, passport number, vehicle identification number, loan numbers, health information, and property and casualty insurance policy information.

What We Are Doing
Upon learning of the error, we promptly took corrective steps to remove the inadvertently posted documents, investigate the incident, and ensure that any inadvertently delivered documents were subsequently delivered to the correct member. We have also undertaken additional measures to prevent the error from occurring in the future, including reviewing and enhancing our IT change management processes.

Complimentary Experian IdentityWorks℠ Membership
As a precaution and to help protect your identity, we are also offering a complimentary two-year membership of Experian's IdentityWorks program. This product provides you with superior identity detection and resolution of identity theft. Please see the additional information we have included as part of this notice on how to sign up.

What You Can Do
Although we have no indication of any fraud or identity theft resulting from this incident, we recommend you closely review the Steps to Take to Protect Your Personal Information document included as part of this notice for steps you can take to help protect against fraud or identity theft, including monitoring your accounts and free credit reports for any suspicious activity.

For More Information

We deeply regret that this incident occurred and take the privacy and security of your personal information very seriously. If you suspect you have been the victim of identity theft or have any questions, please call us at the following number:

Phone: 877-762-7256

As always, it's our honor to serve you.

Sincerely,

Jeff A. Kennedy
Chief Privacy Officer
USAA

787921

Attached: Steps to Take to Protect Your Personal Information
Activate IdentityWorks

9800 Fredericksburg Road
San Antonio, Texas 78288

STEPS TO TAKE TO PROTECT YOUR PERSONAL INFORMATION

Always remain vigilant, including over the next 12-24 months, for signs of fraud or identity theft, and consider taking one or more of the below steps to protect your personal information. You can also obtain information from the below sources about fraud alerts and security freezes.

- For breaches of username/email address in combination with a password or security question and answer that would permit access to an online account: Please promptly change your password or security question or answer, and take appropriate steps to protect your online accounts which use the same username, email address, password, or security question or answer.

- Carefully examine all account transactions, statements, and free credit reports to verify transactions. If anything looks suspicious or unusual, or if you believe you are the victim of identity theft, promptly report it to USAA and your other financial institutions. In addition, you may contact the Federal Trade Commission (FTC) or law enforcement to report incidents of identity theft, file a police report or to learn about steps you can take to protect yourself from identity theft.

- The FTC offers consumer assistance relating to identity theft, fraud alerts and security freezes. You may wish to visit the FTC web site at *www.ftc.gov/idtheft*, call the FTC's toll-free number at 1-877-438-4338, or contact them by mail at 600 Pennsylvania Ave., NW, Washington, DC 20580, to obtain further guidance or report suspected identity theft.

- You may also periodically obtain credit reports from each nationwide credit reporting agency: Equifax, Experian or TransUnion. Under federal law, you are entitled to one free copy of your credit report every 12 months from each of the three nationwide credit reporting agencies. If you discover information on your credit report arising from a fraudulent transaction, you should request that the credit reporting agency correct that information on your credit report file. You may request a free copy of your credit report by going to *www.annualcreditreport.com*, calling toll-free 1-877-322-8228, or completing the Annual Credit Request Form on the FTC's website at www.consumer.ftc.gov and mailing it to Annual Credit Report Service, P.O. Box 105281, Atlanta, GA 30348-5281.

- You may also request that a fraud alert be placed on your credit file. A fraud alert can make it more difficult for someone to get credit in your name because it tells creditors to follow certain procedures to protect you, but it also may delay your ability to obtain credit. To place a fraud alert, contact the fraud department of one of the three nationwide credit reporting agencies detailed below. When you request a fraud alert from one agency, it will notify the other two for you. You can place an initial fraud alert for one year and cancel fraud alerts at any time. During this process, a consumer reporting agency will require you to provide appropriate proof of your identity, which may include your Social Security number.

Equifax	Experian	TransUnion
Equifax Information Services LLC	Experian Inc.	TransUnion LLC
P.O. Box 740241	P.O. Box 9554	P.O. Box 2000
Atlanta, GA 30374	Allen, TX 75013	Chester, PA 19016
(800) 525-6285	(888) 397-3742	(800) 680-7289
www.equifax.com	*www.experian.com*	*www.transunion.com*

- In addition, you can contact the three nationwide credit reporting agencies regarding if and how you may place a security freeze on your credit reports to prohibit a credit reporting agency from releasing information from your credit report without your prior authorization. A security freeze 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 obtain credit. You must separately place a security freeze on your credit file with each nationwide credit reporting agency listed above (Equifax, Experian or TransUnion). There is no charge to place

or lift a security freeze. As the instructions for establishing a security freeze differ from state to state, please contact the three nationwide consumer reporting agencies to find more information.

In order to request a security freeze, you may need to provide the following information:

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.); current residential address; social security number; and date of birth
2. If you have moved in the past five (5) years, you may also need to provide the addresses where you have lived over the prior five years
3. Proof of your current residential address (such as utility bill, pay stub with address or telephone bill)
4. A legible photocopy of a government issued identification card (state driver's license or ID card, military identification, etc.)
5. If you are a victim of identity theft, include a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft

United Services Automobile Association
9800 Fredericksburg Road
San Antonio, Texas 78288

ACTIVATE EXPERIAN IDENTITYWORKS SM NOW IN THREE EASY STEPS

1. Ensure that you **enroll by**: November 30, 2024 (Your code will not work after this date.)
2. **Visit** the Experian IdentityWorks website to enroll: https://www.experianidworks.com/3bcredit
3. Provide your **activation code**: (A credit card is not required for enrollment.): [redacted]

If you have questions about the product, need assistance with identity restoration that arose as a result of this incident or would like an alternative to enrolling in Experian IdentityWorks SM online, please contact Experian's customer care team at 877-890-9332 by November 30, 2024. Be prepared to provide engagement number [redacted] as proof of eligibility for the identity restoration services by Experian.

Additional Details Regarding Your 2 Year Experian Identityworks SM Membership:

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.
- **Identity Restoration:** Identity Restoration specialists are immediately available to help you address credit and non-credit related fraud.
- **Experian IdentityWorks ExtendCARE™:** You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- **$1 Million Identity Theft Insurance**:** Provides coverage for certain costs and unauthorized electronic fund transfers.

What you can do to protect your information: There are additional actions you can consider taking to reduce the chances of identity theft or fraud on your account(s). Please refer to www.ExperianIDWorks.com/restoration for this information.

* Offline members will be eligible to call for additional reports quarterly after enrolling

** Identity theft insurance is underwritten by insurance company subsidiaries or affiliates of American International Group, Inc. (AIG). 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.

[redacted]