corebridge financial

March 1, 2024

BY EMAIL

Office of the Attorney General
200 St. Paul Plaza
Baltimore, MD 21202
Idtheft@oag.state.md.us

To Whom It May Concern:

On behalf of The Variable Annuity Life Insurance Company ("VALIC") and pursuant to Md. Code Ann., Com. Law § 14-3504(h), this letter provides notice of a cybersecurity incident involving Maryland residents.

At the end of September 2023, The Variable Annuity Life Insurance Company ("VALIC") fraud team investigated cases of suspected unauthorized access to VALIC online ("VOL") accounts based on suspicious IP addresses. Over the next couple of months, the fraud team identified patterns and other potentially impacted accounts based on similar IP addresses, banking information and activity once in the online account (updating contact information, adding EFT information, requesting distributions, and updating email address). The list of suspected unauthorized access attempts to VOL accounts grew with a concentration in late December 2023 and early January 2024. Another similarity in the accounts was that the unauthorized individual(s) had the usernames and passwords to log into the VOL accounts. There is no indication the usernames and passwords were obtained from VALIC.

VALIC placed blocks on all impacted online accounts, added enhanced monitoring to the impacted accounts, reached out to customers to confirm the online access and update their contact information, re-register for VOL, and change their usernames and passwords. If account information was changed by the unauthorized individual, VALIC reverted all contact information on the account, removed any compromised email accounts and added a new one. If VALIC was not able to contact the participant, they forced a password reset on the online account and the participant will be required to establish a new username and password. In the interim, no one can access the online account and the customer will have to contact VALIC for assistance with unlocking and re-registering the online profile. Customers were encouraged to add a verbal password to their account, have their computer/devices checked, change usernames and passwords if they use similar ones across accounts and contact their other financial institutions.

Online accounts were accessed for 2 residents of Maryland on September 23, 2023 and December 7, 2023. Account numbers, phone numbers, and email addresses were viewed for both residents and physical address for one resident was viewed. No funds were distributed from these accounts. VALIC plans to notify these individuals the week of March 4, 2024. A sample notification letter is enclosed.

VALIC takes this matter very seriously and is committed to answering any questions you may have. If you have any questions regarding this submission, please do not hesitate to contact me at melissa.cozart@corebridgefinancial.com or 713-831-6371.

***

This correspondence, and any attachments, contains confidential, proprietary commercial or financial information, documentation, business plans, strategies, and other information that are not otherwise available to the public, and that, if disclosed, could cause substantial injury to the competitive position of VALIC and its affiliates. Accordingly, VALIC respectfully requests that this filing and its exhibits be afforded confidential treatment and be excepted from disclosure.

Respectfully yours,

Melissa H. Cozart

Vice President & Chief Privacy Officer

2919 Allen Parkway, 3rd Floor, Houston, TX 77019

T (+1) 713.831.6371

melissa.cozart@corebridgefinancial.com | www.corebridgefinancial.com

February 26, 2024

<<Name 1>> <<Name 2>>
<<Address 1>>
<<Address 2>>
<<City>>, <<State>> <<Zip>>
<<Country>>

Dear <<Name 1>>:

As you are aware, there was recently unauthorized access to your VALIC[1] online account ("VOL"). The unauthorized individual was able to access the account because they had your username and password. There is no indication this information was obtained from VALIC. Once in the online account, the unauthorized individual was able to view some of your personal information and would have been able to make changes to your account.

What Happened? Between September 2023 and January 2024, an unauthorized individual(s) accessed certain VALIC online accounts using VOL usernames and passwords. There is no indication this information was obtained from VALIC. In some cases, the unauthorized individual was able to add banking information to the account, update contact information including email address, and/or request distributions. [No funds were distributed from your account. Steps have been initiated to reimburse your account for any funds distributed.] VALIC investigated the instances of unauthorized access to identify impacted individuals and determine what information was viewed in the online account. We recently completed this review and have concluded that your personal information was impacted.

What Information Was Involved? Our investigation determined that your personal information was impacted by this event and may have included your: name, address, phone number, email address, beneficiary information and/or account number. If your beneficiary's information was impacted, they will receive a similar notification.

What We Are Doing. VALIC takes this event and the security of information in our care seriously. We have placed blocks on all impacted online accounts, added enhanced monitoring to impacted accounts, contacted participants to update contact information, re-register for VOL, and change usernames and passwords. If account information was changed by the unauthorized individual, VALIC has reverted all contact information on the account, removed any compromised email accounts and added a new one.

What You Can Do. We recommend you add a verbal password to your account, have your computer/devices checked, change your username and password if you use similar ones across accounts and contact your other financial institutions. We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your account statements, monitoring your free credit reports for suspicious activity and to detect errors, and reporting any unusual activity to your financial institution. Please also review the enclosed *Steps You Can Take to Help Protect Personal Information*, which contains information on what you can do to safeguard against possible misuse of your information.

For More Information. If you have additional questions, please contact ____________________.

[1] The Variable Annuity Life Insurance Company

Sincerely,

Melissa H. Cozart
Vice President and Chief Privacy Officer
Corebridge Financial, Inc.

STEPS YOU CAN TAKE TO HELP PROTECT PERSONAL INFORMATION

Monitor Your Accounts

Under U.S. law, a consumer is entitled to one free credit report annually from each of the three major credit reporting bureaus, Equifax, Experian, and TransUnion. To order a free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. Consumers may also directly contact the three major credit reporting bureaus listed below to request a free copy of their credit report.

Consumers have the right to place an initial or extended "fraud alert" on a credit file at no cost. An initial fraud alert is a one-year alert that is placed on a consumer's credit file. Upon seeing a fraud alert display on a consumer's credit file, a business is required to take steps to verify the consumer's identity before extending new credit. If consumers are the victim of identity theft, they are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should consumers wish to place a fraud alert, please contact any of the three major credit reporting bureaus listed below.

As an alternative to a fraud alert, consumers have the right to place a "credit freeze" on a credit report, which will prohibit a credit bureau from releasing information in the credit report without the consumer's express authorization. The credit freeze is designed to prevent credit, loans, and services from being approved in a consumer's name without consent. However, consumers should be aware that using a credit freeze to take control over who gets access to the personal and financial information in their credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application they make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, consumers cannot be charged to place or lift a credit freeze on their credit report. To request a credit freeze, individuals may need to provide some or all of the following information:

1. Full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. Addresses for the prior two to five years;
5. Proof of current address, such as a current utility bill or telephone bill;
6. A legible photocopy of a government-issued identification card (state driver's license or ID card, etc.); and
7. A copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft if they are a victim of identity theft.

Should consumers wish to place a credit freeze or fraud alert, please contact the three major credit reporting bureaus listed below:

Equifax	Experian	TransUnion
https://www.equifax.com/personal/credit-report-services/	https://www.experian.com/help/	https://www.transunion.com/credit-help
1-888-298-0045	1-888-397-3742	1-800-916-8800
Equifax Fraud Alert, P.O. Box 105069 Atlanta, GA 30348-5069	Experian Fraud Alert, P.O. Box 9554, Allen, TX 75013	TransUnion Fraud Alert, P.O. Box 2000, Chester, PA 19016
Equifax Credit Freeze, P.O. Box 105788 Atlanta, GA 30348-5788	Experian Credit Freeze, P.O. Box 9554, Allen, TX 75013	TransUnion Credit Freeze, P.O. Box 160, Woodlyn, PA 19094

Additional Information

Consumers may further educate themselves regarding identity theft, fraud alerts, credit freezes, and the steps they can take to protect your personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or their state attorney general. The Federal Trade Commission may be reached at: 600 Pennsylvania Avenue NW, Washington, D.C. 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them.

Consumers can obtain further information on how to file such a complaint by way of the contact information listed above. Consumers have the right to file a police report if they ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, consumers will likely need to provide some proof that they have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and the relevant state attorney general. This notice has not been delayed by law enforcement.

For Maryland residents, the Maryland Attorney General may be contacted at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-410-528-8662 or 1-888-743-0023; and https://www.marylandattorneygeneral.gov/.

For North Carolina residents, the North Carolina Attorney General may be contacted at: 9001 Mail Service Center, Raleigh, NC 27699-9001; 1-877-566-7226 or 1-919-716-6000; and www.ncdoj.gov.