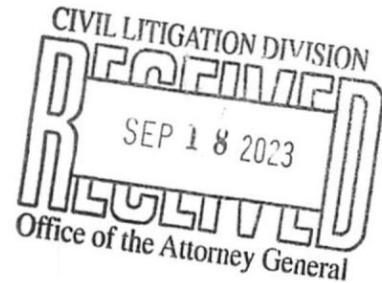




Fidelity Life Association
1350 E. Touhy Avenue Suite 205W
Des Plaines, IL 60018
T/F: 312.379.2397

September 8, 2023

Office of the Attorney General
Attn: Security Incident Reporting
200 St. Paul Place
Baltimore, MD 21202



RE: Fidelity Life Association – Notice of Security Incident

Dear Sir/Madam:

I am notifying you that Fidelity Life Association, an insurance company domiciled in Illinois, recently learned of a security incident involving unauthorized access to 4 Maryland residents' personal information. We are continuing to gather information about this incident, and we will update this notice with additional details as necessary. As of today, our understanding is as follows:

1. **When did the incident occur?** We are still investigating when the incident first started, but we first determined on August 10, 2023, that a small number of files were accessible from outside of our network environment via a unique, complex URL to a restricted webpage.
2. **What happened?** We determined that a small number of internal directories were made accessible online through our website and that information was indexed by a small number of website indexers (such as Google). Because the files were images, the only indexed information was summary details about the image content. Since this incident came to our attention on August 10, 2023, we have been moving quickly to limit access to the online files and identify what information was in those files. We determined on August 10, 2023 that the files contained PII and created a list of all the affected individuals at approximately 11pm on August 16, 2023. And, since then, we have been preparing individual and regulatory notices.
3. **How was the incident discovered?** On August 10, 2023, we were informed by one of our contracted security-monitoring partners that some of our files were available online. We moved quickly to investigate those reports. We confirmed at approximately 11pm on August 16, 2023, that the affected files contained personal information requiring notice to at least one other regulator.
4. **Has data been recovered?** We have not found evidence that third parties downloaded the information, but some third parties appear to have indexed data from our website. We have updated our network settings to restrict access to the data on our servers. Additionally, we reached out to Bing and Google—companies who we believe scraped the customer information from our website—and asked them to remove the data from their indices. The data has now been removed from those indices.

5. **What is the source of the incident?** We are still investigating how this incident occurred. We believe at this time that it was a misconfigured setting that exposed information.
6. **Have we notified law enforcement?** We have not yet alerted law enforcement.
7. **What data was acquired?** The affected information involved some combination of individuals' names, contact information, demographic details, birthdates, Social Security numbers, driver's license numbers, and medical information.
8. **How long did the compromise last?** We are still investigating the date the files were first impacted by this incident. We locked down the at-issue files in under 30 minutes of learning that the misconfiguration exposed the information.
9. **How many residents were affected?** We believe that 4 Maryland residents were affected.
10. **What remediation has been done?** We quickly began investigating this incident. We took steps to identify what happened, how it happened, and what additional safeguards we can implement to prevent a similar incident in the future. Additionally, we have removed the online access to our files, asked third-party scrapers—such as Google—to determine whether they indexed the data (and, if they did, to remove it), and engaged outside counsel to help us assess notification obligations. We are in the process of preparing notices for affected individuals. In those notices, we will include complimentary credit monitoring for individuals who had a driver's license or Social Security number impacted.
11. **What investigation steps have we undertaken?** We engaged experienced outside counsel to advise us on our rights and obligations. We also have our IT team investigating the cause and scope of the incident.
12. **How are we notifying people?** On September 8, 2023, we are mailing notices to the individuals who had personal information impacted by this incident. We will include complimentary credit monitoring for any individuals who had their Social Security number or driver's license number impacted.

I have attached a copy of the notices we are providing to affected Maryland residents. If you have questions or need more details regarding this incident, please contact Colman McCarthy at cdmccarthy@shb.com or 816-559-2081.

Sincerely,



John Buchanan
EVP & General Counsel



Fidelity Life Association
1350 E. Touhy Avenue Suite 205W
Des Plaines, IL 60018
T | F: 312.379.2397

August 31, 2023

VIA U.S. MAIL

<First Name> <Last Name>

<Address>

<City>, <State> <ZIP>

NOTICE OF DATA BREACH

Dear <First Name> <Last Name>,

We are writing to inform you about an incident that may have exposed your personal information.

WHAT HAPPENED

On August 10, 2023, we determined that a small number of our files were accessible from outside of our network environment via a unique, complex URL to a restricted webpage. We believe, however, that some of the files were indexed via automated methods by third-party services, such as Google. Once we learned that the files were accessible, we updated our network settings in under 30 minutes to make those files unavailable outside of our environment.

WHAT INFORMATION WAS INVOLVED

Personal information contained in the files included name, signature, birthdate, medical data, contact information, and demographic details. Not all of those types of information were found in each file. We do not have evidence indicating that any of your information has been or will be misused.

WHAT WE ARE DOING

Upon learning of this incident, we immediately restricted access to the files. We also reached out to companies we believed indexed the data, and we have successfully worked with them to remove the data from their indices. At the same time, we began reviewing the relevant files to determine what information was involved so that we could notify the impacted individuals.

WHAT YOU CAN DO

Remain vigilant – We encourage you to remain vigilant for fraud or identity theft by reviewing your account statements and free credit reports. You can also find additional suggestions at www.IdentityTheft.gov/databreach.

- You should confirm that your credit card company has the correct address on file for you and that all charges on the account are legitimate. If you discover errors or suspicious activity, you should immediately contact the credit card company and inform them that you have received this letter.
- You should obtain and review a free copy of your credit report by visiting www.annualcreditreport.com or calling (877) 322-8228. If the report is incorrect, you should contact the appropriate consumer reporting agency—Equifax, Experian, or TransUnion.

Consider placing a fraud alert or security freeze on your credit file – Consumer reporting agencies have tools you can use to protect your credit, including fraud alerts and security freezes.

- A fraud alert is a cautionary flag you can place on your credit file to notify companies extending you credit that they should take special precautions to verify your identity. You can contact any of the three consumer reporting agencies to place fraud alerts with each agency.
- A security freeze is a more dramatic step that will prevent others from accessing your credit report, which will prevent them from extending you credit. You must contact each consumer reporting agency separately to order a



Fidelity Life Association
1350 E. Touhy Avenue Suite 205W
Des Plaines, IL 60018
T | F: 312.379.2397

security freeze, and they may require you to provide them with your full name, Social Security number, date of birth, and current and previous addresses. You can obtain more information about security freezes by contacting the consumer reporting agencies or the Federal Trade Commission.

Report suspicious activity – If you believe you are the victim of identity theft, consider (1) notifying your Attorney General, local law enforcement, or the Federal Trade Commission; (2) filing a police report and requesting a copy of that report; and (3) visiting IdentityTheft.gov to report the issue and get recovery steps.

Contact relevant authorities – You may contact the below resources to (1) get more information on fraud alerts or security freezes and (2) learn more about protecting yourself from fraud or identity theft.

Equifax
P.O. Box 740241
Atlanta, GA 30374
(800) 685-1111
www.equifax.com

Experian
P.O. Box 9701
Allen, TX 75013
(888) 397-3742
www.experian.com

TransUnion
P.O. Box 2000
Chester, PA 19016
(888) 909-8872
www.transunion.com

Federal Trade Commission
600 Pennsylvania Ave. NW
Washington, DC 20580
(202) 326-2222
www.ftc.gov

Maryland Attorney General
200 St. Paul Place, 25th Floor
Baltimore, MD 21202
(888) 743-0023
www.marylandattorneygeneral.gov

North Carolina Attorney General
9001 Mail Service Center
Raleigh, NC 27699
(919) 716-6400
www.ncdoj.gov

You can also find your Attorney General's contact information at: <https://www.usa.gov/state-attorney-general>.

FOR MORE INFORMATION

Should you have any questions or concerns, you contact us toll-free at 877-704-6279; choose option 1, then option 2, and one of our representatives will be happy to assist you. Thank you for your understanding and patience.

Sincerely,

John Buchanan
EVP & General Counsel



Fidelity Life Association
1350 E. Touhy Avenue Suite 205W
Des Plaines, IL 60018
T | F: 312.379.2397

<Date>

VIA U.S. MAIL

<First Name> <Last Name>

<Address>

<City>, <State> <ZIP>

NOTICE OF DATA BREACH

Dear <First Name> <Last Name>,

We are writing to inform you about an incident that may have exposed your personal information.

WHAT HAPPENED

On August 10, 2023, we determined that a small number of our files were accessible from outside of our network environment via a unique, complex URL to a restricted webpage. We believe, however, that some of the files were indexed via automated methods by third-party services, such as Google. Once we learned that the files were accessible, we updated our network settings in under 30 minutes to make those files unavailable outside of our environment.

WHAT INFORMATION WAS INVOLVED

Personal information contained in the files included name, signature, birthdate, medical data, contact information, demographic details, and government identification (such as a Social Security or driver's license number). Not all of those types of information were found in each file. We do not have evidence indicating that any of your information has been or will be misused.

WHAT WE ARE DOING

Upon learning of this incident, we immediately restricted access to the files. We also reached out to companies we believed indexed the data, and we have successfully worked with them to remove the data from their indices. At the same time, we began reviewing the relevant files to determine what information was involved so that we could notify the impacted individuals.

WHAT YOU CAN DO

Activate your complimentary credit monitoring – To help protect you from fraud or identity theft, we are offering a complimentary one-year membership to Experian's IdentityWorks. This product helps detect possible misuse of your personal information. To register, please:

- Ensure that you **enroll by:** November 30, 2023 (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll: www.experianidworks.com/3bcredit
- Provide your **activation code:** <code>

If you have questions or want an alternative to enrolling in Experian IdentityWorks online, please contact Experian at 877-890-9332 by November 30, 2023, and provide them engagement number <number>.

Remain vigilant – We encourage you to remain vigilant for fraud or identity theft by reviewing your account statements and free credit reports. You can also find additional suggestions at www.IdentityTheft.gov/databreach.

- You should confirm that your credit card company has the correct address on file for you and that all charges on the account are legitimate. If you discover errors or suspicious activity, you should immediately contact the credit card company and inform them that you have received this letter.
- You should obtain and review a free copy of your credit report by visiting www.annualcreditreport.com or calling



Fidelity Life Association
1350 E. Touhy Avenue Suite 205W
Des Plaines, IL 60018
T|F: 312.379.2397

(877) 322-8228. If the report is incorrect, you should contact the appropriate consumer reporting agency—Equifax, Experian, or TransUnion.

Consider placing a fraud alert or security freeze on your credit file – Consumer reporting agencies have tools you can use to protect your credit, including fraud alerts and security freezes.

- A fraud alert is a cautionary flag you can place on your credit file to notify companies extending you credit that they should take special precautions to verify your identity. You can contact any of the three consumer reporting agencies to place fraud alerts with each agency.
- A security freeze is a more dramatic step that will prevent others from accessing your credit report, which will prevent them from extending you credit. You must contact each consumer reporting agency separately to order a security freeze, and they may require you to provide them with your full name, Social Security number, date of birth, and current and previous addresses. You can obtain more information about security freezes by contacting the consumer reporting agencies or the Federal Trade Commission.

Report suspicious activity – If you believe you are the victim of identity theft, consider (1) notifying your Attorney General, local law enforcement, or the Federal Trade Commission; (2) filing a police report and requesting a copy of that report; and (3) visiting IdentityTheft.gov to report the issue and get recovery steps.

Contact relevant authorities – You may contact the below resources to (1) get more information on fraud alerts or security freezes and (2) learn more about protecting yourself from fraud or identity theft.

Equifax
P.O. Box 740241
Atlanta, GA 30374
(800) 685-1111
www.equifax.com

Experian
P.O. Box 9701
Allen, TX 75013
(888) 397-3742
www.experian.com

TransUnion
P.O. Box 2000
Chester, PA 19016
(888) 909-8872
www.transunion.com

Federal Trade Commission
600 Pennsylvania Ave. NW
Washington, DC 20580
(202) 326-2222
www.ftc.gov

Maryland Attorney General
200 St. Paul Place, 25th Floor
Baltimore, MD 21202
(888) 743-0023
www.marylandattorneygeneral.gov

North Carolina Attorney General
9001 Mail Service Center
Raleigh, NC 27699
(919) 716-6400
www.ncdoj.gov

You can also find your Attorney General's contact information at: <https://www.usa.gov/state-attorney-general>.

FOR MORE INFORMATION

Should you have any questions or concerns, you contact us toll-free at 877-704-6279; choose option 1, then option 2 and one of our representatives will be happy to assist you. Thank you for your understanding and patience.

Sincerely,

John Buchanan
EVP & General Counsel