KING & SPALDING

King & Spalding LLP
1180 Peachtree Street, NE
Atlanta, Georgia 30309
Tel: +1 404 572 4600
Fax: +1 404 572 5100
www.kslaw.com

Misty Peterson
Counsel
Direct Dial: +1 404 572 4939
Direct Fax: +1 404 572 5100
mpeterson@kslaw.com

January 4, 2023

Aaron Frey, Maine Attorney General
Via https://appengine.egov.com/apps/me/maine/ag/reportingform

Re: Notice of Security Incident Affecting OneAmerica Financial Partners, Inc. ("OneAmerica")/ The State Life Insurance Company

To all whom it may concern,

We write on behalf of OneAmerica regarding a recent security incident.

On July 15, 2022, OneAmerica learned that phishing messages were being sent from a user's OneAmerica email account. Upon discovery, OneAmerica immediately launched a comprehensive investigation to determine the cause and scope of the incident and retained leading cybersecurity experts to assist with its investigation. OneAmerica also immediately secured the impacted email account, took steps to track and confirm the permanent deletion of any suspected phishing emails, forced password resets for OneAmerica internal and external users, and contained the incident.

OneAmerica determined that the user's email account had been compromised by a phishing message from an external sender that was subsequently leveraged by an unauthorized third-party to send messages to other recipients. However, the unauthorized third-party did not gain access to any of OneAmerica's systems.

When the forensic investigation was concluded, although there was no evidence that personal information was accessed, OneAmerica undertook an extensive analysis of the affected user's mailbox to determine what data could have been affected, and, in the abundance of caution, thereafter manually searched for addresses across multiple databases in order to identify, locate, and notify those whose information could have been affected.

Based on its investigation, OneAmerica determined that the personal information for a small number of individuals contained in certain files located in the user's mailbox may have included the following data elements, in varying combinations: first and last name, and/or one or more of the following: date of birth, treatment information/diagnosis, prescription information, policy number, MRN/patient ID, and/or incidental health reference.

For a very small subset of those individuals, the personal information contained in those files may have included, in varying combinations: Social Security Number; Account Number, Routing Number, and Financial Institution Name; Credit/Debit Card Number, Security Code/PIN, Expiration Date; and/or Passport or U.S. Alien Registration Number.

Although OneAmerica has no reason to believe that any access or misuse of this information has occurred or will occur, it is notifying individuals whose personal information may have been accessed and offering them a complimentary subscription to Kroll's credit and identity monitoring services. On December 5, 2022, the Company identified two (2) Maine residents whose information was in the affected user's mailbox. OneAmerica began mailing notifications from December 31, 2022-January 4, 2023. An unaddressed copy of the letter is attached. OneAmerica has also established a call center to answer consumers' questions ((855) 624-3836). While this investigation was a time-consuming process, it was important that potentially impacted individuals were identified and their contact information gathered into a consistent format for notification, and it was necessary to ensure appropriate precautions and next steps were taken.

OneAmerica remains committed to protecting consumers' personal information and assisting those who may have been affected by this incident. OneAmerica is providing notices to individuals and the Department of Health and Human Services Office of Civil Rights pursuant to 45 CFR §§ 164.400-414 and applicable state laws. By virtue of this notice, OneAmerica does not waive any rights and reserves all rights under such laws. Please do not hesitate to contact me if you have any questions regarding this letter.

Sincerely,

s/Misty L. Peterson

Enclosures

<<Date>> (Format: Month Day, Year)

<<first_name>> <<middle_name>> <<last_name>> <<suffix>>
<<address_1>>
<<address_2>>
<<city>>, <<state_province>> <<postal_code>>
<<country>>

NOTICE OF DATA BREACH

Dear <<first_name>> <<middle_name>> <<last_name>> <<suffix>>,

We are writing to inform you of a security incident involving the unauthorized access of a user's email account that may have affected the privacy of some of your personal information. We want you to understand what happened and the steps we have taken to address this issue.

Although we have no reason to believe that any access to or misuse of this information has occurred or will occur, we have set forth additional steps that can be taken to help protect your personal information. We have also included in this letter instructions on how to activate complimentary identity monitoring services.

What Happened

On July 15, 2022, OneAmerica learned that phishing messages were being sent from a user's OneAmerica email account. Upon discovery, OneAmerica immediately launched a comprehensive investigation to determine the cause and scope of the incident and retained leading cybersecurity experts to assist with its investigation. OneAmerica also immediately secured the impacted email account, took steps to track and confirm the permanent deletion of any suspected phishing emails, and forced password resets for OneAmerica internal and external users.

OneAmerica determined that the user's email account had been compromised by a phishing message from an external sender that was subsequently leveraged by an unauthorized third-party to send messages to other recipients. The unauthorized third-party did not gain access to any of OneAmerica's systems.

Although there is no evidence that personal information was accessed, OneAmerica undertook an extensive analysis of the affected user's mailbox to determine what data could have been affected, and, in the abundance of caution, thereafter manually searched for addresses across multiple databases in order to identify, locate, and notify those whose information could have been affected. On December 5, 2022, the Company identified an extremely limited number of individuals whose information was in the affected user's mailbox.

What Information Was Involved

Based on the investigation, we identified some of your personal information in the user's mailbox, including the following data elements: <<b2b_text_1 (data elements)>><<b2b_text_2 (data elements cont.)>>.

What We Are Doing

As discussed above, upon learning of the incident, we took swift action in response by securing the impacted user's mailbox, deleting any suspected phishing emails, forcing password resets for OneAmerica internal and external users, and containing the incident. We also enhanced our cybersecurity by adding additional monitoring and detection tools as safeguards against cyber threats.

Further, while there is no evidence that your information was accessed, in the abundance of caution we have secured the services of Kroll to provide identity monitoring at no cost to you for one year. Kroll is a global leader in risk mitigation and response, with extensive experience helping people who have sustained an unintentional exposure of confidential data. Your identity monitoring services include Credit Monitoring, Fraud Consultation, and Identity Theft Restoration.

Visit **https://enroll.krollmonitoring.com** to activate and take advantage of your identity monitoring services.

You have until <<b2b_text_6 (activation date)>> to activate your identity monitoring services.

Membership Number: <<Membership Number s_n>>

For more information about Kroll and your Identity Monitoring services, you can visit info.krollmonitoring.com. Additional information describing your services is included with this letter.

Please also review the "What You Can Do" section included with this letter below. This section describes additional steps you can take to help protect your information, including recommendations by the Federal Trade Commission regarding identity theft protection and details on how to place a fraud alert or a security freeze on your credit file.

What You Can Do

Order Your Free Credit Report

To order your free annual credit report, visit www.annualcreditreport.com, call toll-free at (877) 322-8228, or complete the Annual Credit Report Request Form on the U.S. Federal Trade Commission's (FTC) website at www.ftc.gov and mail it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. The three credit bureaus (Equifax, Experian, and TransUnion) provide free annual credit reports only through the website, toll-free number, or request form. You may also purchase a copy of your credit report by contacting any of the credit reporting agencies below:

- Equifax www.equifax.com (800) 685-1111
- Experian www.experian.com (888) 397-3742
- TransUnion www.transunion.com (800) 916-8800

Upon receiving your credit report, review it carefully. Errors may be a warning sign of possible identity theft. Here are a few tips of what to look for:

- Look for accounts you did not open.
- Look in the "inquiries" section for names of creditors from whom you have not requested credit. Some companies bill under names other than their store or commercial names; the credit bureau will be able to tell if this is the case.
- Look in the "personal information" section for any inaccuracies in information (such as home address and Social Security Number).

If you see anything you do not understand, call the credit bureau at the telephone number on the report. You should notify the credit bureaus of any inaccuracies in your report, whether due to error or fraud, as soon as possible so the information can be investigated and, if found to be in error, corrected. If there are accounts or charges you did not authorize, immediately notify the appropriate credit bureau by telephone and in writing. Information that cannot be explained should also be reported to your local police or sheriff's office because it may signal criminal activity. We encourage you to take advantage of these protections and remain vigilant for incidents of fraud and identity theft, including regularly reviewing and monitoring your credit reports and account statements.

If you detect any unauthorized transactions in any of your financial accounts, promptly notify the appropriate payment card company or financial institution. If you detect any incidence of identity theft or fraud, promptly report the matter to your local law enforcement authorities (from whom you can obtain a police report), state Attorney General, and the Federal Trade Commission (FTC). You can contact the FTC to learn more about how to protect yourself from becoming a victim of identity theft by using the contact information below:

Federal Trade Commission Bureau of Consumer Protection
600 Pennsylvania Avenue NW Washington, DC 20580
(877) IDTHEFT (438-4338) / www.ftc.gov/idtheft

Placing a Security Freeze

You have a right to place a "security freeze" on your credit report, which will prohibit a consumer reporting agency from releasing information in your credit report without your express authorization. The security freeze is designed to prevent

credit, loans, and services from being approved in your name without your consent. However, you should be aware that using a security freeze to take control over who gets access to the personal and financial information in your credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit.

You can place, temporarily lift, or permanently remove a security freeze on your credit report online, by phone, or by mail. You will need to provide certain personal information, such as address, date of birth, and Social Security number to request a security freeze and may be provided with a unique personal identification number (PIN) or password, or both, that can be used by you to authorize the removal or lifting of the security freeze. Information on how to place a security freeze with the credit reporting agencies is also contained in the links below:

- https://www.equifax.com/personal/credit-report-services/
- https://www.experian.com/freeze/center.html
- https://www.transunion.com/credit-freeze

As of December 5, 2022, the reporting agencies allow you to place a credit freeze through the online, physical mail and phone numbers and request that you provide the information listed below. Where possible, please consult the websites listed above for the most up-to-date instructions.

Reporting Agency	Online	Physical Mail	Phone Number
Equifax	***Freeze request may be submitted via your myEquifax account, which you can create here***: https://my.equifax.com/consumer-registration/UCSC/#/personal-info	***Mail the Equifax Freeze Request Form to***: Equifax Information Services LLC P.O. Box 105788 Atlanta, GA 30348-5788 ***Form may be found here***: https://assets.equifax.com/assets/personal/Security_Freeze_Request_Form.pdf	888-298-0045
Experian	***Freeze request may be submitted here***: https://www.experian.com/ncaconline/freeze	***Mail the request to***: Experian Security Freeze, P.O. Box 9554, Allen, TX 75013 ***Request must include:*** • Full Name • Social security number • Complete address for last 2 years • Date of birth • One copy of a government issued identification card, such as a driver's license, state ID card, etc. • One copy of a utility bill, bank or insurance statement, etc.	888-397-3742
TransUnion	***Freeze request may be submitted via your TransUnion account, which you can create here***: https://service.transunion.com/dss/orderStep1_form.page?	***Mail the request to***: TransUnion P.O. Box 160 Woodlyn, PA 19094 ***Request must include:*** • Full Name • Social security number • Complete address	888-909-8872

Fees associated with placing, temporarily lifting, or permanently removing a security freeze no longer apply at nationwide consumer reporting agencies.

Placing a Fraud Alert

To protect yourself from possible identity theft, you have the right to place an initial or extended fraud alert on your 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 you are a victim of identity theft, you are entitled to an extended fraud alert, which is a fraud alert lasting

seven years. You may obtain additional information from the FTC and the credit reporting agencies listed above about placing a fraud alert and/or security freeze on your credit report.

***MASSACHUSETTS RESIDENTS ONLY*:**

Obtain a Police Report

Although this incident involved a phishing email, for security incidents generally, you have the right to obtain a copy of a police report.

***RHODE ISLAND RESIDENTS ONLY*:**

File or Obtain a Police Report

Although this incident involved a phishing email, for security incidents generally, you have the right to file or obtain a copy of a police report.

Attorney General

You may obtain information about avoiding identity theft at:

Office of the State of Rhode Island Attorney General
150 South Main Street
Providence, Rhode Island 02903
(401) 274-4400
www.riag.ri.gov]

NORTH CAROLINA RESIDENTS ONLY:

You may obtain information about avoiding identity theft at:

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

On behalf of OneAmerica, we regret any inconvenience or concern this may have caused. If you have any questions concerning this incident, please call (855) 624-3836, Monday through Friday from 8:00 a.m. to 5:30 p.m. Central Time, excluding major U.S. holidays. Please have your membership number ready.

Sincerely,

OneAmerica

KROLL

TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES

You have been provided with access to the following services from Kroll:

Triple Bureau Credit Monitoring

You will receive alerts when there are changes to your credit data at any of the three national credit bureaus—for instance, when a new line of credit is applied for in your name. If you do not recognize the activity, you'll have the option to call a Kroll fraud specialist, who will be able to help you determine if it is an indicator of identity theft.

Fraud Consultation

You have unlimited access to consultation with a Kroll fraud specialist. Support includes showing you the most effective ways to protect your identity, explaining your rights and protections under the law, assistance with fraud alerts, and interpreting how personal information is accessed and used, including investigating suspicious activity that could be tied to an identity theft event.

Identity Theft Restoration

If you become a victim of identity theft, an experienced Kroll licensed investigator will work on your behalf to resolve related issues. You will have access to a dedicated investigator who understands your issues and can do most of the work for you. Your investigator will be able to dig deep to uncover the scope of the identity theft, and then work to resolve it.

Kroll's activation website is only compatible with the current version or one version earlier of Chrome, Firefox, Safari and Edge.

To receive credit services, you must be over the age of 18 and have established credit in the U.S., have a Social Security number in your name, and have a U.S. residential address associated with your credit file.

Breach Tracking Number: **NZ745PHFJJ**

Thank you for filing a breach notification via the website of the Office for Civil Rights (OCR) at the Department of Health and Human Services. This is an automated response to acknowledge receipt of your breach notification. Your breach notification will be assigned to an OCR staff member for review and appropriate action. If OCR has any questions about the breach notification you submitted, we will contact you directly. Otherwise, you will receive a written response indicating whether or not OCR has accepted your breach notification for investigation.

Please do not fax, email, or mail a copy of this breach notification to us as that may delay the processing of your breach notification.

If you have any additional information to add to your breach notification, you may call 1-800-368-1019. Please reference the number given by OCR when submitting your breach notification.

* Breach Affecting: Fewer Than 500 Individuals
* Report Type: Initial Breach Report

* Are you a Business Associate filing on behalf of a Covered Entity? Yes

---

Business Associate

Completion of this section is required if the breach occurred at or by a Business Associate or if you are filing on behalf of a Covered Entity.

Name of Business Associate:	OneAmerica Financial Partners, Inc.
Street Address Line 1:	One American Square
Street Address Line 2:	P.O. Box 368
City:	Indianapolis
State:	Georgia
ZIP:	46206-0368

Business Associate Point of Contact Information

* First Name: Misty * Last Name: Peterson
* Email: mpeterson@kslaw.com

* Phone Number: (Include area code):

Contact Phones

Phone Number	Usage
(404) 572-4939 x_____	Work

Enter the contact information for all Covered Entities you are filing on behalf of.

Covered Entity 1

* Name of Covered Entity: The State Life Insurance Company
* Street Address Line 1: One American Square
Street Address Line 2: P.O. Box 368
* City: Indianapolis

* State: Indiana
* ZIP: 46206-0368

Business Associate Point of Contact Information

* First Name: Misty * Last Name: Peterson
* Email: mpeterson@kslaw.com
* Phone Number: (Include area code):

Contact Phones

Phone Number	Usage
(404) 572-4939	Work

* Type of Covered Entity: Health Plan

* Breach Start Date: 07/15/2022 * Breach End Date: 09/28/2022
* Discovery Start Date: 09/28/2022 * Discovery End Date: 12/05/2022
* Approximate Number of Individuals Affected by the Breach: 384

---

* Type of Breach: Unauthorized Access/Disclosure

---

* Location of Breach: Email

---

* Type of Protected Health Information Involved in Breach:

Clinical
Demographic
Financial

* Clinical

Diagnosis/Conditions
Medications
Other Treatment Information

* Demographic

Date of Birth
Drivers License
Name
SSN
Other Identifier

* Financial

Credit Card/Bank Acct #
Other Financial Information

---

* Brief Description of the Breach: On July 15, 2022, OneAmerica learned that phishing messages were being sent from a user's OneAmerica email account. Upon discovery, OneAmerica immediately launched a comprehensive investigation to determine the cause and scope of the incident and retained leading cybersecurity experts to assist with its investigation. OneAmerica also immediately secured the impacted email account, took steps to track and confirm the permanent deletion of any suspected phishing

emails, and forced password resets for OneAmerica internal and external users. OneAmerica determined that the user's email account had been compromised by a phishing message from an external sender that was subsequently leveraged by an unauthorized third-party to send messages to other recipients. The unauthorized third-party did not gain access to any of OneAmerica's systems. Although there is no evidence that personal information was accessed, OneAmerica undertook an extensive analysis of the affected user's mailbox to determine what data could have been affected, and, in the abundance of caution, thereafter manually searched for addresses across multiple databases in order to identify, locate, and notify those whose information could have been affected. On December 5, 2022, the Company identified 384 individuals whose information was in the affected user's mailbox. OneAmerica began notifying those individuals thereafter. Although this investigation was a time-consuming process, it was important that potentially impacted individuals were identified and their contact information gathered into a consistent format for notification, and it was necessary to ensure appropriate precautions and next steps were taken. Based on its investigation, OneAmerica determined that the personal information for a small number of individuals contained in certain files located in the user's mailbox may have included the following data elements, in varying combinations: first and last name, and/or one or more of the following: date of birth, treatment information/diagnosis, prescription information, policy number, MRN/patient ID, and/or incidental health reference. For a very small subset of those individuals, the personal information contained in those files may have included, in varying combinations: Social Security Number; Account Number, Routing Number, and Financial Institution Name; Credit/Debit Card Number, Security Code/PIN, Expiration Date; and/or Passport or U.S. Alien Registration Number.

---

* Safeguards in Place Prior to Breach:	Privacy Rule Safeguards (Training, Policies and Procedures, etc.) Security Rule Administrative Safeguards (Risk Analysis, Risk Management, etc.) Security Rule Physical Safeguards (Facility Access Controls, Workstation Security, etc.) Security Rule Technical Safeguards (Access Controls, Transmission Security, etc.)

* Individual Notice Provided Start Date:	12/31/2022	Individual Notice Provided Projected/Expected End Date:	01/04/2023
Was Substitute Notice Required?	No		
Was Media Notice Required?	No		

---

* Actions Taken in Response to Breach:	Adopted encryption technologies Changed password/strengthened password requirements Implemented new technical safeguards Provided individuals with free credit monitoring Took steps to mitigate harm Trained or retrained workforce members Other

* Describe Other Actions Taken:	Upon discovery, OneAmerica immediately launched a comprehensive investigation to determine the cause and scope of the incident and retained leading cybersecurity experts to assist with its investigation. OneAmerica also immediately secured the impacted email account, took steps to track and confirm the permanent deletion of any suspected phishing emails, forced password resets for OneAmerica internal and external users, and contained the incident.

Under the Freedom of Information Act (5 U.S.C. §552) and HHS regulations at 45 C.F.R. Part 5, OCR may be required to release information provided in your breach notification. For breaches affecting more than 500 individuals, some of the information provided on this form will be made publicly available by posting on the HHS web site pursuant to § 13402(e)(4) of the Health Information Technology for Economic and Clinical Health (HITECH) Act (Pub. L. 111-5). Additionally, OCR will use this information, pursuant to § 13402(i) of the HITECH Act, to provide an annual report to Congress regarding the number and nature of breaches that are reported each year and the actions taken to respond to such breaches. OCR will make every effort, as permitted by law, to protect information that identifies individuals or that, if released, could constitute a clearly unwarranted invasion of personal privacy.

I attest, to the best of my knowledge, that the above information is accurate.

* Name: Misty Peterson Date: *01/04/2023*