ONEAMERICA®

AMERICAN UNITED LIFE INSURANCE COMPANY®
a ONEAMERICA® company
One American Square, P.O. Box 368
Indianapolis, IN 46206-0368

Phone (317) 285-1877

October 7, 2020
VIA FIRST CLASS MAIL

Consumer Protection Bureau
Office of the Attorney General
33 Capitol Street
Concord, NH 03301

Re: *Notification Pursuant to New Hampshire's Breach Notification Statute*

To Whom It May Concern:

I am writing on behalf of One America Financial Partners, Inc. ("OneAmerica") and its vendor Praxis Consulting, Inc. ("Praxis") to notify you of an incident that potentially affected 1 individual in New Hampshire.

Praxis is a firm OneAmerica utilizes for claims processing and subrogation activities, and it was victim of a phishing attack in which an unauthorized party gained access to a single company e-mail account from June 29, 2020 to July 7, 2020. Praxis identified the unauthorized access on July 7, 2020 and quickly shut off access to the account and began an inquiry into the nature and scope of the event. Praxis brought in outside cybersecurity experts and legal counsel to conduct a more detailed review of the incident. Through its investigation with outside experts, Praxis found no evidence that information about specific individuals was downloaded or viewed without authorization, but information related to claimants was potentially accessible to the unauthorized party. Therefore, Praxis worked with its experts and counsel to identify potentially affected individuals and provided OneAmerica with the full list of these OneAmerica claimants on September 15, 2020.

Forensic evidence indicates that the unauthorized party mainly used the Praxis employee e-mail account for spamming or email purposes; therefore, Praxis believes the risk that personal information was accessed or compromised is low, but in theory that party could have had access to certain personal information, including individuals' health information, Social Security numbers, date of birth, address, and policy number.

Praxis has assured us that they are enhancing their safeguards to mitigate the risk of future attacks, including updating its security systems and implementing multi-factor authentication on all e-mail accounts. Praxis stated that it is also updating its cybersecurity policies and procedures to help respond to and thwart future phishing attacks.

Praxis, on behalf of OneAmerica, is notifying each of the impacted individuals and providing them with details regarding the incident on or before October 15, 2020.

While Praxis and OneAmerica are not aware of any instances of fraud or identity theft as a result of this incident, Praxis has arranged for identity protection and credit monitoring services for one year for the individuals in New Hampshire that may have been impacted.

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

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

RE: Notice of Data Breach

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

Praxis Consulting, Inc. ("Praxis") provides claim processing services for American United Life Insurance Company, a OneAmerica Company, ("OneAmerica") and is writing on behalf of OneAmerica because we both value and respect the privacy of your information. We are writing to advise you of a recent incident that involved Praxis and some of your personal information, advise you about the steps that we have taken to address this incident, and provide you with guidance on what you can do to protect yourself.

What Happened? Praxis was the victim of a phishing attack in which an unauthorized party gained access to a single company e-mail account from June 29, 2020 to July 7, 2020. Praxis identified the unauthorized access on July 7, 2020 and quickly shut off access to the account and began an inquiry into the nature and scope of the event. Praxis also brought in outside cybersecurity experts and legal counsel to conduct a more detailed review of the incident. Through its investigation with outside experts, Praxis found no evidence that your specific information was downloaded or viewed without authorization, but information related to claimants was potentially accessible to the unauthorized party. Therefore, Praxis worked with its experts and counsel to identify potentially affected individuals and provide OneAmerica with the full list of these OneAmerica claimants on September 15, 2020.

What Information Was Involved? Forensic evidence indicates that the unauthorized party mainly used the Praxis employee e-mail account for spamming or email purposes; therefore, Praxis believes the risk that your data was accessed or compromised is low, but in theory that party could have had access to certain personal information, including your health information, Social Security number, date of birth, address, and policy number.

What We Are Doing Praxis is updating its security systems, including implementing multi-factor authentication on all e-mail accounts. Praxis is also updating its cybersecurity policies and procedures to help thwart future phishing attacks. The mailing of this notice was not delayed by law enforcement. Also, to assist you in protecting your information, we are offering you a complimentary one-year membership in identity monitoring through Kroll. This product provides you with identity monitoring services focused on immediate identification and resolution of identity theft. Your services include Credit Monitoring, Web Watcher, Fraud Consultation, and Identity Theft Restoration.

What You Can Do To activate your membership and start monitoring your personal information, please follow the steps below:

Visit **https://enroll.idheadquarters.com** to activate and take advantage of your identity monitoring services.
*You have until **January 11, 2021** to activate your identity monitoring services.*
Membership Number: <<Member ID>>

Additional information describing your services is included with this letter.

For More Information Please review the enclosed attachment called *Preventing Identity Theft and Fraud* for more information on ways to help protect against the potential misuse of your information. Again, we take the security of your information in our care very seriously, and we regret any concern or inconvenience this incident may cause you. If you have additional questions, please contact us at 978-806-2226 or email us at breachinfo@praxisconsulting.com.

Sincerely,

Alison Stackpole

PREVENTING IDENTITY THEFT AND FRAUD

We encourage you to remain vigilant against incidents of identity theft and fraud, to review your account statements, and to monitor your credit reports for suspicious activity. Immediately report any suspicious activity to your bank or credit union. If you do find suspicious activity on your credit reports or other statements, call your local police or sheriff's office or state Attorney General and file a report of identity theft. You have a right to a copy of the police report, and you may need to give copies of the police report to creditors to clear up your records and also to access some services that are free to identity theft victims.

Under the U.S. Fair Credit Reporting Act and other laws, you have certain rights that can help protect yourself from identity theft. Many of these are explained in this document and at www.identitytheft.gov/Know-Your-Rights. For example, you are entitled to one free credit report annually from each of the three major credit reporting bureaus. To order your free credit report, visit www.annualcreditreport.com or call toll-free, 1-877-322-8228. You may also contact the three major credit bureaus directly to request a free copy of your credit report.

At no charge, you can have these credit bureaus place a short-term or an extended "fraud alert" on your file that alerts creditors to take additional steps to verify your identity prior to granting credit in your name. Note, however, that because it tells creditors to follow certain procedures to protect you, it may also delay your ability to obtain credit while the agency verifies your identity. As soon as one credit bureau confirms your fraud alert, the others are notified to place fraud alerts on your file. Should you wish to place a fraud alert, or should you have any questions regarding your credit report, please contact any one of the agencies listed below.

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

You may also place a security freeze on your credit reports, free of charge. A security freeze, also known as a "credit freeze," prohibits a credit bureau from releasing any information from a consumer's credit report without the consumer's written authorization. However, please be advised that placing a security freeze on your credit report may delay, interfere with, or prevent the timely approval of any requests you make for new loans, credit mortgages, employment, housing, or other services. But unlike a fraud alert, you must separately place a security freeze on your credit file at **each** bureau. You can use the following addresses and contact information to place a security freeze with each major credit bureau:

Equifax Security Freeze. 1-800-685-1111. P.O. Box 1057881, Atlanta, GA 30348-0241. www.equifax.com/personal/credit-report-services/credit-freeze/;

Experian Security Freeze. 1-888-EXPERIAN or 1-888-397-3742. P.O. Box 9554, Allen, TX 75013. www.experian.com/freeze/center.html; or

TransUnion. 1-800-680-7289. Fraud Victim Assistance Division, P.O. Box 2000, Chester, PA 19022-2000. www.transunion.com/credit-freeze.

In order to request a security freeze, you may need to supply your full name (including middle initial, as well as Jr., Sr., II, III, etc.), date of birth, Social Security number, all addresses for up to five previous years, email address, a copy of your state identification card or driver's license, and a copy of a utility bill, bank or insurance statement, or other statement to show proof of your current address. If you are a victim of identity theft, include a copy of the police report, investigative report, or complaint to a law enforcement agency concerning your identity theft.

The credit reporting agencies must place a security freeze on your credit report within one (1) business day after receiving a request by phone or secure electronic means, and within (3) business days after receiving your request by mail. The credit bureaus must then send written confirmation to you within five (5) business days of placing the security freeze, along with information about how to remove or lift the security freeze in the future.

You can further educate yourself regarding identity theft, fraud alerts, freezes, and the steps you can take to protect yourself by contacting the Federal Trade Commission or your state Attorney General. The Federal Trade Commission encourages those who discover their information has been misused to file a complaint with them. Instances of known or suspected identity theft should be reported to law enforcement or your state Attorney General as well.

The Federal Trade Commission can be reached at:

Federal Trade Commission
Consumer Resource Center
600 Pennsylvania Avenue NW
Washington, DC 20580
1-877-ID-THEFT (1-877-438-4338)
TTY: 1-866-653-4261
www.identitytheft.gov or www.ftc.gov

OTHER IMPORTANT INFORMATION

You may also file a report with your local police or the police in the community where the identity theft took place. Further, you are entitled to request a copy of the police report filed in this matter.

For California residents:

You can visit the California Office of Privacy Protection (www.oag.ca.gov/privacy) for additional information on protection against identity theft.

For Indiana residents:

You can find more information about avoiding identity theft on the Indiana attorney general's website, https://secure.in.gov/apps/ag/idtheftprevtoolkit/Login.aspx. The attorney general's office can also be contacted by calling (317) 232-6330 or mailing correspondence to 200 W. Washington Street, Suite 219, Indianapolis, Indiana 46204.

For Iowa residents:

You are advised to report any suspected identity theft to law enforcement or to the Iowa Attorney General.

For Maryland residents:

You may obtain information about avoiding identity theft at: Office of the State of Maryland Attorney General 200 St. Paul Place Baltimore, MD 21202 1-888-743-0023, www.marylandattorneygeneral.gov.

For North Carolina residents:

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.

For New Mexico residents:

The Fair Credit Reporting Act provides certain rights in addition to the right to receive a copy of your credit report (including a free copy once every 12 months), including the right to ask for a credit score, dispute incomplete or inaccurate information, limit "prescreened" offers of credit and insurance, and seek damages from violators. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it.

For Oregon residents:

The Oregon Department of Justice can also provide information about preventing identity theft. The address is Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096 and its telephone number is (503) 378-4400, www.doj.state.or.us.

For Rhode Island residents:

The Rhode Island Attorney General's Office can also provide information about preventing identity theft. The attorney general's address is Office of the Attorney General, 150 South Main Street, Providence, Rhode Island 02903 and its telephone number is (401) 274-4400, http://www.riag.ri.gov.

For Colorado, Georgia, Maine, Maryland, Massachusetts, New Jersey, and Puerto Rico residents:

You may obtain one or more (depending on the state) additional copies of your credit report, free of charge. You must contact each of the credit bureaus directly to obtain such additional report(s).

Kroll | A Division of DUFF&PHELPS

TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES

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

Single Bureau Credit Monitoring

You will receive alerts when there are changes to your credit data—for instance, when a new line of credit is applied for in your name. If you do not recognize the activity, you will 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.

Web Watcher

Web Watcher monitors internet sites where criminals may buy, sell, and trade personal identity information. An alert will be generated if evidence of your personal identity information is found.

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.

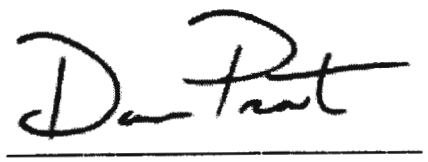
Kroll's activation website is only compatible with the current version or one version earlier of Chrome, Firefox, Safari and Edge.
To receive credit services, you must be over the age of 18 and have established credit in the U.S., have a Social Security number in your name, and have a U.S. residential address associated with your credit file.

October 7th, 2020

If you have any questions or need further information, please feel free to contact me at 317-289-8984 or Daniel.Prout@OneAmerica.com A copy of the Data Breach Notification Letter to individuals is enclosed for your consideration.

Very truly yours,

Sincerely,



Daniel T. Prout | Privacy Officer and Legal Counsel |
OneAmerica Financial Partners, Inc.

US.129555461.01