Notice of Possible Unauthorized Access to Small Number of Agent Email Accounts

May 25, 2018

American Family Life Assurance Company of Columbus and Continental American Insurance Company (collectively, "Aflac") have discovered that potential unauthorized access to certain Office 365 email accounts occurred between Jan. 17, 2018, and April 2, 2018. These accounts were on a business email system hosted by a third party. The incident was discovered through Aflac's data security detection systems.

Based on our review, Aflac email accounts of a small number of our independent contractor insurance agents appear to have been accessed by an unauthorized third party. These agents are not employed by Aflac; they are independent contractors who help us provide services to you. As our HIPAA Business Associates, these agents have also agreed to safeguard and protect your information. These agents' email accounts were hosted by Microsoft Office 365, which is also a third-party vendor to Aflac.

Data analysis, which was completed April 25, 2018, showed that some of the email accounts may have included HIPAA protected health information (PHI) and other personally identifiable information (PII). We immediately instituted multiple robust controls to mitigate and remediate the activity, including resetting passwords, isolating the specific email accounts and contacting the affected insurance agents. We also continue to work with our independent contractor agents and vendors to implement strong security measures. Based on our review, the information in the accounts may have included the following: first and last name, home address, date of birth, policy/certificate number, group number, type of policy (such as life, hospital and dental), Social Security number (SSN) and bank account information. Some general health information as part of the application, enrollment or claims process may have also been involved. **We are not aware of any misuse of your personal or health information at this time.**

The incident did not appear to specifically target Aflac or Aflac's business operations, did not involve Aflac's internal system or network, and did not impact the integrity of your data contained in our system or network. Aflac is informing individuals whose personal and health information may have been involved by mailing a letter to their last known address. Aflac will also offer credit monitoring if an SSN, bank account or credit card information was involved. Policyholders may also wish to watch for any suspicious activity regarding their accounts and contact Aflac with any questions or concerns. We are also providing additional information about various steps individuals can take to protect against potential misuse of their information and to protect their identity. Since it is possible we may have insufficient contact information for some individuals, we are also providing notice on our website as permitted by HIPAA.

We deeply regret any inconvenience this incident may cause you, and we take this matter seriously. For the next 90 days, Aflac has set up a toll-free number (1-855-509-0822) so that individuals can ask questions, learn additional information, and find out whether their information was involved and, if so, what types. This toll-free number is open Monday through Friday between 8 a.m. and 8 p.m. Eastern time, except for U.S. holidays. This substitute notice and toll-free number will remain active for at least 90 days.

Although the incident occurred on a third-party email system, we are further enhancing our security measures as a result of this incident and plan to provide additional security training and education to our independent contractor insurance agents. A third-party team of forensics experts has been retained to assist with the investigation into this matter. Aflac has also reached out to Microsoft and law enforcement to let them know of the incident, which Aflac understands has affected other companies, as well. Thank you.

STEPS YOU CAN TAKE TO PROTECT YOUR PROTECTED HEALTH INFORMATION

Review your account statements. Carefully review statements sent to you from partners as well as from your insurance company to ensure that all of your account activity is valid. Report any questionable charges promptly to the partner's billing office at the phone number listed on the statement or, for insurance statements, to your insurance company.

Provide any updated personal information to your health care provider. Your health care provider's office will ask to see a photo ID to verify your identity. Please bring a photo ID with you to every appointment, if possible. Your provider's office will also ask you to confirm your date of birth, address, telephone and other pertinent information so that all of your information is up to date. Please be sure and tell your provider's office when there are any changes to your information. Carefully reviewing this information with your provider's office at each visit helps to avoid problems and to have them addressed quickly should there be any discrepancies.

Consult the Federal Trade Commission. For more guidance on general steps you can take to protect your information, you also can contact the Federal Trade Commission:

Website:	https://www.consumer.ftc.gov/topics/privacy-identity-online-security
Postal Address:	Federal Trade Commission 600 Pennsylvania Avenue, NW Washington, DC 20580
Telephone:	(202) 326-2222

STEPS YOU CAN TAKE TO PROTECT YOUR IDENTITY

Security freeze. A security freeze prohibits a credit bureau from releasing any information from your credit report without your written consent. Please be aware, however, that placing a security freeze on your credit report may delay or prevent the timely approval of any requests you make for new loans, credit, mortgages or other services. To place a security freeze on your file, you must send a written request to each of the three credit bureaus by regular, certified or overnight mail at the addresses below:

Equifax Security Freeze	Experian Security Freeze	TransUnion Security Freeze
P.O. Box 105788	P.O. Box 9554	P.O. Box 2000
Atlanta, GA 30348	Allen, TX 75013	Chester, PA 19016

When requesting a security freeze, you will need to provide the following information: (1) your full name; (2) your Social Security number; (3) your date of birth; (4) if you have moved in the past five years, the addresses where you have lived during that period; (5) proof of your current address, such as a current utility or telephone bill; and (6) a legible copy of your government-issued identification card, such as a state driver's license, state ID card or military ID card. If you have been a victim of identity theft and you provide the credit reporting agency with a valid police report, it cannot charge you to place, lift or remove a security freeze. In all other cases, the credit reporting agency may charge you up to $5 each to place, temporarily lift or permanently remove a security freeze. You will need to include payment by check, money order or major credit card. Do not send cash through the mail.

The credit reporting agencies have three business days after receiving your request to place a security freeze on your credit report. The credit bureaus also must send written confirmation to you within five business days and provide you with a unique personal identification number (PIN) or password, or both, that you can use to authorize the removal or lifting of the security freeze.

To lift the security freeze in order to allow a specific entity or individual access to your credit report, you must call or send a written request to the credit reporting agencies by mail and include proper identification (name, address and Social Security number) **and** the PIN number or password provided to you when you placed the security freeze, as well as the identities of those entities or individuals you would like to receive your credit report or the specific period of time you want the credit report to be available. The credit reporting agencies have three business days after receiving your request to lift the security freeze for those specific entities or individuals or for the specified period of time.

To remove the security freeze completely, you must send a written request to each of the three credit bureaus by mail and include proper identification (name, address and Social Security number) **and** the PIN number or password provided to you when you placed the security freeze. The credit bureaus have three business days after receiving your request to remove the security freeze.

Review your account statements. Carefully review your bank, credit card and other account statements every month to ensure that all of your account activity is valid. Report any questionable charges promptly and in writing to the card or account issuer.

Check your credit report. Check your credit report to ensure that all of your information is correct. You can obtain a free credit report once per year by visiting www.annualcreditreport.com or by calling 877-322-8228. If you notice any inaccuracies, contact the relevant credit bureau promptly at the telephone number listed on the report. You can also report any suspicious activity to your local law enforcement, in which case you should request a copy of the police report and retain it for your records.

Fraud alert. You have the right to request that the credit bureaus place a fraud alert on your file. A fraud alert tells creditors to contact you before opening any new accounts or increasing credit limits on your existing accounts. You need to contact only one of the three credit bureaus to place a fraud alert; the one you contact is required by law to contact the other two.

For fraud alerts, the credit bureaus can be reached at:

Equifax	Experian	TransUnion
P.O. Box 740241	P.O. Box 9532	P.O. Box 2000
Atlanta, GA 30374	Allen, TX 75013	Chester, PA 19016
800-525-6285	888-397-3742	888-909-8872
www.equifax.com	www.experian.com	www.transunion.com

Consult the Federal Trade Commission. For more guidance on steps you can take to protect your information, you also can contact the Federal Trade Commission at www.ftc.gov/idtheft, 877-ID-THEFT (877-438-4338) or at the Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue NW, Washington, D.C. 20580.