Morgan Lewis

Gregory T. Parks
Partner
215.963.5170
gregory.parks@morganlewis.com

December 4, 2023

VIA EMAIL TO CONSUMER@AG.IOWA.GOV

Consumer Protection Division
Security Breach Notifications
Office of the Attorney General of Iowa
1305 E. Walnut Street
Des Moines, Iowa 50319-0106

Re: Notice of Data Security Incident

Dear Office of the Attorney General:

This Firm represents the Pan-American Life Insurance Group ("PALIG"), and we are writing on their behalf to notify you of a recent data security incident impacting PALIG that involved the secure file transfer software tool MOVEit Transfer, provided by third-party vendor Progress Software. The incident affected 634 Iowa residents.

As you likely know, Progress Software announced a previously unknown, critical, zero-day vulnerability in MOVEit Transfer and recommended users disable the software until it could be patched due to a potential risk of data exposure. PALIG immediately ceased using MOVEit Transfer and disabled it in its system. Progress Software quickly released patches to remedy the vulnerability, which PALIG immediately and successfully deployed on all instances of the MOVEit Transfer applications within its environment. In parallel to the patching activity, PALIG immediately launched an investigation with the assistance of cyber experts to assess the scope of the potential exploitation of the vulnerability and notified law enforcement. The investigation revealed that an unauthorized third party appears to have taken files through PALIG's use of MOVEit transfer.

On October 5, 2023, PALIG determined that the impacted files appear to have included personal information of individuals and may have included names, addresses, social security numbers, dates of birth, driver's license numbers, contact information, medical and medical benefits information, subscriber numbers, certain biometric data, and financial account and credit card information. Notifications are being sent by mail to the affected individuals to explain what happened, what information was involved, what has been done, and how affected individuals can contact Experian with questions. Two years of credit monitoring is being offered to affected customers. PALIG is also giving notice to the US Department of Health and Human Services Office of Civil Rights.

PALIG carefully evaluates the cybersecurity posture of third-party software and will continue this effort. PALIG is also taking steps to further secure its use of all third-party transfer tools.

Further information about what mitigations have been completed to date and what further mitigations are recommended can be found in the enclosed notification that was sent to affected individuals via mail on December 4, 2023.

If you have any questions, please feel free to contact me.

Regards,

Gregory T. Parks

Enclosure

PAN AMERICAN LIFE INSURANCE GROUP
Return Mail Processing
PO Box 589
Claysburg, PA 16625-0589

December 4, 2023

[redacted]

Re: Notice of Data Security Incident

Dear [redacted]:

We are writing to notify you of a data security incident with the Pan-American Life Insurance Company (PALIC) that unfortunately involves some of your personal information. This letter is being sent to provide you with additional information and to advise you of services PALIC is offering at no charge to you to help protect your continued privacy.

It is important to note that we have no evidence at this time that your personal information has been used inappropriately or fraudulently, but we are sending this letter to tell you what happened, what information was involved, what we have done, and what you can do to address this situation.

What Happened?
Like many companies, PALIC used a third-party software application, MOVEit Transfer by Progress Software, to exchange files. Progress Software announced that it found a previously unknown vulnerability in MOVEit. PALIC immediately stopped use of MOVEit, secured its other systems, launched an investigation with the support of a leading cybersecurity firm, and notified law enforcement authorities. Our investigation revealed that an unauthorized third party used the vulnerability in MOVEit to take files that contain personal information, including yours.

What Information Was Involved?
After we were able to determine which files were impacted, we began a thorough review of those documents. This review was concluded on October 31, 2023, and we learned that some of your personal information was included in the files taken. The affected information may have included names, addresses, social security numbers, dates of birth, driver's license numbers, contact information, medical and medical benefits information, subscriber numbers, certain biometric data, and financial account and credit card information. We have no evidence that the personal information has been used in any way that can cause you harm.

What We Are Doing
Immediately upon learning of this incident, we took steps to mitigate the risk to our customers and launched an investigation and recovery effort with the assistance of cybersecurity experts and law enforcement. Forensic evidence showed no unauthorized activity outside of the MOVEit application. Determining whether information was compromised in any way has been one of the top priorities of this effort so that we could notify potentially affected individuals.

As a measure of added security and to help protect your identity, we are offering complimentary access to Experian IdentityWorks^{SM} for 24 months. If you believe there was fraudulent use of your information as a result of this incident and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent. If, after discussing your situation with an agent, it is determined that identity restoration support is needed then an Experian Identity Restoration agent is available to work with you to investigate and resolve each incident of fraud that occurred from the date of the incident (including, as appropriate, helping you with contacting credit grantors to dispute charges and close accounts; assisting you in placing a freeze on your credit file with the three major credit bureaus; and assisting you with contacting government agencies to help restore your identity to its proper condition).

Please note that Identity Restoration is available to you for 24 months from the date of this letter and does not require any action on your part at this time. The Terms and Conditions for this offer are located at www.ExperianIDWorks.com/restoration.

While identity restoration assistance is immediately available to you, we also encourage you to activate the fraud detection tools available through Experian IdentityWorks as a complimentary 24-month membership. This product provides you with superior identity detection and resolution of identity theft. To start monitoring your personal information, please follow the steps below:

- Ensure that you **enroll by** March 31, 2024 (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll: https://www.experianidworks.com/credit
- Provide your **activation code**: [redacted]

If you have questions about the product, need assistance with Identity Restoration that arose as a result of this incident, or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at 833-603-7671 by March 31, 2024. Be prepared to provide engagement number B109876 as proof of eligibility for the Identity Restoration services by Experian.

What You Can Do
To help protect your personal information, we strongly recommend you take the following steps:

- Enroll in the credit monitoring service that we are offering to you. This will enable you to get alerts about any efforts to use your name and personal information to establish credit and to block that credit from being established if you were not the one who initiated it.
- Carefully review statements sent to you by your bank, credit card company, or other financial institutions as well as government institutions like the Internal Revenue Service (IRS). Notify the sender of these statements immediately by phone and in writing if you detect any suspicious transactions or other activity you do not recognize.
- The attached **Reference Guide** describes additional steps that you can take and provides resources for additional information. We encourage you to read and follow these steps as well.

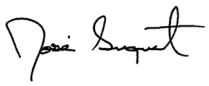
ADDITIONAL DETAILS REGARDING YOUR 24-MONTH EXPERIAN IDENTITYWORKS MEMBERSHIP

A credit card is not required for enrollment in Experian IdentityWorks. You can contact Experian immediately regarding any fraud issues, and have access to the following features once you enroll in Experian IdentityWorks:

- **Experian credit report at signup:** See what information is associated with your credit file. Daily credit reports are available for online members only.*
- **Credit Monitoring:** Actively monitors Experian file for indicators of fraud.
- **Identity Restoration:** Identity Restoration specialists are immediately available to help you address credit and non-credit related fraud.
- **Experian IdentityWorks ExtendCARE™:** You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- **$1 Million Identity Theft Insurance**:** Provides coverage for certain costs and unauthorized electronic fund transfers.

For More Information
We sincerely regret any inconvenience or concern caused by this incident. If you have further questions or concerns, or would like an alternative to enrolling online, please call 833-603-7671 toll-free Monday through Friday from 8 am – 10 pm Central or Saturday and Sunday from 10 am – 7 pm Central (excluding major U.S. holidays). Be prepared to provide your engagement number B109876.

Sincerely,



José S. Suquet
Chairman and CEO

* Offline members will be eligible to call for additional reports quarterly after enrolling.
** The Identity Theft Insurance is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

REFERENCE GUIDE

In the event that you suspect that you are a victim of identity theft, we encourage you to remain vigilant and consider taking the following steps:

Order Your Free Credit Report. To order your free 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 website at www.ftc.gov and mail it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. Do not contact the three credit bureaus individually; they provide your free report only through the website or toll-free number.

When you receive your credit report, review the entire report carefully. Look for any inaccuracies and/or accounts you don't recognize, and notify the credit bureaus as soon as possible in the event there are any.

You have rights under the federal Fair Credit Reporting Act ("FCRA"). These include, among others, the right to know what is in your file; to dispute incomplete or inaccurate information; and to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information. For more information about the FCRA, please visit https://www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf or www.ftc.gov.

Place a Fraud Alert on Your Credit File: To protect yourself from possible identity theft, consider placing a fraud alert on your credit file. A fraud alert helps protect you against the possibility of an identity thief opening new credit accounts in your name. When a merchant checks the credit history of someone applying for credit, the merchant gets a notice that the applicant may be a victim of identity theft. The alert notifies the merchant to take steps to verify the identity of the applicant. You can report potential identity theft to all three of the major credit bureaus by calling any one of the toll-free fraud numbers below. You will reach an automated telephone system that allows you to flag your file with a fraud alert at all three bureaus.

Equifax	P.O. Box 740241 Atlanta, Georgia 30374-0241	1-800-525-6285	www.equifax.com
Experian	P.O. Box 9532 Allen, Texas 75013	1-888-397-3742	www.experian.com
TransUnion	Fraud Victim Assistance Division P.O. Box 2000 Chester, Pennsylvania 19016	1-800-680-7289	www.transunion.com

Place a Security Freeze on Your Credit File. You have the right to place a "security freeze" on your credit file. A security freeze generally will prevent creditors from accessing your credit file at the three nationwide credit bureaus without your consent. You can request a security freeze free of charge by contacting the credit bureaus at:

Equifax	P.O. Box 740241 Atlanta, Georgia 30374-0241	www.equifax.com
Experian	P.O. Box 9554 Allen, Texas 75013	www.experian.com
TransUnion	Fraud Victim Assistance Division P.O. Box 2000 Chester, Pennsylvania 19016	www.transunion.com

The credit bureaus may require that you provide proper identification prior to honoring your request. In order to request a security freeze, you will need to provide the following information:

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.)
2. Social Security number
3. Date of birth
4. If you have moved in the past five (5) years, provide the addresses where you have lived over the prior 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, military identification, etc.)
7. If you are a victim of identity theft, include a copy of either the police report, investigative report, or complaint to law enforcement agency concerning identity theft.

0000001

Placing a security freeze on your credit file may delay, interfere with, or prevent timely approval of any requests you make for credit, loans, employment, housing or other services. For more information regarding credit freezes, please contact the credit reporting agencies directly.

Contact the U.S. Federal Trade Commission. If you detect any incident of identity theft or fraud, promptly report the incident to your local law enforcement authorities, your state Attorney General and the Federal Trade Commission ("FTC"). If you believe you identity has been stolen, the FTC recommends that you take these additional steps.

- Close the accounts that you have confirmed or believe have been tampered with or opened fraudulently. Use the FTC's ID Theft Affidavit (available at www.ftc.gov/idtheft) when you dispute new unauthorized accounts.
- File a local police report. Obtain a copy of the police report and submit it to your creditors and any others that may require proof of the identity theft crime.

You can learn more about how to protect yourself from becoming an identity theft victim (including how to place a fraud alert or security freeze) by contacting the FTC:

Federal Trade Commission
Consumer Response Center
600 Pennsylvania Avenue, NW
Washington, DC 20580
1-877-IDTHEFT (438-4338)
www.ftc.gov/idtheft

For District of Columbia Residents: You can obtain information from the FTC and the Office of the Attorney General for the District of Columbia about steps to take to avoid identity theft. You can contact the D.C. Attorney General at: 441 4th Street, NW, Washington, DC 200001, 202-727-3400, www.oag.dc.gov.

For Iowa Residents: State law advises you to report any suspected identity theft to law enforcement or to the Attorney General.

For Maryland Residents: You can obtain information from the Maryland Office of the Attorney General about steps you can take to help prevent identity theft. You can contact the Maryland Attorney General at: 200 St. Paul Place, Baltimore, MD 21202, 888-743-0023, www.oag.state.md.us.

For Massachusetts Residents: You have a right to request from us a copy of any police report filed in connection with this incident. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it. As noted above, you also have the right to place a security freeze on your credit report at no charge.

For New York Residents: You may also contact the following state agencies for information regarding security breach response and identity theft prevention and protection information:

New York Attorney General's Office
Bureau of Internet and Technology
(212) 416-8433
https://ag.ny.gov/internet/resource-center

NYS Department of State's Division of Consumer Protection
(800) 697-1220
https://www.dos.ny.gov/consumerprotection

For North Carolina Residents: You can obtain information from the Federal Trade Commission and the North Carolina Office of the Attorney General about steps you can take to help prevent identity theft. You can contact the North Carolina Attorney General at: 9001 Mail Service Center, Raleigh, NC 27699, 1-877-566-7226, www.ncdoj.gov.

For Oregon Residents: State laws advise you to report any suspected identity theft to law enforcement, as well as the Federal Trade Commission. You can contact the Oregon Attorney General at: Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, (877) 877-9392, www.doj.state.or.us.

For Rhode Island Residents: You can obtain information from the Rhode Island Office of the Attorney General about steps you can take to help prevent identity theft. You can contact the Rhode Island Attorney General at: 150 South Main Street, Providence, RI 02903, (401) 274-4400, www.riag.ri.gov. As noted above, you have the right to place a security freeze on your credit report at no charge, but note that consumer reporting agencies may charge fees for other services.