

# Morgan Lewis

**Gregory T. Parks**

Partner  
215.963.5170  
gregory.parks@morganlewis.com

March 11, 2021

**VIA US MAIL**

State of New Hampshire  
Office of the Attorney General  
33 Capitol Street  
Concord, NH 03301

Re: Notice of Data Security Incident

Dear Office of the Attorney General:

This Firm represents Pan-American Life Insurance Group and its affiliates ("PALIG") and we are writing to notify you of a recent data security incident that we confirmed on March 9, 2021 to have involved the exfiltration of some personal information. PALIG insures approximately 51 individuals in your state. We are performing more analysis, but currently believe that a relatively small percentage of individuals had information exfiltrated.

On February 19, 2021, PALIG detected suspicious activity within its computer systems. PALIG immediately took its computer network offline as part of its efforts to protect policyholder information, other data and its systems. This resulted in disruptions to PALIG's business. Since learning of this situation, PALIG has been taking steps to further protect and strengthen the security of its systems. PALIG also engaged third-party cyber experts to partner with its team to launch an investigation to better understand what happened and to prevent a similar incident in the future.

PALIG's investigation concluded that a phishing attempt resulted in malware being installed on PALIG's computer network. PALIG's existing defenses and early action prevented this malware from having its full intended effect and PALIG has taken steps to further enhance its security. On March 9, PALIG confirmed that some name, address and date of birth information was exfiltrated. In addition, based on our preliminary analysis, a relatively small percentage of individuals had more sensitive personal information exfiltrated. We will continue our analysis and will update you if our analysis changes. We will also provide specific direct notice and an offer of credit monitoring to any individuals whose more sensitive personal information was exfiltrated. There is no evidence that any of this information was misused for any fraudulent purposes as a result of this incident.

Because direct notice to all policyholders and other affected individuals whose information was just accessed but not exfiltrated would be impossible, infeasible or prohibitively expensive, PALIG is providing substitute notice by posting a notice on its website, issuing a press release on a national wire service covering all US states and territories, and including a reference to the website in

**Morgan, Lewis & Bockius LLP**

1701 Market Street  
Philadelphia, PA 19103-2921  
United States

📞 +1.215.963.5000  
📠 +1.215.963.5001

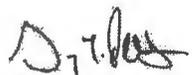
RECEIVED  
MAR 15 2021  
CONSUMER PROTECTION

State of New Hampshire  
Office of the Attorney General  
March 11, 2021  
Page 2

monthly or other periodic communications to policyholders where possible. To be clear, PALIG will be providing further direct notice to any individuals whose more sensitive personal information was actually exfiltrated. PALIG will also offer these individuals credit monitoring.

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

Regards,

A handwritten signature in black ink, appearing to read "G. T. Parks", written in a cursive style.

Gregory T. Parks

Enclosure

**3.11.2021**

## **INFORMATION REGARDING A DATA SECURITY INCIDENT**

At Pan-American Life Insurance Group, we take the privacy and security of our client information very seriously. We are sharing details about a data security incident, what happened, what information was involved, what we are doing to address it, the steps you can take to help protect information, and resources that we are making available to assist our clients.

### **What Happened?**

On February 19, 2021, we detected suspicious activity within our computer systems. We immediately took our computer network offline as part of our efforts to protect policyholder information, other data and our systems. This resulted in disruptions to our business. Since learning of this situation, we have been taking steps to further protect and strengthen the security of our systems. We also engaged third-party cyber experts to partner with our team to launch an investigation to better understand what happened and to prevent a similar incident in the future.

Our investigation confirmed that systems containing personal information were accessed without authorization. Our investigation concluded that a phishing attempt resulted in malware being installed on our computer network. Our existing defenses and early action prevented this malware from having its full intended effect and we have taken steps to further enhance our security. On March 9, 2021, we confirmed that some policyholder and beneficiary information, like name, address and date of birth was taken. It also appears that a relatively small percentage of policyholders and beneficiaries may have had more sensitive information taken, and we will be contacting those individuals directly by mail or email with more information. There is no evidence that any information was misused for fraudulent purposes as a result of this incident.

### **What Information Was Involved?**

Our systems contain various types of personal information related to the servicing of the policies we issue. More information regarding the specific information we collect is included in our Privacy Practices detailed below and more specifically addressed in the privacy policy notifications issued to policyholders periodically.

### **What Are We Doing?**

As soon as we discovered the incident, we took the steps previously described. We have also taken steps to increase the security of our systems. In addition, we are offering information in the reference guide below about steps you can take to help protect your personal information. Out of an abundance of caution, we are also offering additional services to individuals whose information was taken.

### **What Can You Do?**

We recommend that you review the guidance provided in the reference guide below about how to help protect your information.

Beginning on Friday, March 12, 2021, if you have questions or need assistance, please call US Toll Free Number 833-671-0405, Monday through Friday from 8:00AM 10:00PM Central Standard Time. Saturday and Sunday 10:00AM – 7:00PM Central Standard Time

## **Our Privacy Practices**

Pan-American Life Insurance Group (PALIG) and its affiliated companies are highly committed to protecting the privacy of its customers and the security of all confidential information entrusted to us. Depending on which of our products and services you ask us about, buy or use, different affiliated companies within our group will process your information.

This general privacy statement serves as a summary of our privacy practices, and serves to briefly notify you of the information we collect about you, how we use it, how we protect it, and your rights. For more details on the specific policies or practices that may apply to you, please select the appropriate country from the menu at the top of the page.

### **Information Collection, Protection, and Sharing**

- We collect personal information in connection with the products and services we offer. This may include information we receive on applications and other forms, such as name, date of birth, contact information, tax identification number, social security number, cedula or other government issued identification number, assets and income, medical and financial information, information about your transactions with our affiliated companies and information we receive from third-parties, including consumer reporting and inspection services.
- We process your data when necessary to provide the services set out in a contract, when it is in our or a third-party's legitimate interests, or when it is required or allowed by applicable law. When we process your sensitive personal data, it will be in line with applicable law, as necessary to provide you with our services, or with your permission.
- We will not rent or sell personal information to others but we may share your information as necessary within the PALIG Group, with relevant policyholders, and with our business associates who help us provide services to you. We will only share your information as allowed under applicable law.
- We are a global company, and where necessary we may allow your information to be shared with our affiliates or third-party service providers based in the United States and other countries. We will take steps to make sure that appropriate protection is in place to protect your information when it is transferred internationally.
- We keep your personal information in line with appropriate retention periods. The length of these periods is determined by relevant regulations, the information collected, and our obligations to you as a customer.
- We restrict access to your personal information only to those employees who need to know that information to provide product and services to you.
- Protecting your information is of the utmost importance to us. We use technical and physical safeguards to protect the security of your personal information from unauthorized disclosure. We also take every step to ensure that only authorized employees and third-parties with legitimate purposes have access to your personal information.

## **Your Privacy Rights**

- You have the right to access your information and request corrections to your data.
- You may also have the right to object to our use of our information, to request the transfer of information you have provided, to withdraw permission for our use of your information, and to ask us not to use automated decision-making which will affect you.
- However, certain exceptions apply to these rights.

We may change our privacy practices to comply with applicable regulations. When we do, we will revise the “last update” date at the bottom of the statement.

If you have any questions or concerns about this notice or PALIG’s privacy practices, please contact our Global Privacy Office at [privacy@palig.com](mailto:privacy@palig.com) or by mail at:

Pan-American Life Insurance Group  
Attn: Global Privacy Office  
601 Poydras Street, 15th Floor,  
New Orleans, Louisiana 70130

## REFERENCE GUIDE

**Order Your Free Credit Report.** To order your free credit report, visit [www.annualcreditreport.com](http://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](http://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](http://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	<a href="http://www.equifax.com">www.equifax.com</a>
Experian	P.O. Box 9532 Allen, Texas 75013	1-888-397-3742	<a href="http://www.experian.com">www.experian.com</a>
TransUnion	Fraud Victim Assistance Division P.O. Box 2000 Chester, Pennsylvania 19016	1-800-680-7289	<a href="http://www.transunion.com">www.transunion.com</a>

**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	<a href="http://www.equifax.com">www.equifax.com</a>
---------	--	--

Experian	P.O. Box 9554 Allen, Texas 75013	<a href="http://www.experian.com">www.experian.com</a>
TransUnion	Fraud Victim Assistance Division P.O. Box 2000 Chester, Pennsylvania 19016	<a href="http://www.transunion.com">www.transunion.com</a>

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:

- Your full name (including middle initial as well as Jr., Sr., II, III, etc.)
- Social Security number
- Date of birth
- If you have moved in the past five (5) years, provide the addresses where you have lived over the prior five years.
- Proof of current address, such as a current utility bill or telephone bill
- A legible photocopy of a government issued identification card (state driver's license or ID card, military identification, etc.)
- 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

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 your 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](http://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](http://www.ftc.gov/idtheft)

**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](http://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:** Although PALIG is not a licensed insurance provider in New York, because we may have information about NY 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](http://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](http://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](http://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.