October 23, 2024

Jennifer S. Stegmaier
312.821.6167 (direct)
Jennifer.Stegmaier@wilsonelser.com

Via Online Portal

Attorney General Aaron Frey
Office of the Attorney General
6 State House Station
Augusta, ME 04333

Re: Supplemental Notice of Data Breach Involving Landmark Admin, LLC

Dear Attorney General Frey:

Wilson Elser Moskowitz Edelman and Dicker LLP ("Wilson Elser") represents Landmark Admin, LLC ("Landmark"), located at 5750 County Road 225, Brownwood, Texas 76801, with respect to a recent cybersecurity incident that was discovered by Landmark on or about May 13, 2024, and June 17, 2024 (hereinafter, the "Incident"). Please accept this as a supplement to our prior preliminary notices (that were submitted to your office on June 12, 2024, and June 27, 2024).

Landmark is a third-party administrator for insurance carriers, including Liberty Bankers Insurance Group ("LBIG") which includes American Monumental Life InsuranceCompany, Pellerin Life Insurance Company, American Benefit LifeInsurance Company, Liberty Bankers Life Insurance Company,Continental Mutual Insurance Company, and Capitol Life Insurance Company. As such, Landmark received certain of personal information from individuals who are at one time were a producer, policyowner, insured, beneficiary, or payor for insurance policies which Landmark administered, or continues to administer, for LBIG.

Landmark takes the security and privacy of the information in its control very seriously and has taken steps to prevent a similar incident from occurring in the future. This letter will serve to inform you of the nature of the Incident, what information may have been compromised, the number of Maine residents being notified, and the steps that Landmark has taken in response to the Incident. We have also enclosed hereto a copy of Landmark's individual notice letter that was mailed to impacted individuals.

1. Nature of the Incident

On or about May 13, 2024, Landmark discovered unusual activity on its system. Upon discovering this incident Landmark immediately disconnected the affected systems and remote access to the network. Landmark also promptly engaged a specialized third-party cybersecurity firm to assist with securing the environment and to conduct a comprehensive forensic investigation to determine the nature and scope of the incident. While the forensic investigation was underway, the unauthorized actor re-gained access to

Landmark's environment on June 17, 2024. The third-party cybersecurity firm again assisted with securing the environment while it also continued to conduct its forensic investigation. The forensic investigation concluded on or about July 24, 2024. The forensic investigation determined that data was encrypted and exfiltrated from Landmark's system, however, there was insufficient evidence available to identify which files had been compromised. The unauthorized activity occurred between May 13, 2024, and June 17, 2024.

Based on these findings, Landmark began reviewing the affected systems to identify the individuals potentially affected by this incident and the types of information that may have been compromised. This process remains ongoing. In abundance of caution, Landmark is notifying all individuals whose private information may have been contained in its systems at the time of the incident. Individual notice letters will be mailed to these potentially affected individuals by U.S. first-class mail on a rolling basis as they are identified. The first wave of notification letters will be mailed on October 23-24, 2024.

Based on the investigation, the following information related to potentially impacted individuals may have been subject to unauthorized access: full name; address; Social Security number; tax identification number; drivers' license number/state-issued identification card number; passport number; bank account and routing number; medical information; health insurance policy number; date of birth; and/or life and annuity policy information.

Please note that the information above varies for each potentially impacted individual. The specific information which may have been impacted will be identified in each affected individuals' notification letter.

2. Impacted individuals

For Wave 1, Landmark identified 566 Maine residents as potentially affected by this incident. Notification letters to these individuals will be mailed on October 23-24, 2024. A sample copy of the individual notification letter is included with this letter as **Exhibit A**.

Landmark will submit supplemental notice to your office if it determines there are additional Maine residents who may have been impacted (and Landmark will notify these affected individuals by mail), as the information becomes available.

3. Steps taken in response to the Incident

Data privacy and security are among Landmark's highest priorities, and it is committed to doing everything they can to protect the privacy and security of the personal information in its care. Upon discovery of the incident, Landmark moved quickly and diligently to investigate, respond, and assess the security of its systems with the assistance of outside experts.

Landmark has also taken additional technical and administrative steps to further enhance the security of its systems and customer data to mitigate the risk of future harm. Specifically, Landmark acquired servers and deployed after server hardening, deployed a new firewall with the latest firmware, obtained new external IP address assigned by a new Internet Service Provider, implemented new domain controllers with new account naming conventions and forced new passwords, enabled BitLocker on all hard drives, reimaged all printers on the network, reimaged all network switches and updated to the latest firmware, and reimaged and updated all IoT devices with the latest firmware. Landmark also provided additional security training for all staff members, restricted all points of access to its systems, engaged a managed service provider to supplement the existing strong security posture with additional monitoring and protection software, and requires multifactor authentication for all devices (for both user and administrator logins). Landmark also notified law enforcement of this incident and this notice has not been delayed due to any law enforcement investigation.

In response to this incident, Landmark is offering credit monitoring and identity theft protection services through IDX, A ZeroFox Company, the data breach and recovery services expert. IDX identity protection services include 12 months of credit and CyberScan monitoring, a $1,000,000 insurance reimbursement policy, and fully managed id theft recovery services.

Landmark also provided additional guidance on how to better protect against identity theft and fraud, including providing information on how to place a fraud alert and security freeze on one's credit file, the contact details for the national consumer reporting agencies, information on how to obtain a free credit report, a reminder to remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring free credit reports, and the contact details for the Federal Trade Commission.

4. Contact Information

Landmark remains dedicated to protecting the sensitive information in its control. If you have any questions or need additional information, please do not hesitate to contact me at Jennifer.Stegmaier@wilsonelser.com or 312-821-6167.

Very truly yours,

Wilson Elser Moskowitz Edelman & Dicker LLP

Jennifer S. Stegmaier

Exhibit A

Sample Individual Notice Letter

149086

Landmark Admin, LLC
Return to IDX
P.O. Box 989728
West Sacramento, CA 95798-9728

[redacted]

[redacted]

Liberty Bankers Insurance Group | For Life

Enrollment Code: [redacted]
To Enroll, Scan the QR Code Below:

[redacted]

Or Visit:
https://response.idx.us/landmark

Via First Class Mail

October 23, 2024

Re: Notice of Data Breach

Dear [redacted],

We are writing to inform you of a data security incident that may have involved your personal information. We take the protection of your personal information very seriously and are sending you this notice to tell you what happened, what information was involved, what we have done in response, what you can do in response to this incident, and what resources are available to help protect against the potential misuse of sensitive personal information.

Landmark Admin, LLC ("Landmark"), located at 5750 County Road 225, Brownwood, Texas 76801, is a third-party administrator for insurance carriers, including Liberty Bankers Insurance Group ("LBIG") which includes American Monumental Life Insurance Company, Pellerin Life Insurance Company, American Benefit Life Insurance Company, Liberty Bankers Life Insurance Company, Continental Mutual Insurance Company, and Capitol Life Insurance Company. As such, Landmark received certain of your personal information because you are or at one time were a producer, policyowner, insured, beneficiary, or payor for an insurance policy which Landmark administered, or continues to administer, for your carrier.

What Happened

On or about May 13, 2024, Landmark detected suspicious activity on its system. Upon discovery of this incident, Landmark immediately disconnected the affected systems and remote access to the network and promptly engaged a specialized third-party cybersecurity firm and IT personnel to assist with securing the environment, as well as to conduct a comprehensive forensic investigation to determine the nature and scope of the incident. The forensic investigation concluded on or about July 24, 2024, and determined that there was unauthorized access to Landmark's network and data was encrypted and exfiltrated from its system. The unauthorized activity occurred from May 13, 2024 to June 17, 2024.

Based on these findings, Landmark began reviewing the affected systems to identify the individuals potentially affected by this incident and the types of information that may have been compromised. While this process remains ongoing, and in an abundance of caution, Landmark is notifying potentially affected individuals by mail on a rolling basis as they are identified. We determined that some of your personal information may have been affected by the incident.

What Information Was Involved

The personal information that may have been subject to unauthorized access includes: name; tax identification number. For some individuals, it is possible that the following additional information may have been subject to unauthorized

access (if this information was provided to Landmark): driver's license number; passport number; and medical and/or health information. Please note the information impacted varies for each potentially impacted individual.

What We Are Doing

Data privacy and security are among Landmark's highest priorities, and we are committed to doing everything we can to protect the privacy and security of the personal information in our care. Upon discovery of the incident, Landmark moved quickly and diligently to investigate, respond, and assess the security of its systems with the assistance of outside experts.

Landmark has also taken additional technical and administrative steps to further enhance the security of its systems and customer data to mitigate the risk of future harm. Specifically, Landmark acquired servers and deployed after server hardening, deployed a new firewall with the latest firmware, obtained new external IP address assigned by a new Internet Service Provider, implemented new domain controllers with new account naming conventions and forced new passwords, enabled BitLocker on all hard drives, reimaged all printers on the network, reimaged all network switches and updated to the latest firmware, and reimaged and updated all IoT devices with the latest firmware. Landmark also provided additional security training for all staff members, restricted all points of access to its systems, engaged a managed service provider to supplement the existing strong security posture with additional monitoring and protection software, and requires multifactor authentication for all devices (for both user and administrator logins). Landmark also notified law enforcement of this incident and this notice has not been delayed due to any law enforcement investigation.

In addition, we are offering identity theft protection services through IDX, A ZeroFox Company, the data breach and recovery services expert. IDX identity protection services include: 12 months of credit and CyberScan monitoring, a $1,000,000 insurance reimbursement policy, and fully managed id theft recovery services. With this protection, IDX will help you resolve issues if your identity is compromised.

What You Can Do

We encourage you to contact IDX with any questions and to enroll in the free identity protection services by calling 1-866-273-9228, going to https://response.idx.us/landmark, or scanning the QR image and using the Enrollment Code provided above. IDX representatives are available Monday through Friday, during the hours of 9:00 a.m. and 9:00 p.m. Eastern Standard Time (excluding U.S. national holidays). Please note the deadline to enroll is January 24, 2025.

We also recommend that you remain vigilant and take steps to protect yourself against incidents of identity theft and fraud, including monitoring your accounts, account statements, and free credit reports for suspicious or unauthorized activity. Additionally, security experts suggest that you contact your financial institution and all major credit bureaus to inform them of such a breach and then take recommended steps to protect your interests, including the possible placement of a free fraud alert on your credit file. Please review the enclosed ***Steps You Can Take to Help Protect Your Information*** to learn more about how to protect against the possibility of information misuse.

For More Information

If you have any questions or concerns not addressed in this letter, you may contact IDX by calling 1-866-273-9228 (toll free) Monday through Friday, during the hours of 9:00 a.m. and 9:00 p.m. Eastern Standard Time (excluding U.S. national holidays). You can also go to https://response.idx.us/landmark or scanning the QR image to access an informational website. These resources will be available to you for 90 days after the date of this letter.

Landmark sincerely regrets that this incident occurred and any inconvenience that it may cause and remains dedicated to ensuring the privacy and security of all information within our control.

Sincerely,

Thomas A. Munson, President
Landmark Admin, LLC

149086

STEPS YOU CAN TAKE TO HELP PROTECT YOUR INFORMATION

Monitor Your Accounts

We recommend that you remain vigilant for incidents of fraud or identity theft by regularly reviewing your credit reports and financial accounts for any suspicious activity. You should contact the reporting agency using the phone number on the credit report if you find any inaccuracies with your information or if you do not recognize any of the account activity.

You may obtain a free copy of your credit report by visiting www.annualcreditreport.com, calling toll-free at 1-877-322-8228, or by mailing a completed Annual Credit Report Request Form (available at www.annualcreditreport.com) to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281. You may also purchase a copy of your credit report for a fee by contacting one or more of the three national credit reporting agencies.

You have rights under the federal Fair Credit Reporting Act (FCRA). The FCRA governs the collection and use of information about you that is reported by consumer reporting agencies. You can obtain additional information about your rights under the FCRA by visiting https://www.ftc.gov/legal-library/browse/statutes/fair-credit-reporting-act.

Credit Freeze

You have the right to add, temporarily lift and remove a credit freeze, also known as a security freeze, on your credit report at no cost. A credit freeze prevents all third parties, such as credit lenders or other companies, whose use is not exempt under law, from accessing your credit file without your consent. If you have a freeze, you must remove or temporarily lift it to apply for credit. Spouses can request freezes for each other as long as they pass authentication. You can also request a freeze for someone if you have a valid Power of Attorney. If you are a parent/guardian/representative you can request a freeze for a minor 15 and younger. To add a security freeze on your credit report you must make a separate request to each of the three national consumer reporting agencies by phone, online, or by mail by following the instructions found at their websites (see "Contact Information" below). The following information must be included when requesting a security freeze: (i) full name, with middle initial and any suffixes; (ii) Social Security number; (iii) date of birth (month, day, and year); (iv) current address and any previous addresses for the past five (5) years; (v) proof of current address (such as a copy of a government-issued identification card, a recent utility or telephone bill, or bank or insurance statement); and (vi) other personal information as required by the applicable credit reporting agency.

Fraud Alert

You have the right to add, extend, or remove a fraud alert on your credit file at no cost. A fraud alert is a statement that is added to your credit file that will notify potential credit grantors that you may be or have been a victim of identity theft. Before they extend credit, they should use reasonable procedures to verify your identity. Please note that, unlike a credit freeze, a fraud alert only notifies lenders to verify your identity before extending new credit, but it does not block access to your credit report. Fraud alerts are free to add and are valid for one year. Victims of identity theft can obtain an extended fraud alert for seven years. You can add a fraud alert by sending your request to any one of the three national reporting agencies by phone, online, or by mail by following the instructions found at their websites (see "Contact Information" below). The agency you contact will then contact the other credit agencies.

Federal Trade Commission

For more information about credit freezes and fraud alerts and other steps you can take to protect yourself against identity theft, you can contact the Federal Trade Commission (FTC) at 600 Pennsylvania Avenue NW, Washington, DC 20580, www.identitytheft.gov, 1-877-ID-THEFT (1-877-438-4338), TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. You can obtain further information on how to file such a complaint by way of the contact information listed above.

You should also report instances of known or suspected identity theft to local law enforcement and the Attorney General's office in your home state and you have the right to file a police report and obtain a copy of your police report.

Contact Information

Below is the contact information for the three national credit reporting agencies (Experian, Equifax, and Transunion) if you would like to add a fraud alert or credit freeze to your credit report.

Credit Reporting Agency	Access Your Credit Report	Add a Fraud Alert	Add a Security Freeze
Experian	P.O. Box 2002 Allen, TX 75013-9701 1-866-200-6020 www.experian.com	P.O. Box 9554 Allen, TX 75013-9554 1-888-397-3742 https://www.experian.com/fraud/center.html	P.O. Box 9554 Allen, TX 75013-9554 1-888-397-3742 www.experian.com/freeze/center.html
Equifax	P.O. Box 740241 Atlanta, GA 30374-0241 1-866-349-5191 www.equifax.com	P.O. Box 105069 Atlanta, GA 30348-5069 1-800-525-6285 www.equifax.com/personal/credit-report-services/credit-fraud-alerts	P.O. Box 105788 Atlanta, GA 30348-5788 1-888-298-0045 www.equifax.com/personal/credit--report-services
Transunion	P.O. Box 1000 Chester, PA 19016-1000 1-800-888-4213 www.transunion.com	P.O. Box 2000 Chester, PA 19016 1-800-680-7289 www.transunion.com/fraud-alerts	P.O. Box 160 Woodlyn, PA 19094 1-800-916-8800 www.transunion.com/credit-freeze

Iowa and Oregon residents are advised to report suspected incidents of identity theft to local law enforcement, to their respective Attorney General, and the FTC.

Massachusetts residents are advised of their right to obtain a police report in connection with this incident.

District of Columbia residents are advised of their right to obtain a security freeze free of charge and can obtain information about steps to take to avoid identity theft by contacting the FTC (contact information provided above) and the Office of the Attorney General for the District of Columbia, Office of Consumer Protection, at 400 6th St. NW, Washington, D.C. 20001, by calling the Consumer Protection Hotline at (202) 442-9828, by visiting https://oag.dc.gov, or emailing at consumer.protection@dc.gov.

Maryland residents can obtain information about steps they can take to avoid identity theft by contacting the FTC (contact information provided above) or the Maryland Office of the Attorney General, Consumer Protection Division Office at 44 North Potomac Street, Suite 104, Hagerstown, MD 21740, by phone at 1-888-743-0023 or 410-528-8662, or by visiting http://www.marylandattorneygeneral.gov/Pages/contactus.aspx.

New York residents are advised that in response to this incident they can place a fraud alert or security freeze on their credit reports and may report any incidents of suspected identity theft to law enforcement, the FTC, the New York Attorney General, or local law enforcement. Additional information is available at the website of the New York Department of State Division of Consumer Protection at https://dos.ny.gov/consumer-protection; by visiting the New York Attorney General at https://ag.ny.gov/ or by phone at 1-800-771-7755; or by contacting the FTC at www.ftc.gov/bcp/edu/microsites/idtheft/ or https://www.identitytheft.gov/#/.

North Carolina residents are advised to remain vigilant by reviewing account statements and monitoring free credit reports and may obtain information about preventing identity theft by contacting the FTC (contact information provided above) or the North Carolina Office of the Attorney General, Consumer Protection Division at 9001 Mail Service Center, Raleigh, NC 27699-9001, or visiting www.ncdoj.gov, or by phone at 1-877-5-NO-SCAM (1-877-566-7226) or (919) 716-6000.

Rhode Island residents are advised that they may file or obtain a police report in connection with this incident and place a security freeze on their credit file and that fees may be required to be paid to the consumer reporting agencies.