

April 11, 2025

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 Landmark’s prior notice submission.

Landmark is a third-party administrator for various insurance carriers. As such, Landmark received certain personal information regarding individuals who are, or at one time were, a policyowner, insured, beneficiary, payor and/or producer for insurance policies which Landmark administered or continues to administer.

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 provide an update involving the nature of the Incident, what information may have been compromised, the number of residents within your state that were notified, and the steps that Landmark has taken in response to the Incident.¹

1. Nature of the Incident

On or about May 13, 2024, Landmark’s IT vendor detected suspicious activity on its system and, on May 15, 2024, discovered data had been exfiltrated.² 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, remediation and recovery, live forensics, as well as to conduct a comprehensive forensic investigation to determine the nature and scope of the incident. Landmark also notified the insurance carriers which it acted as a third-party administrator whose data was impacted.

¹ Landmark previously submitted a sample individual notice letter from the first wave of notices that were mailed on October 23, 2024 and October 24, 2024 which is substantively similar to the individual notice letter templates used in the subsequent waves of notice.

² On or about May 16, 2024, Landmark recovered all data that had been exfiltrated.
55 West Monroe Street, Suite 3800 • Chicago, IL 60603 • p 312.704.0550 • f 312.704.1522

On or about May 22, 2024, the third-party cybersecurity firm determined that the root cause and initial unauthorized access to Landmark’s system had occurred on May 13, 2024 *via* the VPN using valid credentials based on the available artifacts and live forensics. The forensic investigation was inconclusive as to how the credentials were compromised. The third-party cybersecurity firm also concluded the root cause and attack vector had been mitigated and no longer existed after Landmark changed the account passcodes and Landmark’s environment was safe and secure and free of any malicious activity. Accordingly, Landmark fully reinstated its network and remote access.

On June 17, 2024, Landmark discovered the threat actor had re-entered its environment and exfiltrated data.³ The specialized third-party cybersecurity firm and IT personnel which was engaged by Landmark continued to assist with securing Landmark’s environment and its remediation and recovery efforts. Landmark notified all insurance carriers whose data was might have been impacted within the affected systems.

The forensic investigation concluded on or about July 24, 2024. The investigatoin determined unauthorized access to Landmark’s network occurred from May 13, 2024 to June 17, 2024, and certain systems were encrypted and data had been exfiltrated after the threat actor re-entered its systems. Although the investigation found data had been exfiltrated, it was unable to identify *which* specific files/folders were exfiltrated after the threat actor re-entered Lankmark’s systems. Since Landmark has a significant amount of data which contains *no* personally identifiable information, it is possible that the exfiltrated data did not contain any personally identifiable information. Landmark has no evidence that any of the exfiltrated data *actually* contained personally identifiable information.

Based on these findings, Landmark reviewed the affected systems to identify the individuals potentially affected by this incident and the types of information possibly compromised. In an abundance of caution, Landmark coordinated with each of the insurance carriers to notify the potentially affected individuals for whom it had valid addresses *via* U.S. first class mail on a rolling basis as the information became available. Landmark also posted substitute notice of this incident on its website and publishing media notice in the Houston Chronicle on June 12, 2024. On June 26, 2024, Landmark posted an updated substitute notice on its website and submitted a Media Release to PRNewswire for nationwide distribution.

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/government-issued identification card number; picture of drivers’ license number/government issued identification card; bank account and routing number; medical and/or health information; health insurance policy number; health claim, date of birth, life and annuity policy information, life insurance policy application, and insurance benefit payment amount and payees. The information varied among each potentially affected individual and only applies if the information was actually provided to Landmark.

³ The threat actor had built a backdoor on a third-party backup appliance within Landmark’s envirmoment which was designed with a Linux-based architecture that is hardened against cyber threats.

2. Impacted individuals

Landmark identified a total of 1,528 Maine residents as potentially affected by this incident.⁴ Landmark mailed individual notification letters to the potentially impacted individuals in waves as information became available on October 23, 2024, October 24, 2024, January 24, 2025, January 31, 2025, February 21, 2025, March 17, 2025, March 21, 2025, and April 10, 2025. Landmark previously submitted a sample individual notice letter from the first wave with its prior notice.

Landmark is providing notice on behalf of the insurance carriers (which Landmark acted as a third-party administrator) that were impacted by this Incident, as identified in **Exhibit A**.

3. Steps taken in response to the Incident

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, after June 17, 2024, Landmark never reinstated access to the impacted system for its operations and, instead, build a new system that was totally disconnected from the prior system. The third-party cybersecurity firm set up surveillance and Landmark's IT vendor monitored on the new system from its inception to ensure there was no malicious activity.

In response to this incident, Landmark offered credit monitoring and identity theft protection services through IDX, A ZeroFox Company, the data breach and recovery services expert. IDX identity protection services included a minimum of 12 months (or 24 months for residents of Connecticut, Washington D.C., and Massachusetts) 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

⁴ This is the total number of potentially impacted individuals for all waves of notice.

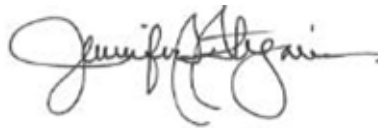
contact details for the national consumer reporting agencies, information on how to obtain a free credit report, a reminder to remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring free credit reports, and the contact details for the Federal Trade Commission.

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

Landmark Providing Notice On Behalf of Insurance Carriers

Landmark is submitting notice on its own behalf and on behalf of the insurance carriers which it acted as a third-party administrator, including:

- Liberty Bankers Insurance Group 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 Capital Life Insurance Company
- Pan-American Life Insurance Company
- TruSpire Retirement Insurance Company
- Continental Life Insurance Company of Brentwood Tennessee
- Accendo Insurance Company
- Tier One Insurance Company
- American Home Life Insurance Company