600 Travis Street, Suite 2800
Houston, TX 77002
www.lockelord.com

Laura L. Ferguson
Telephone: 713-226-1590
Email: LFerguson@lockelord.com

June 16, 2021

Office of the Maine Attorney General
111 Sewall St.
Augusta, ME 04330

Re: Lightfoot, Franklin, & White, LLC
Notice pursuant to Me. Rev. Stat. Ann. tit. 10, § 1346

Dear Attorney General Aaron Frey:

Our client Lightfoot, Franklin, & White, LLC ("Lightfoot") is a law firm based in Birmingham, Alabama that handles commercial litigation, product liability, professional liability, white-collar criminal, and other legal matters. On behalf of Lightfoot, we hereby provide notice pursuant to Me. Rev. Stat. Ann. tit. 10, § 1346 of a security incident involving potential disclosure of the personal information of Maine residents, based on our investigation to date.

What Happened

On April 17, 2021, Lightfoot discovered a ransomware incident that it later determined resulted in unlawful access to its human resources files and certain client files ("Client Files"). Lightfoot took immediate steps to contain the incident and began its investigation, including the engagement of our law firm and outside forensics investigators to determine the scope and nature of the attack, as well as the extent to which security of personal and corporate information may have been compromised. At this time, Lightfoot has no indication that any of the compromised personal information has or will be misused in connection with this incident.

What Information Was Involved

Based on Lightfoot's investigation, which is ongoing, the impacted Client Files contained certain personal information including affected individuals' names, Social Security numbers, and other government-issued identification numbers such as driver's license or passport information, as well as health and medical information. Lightfoot has determined that the compromised Client Files includes personal information for approximately 38 Maine residents. These individuals were not impacted by the unlawful access to Lightfoot's human resources files.

What Lightfoot is Doing

As noted above, immediately upon the discovery of the attack, Lightfoot took steps to terminate it and prevent any further unauthorized access. Lightfoot is continuing to take steps to enhance the security of its systems and the data entrusted to it. These steps include implementing endpoint security software on its systems, enhancing employee education and training, and continuing to work with an independent cybersecurity firm to further review and enhance Lightfoot's security policies and procedures. Furthermore, Lightfoot has engaged a service provider to conduct both public and dark web monitoring for any posting or exchange of personal information related to this incident. Additionally, Lightfoot reached a resolution and has received confirmation from the third party that the compromised information was destroyed.

As required by Me. Rev. Stat. Ann. tit. 10, § 1348(1), Lightfoot is providing notice of this incident to the individuals affected by the compromised Client Files by mail on or about June 16, 2021. A template for the Client Files notification letter is attached. The notification letter describes Lightfoot's offer of credit monitoring services for 12 months at no cost to the affected individuals, and provides additional guidance for affected individuals to protect themselves.

On behalf of Lightfoot, we are notifying state agencies as required in jurisdictions where affected individuals reside.

* * * * *

Please do not hesitate to contact me with any questions related to this matter.

Sincerely,

Laura L. Ferguson

Enclosure