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 Attorney General
Consumer Protection Bureau
33 Capitol Street
Concord, NH 03301
DOJ-CPB@doj.nh.gov

Re: Lightfoot, Franklin, & White, LLC
Notice pursuant to N.H. Rev. Stat. § 359-C:19

Dear Attorney General John Formella:

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 N.H. Rev. Stat. § 359-C:19 of a security incident involving potential disclosure of the personal information of New Hampshire 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 include personal information for approximately 20 New Hampshire 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 N.H. Rev. Stat. § 359-C:20(I), 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

Lightfoot

Return Mail Processing
PO Box 589
Claysburg, PA 16625-0589

June 16, 2021

G5379-L01-0000001 T00001 P001 *****AUTO**MIXED AADC 159
SAMPLE A. SAMPLE - L01
APT ABC
123 ANY ST
ANYTOWN, ST 12345-6789

RE: Notice of Data Breach
Please read this entire letter.

Dear Sample A. Sample:

Lightfoot, Franklin & White, LLC is a law firm based in Birmingham, Alabama that handles commercial litigation, product liability, professional liability, white-collar criminal, and other legal matters. We are notifying you about a ransomware incident that resulted in unlawful access to files which may have contained personal information relating to you. As a result, we are notifying you of this incident to inform you of the immediate steps we have taken and to provide you with tools to help you protect yourself.

What Happened

On April 17, 2021, we learned of and stopped a ransomware incident that resulted in unlawful access by an unauthorized third party to certain clients' case files containing personal information for individuals who may have been related to the case, including plaintiffs, defendants, witnesses, and other non-parties. Your information was contained in one of those files. [EXTRA3]

What Information Was Involved

Your personal information that was potentially exposed may have included your Social Security number and other government-issued identification, as well as health and medical information. **Currently, we have no indication that any of your personal information has been or will be misused in connection with this incident.**

What We Are Doing

Upon discovering this incident, we took immediate steps to contain the incident, engaged outside consultants to conduct an investigation, and notified law enforcement. To take all possible steps to protect your information against disclosure or misuse by the unauthorized third party, we reached a resolution and have received confirmation from the third party that the compromised information was destroyed. We have engaged in an extensive review to identify the individuals whose personal information was compromised and are notifying those individuals on behalf of clients. We also continue to enhance the security of our systems and the data entrusted to us. These steps include implementing endpoint security software on our systems, emphasizing employee education and training, and working with an independent cybersecurity firm to review and enhance our security policies and procedures. Furthermore, we have engaged a service provider to conduct both public and dark web monitoring for any posting or exchange of personal compromised information related to this incident. We have not found any indication that any of your compromised information is available on the dark web. **While we have no indication that any of your personal information has been or will be misused in connection with this incident, we nevertheless have arranged for services and provided the advice described below to help you protect yourself against potential risk and to alleviate any concern related to this incident.**

What You Can Do

We recommend that you remain vigilant by reviewing your account statements and credit reports regularly, as well as reporting any suspicious transactions to your financial services provider. To help you protect yourself against risks related to this incident, we are offering a complimentary [EXTRA2] membership of Experian's® IdentityWorks℠. This product provides you with superior identity detection and resolution of identity theft. Enclosed with this letter is information regarding these services and instructions for enrollment, along with additional information regarding steps you can take to protect yourself against identity theft and fraud.

For More Information

If you have any questions regarding this incident and to enroll in the credit services we are offering at no cost to you, please contact our dedicated call center at (833) 704-9390 and follow the instructions attached to this letter.

Sincerely,

Melody H. Eagan
Managing Partner

[EXTRA1]

To help protect your identity, we are offering a complimentary [EXTRA2] membership of Experian's® IdentityWorks℠. This product helps detect possible misuse of your personal information and provides you with superior identity protection support focused on immediate identification and resolution of identity theft.

Activate IdentityWorks:

To activate your membership and start monitoring your personal information please follow the steps below:

- Ensure that you **enroll by**: **September 30, 2021** (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll: https://www.experianidworks.com/plus
- Provide your **activation code**: ABCDEFGHI

If you have questions about the product, need assistance with identity restoration or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at (833) 704-9390 by **September 30, 2021**. Be prepared to provide engagement number **ENGAGE#** as proof of eligibility for the identity restoration services by Experian.

ADDITIONAL DETAILS REGARDING YOUR [EXTRA2] 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.
- **Internet Surveillance:** Technology searches the web, chat rooms & bulletin boards 24/7 to identify trading or selling of your personal information on the Dark Web.
- **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.
- **Up to $1 Million Identity Theft Insurance**:** Provides coverage for certain costs and unauthorized electronic fund transfers.

If you believe there was fraudulent use of your information and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent at (833) 704-9390. 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 (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 this Identity Restoration support is available to you for [EXTRA2] 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. You will also find self-help tips and information about identity protection at this site.

* 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.

Additional Information and U.S. State Notification Requirements

There are a number of steps you should consider to guard against identity theft.

Review Your Account Statements and Credit Report: It is recommended that you remain vigilant for incidents of fraud and identity theft by regularly reviewing your account statements and monitoring your credit reports. Report any fraudulent transactions to the creditor or credit reporting agency from whom you received the statement or report. You may obtain a free copy of your credit report from each credit reporting agency once every 12 months, whether or not you suspect any unauthorized activity on your account, by visiting https://www.annualcreditreport.com, calling toll-free 877-322-8228, or by completing an Annual Credit Report Request Form available at that website and mailing it to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. You may also purchase a copy of your credit report at any time by contacting any one or more of the national credit reporting agencies listed below.

Equifax
P.O. Box 740241
Atlanta, Georgia 30374
www.equifax.com
1-800-685-1111 Credit Reports
1-888-766-0008 Fraud Alert
1-800-685-1111 Security Freeze

Experian
P.O. Box 2002
Allen, TX 75013
www.experian.com
1-888-397-3742 Credit Reports
1-888-397-3742 Fraud Alert
1-888-397-3742 Security Freeze

TransUnion (FVAD)
P.O. Box 105281
Atlanta, GA 30348-5281
www.transunion.com
1-800-888-4213 Credit Reports
1-800-680-7289 Fraud Alert
1-800-680-7289 Security Freeze

Federal Trade Commission (FTC) and State Resources: General guidance on protecting yourself from identify theft is available from the Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Ave. NW, Washington D.C. 20580, by phone at 877-ID-THEFT (438-4338), and/or from the FTC website at http://www.ftc.gov/bcp/edu/microsites/idtheft. In many states, additional information is also available from your state's Attorney General's Office.

Fraud Alerts and Security Freezes: You may obtain information about fraud alerts and security freezes (also referred to as credit freezes), including how to place a fraud alert or security freeze, from the Federal Trade Commission or credit reporting agencies at the contact information provided above. However, be aware that a fraud alert or security freeze may require fees to be paid, may interfere with or delay legitimate requests for credit approval. You'll need to supply your name, address, date of birth, Social Security number and other personal information in order to place a security freeze on your credit.

Additional Information: You may further educate yourself regarding identity theft, fraud alerts, credit freezes, and the steps you can take to protect your personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or your state Attorney General. The Federal Trade Commission may be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and 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 have the right to file a police report if you ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, you will likely need to provide some proof that you have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and your state Attorney General. This notice has not been delayed by law enforcement.

For Maryland residents, the Maryland Office of the Attorney General may be contacted at: 200 St. Paul Place, Baltimore, MD 21202; 1-888-743-0023; or www.oag.state.md.us.

For New York residents, the New York Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; or https://ag.ny.gov/.

For North Carolina residents, the North Carolina Attorney General may be contacted at: 9001 Mail Service Center, Raleigh, NC 27699-9001; 1-877-566-7226 or 1-919-716-6000; and www.ncdoj.gov.

For Oregon residents, state law advises you to report any suspected identity theft to law enforcement or to the Attorney General.

For Rhode Island residents, the Rhode Island Attorney General may be reached at: 150 South Main Street, Providence, RI 02903; www.riag.ri.gov; and 1-401-274-4400. Under Rhode Island law, you have the right to obtain any police report filed in regard to this incident.