Much Shelist, P.C.
Attorneys at Law

191 N. Wacker Drive
Suite 1800
Chicago, IL 60606

312.521.2000
muchlaw.com

January 15, 2021

DIRECT DIAL: 312.521.2446
nbrankle@muchlaw.com

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

Re: Incident Notification

Dear Attorney General MacDonald:

We are writing on behalf of our client, Moss, Inc., to notify you of a data security incident that may have involved information belonging to New Hampshire residents.

Moss recently confirmed that some consumer information was involved in a ransomware incident that disrupted the operations of the Moss IT systems. The incident was first identified by Moss on September 20, 2020, and Moss immediately took steps to secure its systems. Shortly thereafter, Moss engaged an expert cybersecurity consulting firm to launch a thorough investigation, and notified relevant law enforcement agencies, including the Federal Bureau of Investigation. Through the investigation, it was determined that an unauthorized party operating from an international location had access to certain files on the Moss systems and had removed those same files.

The investigation and review of the files potentially accessed determined that they contained the names and Social Security numbers for one (1) New Hampshire resident. Moss mailed notification letters to those residents on January 13, 2021 in accordance with applicable law. A copy of the notification letter is enclosed. To help prevent something like this from happening again, Moss is working with expert cybersecurity consulting firms and has implemented additional solutions to further safeguard and monitor its systems.

Please do not hesitate to contact me directly if you have any questions regarding this matter.

Sincerely,

Nicholas Brankle

10501 Seymour Avenue
Suite 200
Franklin Park, IL 60131

800.341.1557
www.mossinc.com

NOTICE OF DATA BREACH

We recently discovered that we were the victim of a ransomware attack, which was apparently perpetrated by international actors. Upon discovery, we promptly initiated standard remediation plans. We successfully mitigated the attack and restored our systems, and we have also been in communication with the Federal Bureau of Investigation and other law enforcement authorities concerning the same.

Upon restoration of our systems, an analysis to determine what data may have been lost or compromised was launched. We were specifically concerned with the potential loss of personal data and similar sensitive information from its systems. This analysis eventually revealed that certain personal data from our systems was present online. Specifically, the files in question contained name, address, and credit card number.

We want you to be aware of some of the actions that you can take to protect your personal information and online identity. These include the following:

You can place a fraud alert on your credit file free of charge. A fraud alert tells creditors to contact you before they open any new accounts or change your existing accounts. To place a fraud alert, you only need to contact one of the three major credit bureaus. As soon as one credit bureau confirms your fraud alert, the others are notified to place fraud alerts on your account as well. The initial fraud alert stays on your credit report for one year, at which time you can renew it if you so choose. The credit bureaus can be reached as follows:

- TransUnion, www.transunion.com or 1-888-680-7289
- Equifax, www.equifax.com or 1-800-525-6285
- Experian, www.experian.com or 1-888-397-3742

10501 Seymour Avenue
Suite 200
Franklin Park, IL 60131

800.341.1557
www.mossinc.com

You can also request to receive all three of your credit reports, free of charge, for your review. Even if you do not find any suspicious activity on your initial credit reports, the Federal Trade Commission (FTC) recommends that you check your credit reports periodically. Thieves may hold stolen information to use at different times. Checking your credit reports periodically can help you spot problems and address them quickly.

You may want to consider contacting each of the credit bureaus listed above to place a free credit freeze on your credit file (for clarity, unlike a fraud alert, a credit freeze requires you to contact each bureau individually). A credit freeze means that potential creditors cannot get your credit report from the credit bureaus at all. That makes it less likely that an identity thief can open new accounts in your name.

If you do determine at any point that your personal information has been misused, you can visit the FTC's site at www.IdentityTheft.gov or call 1-877-ID-THEFT (877-438-4338) to get recovery steps and to file an identity theft complaint. Your complaint will be added to the FTC's Consumer Sentinel Network, where it will be accessible to law enforcement for their investigations. The FTC can help guide you through steps you can to take to better protect your personal information from being misused online. There is no charge for the FTC's assistance.

If you have any questions or concerns, please don't hesitate to reach out and contact us at: breachinfo@mossinc.com.

Moss Executive Team