EXHIBIT 1

We represent Burns & Levinson LLP ("Burns & Levinson") located at 125 High Street, Boston, Massachusetts 02110, and are writing to notify your office of an incident that may affect the security of certain personal information relating to one (1) Maine resident. This notice may be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, Burns & Levinson does not waive any rights or defenses regarding the applicability of Maine law, the applicability of the Maine data event notification statute, or personal jurisdiction.

Nature of the Data Event

On February 6, 2023, Burns & Levinson LLP ("Burns & Levinson") became aware of potential unauthorized access to its network. Upon discovery, Burns & Levinson promptly launched an investigation, aided by third-party forensic specialists, to determine the full nature and scope of the incident. The investigation determined that certain locations on its systems may have been accessed and some files related to representation of select clients may have been removed without authorization. Although Burns & Levinson has no evidence of any actual or attempted misuse of the information impacted, out of an abundance of caution, Burns & Levinson is providing notice to potentially impacted individuals whose information was present on these systems at the time of the incident and may have been impacted.

The information that could have been subject to unauthorized access includes name and Social Security number.

Notice to Maine Resident

On or about March 13, 2023, Burns & Levinson provided written notice of this incident to one (1) Maine resident. Written notice is being provided in substantially the same form as the letter attached here as ***Exhibit A***.

Other Steps Taken and To Be Taken

Upon discovering the event, Burns & Levinson moved quickly to investigate and respond to the incident, assess the security of Burns & Levinson systems, and identify potentially affected individuals. Further, Burns & Levinson notified federal law enforcement regarding the event. Burns & Levinson is also working to implement additional safeguards and training to its employees. Burns & Levinson is providing access to credit monitoring services for two (2) years, through Cyberscout, to individuals whose personal information was potentially affected by this incident, at no cost to these individuals.

Additionally, Burns & Levinson is providing impacted individuals with guidance on how to better protect against identity theft and fraud. Burns & Levinson is providing individuals with 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 encouragement to contact the Federal Trade Commission, their state Attorney General, and law enforcement to report attempted or actual identity theft and fraud.

Burns & Levinson is providing written notice of this incident to relevant state regulators, as necessary.

EXHIBIT A

Burns & Levinson LLP
c/o Cyberscout
1 Keystone Ave., Unit 700
Cherry Hill, NJ 08003
DB07280

[redacted]

March 13, 2023

NOTICE OF SECURITY INCIDENT

Dear [redacted]:

Burns & Levinson LLP ("Burns & Levinson") writes to inform you of an incident that may affect the security of your personal information. Although we have no evidence of actual or attempted misuse of your information, this letter provides details of the incident, our response, and resources available to you to help protect your personal information from possible misuse, should you feel it is appropriate to do so.

What Happened? On February 6, 2023, Burns & Levinson became aware of potential unauthorized access to our network. Upon discovery, we promptly began an investigation, aided by third-party forensic specialists, to determine the full nature and scope of the incident. As a result of our investigation, we confirmed that certain locations on our systems may have been accessed and some files related to our representation of you may have been removed without authorization.

What Information Was Involved? We determined that the following information may have been accessed or taken as the result of this incident: your name Social Security number. Although we are unaware of any actual or attempted misuse of your personal information, we are providing you with this notice out of an abundance of caution.

What We Are Doing. We take this incident and the security of personal information in our care very seriously. Upon learning of this incident, we moved quickly to investigate and respond to this incident, assess the security of our systems, restore functionality to our environment, and notify potentially affected individuals. As part of our ongoing commitment to the security of information, we notified federal law enforcement and are reviewing and enhancing our existing policies and procedures related to data privacy to reduce the likelihood of a similar future event.

As an added precaution, we are providing you with access to [redacted] months of credit monitoring and identity protection services provided by Cyberscout through Identity Force, a TransUnion company specializing in fraud assistance and remediation services. A description of services and instructions on how to enroll can be found within the enclosed *Steps You Can Take to Help Protect Your Information*. Please note that you must complete the enrollment process yourself, as we are not permitted to enroll you in these services on your behalf.

What You Can Do. Please review the enclosed *Steps You Can Take to Help Protect Your Information*, which contains information on what you can do to better protect against possible misuse of your information. We encourage you to remain vigilant against potential incidents of identity theft and fraud, to review your account statements, and to monitor your credit reports for suspicious activity. You will also find information on how to enroll in the credit monitoring services offered.

For More Information. We understand that you may have questions that are not addressed in this letter. If you have additional questions, please call the dedicated assistance line at 1-800-405-6108, which is available Monday through Friday, between the hours of 8:00 a.m. and 8:00 p.m. Eastern Time, excluding

holidays. You may also contact the partner working your matter. Burns & Levinson is located at 125 High Street, Boston, MA 02110.

Sincerely,

Paul Mastrocola
Co-Managing Partner
Burns & Levinson

David Rosenblatt
Co-Managing Partner
Burns & Levinson

STEPS YOU CAN TAKE TO HELP PROTECT YOUR INFORMATION

Enroll in Credit Monitoring

In response to the incident, we are providing you with access to **Single Bureau Credit Monitoring/Single Bureau Credit Report/Single Bureau Credit Score** services at no charge. These services provide you with alerts for twenty-four months from the date of enrollment when changes occur to your credit file. This notification is sent to you the same day that the change or update takes place with the bureau. Finally, we are providing you with proactive fraud assistance to help with any questions that you might have or in event that you become a victim of fraud. These services will be provided by Cyberscout through Identity Force, a TransUnion company specializing in fraud assistance and remediation services.

To enroll in Credit Monitoring services at no charge, please log on to **https://secure.identityforce.com/benefit/burnslevinson** and follow the instructions provided. When prompted please provide the following unique code to receive services: [redacted]**.** In order for you to receive the monitoring services described above, you must enroll within 90 days from the date of this letter. The enrollment requires an internet connection and e-mail account and may not be available to minors under the age of 18 years of age. Please note that when signing up for monitoring services, you may be asked to verify personal information for your own protection to confirm your identity.

Monitor Your Accounts

Under U.S. law, a consumer is entitled to one free credit report annually from each of the three major credit reporting bureaus, Equifax, Experian, and TransUnion. To order your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also directly contact the three major credit reporting bureaus listed below to request a free copy of your credit report.

Consumers have the right to place an initial or extended "fraud alert" on a credit file at no cost. An initial fraud alert is a 1-year alert that is placed on a consumer's credit file. Upon seeing a fraud alert display on a consumer's credit file, a business is required to take steps to verify the consumer's identity before extending new credit. If you are a victim of identity theft, you are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should you wish to place a fraud alert, please contact any one of the three major credit reporting bureaus listed below.

As an alternative to a fraud alert, consumers have the right to place a "credit freeze" on a credit report, which will prohibit a credit bureau from releasing information in the credit report without the consumer's express authorization. The credit freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, you should be aware that using a credit freeze to take control over who gets access to the personal and financial information in your credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, you cannot be charged to place or lift a credit freeze on your credit report. To request a security freeze, you will need to provide the following information:

1. Full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. Addresses for the prior two to five years;
5. Proof of current address, such as a current utility bill or telephone bill;
6. A legible photocopy of a government-issued identification card (state driver's license or ID card, etc.); and
7. A copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft if you are a victim of identity theft.

Should you wish to place a credit freeze, please contact the three major credit reporting bureaus listed below:

Equifax	**Experian**	**TransUnion**
https://www.equifax.com/personal/credit-report-services/	https://www.experian.com/help/	https://www.transunion.com/credit-help
1-888-298-0045	1-888-397-3742	1-800-916-8800
Equifax Fraud Alert, P.O. Box 105069 Atlanta, GA 30348-5069	Experian Fraud Alert, P.O. Box 9554, Allen, TX 75013	TransUnion Fraud Alert, P.O. Box 2000, Chester, PA 19016
Equifax Credit Freeze, P.O. Box 105788 Atlanta, GA 30348-5788	Experian Credit Freeze, P.O. Box 9554, Allen, TX 75013	TransUnion Credit Freeze, P.O. Box 160, Woodlyn, PA 19094

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.