EXHIBIT 1

By providing this notice, NYLAG 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 September 8, 2020, NYLAG learned of unusual activity in certain employee email accounts and immediately launched an investigation, with the assistance of a third-party computer forensic investigator. The investigation included a review of NYLAG's entire email tenant and identified unauthorized access to certain employee email accounts between August 15, 2020 and September 24, 2020. Upon discovery, NYLAG immediately forced a password reset for the entire organization to stop any further access, and the accounts were secured.

NYLAG then conducted a review of its files to determine what type of information may have been present in the email accounts at the time of the incident. The investigation was unable to confirm if specific information in the email account was actually seen by the unknown person(s) who accessed the accounts; however, NYLAG opted to notify individuals who may have information in the email accounts out of an abundance of caution. Therefore, NYLAG conducted a review of its files to determine contact information to provide written notice to potentially impacted individuals. This review was completed on December 11, 2020.

The information that could have been subject to unauthorized access includes first and last name, address, as well as one or more of the following: Social Security number, driver's license or other government issued ID number, financial account/payment card information, passport number, medical/health insurance information, and username and password.

Notice to Maine Residents

On or about January 19, 2021, NYLAG provided written notice of this incident to affected individuals, which include two Maine residents. 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, NYLAG moved quickly to investigate and respond to the incident and assess the security of NYLAG systems NYLAG is also implementing additional safeguards, including enterprise wide multi-factor authentication for email, as well as additional training to its employees. NYLAG is providing access to credit monitoring and identity protection services for one year through TransUnion to individuals whose personal information was potentially affected by this incident, at no cost to these individuals.

Additionally, NYLAG is providing impacted individuals with guidance on how to better protect against identity theft and fraud, including advising individuals to report any suspected incidents of identity theft or fraud. NYLAG 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.

EXHIBIT A

NYLAG
New York Legal Assistance Group

Return Mail Processing Center
P.O. Box 6336
Portland, OR 97228-6336

<<Mail ID>>
<<Name 1>>
<<Name 2>>
<<Address 1>>
<<Address 2>>
<<Address 3>>
<<Address 4>>
<<Address 5>>
<<City>><<State>><<Zip>>
<<Country>>

<<Date>>

Dear <<Name 1>>:

New York Legal Assistance Group ("NYLAG") is writing to let you know that one or more people outside of NYLAG accessed some of our employee email accounts without our permission. As a result, some of your personal information may have been seen by them, and although we have no evidence of actual or attempted misuse of information, there is a risk that this information has been, or could be misused. We are offering free resources to help prevent this from happening to you. If you would like to use these services, you must sign up for them by <<Enrollment Deadline>>, following the directions provided in the materials that follow. This letter has more information about what happened, our response, and the free resources that can help you protect your personal information from possible misuse. The confidentiality, privacy, and security of your personal information is one of our highest priorities.

What Happened? On September 8, 2020, we learned of unusual activity in our employee's email account. We immediately started an investigation to learn everything we could about what happened. We worked with a computer specialist that has expertise in email security incidents like this one, to handle the investigation.

From our investigation, we learned that an unknown person(s) accessed certain employee email accounts between August 15, 2020 and September 24, 2020. Once we identified these email accounts, we immediately forced a password reset for the entire organization to stop any further access by the unknown person(s). Although we are unable to confirm if specific information in the email accounts was actually seen by the unknown person(s) who accessed the accounts, to be safe, we are notifying individuals who may have information in the email accounts.

What Information Was Involved? The personal information that may have been present in the email accounts at the time of the incident would have been information provided to NYLAG or otherwise obtained by NYLAG in the normal course of providing you services. This information may have included your first and last name as well as one or more of the following: Social Security number, driver's license or other government issued ID number, financial account/payment card information, passport number, medical/health insurance information, and username and password.

What We Are Doing. We put additional security measures in place to protect against another incident in the future. Also, although we do not know for sure that any of your personal information was seen or misused, we are notifying you about what happened so that you may take further steps to help protect yourself from identity theft or fraud if you wish to do so.

We are offering you free identity monitoring services for 12 months through TransUnion Interactive, a subsidiary of TransUnion® (a private company with a lot of experience helping people with matters like this) as an added precaution. If you would like to use these resources, you must sign up for them by <<Enrollment Deadline>>. NYLAG will pay for the cost of these services. More information about these services is included with this letter on a separate page with the heading, "Steps You May Take To Help Protect Personal Information."

What You Can Do. We also recommend that you watch out for identity theft and any signs of fraud using your personal information. You should review your bank and credit card account statements, credit reports, and any insurance benefits or other similar forms for suspicious activity or errors. You should also consider changing any usernames or passwords provided to NYLAG. Please also read the enclosed "Steps You May Take to Help Protect Personal Information."

For More Information. We understand you may have questions that are not answered in this letter. If you have questions, please contact our free help line at 877-853-3842, Monday through Friday, between 9:00 a.m. and 9:00 p.m. Eastern Time. An interpreter will be provided free of charge if you need it.

Protecting your personal information and protecting you from identity theft or fraud is very important to us, and we are committed to working with you to make sure that happens.

Sincerely,

New York Legal Assistance Group

Steps You May Take To Help Protect Personal Information

You May Activate Free Identity Monitoring Services

Complimentary One-Year *my*TrueIdentity Credit Monitoring Service

As a safeguard, we have arranged for you to enroll, at no cost to you, in an online credit monitoring service (*my*TrueIdentity) for one year provided by TransUnion Interactive, a subsidiary of TransUnion,® one of the three nationwide credit reporting companies.

How to Enroll: You can sign up online or via U.S. mail delivery

- To enroll in this service, go to the *my*TrueIdentity website at **www.MyTrueIdentity.com** and, in the space referenced as "Enter Activation Code," enter the 12-letter Activation Code **<<Insert Unique 12-letter Activation Code>>** and follow the three steps to receive your credit monitoring service online within minutes.
- If you do not have access to the Internet and wish to enroll in a similar offline, paper-based credit monitoring service, via U.S. mail delivery, please call the TransUnion Fraud Response Services toll-free hotline at **1-855-288-5422**. When prompted, enter the six-digit telephone passcode **<<Insert static 6-digit Telephone Pass Code>>** and follow the steps to enroll in the offline credit monitoring service, add an initial fraud alert to your credit file, or to speak to a TransUnion representative if you believe you may be a victim of identity theft.

You can sign up for the online or offline credit monitoring service anytime between now and **<<Enrollment Deadline>>**. Due to privacy laws, we cannot register you directly. Please note that credit monitoring services might not be available for individuals who do not have a credit file with TransUnion or an address in the United States (or its territories) and a valid Social Security number. Enrolling in this service will not affect your credit score.

ADDITIONAL DETAILS REGARDING YOUR 12-MONTH COMPLIMENTARY CREDIT MONITORING SERVICE:

- Once you are enrolled, you will be able to obtain one year of unlimited access to your TransUnion credit report and credit score.
- The daily credit monitoring service will notify you if there are any critical changes to your credit file at TransUnion, including fraud alerts, new inquiries, new accounts, new public records, late payments, changes of address, and more.
- The service also includes access to an identity restoration program that provides assistance in the event that your identity is compromised and up to $1,000,000 in identity theft insurance with no deductible. (Policy limitations and exclusions may apply.)

Watch Your Financial Accounts Carefully

Order Free Credit Reports
A credit report is a statement that has information about your credit situation, such as loan paying history and the status of your credit accounts. Under U.S. law, you are entitled to one free credit report per year from each of the three major credit reporting bureaus - Experian, TransUnion, and Equifax.

To order your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also contact Experian, TransUnion, and Experian (see below) to request a free copy of your credit report.

Place a Security Freeze
You have the right to place a "security freeze" on your credit report, which will stop a consumer reporting agency (a private company that collects and shares information about your finances) from sharing information in your credit report without your permission. Under U.S. law, it is free to place or lift a security freeze on your credit report.

The security freeze is designed to prevent credit, loans, and services from being approved in your name without your permission. However, it is important to know that using a security freeze may delay or stop the on-time approval of applications you make for a new loan, credit, mortgage, or any other account involving the extension of credit. To place a security freeze, you will need to contact each of the consumer reporting agencies below and provide the following information:

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. If you have moved in the past 5 years, provide the addresses where you have lived over the prior 5 years;
5. Proof of current address, such as a current utility bill or telephone bill;
6. A readable photocopy of a government-issued identification card (state driver's license or ID card, etc.);
7. If you are a victim of identity theft, include a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft.

To place a security freeze or learn more about it, please contact:

Experian	**TransUnion**	**Equifax**
P.O. Box 9554	P.O. Box 160	P.O. Box 105788
Allen, TX 75013	Woodlyn, PA 19094	Atlanta, GA 30348-5788
1-888-397-3742	1-888-909-8872	1-800-685-1111
www.experian.com/freeze/center.html	www.transunion.com/credit-freeze	www.equifax.com/personal/credit-report-services

Place a Fraud Alert on Your Credit File
As an alternative to a security freeze, you have the right to place an initial or extended "fraud alert" on your consumer credit file, for free. A "consumer credit file" is the information Experian, TransUnion, or Equifax has about you in its database. For example, it may include information you give when you apply for a credit card, your credit limit on a credit card, and whether you pay on time.

An "initial fraud alert" is a 1-year alert you can place on your credit file. When you have this, a business must take extra steps to confirm the identity of anyone who applies for credit using your name, before approving the application. If you are a victim of identity theft, you are entitled to a free "extended fraud alert," which is a fraud alert that lasts seven years.

To place a fraud alert or learn more, please contact any one of the agencies listed below:

Experian	**TransUnion**	**Equifax**
P.O. Box 9554	P.O. Box 2000	P.O. Box 105069
Allen, TX 75013	Chester, PA 19016	Atlanta, GA 30348
1-888-397-3742	1-800-680-7289	1-888-766-0008
www.experian.com/fraud/center.html	www.transunion.com/fraud-victim-resource/place-fraud-alert	www.equifax.com/personal/credit-report-services

How to Contact Law Enforcement if You are a Victim of Identity Theft or Fraud

Federal Trade Commission
You can further educate yourself regarding identity theft, fraud alerts, security freezes, and the steps you can take to protect your information by contacting the consumer reporting agencies, the Federal Trade Commission, or your state Attorney General. The Federal Trade Commission (FTC) is the U.S. agency that oversees federal services for victims of identity theft. The FTC can be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580, www.identitytheft.gov, 1-877-ID-THEFT (1-877-438-4338); TTY: 1-866-653-4261. The FTC encourages anyone whose personal information has been misused to file a complaint with them. Contact the FTC to learn more about how to file a complaint.

Local Police Department
You have the right to file a police report if you ever experience identity theft or fraud, and you also have the right to file a police report with your local police. To file a report with law enforcement for identity theft, you will likely need to provide some proof that you have been a victim.

Learn More

To learn more about identity theft and the steps you can take to protect yourself or your family members, contact the consumer reporting agencies (Experian, TransUnion, and Equifax), the Federal Trade Commission, or your state Attorney General. This notice has not been delayed by law enforcement.

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

For New Mexico residents, you have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for credit reports to be provided to employers; you may limit "prescreened" offers of credit and insurance you get based on information in your credit report; and you may seek damages from violators. You may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. We encourage you to review your rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

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

For North Carolina residents, the Attorney General may be contacted at: 9001 Mail Service Center, Raleigh, NC 27699-9001, 1-877-566-7226 (toll free within NC) or 1-919-716-6400, www.ncdoj.gov.