EXHIBIT 1

This notice will be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, Wade Clark Mulcahy, LLP ("Wade Clark Mulcahy") 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

Wade Clark Mulcahy recently concluded its investigation into a February 2022 data security incident involving a malware infection that impacted its computer systems and caused a temporary disruption to services. Upon learning of the incident, Wade Clark Mulcahy immediately began working with third party forensic specialists to confirm the nature and scope of the incident and ensure the security of its environment. Through the investigation, Wade Clark Mulcahy learned that it was the victim of a sophisticated cyberattack involving ransomware, and that an unauthorized actor may have accessed or acquired a limited amount of data stored within its environment between February 2, 2022 and February 7, 2022. Through a third party data analytics vendor, Wade Clark Mulcahy conducted a thorough review of the data that was potentially impacted to determine whether it contained any sensitive information. However, because the review was unable to capture address information for the potentially affected individuals, Wade Clark Mulcahy underwent a further time-consuming review to locate the missing address information. This review was recently concluded on or around July 15, 2022.

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

Notice to Maine Residents

On or about July 21, 2022, Wade Clark Mulcahy provided written notice of this incident to approximately two (2) 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, Wade Clark Mulcahy moved quickly to investigate and respond to the incident, assess the security of Wade Clark Mulcahy systems, and identify potentially affected individuals. Further, Wade Clark Mulcahy notified federal law enforcement regarding the event. Wade Clark Mulcahy is providing access to credit monitoring services for 12 months, through Experian, to individuals whose personal information was potentially affected by this incident, at no cost to these individuals.

Additionally, Wade Clark Mulcahy 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 to their credit card company and/or bank. Wade Clark Mulcahy 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. Wade Clark Mulcahy is providing written notice of this incident to relevant regulators, as necessary.

EXHIBIT A

WADE CLARK MULCAHY LLP | ATTORNEYS

Return Mail Processing
PO Box 999
Suwanee, GA 30024

SAMPLE A. SAMPLE - L01
APT ABC
123 ANY ST
ANYTOWN, US 12345-6789

[Extra1]

Dear Sample A. Sample:

Wade Clark Mulcahy LLP ("Wade Clark Mulcahy") is writing to notify you of a recent incident that may affect the security of your information. You are receiving this letter because you are a current or former client of Wade Clark Mulcahy, or a witness or other individual associated with a matter the firm previously handled. While we are unaware of any actual misuse of your information, we are providing you with notice of the incident, steps we are taking in response, and resources available to help you better protect your information, should you feel it is appropriate to do so.

What Happened?

On February 7, 2022, we experienced a data security incident that impacted our computer systems and caused a temporary disruption to services. Upon learning of the incident, we immediately worked to secure our systems and with the assistance of third party forensic specialists, commenced an investigation to confirm the nature and scope of the incident. The investigation determined that we were the victim of a sophisticated cyberattack involving ransomware, and that an unauthorized actor may have accessed and/or acquired a limited amount of information stored on our systems between February 2, 2022 and February 7, 2022. We conducted a thorough and time-consuming review of the affected data to determine whether any sensitive information was accessed or acquired as a result of this event. This review was completed on July 15,2022, and it determined that your information was in the files that may have been accessed or acquired without authorization.

What Information Was Involved?

As indicated above, we are unaware of any actual or attempted misuse of your personal information. However, we are providing you with this notification out of an abundance of caution. The information present in the files that were potentially impacted by this incident may have included your [Extra2], and name.

What We Are Doing.

Wade Clark Mulcahy treats its responsibility to safeguard information as an utmost priority. We responded immediately to this incident and worked diligently to provide you with an accurate and complete notice of the incident as soon as possible. As part of our ongoing commitment to the privacy and security of personal information in our care, we are reviewing and updating existing policies and procedures relating to data protection and security. We are also investigating additional security measures to mitigate any risk associated with this incident and to better prevent future similar incidents. We are providing notice of this incident to potentially impacted individuals and to regulators where required.

Out of an abundance of caution, we are also providing you with [Extra3] months of complimentary access to credit monitoring services through Experian, as well as guidance on how to better protect your information, should you feel it is appropriate to do so. Although we are covering the cost of these services, due to privacy restrictions, you will need to complete the activation process yourself.

What You Can Do.

You can find out more about how to safeguard your information in the enclosed *Steps You Can Take To Protect Personal Information*. We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your account statements and monitoring your free credit reports for suspicious activity and to detect errors. We also encourage you to enroll in the complementary credit monitoring services. Enrollment instructions are enclosed with this letter.

For More Information.

If you have additional questions, please contact our dedicated assistance line at (877) 653-0510, toll-free Monday through Friday from 8 am - 10 pm Central, or Saturday and Sunday from 10 am - 7 pm Central (excluding major U.S. holidays). Be prepared to provide your engagement number: **[Engagement Number]**. You may also write to us at: 180 Maiden Lane, Suite 901, New York, NY 10038.

Sincerely,

Rachel Wade
Office Manager

STEPS YOU CAN TAKE TO PROTECT PERSONAL INFORMATION

Enroll in Complimentary Credit Monitoring

To help protect your identity, we are offering complimentary access to Experian IdentityWorks[SM] for [Extra3] months.

If you believe there was fraudulent use of your information as a result of this incident and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent. 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 from the date of the incident (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 Identity Restoration is available to you for [Extra3] months 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.

While identity restoration assistance is immediately available to you, we also encourage you to activate the fraud detection tools available through Experian IdentityWorks as a complimentary [Extra3] month membership. This product provides you with superior identity detection and resolution of identity theft. To start monitoring your personal information, please follow the steps below:

- Ensure that you **enroll by October 31, 2022** (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll: www.experianidworks.com/credit
- Provide your **activation code**: **ABCDEFGHI**

If you have questions about the product, need assistance with Identity Restoration that arose as a result of this incident, or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at **(877) 653-0510** by **October 31, 2022**. Be prepared to provide engagement number **[Engagement Number]** as proof of eligibility for the Identity Restoration services by Experian.

ADDITIONAL DETAILS REGARDING YOUR [Extra3] MONTH 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.
- **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.
- **$1 Million Identity Theft Insurance**:** Provides coverage for certain costs and unauthorized electronic fund transfers.

* 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.

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	1-833-395-6938
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.

For Maryland residents, the Maryland Attorney General may be contacted at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-410-528-8662 or 1-888-743-0023; and www.oag.state.md.us.

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 bureaus 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 violator. 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 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.