EXHIBIT 1

This notice will be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, Digital Prospectors Corp. ("DPC"), located at 100 Domain Drive, Suite 103, Exeter, NH 03833 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 or about September 26, 2022, DPC discovered unusual activity impacting a single employee laptop. Upon this discovery, it quickly commenced an investigation that included working with third-party cybersecurity specialists to understand the nature and scope of the incident and to confirm that it did not impact the larger DPC network. DPC's investigation determined that an unknown actor accessed the laptop only and that certain data housed on it may have been placed at risk as a result. DPC conducted an exhaustive review of the data on the laptop to identify the type of information it contained and to whom that information related. On December 20, 2022, the review determined that certain information resided in files on the laptop and that those files were accessible to an unknown actor briefly on September 26, 2022.

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

Notice to Maine Residents

On or about January 19, 2023, DPC provided written notice of this incident to seven (7) 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, DPC moved quickly to investigate and respond to the incident, assess the security of DPC systems, and identify potentially affected individuals. DPC is also reviewing and enhancing its existing policies and procedures to reduce the likelihood of a similar future incident. DPC 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, DPC is providing impacted individuals with guidance on how to better protect against identity theft and fraud. DPC 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.

DPC is providing written notice of this incident to relevant state regulators, as necessary.

EXHIBIT A

<Return Name>
c/o Cyberscout
<Return Address>
<City> <State> <Zip>

<FirstName> <LastName>
<Address1>
<Address2>
<City><State><Zip>

January x, 2023

NOTICE OF <<variable text 1>>

Dear <<first name>> <<last name>>:

Digital Prospectors Corp. ("DPC") is writing to notify you as a current/former employee or a dependent of an employee, about a recent incident that may impact the privacy of some of your information. This notice provides you with information about the incident, our response, and additional steps you may take to protect your information, should you determine it is appropriate to do so. Although we are unaware of any actual or attempted misuse of your information, we are offering you complimentary credit and fraud monitoring with identity theft insurance, at no cost to you; enrollment instructions are found on the next page.

What Happened? On September 26, 2022, DPC discovered unusual activity impacting a single employee laptop. Upon this discovery, we quickly commenced an investigation that included working with third-party cybersecurity specialists to understand the nature and scope of the incident and to confirm that it did not impact the larger DPC network. Our investigation determined that an unknown actor accessed the laptop only and that certain data housed on it may have been placed at risk as a result. DPC conducted an exhaustive review of the data on the laptop to identify the type of information it contained and to whom that information related. On December 20, 2022, the review determined that your information resided in files on the laptop and that those files were accessible to an unknown actor briefly on a single day. Please note that we have no information indicating that the unknown actor actually accessed or acquired any of your information. We provide this notice out of an abundance of caution.

What Information Was Involved? The involved DPC systems contained your name, <<exposed data elements>>.

What We Are Doing. Upon discovering this incident, we quickly took steps to investigate and respond, including reviewing and enhancing our existing policies and procedures to reduce the likelihood of a similar future incident. DPC is notifying individuals and relevant regulators as required. Moreover, as an added precaution, DPC is offering complimentary access to credit monitoring and identity restoration services to potentially impacted individuals out of an abundance of caution.

What You Can Do. DPC encourages you to remain vigilant against incidents of identity theft and fraud by reviewing your account statements and explanation of benefits and by monitoring your free credit reports for suspicious activity. You may also review and consider the information and resources outlined in the below "Steps You Can Take to Help Protect Personal Information."

For More Information. If you have additional questions, please call our dedicated assistance line at 1-800-405-6108 (toll free), Monday through Friday, from 8:00 am – 8:00 pm Eastern Time (excluding U.S. holidays).

Sincerely,

Digital Prospectors Corp.

STEPS YOU CAN TAKE TO PROTECT PERSONAL INFORMATION

Enroll in Credit Monitoring Services

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/digitalprospectors** and follow the instructions provided. When prompted please provide the following unique code to receive services: **<<unique code>>** 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 one-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 credit 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 fraud alert or 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

Internal Revenue Service Identity Protection PIN (IP PIN)

You may also obtain an Identity Protection PIN (IP PIN) from the Internal Revenue Service, a six-digit number that prevents someone else from filing a tax return using your Social Security number or Individual Taxpayer Identification Number. The IP PIN is known only to you and the IRS, and helps the IRS verify your identity when you file your electronic or paper tax return. Even though you may not have a filing requirement, an IP PIN still protects your account. If you do not already have an IP PIN, you may get an IP PIN as a proactive step to protect yourself from tax-related identity theft either online, by paper application or in-person. Information about the IP PIN program can be found here: https://www.irs.gov/identity-theft-fraud-scams/get-an-identity-protection-pin.

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 District of Columbia residents, the District of Columbia Attorney General may be contacted at: 400 6th Street, NW, Washington, DC 20001; 202-727-3400; and oag.dc.gov.

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 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. Digital Prospectors Corp. is located at 100 Domain Drive, Suite 103, Exeter, NH 03833.

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 Rhode Island residents, the Rhode Island Attorney General may be reached at: 150 South Main Street, Providence, RI 02903; 1-401-274-4400; and www.riag.ri.gov. Under Rhode Island law, you have the right to obtain any police report filed in regard to this incident. There are 11 Rhode Island residents impacted by this incident.