EXHIBIT 1

Infotek reserves the right to supplement this notice. By providing this notice, Infotek 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 around February 18, 2022, Infotek identified suspicious activity within its systems. Infotek promptly responded to this activity and took its systems offline as a precautionary measure, initiated response protocols, and implemented its business continuity plans to minimize disruption to its customers and to ensure the ongoing security of its systems. Infotek also launched a comprehensive investigation with the assistance of computer forensic specialists. The subsequent investigation determined an unknown individual(s) gained access to segments of Infotek's network and exfiltrated certain documents contained within these locations from December 29, 2021 until February 28, 2022.

Infotek thereafter undertook a comprehensive review of the potentially impacted data to identify the impacted individuals so they could be notified. On May 16, 2022, Infotek determined information related to residents of Maine was impacted by this event. The information that could have been subject to unauthorized access includes name, Social Security number, driver's license or state identification number, and financial account information.

Notice to Maine Residents

On or about June 7, 2022, Infotek provided written notice of this incident to approximately four (4) 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, Infotek moved quickly to respond to the incident and to assess the security of its systems. Infotek conducted a comprehensive investigation to determine the nature and scope of unauthorized activity, including what information was at risk, so it could notify potentially affected individuals. Infotek is also working to implement additional safeguards within its network environment as appropriate.

Infotek is providing access to credit monitoring services for 24 months, through CyberScout, to individuals whose personal information was potentially affected by this incident, at no cost to these individuals. Additionally, Infotek is providing impacted individuals with guidance on how to better protect against identity theft and fraud. Infotek 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 for 12 to 24 months by reviewing account statements and monitoring free credit reports, and encouragement to contact the Federal Trade Commission, their state Attorney General, and/or law enforcement to report attempted or actual identity theft and fraud.

EXHIBIT A

DATE

«AddressBlock»

File #: «Resource_ID»

Re: Notice of Data Incident

Dear «Cleansed_Full_Name»:

Infotek Consulting Services Inc. and its related companies are writing to inform you of an incident that impacts some of your personal information. We have been working hard to complete an extensive investigation into the incident and a comprehensive review of the data concerned to identify those involved. We are writing to provide you with some information about the incident so that you can understand what happened, how you may be affected, our response and additional steps that can be taken to protect your information, should you feel it appropriate to do so.

What happened? On or around February 18, 2022, we detected an event involving our internal systems. We promptly took our systems offline as a precautionary measure, initiated response protocols, launched an investigation with the assistance of third-party cybersecurity and forensic specialists, and implemented our business continuity plans to minimize disruption to our customers, and ensure the ongoing security of our systems. Our investigation determined that this was a highly sophisticated attack which led to an unknown individual(s) gaining access to and exfiltrating data contained within certain segments of our network. The forensic investigation revealed that the first traces of successful unauthorized access of our systems date back to December 29, 2021.

Therefore, adopting a cautious approach, we undertook a comprehensive automated and manual review of the data with the assistance of computer forensic specialists, to identify what information could have been involved in this incident. On May 16, 2022, we completed this review and identified the potentially impacted information, including your information.

What information was involved? We have no evidence of any actual or attempted fraudulent misuse of any of your information. However, as the potentially impacted information included your «Data_Elements», we wanted to make you aware of what our investigation has identified so that you can take any appropriate steps should you wish to do so.

What are we doing? The privacy and security of consultants' and employees' information is one of our highest priorities and we have strict security measures in place to protect all information in our care. In parallel with our investigation into this isolated incident, we have reviewed our existing security policies and implemented additional measures and enhanced security tools to further protect information in our systems. We have also reported this incident to appropriate law enforcement authorities.

In addition to the information we are sharing in this letter, for additional security and peace of mind, we are offering you, with no costs to you, identity and credit monitoring services for 24 months. Information and instructions on how to enroll in these complimentary services can be found in the “Steps You Can Take to Help Protect Your Information” attached to this letter, as well as additional steps you can take to increase the protection of your data.

What can you do? You can review the enclosed ***schedule***. You can also enroll to receive the complimentary credit monitoring and identity protection services through CyberScout. We also encourage you to remain vigilant against incidents of identity theft and fraud, to review your account statements, and to monitor your credit reports for suspicious activity.

For more information. We recognize that you may have questions not addressed in this letter. If you have additional questions, please email helpline@infotek-consulting.com or call 1-(647) 245-5710.

We apologize for any inconvenience this incident cause, protecting your personal information is extremely important to us, and we remain committed to safeguarding all data in our control.

Yours sincerely,

Sherine Marzouk
Vice-President
Infotek Consulting Services Inc.

Schedule: Steps You Can Take to Help Protect Your Information

[Customer Logo]

Activation Code: XXXX-XXXX-XXXX-XXXX

We have retained the assistance of CyberScout, a company specializing in fraud assistance and remediation services.

Through CyberScout, we have arranged **24 month** subscription to Credit Monitoring services* , at no cost to you. CyberScout has been retained to help you with any questions or problems you may encounter, including assisting you with obtaining a credit report and placing fraud alerts.

We encourage you to take advantage of this service and help protect your identity. To activate your service, please visit:

https://www.myidmanager.com

You will be prompted to enter the following activation code:

xxxx-xxxx-xxxx-xxxx

Please ensure that you redeem your activation code before **9/30/2022** to take advantage of the service.

Upon your completion of the enrollment process, you will have access to the following features:

- Access to a credit report with credit score. A credit report is a snapshot of a consumer's financial history and primary tool leveraged for determining credit-related identity theft or fraud.
- Credit monitoring alerts with email notifications to key changes on a consumer's credit file. In today's virtual world, credit alerts are a powerful tool to protect against identity theft, enable quick action against potentially fraudulent activity, and provide overall confidence to potentially impacted consumers.
- Dark Web Monitoring to provide monitoring of surface, social, deep, and dark websites for potentially exposed personal, identity and financial information in order to help protect consumers against identity theft.
- Identity theft insurance of up to $1,000,000 in coverage to protect against potential damages related to identity theft and fraud
- Assistance with reading and interpreting credit reports for any possible fraud indicators.
- Assistance with answering any questions individuals may have about fraud.

Services marked with an "" require 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.

Should you have any questions regarding the CyberScout solution, have difficulty enrolling, or require additional support, please contact CyberScout at 1-800-405-6108 from Monday to Friday 8:00 am – 8:00 pm EST, excluding holidays.

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 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 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, D.C. 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. Infotek Consulting Services Inc. is located at 135 Yorkville Ave #700, Toronto, ON M5R 0C7.

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.