EXHIBIT 1

This notice will be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, DMS Health Technologies Inc. ("DMS") located at 728 East Beaton Drive, Suite 101, West Fargo, North Dakota, 58078, 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 April 23, 2023, DMS became aware of suspicious activity related to certain computer systems. DMS immediately launched an investigation, with the assistance of third-party forensic specialists, to secure its network and determine the nature and scope of the activity. Through the investigation, it was determined that there was unauthorized access to DMS's systems between March 27, 2023, and April 24, 2023. Therefore, DMS undertook a comprehensive review of the data determined to be at risk to assess if any sensitive information could be affected and to whom it related. The information that could have been subject to unauthorized access includes name, Social Security number, and driver's license number.

Notice to Maine Resident

On or about June 21, 2023, July 6, 2023, and September 21, 2023, DMS provided written notice of this incident to affected individuals which include one (1) Maine resident. Written notice is being provided in substantially the same form as the letter attached here as ***Exhibit A***. As DMS does not own some of the data at issue, DMS also provided notice to appropriate data owners who may request that DMS provide additional notices on their behalf to individuals and regulators. DMS may supplement this notice as needed to report additional resident who are notified on behalf of one or more data owners.

Other Steps Taken and To Be Taken

Upon discovering the event, DMS moved quickly to investigate, assess the security of its systems, and identify potentially affected individuals. Further, DMS notified federal law enforcement regarding the event and is providing individuals who had a Social Security number potentially affected by this incident with access to twelve (12) months of credit monitoring services through Kroll at no cost to the individuals.

DMS is providing impacted individuals with guidance on how to better protect against identity theft and fraud. DMS is also 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. DMS is also providing written notice of this incident to relevant state and federal regulators, as necessary.

EXHIBIT A

<<Date>> (Format: Month Day, Year)

<<first_name>> <<middle_name>> <<last_name>> <<suffix>>
<<address_1>>
<<address_2>>
<<city>>, <<state_province>> <<postal_code>>
<<country>>

<<b2b_text_1 (NOTICE OF [SECURITY INCIDENT] / [DATA BREACH])>>

Dear <<first_name>> <<middle_name>> <<last_name>> <<suffix>>,

DMS Health Technologies ("DMS") is writing to inform you of an incident that may involve some of your information. We are providing you with information about the event, our response, and resources available to you to help protect your information, should you feel it appropriate to do so.

What Happened? On April 23, 2023, DMS became aware of suspicious activity related to certain computer systems. We immediately launched an investigation, with the assistance of third-party forensic specialists, to secure our network and determine the nature and scope of the activity. The investigation determined that there was unauthorized access to DMS's network between March 27 and April 24, 2023, and the unauthorized actor had the ability to access certain information stored on the network during the period of access. Therefore, DMS undertook a comprehensive review of the data at risk to assess if any sensitive information could be affected and to whom it related. Although our forensics team has not identified definitive proof that any information was acquired, as an added precaution, we are notifying you because certain information related to you could be affected.

What Information Was Involved? The types of information potentially affected by this incident include your: <<b2b_text_3 (Data Elements)>>. DMS has no indication that your information has been misused in relation to this incident.

What We Are Doing. We take this event and the security of your information very seriously. Upon learning of this event, we immediately took steps to secure our network and implement additional administrative and technical safeguards to further secure the information in our care. Notice was also provided to federal law enforcement and the Department of Health and Human Services as part of our comprehensive incident response. Additionally, out of an abundance of caution, DMS is providing you with 12 months of complimentary identity monitoring services through Kroll. Although we are covering the cost of these services, you will need to complete the activation process yourself. Instructions on how to activate the services can be found in the enclosure.

What You Can Do. We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your account statements, explanation of benefits, and monitoring your free credit reports for suspicious activity. You can also find out more about how to safeguard your information in the enclosed *Steps You Can Take to Help Protect Personal Information*.

For More Information. If you have questions, you may call our dedicated assistance line at TFN, Monday through Friday from 8:00 a.m. to 5:30 p.m. Central Time excluding major U.S. holidays. You may also write to DMS directly at 728 East Beaton Drive, Suite 101, West Fargo, ND 58078.

Sincerely,

Patrick Doyle
CEO
DMS Health Technologies

Steps You Can Take To Help Protect Personal Information

Activate the Monitoring Services

Visit **https://enroll.krollmonitoring.com** to activate and take advantage of your identity monitoring services.
You have until ***<<b2b_text_6(activation deadline)>>*** *to activate your identity monitoring services.*
Membership Number: **<<Membership Number s_n>>**

For more information about Kroll and your Identity Monitoring services, you can visit info.krollmonitoring.com.

KROLL

TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES

You have been provided with access to the following services from Kroll:

Single Bureau Credit Monitoring

You will receive alerts when there are changes to your credit data—for instance, when a new line of credit is applied for in your name. If you do not recognize the activity, you'll have the option to call a Kroll fraud specialist, who will be able to help you determine if it is an indicator of identity theft.

Fraud Consultation

You have unlimited access to consultation with a Kroll fraud specialist. Support includes showing you the most effective ways to help protect your identity, explaining your rights and protections under the law, assistance with fraud alerts, and interpreting how personal information is accessed and used, including investigating suspicious activity that could be tied to an identity theft event.

Identity Theft Restoration

If you become a victim of identity theft, an experienced Kroll licensed investigator will work on your behalf to resolve related issues. You will have access to a dedicated investigator who understands your issues and can do most of the work for you. Your investigator will be able to dig deep to uncover the scope of the identity theft, and then work to resolve it.

Kroll's activation website is only compatible with the current version or one version earlier of Chrome, Firefox, Safari and Edge.
To receive credit services, you must be over the age of 18 and have established credit in the U.S., have a Social Security number in your name, and have a U.S. residential address associated with your credit file.

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 a free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. Consumers may also directly contact the three major credit reporting bureaus listed below to request a free copy of their 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 consumers are the victim of identity theft, they are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should consumers wish to place a fraud alert, please contact any 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 a consumer's name without consent. However, consumers should be aware that using a credit freeze to take control over who gets access to the personal and financial information in their credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application they make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, consumers cannot be charged to place or lift a credit freeze on their credit report. To request a credit freeze, individuals may need to provide some or all of 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 they are a victim of identity theft.

Should consumers wish to place a credit freeze or fraud alert, 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

Consumers may further educate themselves regarding identity theft, fraud alerts, credit freezes, and the steps they can take to help protect your personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or their 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. Consumers can obtain further information on how to file such a complaint by way of the contact information listed above. Consumers have the right to file a police report if they ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, consumers will likely need to provide some proof that they have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and the relevant 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 https://www.marylandattorneygeneral.gov/.

For New Mexico residents, consumers have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in their credit file has been used against them, the right to know what is in their credit file, the right to ask for their 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 consumers' files is limited; consumers must give consent for credit reports to be provided to employers; consumers may limit "prescreened" offers of credit and insurance based on information in their credit report; and consumers may seek damages from violators. Consumers 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 consumers to review their 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.

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