EXHIBIT 1

This notice may be supplemented with any significant facts learned subsequent to its submission. By providing this notice, Globalstar 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 4, 2020, Globalstar became aware of unusual activity related to an employee's email account. Globalstar immediately took steps to change the user's password and commenced an investigation to determine the nature and scope of the incident with assistance from third-party computer forensic specialists. On September 23, 2020, the investigation determined that an unauthorized actor(s) gained access to certain Globalstar employee email accounts at various times between July 8, 2020 and September 11, 2020.

The contents of the impacted email accounts were next reviewed through a time-consuming manual and programmatic process to determine what sensitive data may have been accessible. Globalstar confirmed the identities of the individuals who may have had information accessible as a result of the incident and launched a review of internal files to ascertain address information for the potentially impacted individuals. This process was completed on January 22, 2021. Although Globalstar is unaware of any actual or attempted misuse of any information, Globalstar is notifying potentially affected individuals out of an abundance of caution.

The information that could have been subject to unauthorized access includes name, address, and payment card information.

Notice to Maine Resident

On February 9, 2021, Globalstar began providing written notice of this incident to potentially affected individuals, which includes one (1) Maine resident. 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, Globalstar moved quickly to investigate and respond to the incident, assess the security of Globalstar systems, and notify potentially affected individuals. Globalstar is also working to implement additional safeguards and training to its employees. Globalstar is providing access to credit monitoring services for one (1) year, through Kroll, to individuals whose personal information was potentially affected by this incident, at no cost to these individuals.

Additionally, Globalstar 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. Globalstar 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

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

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

Dear <<first_name>> <<middle_name>> <<last_name>> <<suffix>>:

Globalstar, Inc. ("Globalstar") writes to inform you of a recent event that may affect the security of some of your personal information. While, to date, we have no evidence that your information has been misused, we are making you aware of the event so you may take steps to better protect your information, should you feel it appropriate to do so.

What Happened. On September 4, 2020, Globalstar became aware of unusual activity related to an employee's email account. Globalstar immediately took steps to change the user's password and commenced an investigation to determine the nature and scope of the incident with assistance from third-party computer forensic specialists. On September 23, 2020, the investigation determined that an unauthorized actor(s) gained access to certain Globalstar employee email accounts at various times between July 8, 2020 and September 11, 2020.

The contents of the impacted email accounts were next reviewed through a time-consuming manual and programmatic process to determine what sensitive data may have been accessible. We confirmed the identities of the individuals who may have had information accessible as a result of the incident and launched a review of our files to ascertain address information for the impacted individuals. This process was completed on January 22, 2021. Although we are unaware of any actual or attempted misuse of your information, we are providing you this notification out of an abundance of caution because your information was present in the impacted email accounts.

What Information Was Involved. Our investigation determined that the following information related to you was present in the email accounts at the time of the incident: <<b2b_text_1(Data Elements)>>.

What We Are Doing. The confidentiality, privacy, and security of information in our care is one of our highest priorities. Upon learning of unusual activity in an employee email account, we immediately commenced an investigation to confirm the nature and scope of the event and identify what personal information may have been present in the affected emails. With the assistance of third-party forensic investigators, we have been working to identify and put in place resources to assist potentially affected individuals. While we have stringent security measures in place to protect information in our care, we are implementing additional safeguards to further protect the security of information in our systems, including the implementation of multi-factor authentication for all employee email accounts and disabling legacy email protocols throughout the environment. We will also be reporting this incident to state regulators, where appropriate.

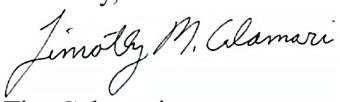
As an added precaution, we are offering you access to twelve (12) months of Credit Monitoring, Fraud Consultation and Identity Theft Restoration services through Kroll at no cost to you. The cost of these services will be paid for by Globalstar. More information on these services, as well as instructions about how to activate, may be found in the enclosed "Steps You Can Take To Help Safeguard Your Information." Please note that you must complete the activation process, as we are not able to activate these services on your behalf.

What You Can Do. We encourage you to review the enclosed "Steps You Can Take to Help Safeguard Your Information." You may also activate to receive the credit monitoring and identity restoration services we are offering at no cost to you.

For More Information. We understand you may have questions about this incident that are not addressed in this letter. If you have additional questions, please call our dedicated assistance line at 1-855-763-0487 (toll free), Monday through Friday, from 8:00 a.m. to 5:30 p.m. Central time.

Again, Globalstar takes the privacy and security of the personal information in our care seriously. We sincerely regret any inconvenience or concern this incident may cause you.

Sincerely,



Tim Calamari
Data Protection Officer

Steps You Can Take to Help Safeguard Your Information

Enroll in Credit Monitoring

We have secured the services of Kroll to provide identity monitoring at no cost to you for one year. Kroll is a global leader in risk mitigation and response, and their team has extensive experience helping people who have sustained an unintentional exposure of confidential data. Your identity monitoring services include Credit Monitoring, Fraud Consultation, and Identity Theft Restoration.

Visit **https://enroll.idheadquarters.com** to activate and take advantage of your identity monitoring services.

*You have until **May 10, 2021** to activate your identity monitoring services.*

Membership Number: **<<Member ID>>**

Monitor Accounts

We 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. Under U.S. law you are entitled to one free credit report annually from each of the three major credit reporting bureaus. To order your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also contact the three major credit bureaus directly to request a free copy of your credit report.

You have the right to place a "security freeze" on your credit report, which will prohibit a consumer reporting agency from releasing information in your credit report without your express authorization. The security 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 security 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 security freeze on your credit report. Should you wish to place a security freeze, please contact the major consumer reporting agencies listed below:

Experian
P.O. Box 9554
Allen, TX 75013
1-888-397-3742
www.experian.com/freeze/center.html

TransUnion
P.O. Box 160
Woodlyn, PA 19094
1-888-909-8872
www.transunion.com/credit-freeze

Equifax
P.O. Box 105788
Atlanta, GA 30348-5788
1-800-685-1111
www.equifax.com/personal/credit-report-services

In order to request a security freeze, you will need to 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 five (5) years, provide the addresses where you have lived over the prior 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, military identification, 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.

As an alternative to a security freeze, you have the right to place an initial or extended "fraud alert" on your 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 agencies listed below:

Experian
P.O. Box 9554
Allen, TX 75013
1-888-397-3742
www.experian.com/fraud/center.html

TransUnion
P.O. Box 2000
Chester, PA 19106
1-800-680-7289
www.transunion.com/fraud-victim-resource/place-fraud-alert

Equifax
P.O. Box 105069
Atlanta, GA 30348
1-888-766-0008
www.equifax.com/personal/credit-report-services

Additional Information

You can further educate yourself regarding identity theft, fraud alerts, security freezes, and the steps you can take to protect yourself, by contacting the consumer reporting agencies, the Federal Trade Commission, or your state Attorney

General. The Federal Trade Commission can be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580; www.identitytheft.gov; and 1-877-ID-THEFT (1-877-438-4338). 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.

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/.

North Carolina Residents: Office of the Attorney General of North Carolina**,** Consumer Protection Division, 9001 Mail Service Center Raleigh, NC 27699-9001, www.ncdoj.gov, Telephone: 1-919-716-6400, 877-566-7226 (toll free within NC).

Rhode Island Residents: Office of the Attorney General, 150 South Main Street, Providence, Rhode Island 02903, www.riag.ri.gov, Telephone: 401-274-4400. Under Rhode Island law, you have the right to obtain any police report filed in regard to this incident. There is 1 Rhode Island resident impacted by this incident.

Washington D.C. Residents: the Office of Attorney General for the District of Columbia can be reached at: 441 4thStreet NW, Suite 1100 South, Washington, D.C. 20001; 1-202-442-9828; https://oag.dc.gov.

Kroll | A Division of DUFF&PHELPS

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 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.