EXHIBIT 1

The investigation into this matter is ongoing, and this notice will be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, MTS 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 November 15, 2020, MTS became aware of suspicious activity on its computer network. MTS immediately launched an investigation, with the assistance of third-party specialists, and determined that portions of its network and certain applications connected to those servers had been infected with malware which prevented access to certain files on the system. The investigation determined that the malware was introduced into the system by an unauthorized actor who temporarily viewed and held certain files from within MTS' computer systems. MTS then undertook a lengthy and labor-intensive review of the potentially impacted files to identify data that may have been contained within impacted files, and to identify individuals whose personal information may have been impacted.

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

Notice to Maine Residents

On or about March 23, 2021, MTS provided written notice of this incident to affected individuals, which includes approximately two (2) Maine residents. Written notice is being provided in substantially the same form as the letter attached here as ***Exhibit A***. MTS's review of impacted data is ongoing, and this notification may be supplemented if it is determined that additional Maine residents will receive notice.

Other Steps Taken and To Be Taken

Upon discovering the event, MTS moved quickly to investigate and respond to the incident, assess the security of MTS systems, and notify potentially affected individuals. MTS is also working to implement additional safeguards and training for its employees. While MTS is not aware of any attempted or actual misuse of personal information, MTS is providing access to credit monitoring services for twelve (12) months, through Experian, to individuals whose personal information was potentially affected by this incident, at no cost to these individuals.

Additionally, MTS is providing impacted individuals with guidance on how to 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. MTS is providing individuals with information on how to place a fraud alert and security freeze on one's credit file, information on protecting against tax fraud, 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. MTS is also reporting this matter to other regulators as required.

EXHIBIT A

Return Mail Processing
PO Box 589
Claysburg, PA 16625-0589

March 23, 2021

G3216-L01-0000001 T00001 P001 *****AUTO**MIXED AADC 159
SAMPLE A. SAMPLE - L01 GENERAL
APT ABC
123 ANY ST
ANYTOWN, ST 12345-6789

Re: Notice of Security Incident

Dear Sample A. Sample,

MTS Systems Corporation ("MTS") is writing to inform you of a recent event that may impact the privacy of some of your personal information. While we are unaware of any misuse of your information, we are providing you with information about the event, our response, and steps you may take to protect yourself.

What Happened? On November 15, 2020, MTS became aware of suspicious activity on its computer network. MTS immediately launched an investigation, with the assistance of third-party specialists, and determined that portions of its network had been infected with malware which prevented access to certain files on the system. The investigation determined that the malware was introduced into the system by an unauthorized actor who temporarily viewed and held certain files from within MTS' computer systems in October and November 2020. MTS then began a comprehensive process to identify data that may have been contained within impacted files, to identify the individuals whose information may have been impacted, and to obtain contact information for those individuals. We are notifying you because the investigation determined certain information related to you may have been impacted by this event.

What Information Was Involved? The information which may have been impacted by this event includes your name, [EXTRA1]. We have no evidence your information was subject to misuse.

What We Are Doing. MTS takes this incident and the security of your personal information seriously. Upon discovery, we immediately took steps to secure our systems and launched an investigation. We are reviewing our policies, procedures, and processes related to storage of and access to personal information.

As an added precaution, we are also offering one year of complimentary access to credit monitoring, fraud consultation, and identity theft restoration services through Experian. Individuals who wish to receive these services must enroll by following the attached enrollment instructions.

What You Can Do. You can review the enclosed Steps You Can Take to Help Protect Your Information to learn helpful tips on steps you can take to protect your information. We also encourage you to review your financial and account statements and report suspicious activity to the institution that issued the statement.

For More Information. If you have questions, please contact us at (888) 994-0282 during Monday through Friday from 6:00 am - 8:00 pm Pacific Standard Time and Saturday/Sunday from 8:00 am - 5:00 pm Pacific Standard Time. You can also write to us at MTS Systems Corporation, Attention: Office of Risk & Compliance, 14000 Technology Drive, Eden Prairie, MN 55344.

We sincerely regret any inconvenience or concern this incident has caused.

Sincerely,
MTS Privacy Office

Steps You Can Take to Protect Your Information

Enroll in Credit Monitoring.

To help protect your identity, we are offering a complimentary one-year membership in Experian's® IdentityWorks℠. This Experian product provides you with identity detection and resolution of identity theft. To activate your membership and start monitoring your personal information, please follow the steps below:

- **Enrollment Deadline:** Ensure that you enroll by June 30, 2021 (Your code will not work after this date.)
- **Sign Up Process:**
  - Visit Website: Visit the Experian IdentityWorks website to enroll: **https://www.experianidworks.com/credit**
  - Activation Code: Provide your activation code: **ABCDEFGHI**

If you have questions about the product, need assistance with identity restoration or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at (888) 994-0282 by June 30, 2021. Be prepared to provide engagement number ENGAGE# as proof of eligibility for the identity restoration services by Experian.

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, military identification, 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 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
888-298-0045	1-888-397-3742	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 District of Columbia residents, the District of Columbia Attorney General may be contacted at: 441 4th St. NW #1100 Washington, D.C. 20001; 202-727-3400; and oag@dc.gov.

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. MTS is located at 14000 Technology Drive, Eden Prairie, MN 55344.

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, you have the right to obtain any police report filed in regard to this incident. There are 1 Rhode Island residents impacted by this incident.

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/.