EXHIBIT 1

Although the investigation into this matter is complete, if necessary, this notice may be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, Numerix LLC ("Numerix") 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 April 3, 2023, Numerix discovered suspicious activity within its environment. In response, Numerix promptly took steps to secure it systems, engaged cyber security specialists, and launched an investigation to determine the full nature and scope of this incident. The investigation determined that an unauthorized actor accessed certain computer systems in the Numerix network between March 23 and April 3, 2023, and downloaded certain files. Given this unauthorized access, Numerix diligently reviewed the files accessed/downloaded by the unauthorized actor, and on May 3, 2023, confirmed the information present and to whom it related for purposes of notification. Numerix thereafter worked to reconcile the information with its internal records to identify complete and accurate contact information, and also leveraged third-party resources to supplement and supply necessary contact information so that notification could timely commence.

The categories of information related to Numerix employees residing in Maine stored on the impacted systems may include name, contact information, and Social Security number, tax identification number, driver's license or equivalent identification number, date of birth, passport, financial account information, employee identification number, username and password, and/or wage/salary/compensation information.

Notice to Maine Residents

On or about June 2, 2023, Numerix began providing written notice of this incident to potentially impacted individuals, which includes four (4) Maine residents. Written notice is being provided in substantially the same form as the letter attached hereto as ***Exhibit A***.

Other Steps Taken and To Be Taken

Upon discovering the event, Numerix moved quickly to investigate and respond to the incident, assess the security of Numerix systems, and identify potentially affected individuals. Numerix's internal team moved swiftly to shut down systems and reset passwords in an effort to contain the activity. Thereafter, a comprehensive investigation was performed by third-party forensic specialists, and significant steps were taken to promptly and diligently respond to the incident. Upon completion of the investigation, Numerix took several targeted actions in response to further secure its environment and the information housed therein, and took further steps in an attempt to mitigate potential harm resulting from this event. Further, Numerix promptly notified federal law enforcement regarding the incident. Numerix is also notifying other requisite regulatory authorities, as required.

Additionally, as an added measure, Numerix is providing access to credit/identity 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.

Moreover, as part of its ongoing commitment to data privacy and security, Numerix also implemented additional security measures and safeguards to further protect against future similar incidents, and is enhancing existing policies and procedures related to cybersecurity, and providing additional training to employees regarding the importance of safeguarding data.

Additionally, Numerix is providing impacted individuals with guidance on how to better protect against identity theft and fraud, including 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.

EXHIBIT A

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

June 2, 2023

J5159-L01-0000001 T00001 P001 ********SCH 5-DIGIT 12345
SAMPLE A SAMPLE - L01 INDIVIDUAL
APT ABC
123 ANY STREET
ANYTOWN, ST 12345-6789

RE: NOTICE OF DATA [Extra1]

Dear Sample A. Sample:

As you may know, we recently experienced a technical disruption to certain of our networks. We diligently investigated the source of the disruption to confirm the full nature and scope of the incident. Our investigation is now complete, and accordingly, we are writing to provide you with additional information regarding the incident, as it may affect the privacy of some of your information. This notice provides information about the incident, our response, and resources available to help protect your information from possible misuse, should you feel it is necessary to do so.

What Happened? On April 3, 2023, Numerix discovered suspicious activity within our systems. Upon discovery of the event, we promptly launched an investigation to determine the full nature and scope of this incident. The investigation determined that an unauthorized actor accessed certain computer systems in our network between March 23 and April 3, 2023, and downloaded certain files. We diligently reviewed the files accessed/downloaded by the unauthorized actor and on May 3, 2023, determined your information was present and therefore may have been affected. Accordingly, we are providing this notice to you.

What Information Was Involved? The categories of information related to you that Numerix collects/stores on the impacted systems may include your name, contact information, and Social Security number, tax identification number, driver's license or equivalent identification number, date of birth, passport, financial account information, employee identification number, username and password, and/or wage/salary/compensation information.

What We Are Doing. Numerix takes the confidentiality, privacy, and security of information in our care seriously. Upon identifying the activity, we promptly investigated to determine the full nature and scope of the event. Further, we notified federal law enforcement, and are notifying relevant regulatory authorities as required. Moreover, as part of our ongoing commitment to the privacy and security of information in our care, we have a process in place to ensure regular and timely review and, where necessary, the updating of our existing policies and procedures related to data protection and security. We have also implemented additional security measures as appropriate to further secure the information in our systems, and are increasing frequency and scope of our training to employees regarding the importance of safeguarding of data. As an added measure, Numerix is providing you with access to [Extra2] months of credit monitoring and identity protection services through Experian at no cost to you. A description of services and instructions on how to enroll can be found within the enclosed *Steps You Can Take to Help Protect Personal Information*. Please note that you must complete the enrollment process yourself, as we are unable to enroll you in these services on your behalf.

What You Can Do. We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your account statements and monitoring your free credit reports for any suspicious activity and to detect errors. You should promptly report any such suspicious activity to law enforcement. You should report any suspicious charges on your credit or debit card to the bank that issued the card or the card company, as appropriate. Please also review the enclosed *Steps You Can Take to Help Protect Personal Information*, which contains additional information and resources.

For More Information. We understand that you may have questions about the incident that are not addressed in this letter. If you have questions, please call (833) 468-0575, toll-free Monday through Friday from 9 am – 11 pm Eastern, or Saturday and Sunday from 11 am – 8 pm Eastern (excluding major U.S. holidays). Be prepared to provide engagement number ENGAGE#. You may also write to Numerix LLC at hr.assist@numerix.com.

Sincerely,

Emanuele Conti
Chief Executive Officer
Numerix

STEPS YOU CAN TAKE TO HELP PROTECT PERSONAL INFORMATION

Enroll in Offered Monitoring Services

To help protect your identity, we are offering a complimentary [Extra3]-month membership of Experian's® IdentityWorks℠. This product provides you with superior identity detection and resolution of identity theft. To activate your membership and start monitoring your personal information please follow the steps below:

- Ensure that you **enroll by**: **September 30, 2023** (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll: https://www.experianidworks.com/credit
- 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 (833) 468-0575 by September 30, 2023. Be prepared to provide engagement number ENGAGE# as proof of eligibility for the identity restoration services by Experian.

ADDITIONAL DETAILS REGARDING YOUR [Extra3]-MONTH EXPERIAN IDENTITYWORKS MEMBERSHIP:

A credit card is **not** required for enrollment in Experian IdentityWorks. You can contact Experian **immediately** regarding any fraud issues, and have access to the following features once you enroll in Experian IdentityWorks:

- **Experian credit report at signup:** See what information is associated with your credit file. Daily credit reports are available for online members only.*
- **Credit Monitoring:** Actively monitors Experian file for indicators of fraud.
- **Identity Restoration:** Identity Restoration agents are immediately available to help you address credit and non-credit related fraud.
- **Experian IdentityWorks ExtendCARE™**: You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- **Up to $1 Million Identity Theft Insurance**:** Provides coverage for certain costs and unauthorized electronic fund transfers.

If you believe there was fraudulent use of your information and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent at (833) 468-0575. If, after discussing your situation with an agent, it is determined that Identity Restoration support is needed, then an Experian Identity Restoration agent is available to work with you to investigate and resolve each incident of fraud that occurred (including, as appropriate, helping you with contacting credit grantors to dispute charges and close accounts; assisting you in placing a freeze on your credit file with the three major credit bureaus; and assisting you with contacting government agencies to help restore your identity to its proper condition).

Please note that this Identity Restoration support is available to you for [Extra3] months from the date of this letter and does not require any action on your part at this time. The Terms and Conditions for this offer are located at www.ExperianIDWorks.com/restoration. You will also find self-help tips and information about identity protection at this site.

* Offline members will be eligible to call for additional reports quarterly after enrolling

** The Identity Theft Insurance is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

Change Your Passwords

In addition to the changes to our work passwords, as a best practice we would encourage employees to consider changing passwords for any account you may regularly access from work computers, such as Gmail, Amazon, Facebook, or your personal bank or credit card accounts, and any other passwords that you have not changed recently. This is particularly important if you have any of your passwords stored in your web browser, like Google Chrome. If you are able, we would also encourage you to implement multi-factor / two-factor authentication whenever possible. Also, as many people often use the same password for many accounts, we are also encouraging you to take this opportunity to change the passwords for any personal accounts which would share the same or similar credentials as other accounts, including accounts accessed from company devices. Best practice is to ensure you are changing any password(s) from a non-Numerix device.

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 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 District of Columbia residents, the District of Columbia Attorney General may be contacted at: 400 6th Street, NW, 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 https://www.marylandattorneygeneral.gov/. Numerix LLC is located at 99 Park Avenue, 5th FL, New York, NY 10016

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 is/are approximately 2 Rhode Island residents that may be impacted by this event.