Dear **[NAME]**,

RE: Notice of Data Breach

<<OPERATING GROUP NAME/BUSINESS UNIT>> ("we", "our") takes the privacy and security of information in our care seriously. As such, we are writing to inform you of a recent cybersecurity incident that may have impacted some of your personal information. Out of an abundance of caution, we are providing you with this letter to inform you of this incident, the steps we are taking in response and steps that you can take to further protect your information, should you wish to do so.

What happened?

Our parent company, Constellation Software Inc. ("Constellation"), recently discovered that an unauthorized third party gained access to a limited number of its systems. Like other Constellation businesses, we utilize some of those systems for our own financial reporting and accounting purposes. Upon discovering this incident, Constellation immediately took steps to prevent against further unauthorized activity and a third-party cybersecurity firm was retained to assist with containment, remediation and to conduct a forensic investigation into the cause and extent of this incident. Constellation also notified law enforcement and is supporting its investigation

The evidence showed unauthorized activity in Constellation's network between February 27, 2023 and April 3, 2023. During that time, the unauthorized third party viewed and took files from certain servers in the network. In collaboration with Constellation and the other Constellation businesses, we have been conducting a comprehensive review of these files and, between April 28, 2023 and May 2, 2023 determined that one or more of the files contained certain of your personal information.

At this time, there is no reason to believe that **<<OPERATING GROUP NAME/BUSINESS UNIT>>**s systems were involved in the incident.

What information is involved?

The information included your**:<<data element(s)>>.**

What we are doing.

Upon discovering this incident, Constellation moved quickly to respond with the assistance of its third party cybersecurity firm. We understand those efforts included isolating affected systems and securely restoring them from backups, deploying endpoint detection and response tooling across the environment along with active threat monitoring, reinforcing network perimeter security, and notifying law enforcement.

To protect against the potential misuse of your information, we are providing you with 12 months of credit monitoring and identity theft protection. We urge you to sign up for this service.

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

Through Cyberscout, we have arranged a **[Click here to enter subscription period]** subscription to an online monitoring service, at no cost to you. This credit monitoring service will notify you by email of critical changes to your Credit Report. Should you receive an email alert, you can review and validate the reported change by logging into the portal. This allows you to identify any potentially fraudulent activity on your Credit Report.

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

https://secure.identityforce.com/benefit/clientname

You will be prompted to enter the following activation code:

xxxx-xxxx-xxxx-xxxx

Please ensure that you redeem your activation code before **[Click here to enter a date]** to take advantage of the service.

Upon 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.

Should you have any questions regarding the Cyberscout solution, have difficulty enrolling, or require additional support, please contact Cyberscout at 1-877-694-3367.

What you can do.

In addition to enrolling in your complimentary credit monitoring service, we encourage you to remain vigilant by taking the following preventive measures:

- If you receive communications purporting to be from [operating group/business unit] asking for account or any other personal information that you were not expecting, please consider such communications to be fraudulent, and contact the undersigned immediately.
- Never respond to any unsolicited requests for your financial information.

- Remain vigilant about any unauthorized transactions on your financial or credit accounts. If you see anything that looks suspicious, or suspect fraudulent transactions have taken place, call your bank immediately.
- Remain vigilant of any phishing or spoofing attempts. A phishing email is an impersonation tactic used to deceive individuals into thinking that the email came from a trusted source. For example, the displayed name may say that the email came from John Doe, however, the sender's email address contains an extra symbol or letter than the genuine business email address.
- Avoid clicking on links or downloading attachments from suspicious emails.

For more information about steps you can take in response, please review the pages that follow this letter.

For more information.

We apologize for any inconvenience or concern this incident may cause you. We are committed to further improving our information security and data storage practices in order to prevent an incident like this from happening again in the future. Should you have any questions, we invite you to contact our dedicated incident response line at **xxx-xxx-xxx**, and one of our representatives will be happy to assist you. Thank you for your understanding and patience.

Sincerely,

Constellation Software Inc.

ADDITIONAL STEPS YOU CAN TAKE

We remind you it is always advisable to be vigilant for incidents of fraud or identity theft by reviewing your account statements and free credit reports for any unauthorized activity. You may obtain a copy of your credit report, free of charge, once every 12 months from each of the three nationwide credit reporting companies. To order your annual free credit report, please visit www.annualcreditreport.com or call toll free at 1-877-322-8228. Contact information for the three nationwide credit reporting companies is as follows:

- *Equifax*, PO Box 740241, Atlanta, GA 30374, www.equifax.com, 1-888-378-4329
- *Experian*, PO Box 2002, Allen, TX 75013, www.experian.com, 1-888-397-3742
- *TransUnion*, PO Box 1000, Chester, PA 19016, www.transunion.com, 1-800-916-8800

If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should immediately contact the Federal Trade Commission and/or the Attorney General's office in your state. You can obtain information from these sources about steps an individual can take to avoid identity theft as well as information about fraud alerts and security freezes. You should also contact your local law enforcement authorities and file a police report. Obtain a copy of the police report in case you are asked to provide copies to creditors to correct your records. Contact information for the Federal Trade Commission is as follows:

- *Federal Trade Commission*, Consumer Response Center, 600 Pennsylvania Avenue NW, Washington, DC 20580, 1-877-IDTHEFT (438-4338), www.identitytheft.gov

Fraud Alerts and Credit or Security Freezes:

Fraud Alerts: There are two types of general fraud alerts you can place on your credit report to put your creditors on notice that you may be a victim of fraud—an initial alert and an extended alert. You may ask that an initial fraud alert be placed on your credit report if you suspect you have been, or are about to be, a victim of identity theft. An initial fraud alert stays on your credit report for one year. You may have an extended alert placed on your credit report if you have already been a victim of identity theft with the appropriate documentary proof. An extended fraud alert stays on your credit report for seven years.

To place a fraud alert on your credit reports, contact one of the nationwide credit bureaus. A fraud alert is free. The credit bureau you contact must tell the other two, and all three will place an alert on their versions of your report.

For those in the military who want to protect their credit while deployed, an Active Duty Military Fraud Alert lasts for one year and can be renewed for the length of your deployment. The credit bureaus will also take you off their marketing lists for pre-screened credit card offers for two years, unless you ask them not to.

Credit or Security Freezes: You have the right to put a credit freeze, also known as a security freeze, on your credit file, free of charge, which makes it more difficult for identity thieves to open new accounts in your name. That's because most creditors need to see your credit report before they approve a new account. If they can't see your report, they may not extend the credit.

How do I place a freeze on my credit reports? There is no fee to place or lift a security freeze. Unlike a fraud alert, you must separately place a security freeze on your credit file at each credit reporting company. For information and instructions to place a security freeze, contact each of the credit reporting agencies at the addresses below:

- **Experian Security Freeze**, PO Box 9554, Allen, TX 75013, www.experian.com
- **TransUnion Security Freeze**, PO Box 160, Woodlyn, PA 19094, www.transunion.com
- **Equifax Security Freeze**, PO Box 105788, Atlanta, GA 30348, www.equifax.com

You'll need to supply your name, address, date of birth, Social Security number and other personal information.

After receiving your freeze request, each credit bureau will provide you with a unique PIN (personal identification number) or password. Keep the PIN or password in a safe place. You will need it if you choose to lift the freeze.

How do I lift a freeze? A freeze remains in place until you ask the credit bureau to temporarily lift it or remove it altogether. If the request is made online or by phone, a credit bureau must lift a freeze within one hour. If the request is made by mail, then the bureau must lift the freeze no later than three business days after getting your request.

If you opt for a temporary lift because you are applying for credit or a job, and you can find out which credit bureau the business will contact for your file, you can save some time by lifting the freeze only at that particular credit bureau. Otherwise, you need to make the request with all three credit bureaus.

Constellation Software Inc. is located at #1200 – 20 Adelaide Street East, Toronto, ON M5C 2T6, Canada.

Additional information for residents of the following states:

Maryland: You may contact and obtain information from your state attorney general at: *Maryland Attorney General's Office*, 200 St. Paul Place, Baltimore, MD 21202, 1-888-743-0023 / 1-410-576-6300, www.oag.state.md.us

New York: You may contact and obtain information from these state agencies: *New York Department of State Division of Consumer Protection,* One Commerce Plaza, 99 Washington Ave., Albany, NY 12231-0001, 518-474-8583 / 1-800-697-1220, http://www.dos.ny.gov/consumerprotection; and *New York State Office of the Attorney General,* The Capitol, Albany, NY 12224-0341, 1-800-771-7755, https://ag.ny.gov

North Carolina: You may contact and obtain information from your state attorney general at: *North Carolina Attorney General's Office*, 9001 Mail Service Centre, Raleigh, NC 27699, 1-919-716-6000 / 1-877- 566-7226, www.ncdoj.gov

A Summary of Your Rights Under the Fair Credit Reporting Act: The federal Fair Credit Reporting Act (FCRA) promotes the accuracy, fairness, and privacy of information in the files of consumer reporting agencies. There are many types of consumer reporting agencies, including credit bureaus and specialty agencies (such as agencies that sell information about check writing histories, medical records, and rental history records). Your major rights under the FCRA are summarized below. For more information, including information about additional rights, go to www.consumerfinance.gov/learnmore or write to: Consumer Financial Protection Bureau, 1700 G Street NW, Washington, DC 20552.

- You must be told if information in your file has been used against you.
- You have the right to know what is in your file.
- You have the right to ask for a credit score.
- You have the right to dispute incomplete or inaccurate information.
- Consumer reporting agencies 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 reports to be provided to employers.
- You may limit "prescreened" offers of credit and insurance you get based on information in your credit report.
- You have a 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.
- You may seek damages from violators.
- Identity theft victims and active duty military personnel have additional rights.