Subject: Important Notice Regarding Network Security Incident

Dear [Employee Name],

We are writing to inform you of a recent network security incident that affected EG America, LLC's ("EG America") third-party payroll system, provided by The Ultimate Software Group, Inc. ("UltiPro"). On or about March 30, 2023, EG America was alerted of suspicious activity on UltiPro when an unknown individual attempted to use valid employee names and Social Security number ("SSN") to gain access to and change information in employees' UltiPro accounts, including banking information (the "Incident").

Upon becoming aware of the Incident, we immediately activated our data incident response plan and launched an internal investigation to determine the scope of the Incident. We regret to inform you that our investigation determined the threat actor may have attempted to use your personal information (i.e., name and SSN) to access your UltiPro account. Our investigation is ongoing, but we assure you that, at this time, there is no evidence indicating any payroll funds, including your payroll funds, were misdirected as a result of the Incident.

We are sorry for any inconvenience. The privacy and security of the personal information of our employees is our top priority. We assure you that we are taking appropriate steps to respond to and address the Incident and to mitigate the risk of future incidents. To protect your personal information and reduce the risk of potential harm, we have taken precautionary steps including, but not limited to, immediately resetting your UltiPro credentials, engaging the assistance of third-party experts to assist us with our Incident investigation and remediation activities, enabling multi-factor authentication for all UltiPro accounts, and arranging for Cyberscout to provide you with twenty-four (24) months of credit monitoring services at no cost to you. To enroll for these complimentary services, please follow the instructions provided below.

We encourage you to take the following additional steps to protect your personal information:

- Monitor your UltiPro account, credit reports, and bank statements regularly for any unauthorized or suspicious activity.
- Place a fraud alert on your credit reports with the three major credit bureaus.
- Close any accounts that may have been affected and open new ones.
- Be cautious of phishing scams and suspicious emails that ask for personal information.
- File a report with your local police department if you detect suspicious activity in your accounts.

If you suspect that your personal information has been compromised, please report it to the appropriate authorities immediately. We are committed to ensuring that the privacy and security of our employees' personal information, and we are taking appropriate steps to respond to and remediate the Incident. If you have any questions, please do not hesitate to reach out to us at this email address.

Sincerely,

[Your Name]
[Your Title]
EG America, LLC

Credit Monitoring Services

In response to the network security incident, EG America has arranged for Cyberscout to provide the following services through Identity Force:

- Single Bureau Credit Monitoring, Report and Score*;
- Cyber Monitoring

These services provide you with alerts for twenty-four (24) months from the date of enrollment when changes occur to your credit file. A notification will be sent to you the same day that the changes or updates takes place with the bureau. Cyber monitoring will look out for your personal data on the dark web and alert you if your personally identifiable information is found online. To safeguard your privacy and security, you will be asked to verify your identity before monitoring can be activated. These services will be provided by Cyberscout through Identity Force, a TransUnion company specializing in fraud assistance and remediation services.

How do I enroll for the free services?

To enroll in Credit Monitoring Services at no charge, please log on to **https://secure.identityforce.com/benefit/egamerica** and follow the instructions provided. When prompted please provide the following unique code to receive services: **<<CODE HERE>>**. In order for you to receive the monitoring services described above, you must enroll within 90 days from the date of this letter. The enrollment requires an internet connection and e-mail account and may not be available to minors under the age of 18 years old. Please note that when signing up for monitoring services, you may be asked to verify personal information for your own protection to confirm your identity.

What can I do on my own to address this situation?

If you choose not to use these services, we strongly urge you to do the following:

If you choose to place a fraud alert on your own, you will need to contact one of the three major credit agencies directly at:

Experian (1-888-397-3742)	**Equifax (1-800-525-6285)**	**TransUnion (1-800-680-7289)**
P.O. Box 4500	**P.O. Box 740241**	**P.O. Box 2000**
Allen, TX 75013	**Atlanta, GA 30374**	**Chester, PA 19016**
www.experian.com	www.equifax.com	www.transunion.com

Also, should you wish to obtain a credit report and monitor it on your own:

- **IMMEDIATELY** obtain free copies of your credit report and monitor them upon receipt for any suspicious activity. You can obtain your free copies by going to the following website: www.annualcreditreport.com or by calling them toll-free at 1-877-322-8228. (Hearing impaired consumers can access their TDD service at 1-877-730-4204.
- **Upon receipt of your credit report,** we recommend that you review it carefully for any suspicious activity.
- Be sure to promptly report any suspicious activity to the appropriate authorities.

You can also obtain more information from the Federal Trade Commission (FTC) about identity theft and ways to protect yourself. The FTC has an identity theft hotline: 877-438-4338; TTY: 1-866-653-4261. They also provide information on-line at www.ftc.gov/idtheft.