Dear_____:

We regret to inform you of an incident that may affect the security of your personal information. On November 20, 2024, we determined that a security breach of our network may have allowed an outside party engaged in ransomware attacks to access the names and social security numbers of employees and former employees who participated in our 401(K) program.

We are in the process of determining the scope of the breach and working to engage a credit monitoring service for impacted individuals. If your personal information is affected by the breach, you will receive further information on how to access those services.

This communication is intended to ensure that you are aware of this issue and to alert you to steps you may wish to take to monitor your identity, financial accounts and credit files. We encourage you to remain vigilant, to review all payment invoices you receive and to monitor your credit reports for suspicious activity. Be aware to only respond to emails from a known/authenticated sender, and do not provide your log in credentials for any services to third parties.

At no charge you may have the major credit bureaus place a fraud alert on your file which notifies creditors to take steps to verify your identity prior to granting credit in your name. You may also place a credit freeze on any one or all of the following agencies:

Equifax	Experian	TransUnion
888 298 0045	888 397 3742	800 916 8800
Equifax.com	Experian.com	transunion.com

Please contact our Human Resources Department at _____ if you require further assistance or information.

Very truly yours,