Notice to Former Vista Employees of Security Incident

Vista Proppants & Logistics LLC takes the privacy and security of employee information very seriously. We identified and addressed a security incident that may have involved information pertaining to our former employees. This notice explains the incident, outlines the measures we have taken, and steps employees can take in response.

We recently learned that an unauthorized actor accessed our network. We immediately took steps to secure the network and began an investigation with the assistance of a computer forensic firm. The investigation determined that an unauthorized actor gained access to our network between July 15, 2020 and August 16, 2020. During that time, the unauthorized actor acquired copies of some of the information on our systems. On September 3, 2020, we determined that the files taken by the unauthorized actor may have contained employment related information, including former employees' names, Social Security numbers, drivers' license numbers, and/or bank account information.

We arranged for the unauthorized actor to delete the files that were removed from our network. The unauthorized actor confirmed that the files were deleted, and we have no reason to believe any of your information has been or will be misused. However, in an abundance of caution, we are mailing letters to former employees notifying them of the incident and providing additional information on identity theft prevention. We have also established a dedicated, toll-free call center to answer questions individuals may have. If you have questions or do not receive a letter but think your information may have been involved, please call 1-833-971-3235, Monday through Friday, from 8:00 am to 5:30 pm, Central Time.

We encourage our former employees to remain vigilant by reviewing their account statements and free credit reports for any unauthorized activity. You should immediately report any unauthorized charges to your financial institution.

We deeply regret that this incident occurred and for any concern this may cause. To help prevent something like this from happening again, we are continuing to regularly audit our system for potential unauthorized activity, and are implementing enhanced network monitoring tools.