Dear Omnex customer,

We are reaching out to inform you about a recent security breach that has potentially affected your personal information associated with Omnex transfers through Unitransfer USA, Inc. The breach was in the Unitransfer system and we have only been notified in the last 24 hours that it may have affected Omnex customers. We are still investigating the specifics of the incident with help from Unitransfer but we wanted to let you know quickly so that you can take necessary precautions. We will continue to update you so that you can stay informed about the incident.

Details of the Incident:

On November 15, 2023, Unitransfer identified a potential ransomware attack. Following their investigation, they confirmed to us that the compromised data originated from their compliance system. As soon as this activity was detected, Unitransfer promptly initiated an investigation with the assistance of technical and forensic experts as well as legal professionals. As of December 6, Unitransfer has confirmed that they successfully secured all systems and are actively working to minimize the risk of further data compromise.

Nature of the Compromised Information:

The stolen data includes complete names, physical and email addresses, and in some instances, _____. We are still reviewing what other information may have been exposed.

What We Are Doing:

We have been working with Unitransfer and they have confirmed to us that they, along with trusted consultants from a renowned cybersecurity firm, have successfully eliminated the malware from our systems. In addition, they are actively monitoring their compliance system and transaction platform, and enhancing the existing safeguards. The goal is not only to safeguard the information but also to prevent any future unauthorized access. Unitransfer has also informed law enforcement and are closely collaborating with them to ensure the investigation and assessment of missing data is complete. Upholding industry standards for data protection, we are committed to maintaining security and privacy. Our systems will undergo continuous monitoring and auditing to ensure their security.

What You Can Do:

While we have no confirmation that any more than names and addresses have been compromised, we recommend considering the following actions to safeguard you from potential fraud.

Place a free fraud alert on your credit file. A fraud alert tells creditors to contact you before they open any new accounts or change your existing accounts. Contact any one of the three major credit bureaus. As soon as one credit bureau confirms your fraud alert, the others are notified to place fraud alerts. The initial fraud alert stays on your credit report for one year. You can renew it after one year.

- Equifax: equifax.com/personal/credit-report-services or 1-800-685-1111
- Experian: experian.com/help or 1-888-397-3742
- TransUnion: transunion.com/credit-help or 1-888-909-8872

Ask each credit bureau to send you a free credit report after it places a fraud alert on your file. Review your credit reports for accounts and inquiries you don't recognize. These can be signs of identity theft. If your personal information has been misused, visit the FTC's site at IdentityTheft.gov to report the identity theft and get recovery steps. Even if you do not find any suspicious activity on your initial credit reports, the FTC recommends that you check your credit reports periodically so you can spot problems and address them quickly.

You may also want to consider placing a free credit freeze. A credit freeze means potential creditors cannot get your credit report. That makes it less likely that an identity thief can open new accounts in your name. To place a freeze, contact each of the major credit bureaus at the links or phone numbers above. A freeze remains in place until you ask the credit bureau to temporarily lift it or remove it.

We also recommend you visit the FTC's website, IdentityTheft.gov/databreach, about steps you can take to help protect yourself from identity theft.

Additional Information:

We are committed to supporting you through this situation. For assistance or more information, please contact _____.

Sincerely,