NOTICE OF DATA BREACH

Dear Valued Customer:

We are contacting you about a data breach that has occurred at Unitransfer USA, Inc. ("**Unitransfer**"). Unitransfer was formerly a Florida based money transfer operator that has since ceased its U.S. operations. Though Unitransfer has ceased its operations, some of your personal information continued to be stored by us for compliance purposes. Although we have no indication of actual misuse of your information, we are providing you with information about the incident, our response to it, and resources available to you in an abundance of caution.

What Happened?

On November 15, 2023, Unitransfer identified slowdown in its systems and immediately informed its internal and external cybersecurity teams. Upon investigating the nature and scope of the incident, we have determined that an unauthorized access to our network likely took place on that date. As such, we have retained external IT and cybersecurity experts to help secure our network and remediate the threat.

Unitransfer has taken extensive action to ensure the affected compliance software has been hardened and the impacted information has been recovered and backed up to the fullest extent possible. We have taken a time-consuming and detailed effort to recover and protect this information. In doing so, we have determined that your information was on the system which suffered the incident.

At this point, the investigation is ongoing, but we are informing you that it is possible your information was accessed by an unauthorized third party.

What Information Was Involved?

For the most part, the information that was potentially accessed in an unauthorized manner involves only non-sensitive personal information such as names and addresses. However, for some of our clients, the impacted information may also include driver's license numbers, account numbers, bank statements, and social security numbers.

What Are We Doing?

Since being informed of the data breach, Unitransfer has worked with a top cyber security team to harden its system and provide 24/7 monitoring. Unitransfer has taken action to secure its systems, including disabling all VPN tunnels and remote access, changing the credentials of all Windows machines, further segmenting the network, adding to monitoring and detection capabilities amongst other protective activities. Unitransfer has also been working with its cyber security experts to ensure there are no further intrusions. We have been monitoring all systems 24/7 and since the initial incident in November 2023, there has been no evidence of further intrusion or other unauthorized activity in the system.

What Can You Do?

We encourage you to remain vigilant against incidents of identity theft and fraud by regularly reviewing your account statements and monitoring your free credit alerts for suspicious activity.

The Federal Trade Commission (FTC) recommends that you 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.

We are also providing information for credit monitoring services. Unitransfer will cover the cost of these services for up to 2 years. However, you will need to complete the initial activation process. Enrollment instructions will be provided with this letter (see Schedule A: Complimentary Identity Theft Protection Service).

For More Information

We are committed to supporting you through this situation. If you have reason to believe your information has been improperly accessed, you have the right to obtain a police report. For assistance or more information, please contact our Customer Care Department at customercare@unitransfer.com.

Sincerely,

Unitransfer Customer Care Team

Schedule A: Enrollment in Credit Monitoring Services

Activation Code: XXXX-XXXX-XXXX-XXXX

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.[1]
- ✓ 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.

Schedule B: Monitor Your Accounts

Under U.S. law, a consumer is entitled to one free credit report annually from each of the three major credit reporting bureaus, Equifax, Experian, and TransUnion. To order your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also directly contact the three major credit reporting bureaus listed below to request a free copy of your credit report.

Consumers have the right to place an initial or extended "fraud alert" on a credit file at no cost. An initial fraud alert is a one-year alert that is placed on a consumer's credit file. Upon seeing a fraud alert display on a consumer's credit file, a business is required to take steps to verify the consumer's identity before extending new credit. If you are a victim of identity theft, you are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should you wish to place a fraud alert, please contact any one of the three major credit reporting bureaus listed below.

As an alternative to a fraud alert, consumers have the right to place a "credit freeze" on a credit report, which will prohibit a credit bureau from releasing information in the credit report without the consumer's express authorization. The credit freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, you should be aware that using a credit freeze to take control over who gets access to the personal and financial information in your credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, you cannot be charged to place or lift a credit freeze on your credit report. To request a credit freeze, you may need to provide some or all of the following information:

1. Full name (including middle initial, as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. Addresses for the prior two to five years;
5. Proof of current address, such as a current utility bill or telephone bill;
6. A legible photocopy of a government-issued identification card (state driver's license or ID card, etc.); and
7. A copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft if you are a victim of identity theft.

Should you wish to place a fraud alert or a credit freeze, please contact the three major credit reporting bureaus listed below:

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

Schedule C: Additional Information

You may further educate yourself regarding identity theft, fraud alerts, credit freezes, and the steps you can take to protect your personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or your state Attorney General. The Federal Trade Commission may be reached at: www.identitytheft.gov or 1-877-ID-THEFT (1-877-438-4338). The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. You can obtain further information on how to file such a complaint by way of the contact information listed above. You have the right to file a police report if you ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, you will likely need to provide some proof that you have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and your state Attorney General. This notice has not been delayed by law enforcement.