24634

[Vistra Letterhead]

[Date]

[Name]
[Address 1]
[Address 2]
[City], [State] [Zip]

Re: Notice of [Security Incident]

Dear [Name],

Vistra International Expansion (USA), Inc. ("Vistra" or "We") writes to inform you of a recent incident that may affect the privacy of some of your personal information. This notice provides information about the incident, our response, and resources available to you to help protect your information from possible misuse, should you feel it necessary to do so.

Vistra was the victim of an attempt by an unauthorized third party to take control of our data network. Vistra has provided a range of services to your employer (or prior employer) and these services have necessitated that we have your documents on file in order to provide appropriate services. Our countermeasures worked well, and we contained their efforts almost immediately.

What Happened? The attempt started on October 25, 2021. Our security systems detected it and took appropriate actions to curtail all attempts to access our systems. However, on October 28, 2021, the attack escalated. This is when we took action and shut down parts of our system to combat it. We immediately shut down the circuits and internet tunnels and went through our standard security processes. As a result, we immediately contained the incident and isolated the impacted systems and brought in leading external security consultants to assist us.

When did this happen? It's now clear that certain documents were copied on October 28, 2021. We became aware of this on November 12, 2021, after a detailed forensic investigation and after reviewing files published on a file leak-site used by the attacker. Between now and then we have been reviewing the documents involved to identify which of the ultimate owners of the documents involved. We are continuing to investigate the incident with utmost urgency in partnership with leading professional advisors.

What Information is Involved? Unfortunately, in the short period between the attack and our response, the third party took a copy of <your passport> and <associated identification documents>. The incident is now contained, and the impacted system has been isolated. Vistra has contacted the necessary local authorities and law enforcement agencies.

What Are We Doing? We take the security of information entrusted to us very seriously and apologize for any inconvenience this incident may have caused. As soon as we became aware of the cyber-security incident, our priority was to ensure our systems and the data we hold on file for clients was secure. We took immediate steps to contain the incident and isolate the impacted systems containing your data.

As a precautionary measure, we reset the log-in credentials for all systems that we use to manage services and have rolled out new cutting-edge endpoint detection and response tools across the entire business. We continue to monitor third party leak sites to see if the attacker publishes any further data.

What You Can Do. As a best practice, we encourage you to remain vigilant against incidents of identity theft and fraud and to review your account statements and credit reports for suspicious activity. You may also review the information contained in the attached *Steps You Can Take to Protect Personal Information.*

For More Information. We understand that you may have questions about this incident that are not addressed in this letter. If you have additional questions, don't hesitate to get in contact with us at clientenquiries@vistra.com.

Sincerely,

Antonio Soler, Managing Director & Head of Americas - Corporates
President, Vistra International Expansion (USA), Inc.

STEPS YOU CAN TAKE TO HELP PROTECT PERSONAL INFORMATION

What we are doing to protect your information:

To help protect your identity, we are offering a complimentary 12-month membership of Experian's® IdentityWorks℠. This product provides you with superior identity detection and resolution of identity theft. To activate your membership and start monitoring your personal information please follow the steps below:

- Ensure that you enroll by: March 31, 2022 (Your code will not work after this date.)
- Visit the Experian IdentityWorks website to enroll: https://www.experianidworks.com/credit
- Provide your activation code: [code]

If you have questions about the product, need assistance with identity restoration or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at 877-890-9332 by March 31, 2022. Be prepared to provide engagement number B022457 as proof of eligibility for the identity restoration services by Experian.

Additional details regarding your 12-month Experian IdentityWorks Membership:

A credit card is not required for enrollment in Experian IdentityWorks.

You can contact Experian immediately regarding any fraud issues, and have access to the following features once you enroll in Experian IdentityWorks:

- Experian credit report at signup: See what information is associated with your credit file. Daily credit reports are available for online members only.[1]
- Credit Monitoring: Actively monitors Experian file for indicators of fraud.
- Identity Restoration: Identity Restoration agents are immediately available to help you address credit and non-credit related fraud.
- Experian IdentityWorks ExtendCARE™: You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- Up to $1 Million Identity Theft Insurance[2]: Provides coverage for certain costs and unauthorized electronic fund transfers.

If you believe there was fraudulent use of your information and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent at 877-890-9332. If, after discussing your situation with an agent, it is determined that Identity Restoration support is needed, then an Experian Identity Restoration agent is available to work with you to investigate and resolve each incident of fraud that occurred (including, as appropriate, helping you with contacting credit grantors to dispute charges and close accounts; assisting you in placing a freeze on your credit file with the three major credit bureaus; and assisting you with contacting government agencies to help restore your identity to its proper condition).

Please note that this Identity Restoration support is available to you for twelve (12) months from the date of this letter and does not require any action on your part at this time. The Terms and Conditions for this

---

[1] Offline members will be eligible to call for additional reports quarterly after enrolling

[2] The Identity Theft Insurance is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

offer are located at www.ExperianIDWorks.com/restoration. You will also find self-help tips and information about identity protection at this site.

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 1-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 security freeze, you will need to provide 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 credit freeze, please contact the three major credit reporting bureaus listed below:

Equifax	**Experian**	**TransUnion**
https://www.equifax.com/personal/credit-report-services/	https://www.experian.com/help/	https://www.transunion.com/credit-help
888-298-0045	1-888-397-3742	833-395-6938
Equifax Fraud Alert, P.O. Box 105069 Atlanta, GA 30348-5069	Experian Fraud Alert, P.O. Box 9554, Allen, TX 75013	TransUnion Fraud Alert, P.O. Box 2000, Chester, PA 19016
Equifax Credit Freeze, P.O. Box 105788 Atlanta, GA 30348-5788	Experian Credit Freeze, P.O. Box 9554, Allen, TX 75013	TransUnion Credit Freeze, P.O. Box 160, Woodlyn, PA 19094

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: 600 Pennsylvania Avenue NW, Washington, DC 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261. 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.

For Maryland residents, the Maryland Attorney General may be contacted at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-410-528-8662 or 1-888-743-0023; and www.oag.state.md.us. Aria is located at 505 Montgomery Street, 11th Floor, San Francisco, CA 94111.

For North Carolina residents, the North Carolina Attorney General may be contacted at: 9001 Mail Service Center, Raleigh, NC 27699-9001; 1-877-566-7226 or 1-919-716-6000; and www.ncdoj.gov.