[Date]

**VIA E-MAIL AND USPS First Class Mail**

**Notice of Cyber Incident**

Dear [NAME],

Continental values your privacy, and the safety and security of your personal information is important to us. We commit ourselves to improving the protection of the privacy and security of your information and transparency around your personal data. We are providing this notice to inform you about a recent cyber incident that impacted the security of your personal information.

This notification provides some information about the cyber incident and the resources available to you to help protect your personal information.

**What Happened**

The event happened as a result of a cyber incident launched by cyber criminals. We first became aware of the incident on the morning of Friday, October 18, 2024 when we noticed unusual activity affecting the functionality of some of our servers. Continental moved immediately to secure its systems, including isolating the network from further access and to minimize harm. We then worked to assess the scope of potential impact. In addition to marshalling our internal leadership team, IT, human resources, and legal, we also engaged an external team of legal, cybersecurity, and IT experts to contain the issue, mitigate harm, and restore our systems to full operational capacity. Our investigation is ongoing, and we continue to assess and strengthen our systems and processes to mitigate additional harm.

**What Information Was Involved**

The types of information potentially affected by this incident includes elements of your personal data. As a results of this incident, the cyber criminals may have viewed or accessed your personal information which may include your full name, residential address, phone number, date of birth, financial information, driver's license, passport, and Social Security Number. In addition, certain aspects of personal health information, as defined by the Health Insurance Portability and Accountability Act (HIPAA), provided to us by you in connection with the provision of insurance and employee benefits may have also been affected, including, full name, your participation in our health insurance plan and the name and assigned number for the health insurance provider. Finally, the data sets compromised may have also included health-related information you shared with us pertaining to conditions that impacted your ability to work, doctor's notes for medical conditions or work absences, and information about our administration of Family Medical Leave Act accommodations for you.

**What We Are Doing**

Upon learning of this event, we responded to the incident without delay, isolated and contained the IT systems, and began an investigation to determine the scope of its effects. Continental immediately engaged a team that includes law enforcement officials, a security assessment and cyber forensics firm, and IT infrastructure professionals as we set out to return our systems safely to operational status. We have taken precautionary measures, including resetting internal passwords, enhancing our monitoring capabilities to detect viruses, malware, and malicious code, and implementing other security-related enhancements.

As detailed more fully below, we have internal and external resources to assist you in understanding this event and protecting your information.

**What You Can Do**

Please review the attached *Steps You Can Take to Protect Your Personal Information*. We also encourage you to enroll in the complimentary credit monitoring services we are offering you. In addition, we would recommend that you change your passwords and security questions, particularly for accounts where passwords or security question answers that are reused. We also encourage you to actively monitor your financial accounts, including your banking, credit card, and other account statements. You should carefully review your credit reports to verify that your name, address, account, and any other information is accurate. Notify the credit reporting agencies of any errors you detect, any accounts you did not open, or inquiries from creditors you did not initiate.

You should also be suspicious of any unanticipated emails, text messages, chats, or voicemails that you may receive (as they may be phishing attempts), and you must be vigilant about monitoring your identity and credit to guard against criminals taking advantage.

Be suspicious of anything you're not expecting or is out of the ordinary (including links and attachments) received via email, text, or social media, and be particularly vigilant. When you encounter a suspicious message:

1. Hover over (don't click) the sender's email address to see if it looks legitimate.
2. Pay close attention to the domain name (e.g., company website) and look for misspellings or typos.
3. Hover over (don't click) links to check the domain name and compare it against the official website domain through an online search prior to clicking.
4. Do not click links or open attachments you're not sure about.
5. Call service providers, individuals, or any company at the number you have stored or the number you are able to independently look up to verify messages, texts, or phone calls instead of clicking on links or replying to text or email from unverified and unknown senders.

We take our partnership very seriously and deeply regret the incident. The protection of our client and team member data will remain our highest priority, and we will continue to review and adapt our cyber security measures to better safeguard the information held by us.

**For More Information**

We hope that we can answer the questions that are most important to you with this letter and an FAQ that has been sent to you. We understand you may have questions about the incident that are not addressed in this letter. If you have questions, please email humanresources@continentalserves.com or you may contact the call center provided by TransUnion.

With kind regards,

Your Continental HR Team
humanresources@continentalserves.com

**Steps You Can Take to Help Protect Your Personal Information**

In response to the incident, we are providing you with access to three bureau credit monitoring services at no charge. These services provide you with alerts for 12 months (or longer, where applicable) from the date of enrollment when changes occur to your credit file. This notification is sent to you the same day that the change or update takes place with the bureau. Finally, we are providing you with proactive fraud assistance to help with any questions that you might have or in the event that you become a victim of fraud. These services will be provided by **Cyberscout**, a TransUnion company specializing in fraud assistance and remediation services.

**How do I enroll for the free services?**

To enroll in Credit Monitoring services at no charge, please log on to **<<URL>>** and follow the instructions provided. When prompted please provide the following unique code to receive services: **<CODE HERE>**

To receive the monitoring services described above, you must enroll within 90 days from the date of this letter. The enrollment requires an internet connection and e-mail account and may not be available to minors under the age of 18 years of age. Please note that when signing up for monitoring services, you may be asked to verify personal information for your own protection to confirm your identity.

**If you do not wish to take part in the TransUnion credit monitoring, we strongly encourage you to:**

**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.

**Credit Freeze**

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 may need to provide the following information, depending on whether you make the request online, by phone, or by mail:

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.);
7. Social Security Card, pay stub, or W2;
8. If you are a victim of identity theft, include a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning 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 |
| 1-888-298-0045 | 1-888-397-3742 | 1-800-916-8800 |
| Equifax Fraud Alert<br>P.O. Box 105069<br>Atlanta, GA 30348-5069 | Experian Fraud Alert<br>P.O. Box 9554<br>Allen, TX 75013 | TransUnion Fraud Alert<br>P.O. Box 2000<br>Chester, PA 19016 |
| Equifax Credit Freeze,<br>P.O. Box 105788<br>Atlanta, GA 30348-5788 | Experian Credit Freeze,<br>P.O. Box 9554<br>Allen, TX 75013 | TransUnion Credit Freeze,<br>P.O. Box 160<br>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, your state Attorney General, and the Federal Trade Commission. This notice has not been delayed by law enforcement.

*For District of Columbia Residents:* You may obtain information about preventing and avoiding identity theft from the Office of the Attorney General for the District of Columbia at: Office of the Attorney General for the District of Columbia, 400 6th Street NW, Washington, D.C. 20001; (202) 727-3400; https://oag.dc.gov/.

*For Maryland residents*, the Maryland Attorney General may be contacted at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-410-576-6300 or 1-888-743-0023; and https://www.marylandattorneygeneral.gov/.

*For New York residents*, the New York Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; or https://ag.ny.gov.

*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 https://www.ncdoj.gov.

*For New Mexico residents*, consumers have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in their credit file has been used against them, the right to know what is in their credit file, the right to ask for their credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting bureaus must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to consumers' files is limited; consumers must give consent for credit reports to be provided to employers; consumers may limit "prescreened" offers of credit and insurance based on information in their credit report; and consumers may seek damages from violators. Consumers may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active-duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. We encourage consumers to review their rights pursuant to the Fair Credit Reporting Act by visiting https://www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.