December <XX>, 2022

<First Name> <Last Name>
<Street Address 1>
<Street Address 2>
<City>, <State> <Zip Code>

NOTICE OF SECURITY INCIDENT

Dear *<First Name>*,

We are writing to let you know about a cyber security incident that occurred at Teleperformance USA ("TPUSA"). We want to make clear at the outset that keeping personal data safe and secure is extremely important to us, and we deeply regret that this incident occurred.

WHAT HAPPENED?

On November 4, 2022, we detected that an unauthorized third party gained remote access to a portion of TPUSA's network. We immediately began an investigation of the incident with the support of leading outside cybersecurity experts and notified law enforcement. Our investigation revealed that the unauthorized party acquired some of TPUSA's internal company data, which included personal information of certain individuals, including certain of your personal information.

WHAT INFORMATION WAS INVOLVED?

The personal information that may have been affected includes your [variable text]. As of the time of writing, we have no information suggesting that your personal information has been misused as a result of this incident. Targeted online monitoring commissioned by Teleperformance has not revealed any publication, sale or other exploitation of your personal information.

WHAT WE ARE DOING

We took prompt steps to address this incident after discovery. As previously mentioned, we initiated an investigation with the assistance of external cybersecurity experts to help remediate and ensure the ongoing security of our network. We have also notified law enforcement of this incident but have not delayed notification as a result of any law enforcement investigation.

To help protect your identity, we are offering a complimentary 24-month membership of Experian's® IdentityWorks^{SM} - Credit 1B. 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:

Enrollment Instructions - IdentityWorks - Credit 1B

- Ensure that you **enroll by**: March 31, 2023 (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]

Additional details regarding your 24-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.*
- **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^{TM}**: 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***:** Provides coverage for certain costs and unauthorized electronic fund transfers.

* Offline members will be eligible to call for additional reports quarterly after enrolling

**Please note that this Identity Restoration support is available to you for 24 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 offer are located at www.ExperianIDWorks.com/restoration. You will also find self-help tips and information about identity protection at this site.

***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.

WHAT YOU CAN DO

We strongly encourage you to contact Experian and take advantage of the credit monitoring and identity theft protection services that we are providing to you free of charge. In addition, you should remain vigilant and carefully review your accounts for any suspicious activity. This is a best practice for all individuals.

If you detect any suspicious activity on an account, you should change the password and security questions associated with the account, and promptly notify the financial institution or company with which the account is maintained and any relevant government agency, such as IRS, SSA, or state DMV, as applicable.

If you would like to take additional steps to protect your personal information, attached to this letter are helpful resources on how to do so, including recommendations from the Federal Trade Commission regarding identity theft protection and details on how to place a fraud alert or a security freeze on your credit file.

FOR MORE INFORMATION

We take our responsibility to protect your personal information extremely seriously. We will continue to take all appropriate steps to keep information safe and continually enhance our posture, policies, and processes.

If you have any questions regarding this incident or the services available to you, please contact us via email at TPUS_HRSupport@Teleperformance.com or call 877-877-3944 using the following instructions.

- Select Option 1 for US Human resources; and then select Option 1 again (for "If you have received a mailer with reference number")
- Reference number is CTSS1222

Sincerely,

Katrina Sevier
Chief Human Resources Officer
Teleperformance USA

Additional Resources

Below are additional helpful tips you may want to consider to protect your personal information.

Review Your Credit Reports and Account Statements; Notify Law Enforcement of Suspicious Activity
As a precautionary measure, we recommend that you remain vigilant by reviewing your credit reports and account statements closely. If you detect any suspicious activity on an account, you should promptly notify the financial institution or other company with which the account is maintained. You also should promptly report any fraudulent activity or any suspected incidents of identity theft to proper law enforcement authorities. If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should immediately contact law enforcement, the Federal Trade Commission ("FTC") and/or the Attorney General's office in your home state. You can also contact these agencies for information on how to prevent or avoid identity theft, and you can contact the FTC at:

Federal Trade Commission
Consumer Response Center
600 Pennsylvania Avenue, NW
Washington, DC 20580
www.ftc.gov/IDTHEFT
1-877-IDTHEFT (438-4338)

Copy of Credit Report
You may obtain a free copy of your credit report from each of the three major credit reporting agencies once every 12 months by visiting https://www.annualcreditreport.com, calling toll-free 877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to the Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. You can print this form at https://www.annualcreditreport.com/manualRequestForm.action. Credit reporting agency contact details are provided below.

Equifax:	**Experian**:	**TransUnion**:
equifax.com	experian.com	transunion.com
equifax.com/personal/credit-report-services	experian.com/help	transunion.com/credit-help
P.O. Box 740241	P.O. Box 2002	P.O. Box 1000
Atlanta, GA 30374	Allen, TX 75013	Chester, PA 19016
866-349-5191	888-397-3742	888-909-8872

When you receive your credit reports, review them carefully. Look for accounts or credit inquiries that you did not initiate or do not recognize. Look for information, such as home address and Social Security number, that is inaccurate. If you see anything you do not understand, call the credit reporting agency at the telephone number on the report.

Fraud Alert
You may want to consider placing a fraud alert on your credit file. An initial fraud alert is free and will stay on your credit file for at least 90 days. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any accounts in your name. If you have already been a victim of identity theft, you may have an extended alert placed on your report if you provide the appropriate documentary proof. An extended fraud alert stays on your credit report for seven years. To place a fraud alert on your credit report, contact any of the three credit reporting agencies identified above.

Security Freeze
You have the right to place a security freeze on your credit file free of charge. This will prevent new credit from being opened in your name without the use of a PIN number that is issued to you when you initiate the freeze. A security freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. As a result, using a security freeze may delay your ability to obtain credit. In order to place a security freeze, you may be required to provide the consumer reporting agency with information that identifies you including your full name; social security number; date of birth; current and previous addresses; a copy of your state-issued identification card; and a recent utility bill, bank statement, or telephone bill.

Federal Fair Credit Reporting Act Rights
The Fair Credit Reporting Act (FCRA) is federal legislation that regulates how consumer reporting agencies use your information. It promotes the accuracy, fairness, and privacy of consumer information in the files of consumer reporting agencies. As a consumer, you have certain rights under the FCRA, which the FTC has summarized as follows: you must be told if information in your file has been used against you; you have the right to know what is in your file; you have the right to ask for a credit score; you have the right to dispute incomplete or inaccurate information; consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for reports to be provided to employers; you may limit "prescreened" offers of credit and insurance you get based on information in your credit report; and you may seek damages from violators. Identity theft victims and active duty military personnel have additional rights.

For more information about these rights, you may go to www.ftc.gov/credit or write to: Consumer Response Center, Room 13-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

Additional Information
You have the right to obtain any police report filed in regard to this incident. If you are the victim of fraud or identity theft, you also have the right to file a police report.

You may consider starting a file with copies of your credit reports, any police report, any correspondence, and copies of disputed bills. It is also useful to keep a log of your conversations with creditors, law enforcement officials, and other relevant parties.

For Colorado and Illinois residents: You may obtain information from the Federal Trade Commission and the credit reporting agencies about fraud alerts and security freezes.

For Iowa and Oregon residents: You are advised to report any suspected identity theft to law enforcement, including the Federal Trade Commission and the state Attorney General.

For Maryland residents: You may contact the Office of the Maryland Attorney General, 200 St. Paul Place, Baltimore, MD 21202, http://www.marylandattorneygeneral.gov, 1-888-743-0023. The Office of the Maryland Attorney General may be able to provide you with information about the steps you can take to avoid identity theft.

For New York residents: For more information on identity theft, you can contact the following: New York Department of State Division of Consumer Protection at http://www.dos.ny.gov/consumerprotection or (800) 697-1220 or NYS Attorney General at http://www.ag.ny.gov/home.html or (800) 771-7755.

For North Carolina residents: You may contact the North Carolina Office of the Attorney General, 9001 Mail Service Center, Raleigh, NC 27699-9001, http://www.ncdoj.gov, 1-877-566-7226. You are also advised to report any suspected identity theft to law enforcement or to the North Carolina Attorney General.

For Connecticut, Florida, Indiana, Louisiana, Maine, Maryland, Nebraska, New Jersey, Texas, and Virginia residents: You may obtain one or more (depending on the state) additional copies of your credit report, free of charge. You must contact each of the credit bureaus directly to obtain such additional report(s).