TELUS International AI, Inc
c/o Cyberscout
PO Box 1286
Dearborn, MI 48120-9998

P
JANE LAUREANNE DEGALA MAURICIO
12345 RODEO DR
BEVERLY HILLS CA, 90210

000010102G0500

P

July 28, 2026

Individual Notice - Tranche 3A U.S. Current and Former Employee Personal Information Breach Notification Template_TELUS Digital

Dear JANE LAUREANNE MAURICIO,

TELUS International AI, Inc., d/b/a TELUS Digital ("TELUS Digital"), writes to inform you of a data security incident that may have impacted your personal information. Below is information about what happened, the steps we have taken in response, and steps you can take if you feel it is appropriate to do so.

What Happened?
On November 12, 2025, TELUS Digital identified unauthorized activity. Upon discovery of the incident, TELUS Digital activated its incident response protocols and engaged external experts to support our incident response efforts. As part of our investigation, we have been conducting a careful review of documents that may have been copied by an unauthorized third party. On June 26, 2026, TELUS Digital determined that certain documents contained your personal information.

What Information was Involved?
We collect your name and contact information, along with your employment and human resources information; date of birth and other demographic information; family, dependent, spouse or relationship information; emergency contact information; and work-related role and role history, some or all of which could have been affected. For some individuals, the information may also have included Social Security number, passport number, tax identification number, health information, personal identification document number, or similar government identification number.

What Are We Doing?
As part of our response, we launched an investigation alongside leading cybersecurity experts and have been working with law enforcement. We also took steps to further strengthen our existing safeguards, including implementing additional security measures to address the continually evolving threat landscape.

Additionally, we are providing you with access to **Single Bureau Credit Monitoring/Single Bureau Credit Report/Single Bureau Credit Score** services at no charge. These services are being provided to you with alerts for twenty-four (24) months from the date of enrollment when changes occur to your credit file. This notification is sent to you on 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.

To enroll in Credit Monitoring services at no charge, please log on to https://bfs.cyberscout.com/activate and follow the instructions provided. When prompted please provide the following unique code to receive services **4B0EFCAF9C96**. 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 an email 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.

What You Can Do.
Although we have no reports of misuse of your information, we encourage you to enroll in the cyber monitoring services we are providing at no cost to you.

For More Information.
If you have any questions or need assistance in signing up for the complimentary services being provided, please call **1- 833-289-9956,** Monday through Friday from 8:00 am - 8:00 pm Eastern Time. We appreciate your patience and understanding, and we sincerely apologize for any inconvenience or concern this incident may cause you.

Sincerely,

TELUS International AI, Inc.

Additional Important Information

Monitoring: You should always remain vigilant for incidents of fraud and identity theft, especially during the next 12-24 months, by reviewing financial account statements and monitoring your credit reports for suspicious or unusual activity and immediately report any suspicious activity or incidents of identity theft. You have the right to obtain or file a police report. You can contact the Federal Trade Commission (FTC) for more information on preventing identity theft. We encourage you to report any incidents of identity theft to the FTC.

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

Credit Reports: You may obtain a copy of your credit report, for free, whether or not you suspect any unauthorized activity on your account, from each of the three nationwide credit reporting agencies. To order your free credit report, please visit www.annualcreditreport.com, or call toll-free at 1-877-322-8228. You can also order your annual free credit report by mailing a completed Annual Credit Report Request Form (available at www.consumer.ftc.gov/articles/0155-free-credit-reports) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281.

Fraud Alerts: You have the right to place fraud alerts with the three credit bureaus by phone and online with Equifax (https://assets.equifax.com/assets/personal/Fraud_Alert_Request_Form.pdf), Experian (www.experian.com/fraud/center.html) or Transunion (www.transunion.com/fraud-victim-resource/place-fraud-alert). A fraud alert tells creditors to follow certain procedures, including contacting you, before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit. Initial fraud alerts last for one year. Victims of identity theft can also get an extended fraud alert for seven years. The phone numbers for all three credit bureaus are at the bottom of this page.

Security Freeze: You also have the right to place a security freeze on your credit report. A security freeze is intended to prevent credit, loans, and services from being approved in your name without your consent. To place a security freeze on your credit report, you need to make a request to each consumer reporting agency by visiting their websites below or by mail. To place the security freeze for yourself, your spouse, or a minor under the age of 16, you will need to provide your name, address for the past two years, date of birth, Social Security number, proof of identity and proof of address as requested by the credit reporting company. After receiving your freeze request, each credit reporting company will send you a confirmation letter containing a unique PIN (personal identification number) or password, which will be needed to lift the freeze, which you can do either temporarily or permanently. It is free to place, lift, or remove a security freeze.

Equifax Security Freeze
P.O. Box 105788
Atlanta, GA 30348-5788
www.equifax.com/personal/credit-report-services/credit-freeze/
1-866-478-0027

Experian Security Freeze
P.O. Box 9554
Allen, TX 75013-9544
http://www.experian.com/freeze/center.html
1-888-397-3742

TransUnion Security Freeze
P.O. Box 160
Woodlyn, PA 19094
www.transunion.com/credit-freeze
1-800-916-8800

For residents of *Iowa* and *Oregon*: *Y*ou are advised to report any suspected identity theft to law enforcement or to the state Attorney General and Federal Trade Commission.

For residents of New Mexico: You are advised to review personal account statements and credit reports, as applicable, to detect errors resulting from the security incident. You have rights under the federal Fair Credit Reporting Act (FCRA). These include, among others, the right to know what is in your file, to dispute incomplete or inaccurate information, and to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information. For more information about the FCRA, please visit https://files.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf or see the contact information for the Federal Trade Commission.

For residents of District of Columbia, Maryland, New York, North Carolina, and Rhode Island:
You can obtain information from the District of Columbia, Maryland, North Carolina, New York, and Rhode Island Offices of the Attorney General and the FTC about fraud alerts, security freezes, and steps you can take to prevent identity theft.

District of Columbia Attorney General 400 6th Street NW Washington, DC 20001 1-202-442-9828 www.oag.dc.gov	**Maryland Office of Attorney General** 200 St. Paul Pl Baltimore, MD 21202 1-888-743-0023 https://www.marylandattorneygeneral.gov/	**New York Attorney General** 120 Broadway, 3rd Fl New York, NY 10271 1-800-771-7755 www.ag.ny.gov	**North Carolina Attorney General** 9001 Mail Service Ctr Raleigh, NC 27699 1-877-566-7226 https://ncdoj.gov/	**Rhode Island Attorney General** 150 South Main St Providence RI 02903 1-401-274-4400 www.riag.ri.gov