

Via Email (Idtheft@oag.state.md.us)

Office of the Maryland Attorney General
200 St. Paul Place
Baltimore, MD 21202

To Attorney General Brown:

Pursuant to Md. Code Ann., Com. Law § 14-3504, we are writing to inform you that Tesla, Inc. (*Tesla*) is sending notices to Maryland residents advising them of a data incident.

A foreign media outlet (named Handelsblatt) informed Tesla on May 10, 2023 that it was in possession of confidential Tesla data. Tesla promptly initiated an investigation of the incident, which revealed that the media outlet received the data from two former Tesla employees who misappropriated the information in violation of Tesla's IT security and data protection policies.¹

Tesla immediately took steps to determine the scope of the incident and the data that was misappropriated, followed by an expedited review of the contents of that data. That review recently revealed that the misappropriated data included certain personal information concerning certain current and former Tesla employees potentially giving rise to a notification obligation under Maryland law.

At this time, Tesla has identified 494 affected records of personal information for which the corresponding person appears to be a Maryland resident. By providing this notice, Tesla does not waive any rights or defenses regarding the applicability of Maryland law, the applicability of the Maryland data event notification statute, or personal jurisdiction.

The data affected in this incident varies from person to person and includes some combination of the following: name, address, phone number, email address, passport number, social security number, and some health-related information, which Tesla maintains in the ordinary course of business in its capacity as the individuals' employer. Any exposed health-related information did not include medical practitioner records, detailed or sensitive medical diagnoses, or treatment information.

Commencing on August 18, 2023, a formal notice of the incident is being sent by U.S. mail to the individuals for whom Tesla has identified a Maryland mailing address. A copy of the anticipated notice is attached.

Tesla is not currently aware of any evidence indicating that the personal information involved in this incident has been misused in any manner that would cause harm to the impacted employees. The outlet has stated that it does not intend to publish the personal information, and in any event, is legally prohibited from using it inappropriately pursuant to the European Union's General Data Protection Regulation. With respect to the former Tesla employees who misappropriated the data,

¹ Although Tesla first learned of the incident on May 10, 2023, it does not have information confirming the date on which the misappropriated data was actually provided to Handelsblatt by the former employees.

Tesla filed lawsuits against both individuals that resulted in the seizure of the employees' electronic devices that were believed to have contained the Tesla information. The lawsuits also resulted in Tesla obtaining court orders that prohibit the former employees from further use, access, or dissemination of the data, subject to criminal penalties.

Tesla takes the security, data privacy, and integrity of its employees' personal information seriously and maintains information technology measures designed to protect the company against misuse of company data. Tesla is committed to the protection of the data it handles and will continue to confirm its safeguards and implement appropriate measures, as well as ensure employees are trained on responsible data handling practices.

Please contact me if you have any questions.

Sincerely,

/s/

Steven Elentukh
Data Privacy Officer

Enclosure



Return Mail Processing
PO Box 589
Claysburg, PA 16625-0589

August 18, 2023

J8824-L03-0000002 T00001 P001 *****SCH 5-DIGIT 12345

SAMPLE A SAMPLE - L03 NONCA

APT ABC



123 ANY STREET

ANYTOWN, FC 1A2 B3C

COUNTRY



Notice of Data Incident

At Tesla, we take data privacy and security seriously— so we are writing to tell you about a data incident that involved your information. While we have not identified evidence of misuse of the data in a manner that may cause harm to you, we are nonetheless providing you with this notice to ensure that you are aware of what happened and the measures we have taken.

What Happened

A foreign media outlet (named Handelsblatt) informed Tesla on May 10, 2023 that it had obtained Tesla confidential information. The investigation revealed that two former Tesla employees misappropriated the information in violation of Tesla's IT security and data protection policies and shared it with the media outlet. The outlet has stated that it does not intend to publish the personal information, and in any event, is legally prohibited from using it inappropriately.

Tesla immediately took steps to contain the incident, understand the scope, and protect your information. Among other things, we identified and filed lawsuits against the two former employees. These lawsuits resulted in the seizure of the former employees' electronic devices that were believed to have contained the Tesla information. Tesla also obtained court orders that prohibit the former employees from further use, access, or dissemination of the data, subject to criminal penalties. Tesla cooperated with law enforcement and external forensics experts and will continue to take appropriate steps as necessary.

We also arranged resources to determine what data was involved and identify potentially affected individuals. As discussed below, we recently confirmed that certain employee-related records were among the confidential information affected as part of this incident.

What Information Was Involved

The personal information involved concerns data for certain current and former employees, including your name, certain contact information (such as address, phone number, and/or email address), [Extra2] that Tesla maintains in the ordinary course of business in its capacity as an employer. [Extra3]

What We Are Doing

Tesla is committed to the protection of the data it handles and will continue to confirm its safeguards and implement appropriate measures, as well as ensure employees are trained on responsible data handling practices. In addition, although we have no evidence that any personal information was misused in a manner that could harm you, we are supporting those affected by offering a complimentary [Extra1] membership of Experian's IdentityWorks. This product provides you with credit monitoring, and identity detection and resolution services. Please see Attachment A for instructions on how to enroll.



What You Can Do

In addition to signing up for complimentary credit monitoring, you can review Attachment B, which provides further information about steps you can take to protect your identity in general, should you feel it is appropriate to do so.

For More Information

If you have any questions about the incident, you can call our dedicated toll-free telephone line at 800-607-1589, Monday through Friday 8 am – 10 pm CST, and Saturday and Sunday 10 am – 7 pm CST (excluding major U.S. holidays).

Yours sincerely,

Steven Elentukh

Data Privacy Officer

ATTACHMENT A

We are offering complimentary access to Experian IdentityWorksSM for ## months.

If you believe there was fraudulent use of your information as a result of this incident and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent. 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 from the date of the incident (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 Identity Restoration is available to you for ## months from the date of this letter and does not require any action on your part at this time. The Terms and Conditions can be found at www.ExperianIDWorks.com/restoration.

While identity restoration assistance is **immediately available to you**, we also encourage you to activate the fraud detection tools available through Experian IdentityWorks as a complimentary ##-month membership. This product provides you with superior identity detection and resolution of identity theft. To start monitoring your personal information, please follow the steps below:

- Ensure that you enroll by November 30, 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: **ABCDEFGHI**

If you have questions about the product, need assistance with Identity Restoration that arose as a result of this incident, or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at 800-607-1589 by November 30, 2023. To expedite your call, provide your engagement number ENGAGE# as proof of eligibility for the Identity Restoration services by Experian.

ADDITIONAL DETAILS REGARDING YOUR ##-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 specialists are immediately available to help you address credit and non-credit related fraud.
- Experian IdentityWorks ExtendCARETM: You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- \$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.

** 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.

0000003



ATTACHMENT B

GENERAL STEPS TO TAKE TO PROTECT YOUR PERSONAL INFORMATION

- You should be vigilant against possible “phishing” communications, including from emails that appear to be (but are not) sent from a particular organization.
- Regularly review your account statements and credit history for any signs of unauthorized transactions or activity, and remain vigilant against threats of identity theft or fraud.

STEPS YOU CAN TAKE TO PROTECT YOURSELF WITH REGARD TO CONSUMER CREDIT REPORTING BUREAUS

Ordering 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 Alert. When you place a “fraud alert” on your credit report, businesses who pull your credit report will see that you may be a victim of identity theft. The company may then choose to verify your identity before they extend credit to anyone who purports to be you. To place an alert, contact any one of the three main credit reporting bureaus. That company is required to tell the other two bureaus about the alert. When you first place a fraud alert on your account, it will remain for at least 90 days, after which you can renew it. When you do place an alert on your report, be sure that all three major credit reporting companies have your current contact information so they can get in touch with you.

Security Freeze. A “security freeze” or “credit freeze” goes further than an alert and lets you restrict access to your credit report entirely. This is because most creditors need to see your credit report before they approve a new account. If creditors cannot see your file, they may not extend the credit. A credit freeze does not affect your credit score, but you may need to lift the freeze temporarily, either for a specific time or for a specific party if you are opening a new account, applying for a job, renting an apartment or buying insurance.

To place a freeze, you need to contact each of the major credit reporting bureaus. You will need to supply your name, address, date of birth, social security number and other personal information. Credit reporting agencies are required to place/remove a freeze on your credit report without charge.

Below, we provide contact information for the major credit reporting agencies. They can provide additional resources about preventing or remedying identity theft, including by setting up fraud alerts/security freezes and by reviewing your credit report. Fees may be required for some services.

EQUIFAX
P.O. Box 105069
Atlanta, GA 30348-5069
866-478-0027
www.equifax.com/personal/credit-report-services

EXPERIAN
P.O. Box 9554
Allen, TX 75013
888-397-3742
www.experian.com/freeze

TRANSUNION
P.O. Box 160
Woodlyn, PA 19094
800-916-8800
freeze.transunion.com

INFORMATION AND ASSISTANCE THAT YOU CAN OBTAIN FROM FEDERAL AND STATE LAW ENFORCEMENT AND CONSUMER PROTECTION AGENCIES:

If you believe that you may be the victim of identity theft, you should report that immediately to law enforcement, your state Attorney General, or the Federal Trade Commission. You also may wish to review the resources provided by the Federal Trade Commission on how to avoid identity theft. You can reach the FTC at:

Bureau of Consumer Protection
Federal Trade Commission
600 Pennsylvania Ave., NW
Washington, DC 20580

1-877-ID-THEFT (877-438-4338)
www.identitytheft.gov

PROTECTIONS OF THE FEDERAL FAIR CREDIT REPORTING ACT

The Fair Credit Reporting Act (FCRA) promotes the accuracy, fairness, and privacy of information in the files of consumer reporting agencies. In particular, the FCRA enables identity-theft victims to demand the removal of false entries on their credit reports that result from the theft. Your major rights under the FCRA include:

- 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.
- You may seek damages from violators.

You can obtain more information, including information regarding additional rights at www.ftc.gov/credit, or at https://files.consumerfinance.gov/f/documents/bcfr_consumer-rights-summary_2018-09.pdf.

IF YOU ARE A RESIDENT OF CERTAIN STATES, YOU HAVE ADDITIONAL RIGHTS:

DISTRICT OF COLUMBIA

You can contact the Attorney General at:
400 6th Street NW, Washington, D.C. 20001
202-727-3400
<https://oag.dc.gov/>

MARYLAND

You can contact the Attorney General at:
200 St. Paul Place, 25th Floor, Baltimore, MD 21202
410-576-6491
<https://www.marylandattorneygeneral.gov/>

MASSACHUSETTS

You have the right to obtain a police report in regard to this incident.

NORTH CAROLINA

You can contact the Attorney General at:
9001 Mail Service Center, Raleigh, NC 27699-9001
919-716-6400
<http://www.ncdoj.gov>



