O'Melveny & Myers LLP
2501 North Harwood St., Suite 1700
Dallas, TX 75201-1663

T: +1 972 360 1900
F: +1 972 360 1901
omm.com

March 1, 2024

VIA ELECTRONIC DELIVERY

Consumer Protection & Antitrust Bureau
New Hampshire Department of Justice
33 Capital Street
Concord, NH 03301
DOJ-CPB@doj.nh.gov
attorneygeneral@doj.nh.gov

Re: Supplemental Notice of Data Security Incident

Office of the Attorney General:

On behalf of my client, TTM Technologies ("TTM" or the "company"), and pursuant to N.H. Rev. Stat. 359-C:20, I am writing to update you regarding the data incident previously disclosed to you on December 19, 2023, and to notify you that the data incident involved the personal information of five (5) additional New Hampshire residents.

A copy of my previous letter is attached as Exhibit A. Since my first notification, the company has completed its investigation and is now supplementally notifying any additionally identified individuals who may have been affected by the breach. Attached as Exhibit B is the notification that will be sent to the five additional New Hampshire residents on March 1, 2024.

As previously stated, TTM is dedicated to protecting personal information within its control and has taken steps to minimize the risk of a similar incident occurring in the future. Should you have any questions or need additional information concerning this incident, please contact me by email at

Sincerely,

Sid Mody
O'Melveny & Myers LLP

Exhibit A

O'Melveny & Myers LLP
2501 North Harwood St., Suite 1700
Dallas, TX 75201-1663

T: +1 972 360 1900
F: +1 972 360 1901
omm.com

December 19, 2023

VIA ELECTRONIC DELIVERY

Consumer Protection & Antitrust Bureau
New Hampshire Department of Justice
33 Capital Street
Concord, NH 03301
DOJ-CPB@doj.nh.gov
attorneygeneral@doj.nh.gov

Re: Notice of Data Security Incident

Office of the Attorney General:

On behalf of my client, TTM Technologies ("TTM" or the "company"), and pursuant to N.H. Rev. Stat. 359-C:20, I am writing to notify you of a data breach involving the personal information of fourteen (14) New Hampshire residents.

On October 4, 2023, the company learned that an unauthorized third-party, not located at any TTM facility, accessed TTM's servers containing employee PII through use of a port scanner. As soon as TTM discovered the unauthorized access, the company shut down the impacted systems, terminated the unauthorized access, and engaged cyber security consultants to investigate the incident. Through its investigation, TTM discovered that the personal information of New Hampshire residents was potentially accessed.

A copy of the employee notice is attached as Exhibit A. The notification will be sent to the New Hampshire residents on December 19, 2023.

TTM is dedicated to protecting personal information within its control and has taken steps to minimize the risk of a similar incident occurring in the future. Should you have any questions or need additional information concerning this incident, please contact me by email at

Sincerely,

Sid Mody
O'Melveny & Myers LLP

Exhibit B

TTM Technologies
Time-To-Market Interconnect Solutions

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

[Addressee Address]

NOTICE OF DATA BREACH

[Date]

Dear [Name],

We are writing to inform you of a data security incident that TTM Technologies experienced that may have affected your personal information. This letter is meant to provide you with information about the incident and about resources available to you.

What Happened?

On October 4, 2023, TTM identified suspicious activity on its network and determined that on or around September 26, 2023, an unauthorized third-party had gained access to TTM's systems. TTM immediately shut down the impacted systems, terminated the unauthorized access, and engaged cyber security consultants to investigate the incident. After a comprehensive and thorough investigation, TTM determined that your personal information may have been accessed.

What Information was Involved?

The type of personal information potentially accessed by the unauthorized third-party includes:

. Please note that not all types of personal information potentially accessed by the unauthorized party apply to all individuals and TTM is not aware of any actual fraud or identity theft involving your information.

What We Are Doing

TTM takes the privacy and security of personal information seriously. After discovering the unauthorized access, TTM took immediate steps to mitigate and remediate the incident and to restrict further access. TTM commenced a prompt and thorough investigation involving IT and cyber security professionals. In response to this incident, and as a part of TTM's ongoing process of reflection and refinement, TTM has made adjustments to its cyber security systems and procedures to minimize the risk of a similar incident occurring in the future.

Out of an abundance of caution, TTM will provide of free credit and identity theft monitoring services through Experian. Instructions for signing-up are below. Please note that you must enroll in credit monitoring no later than

What You Can Do

In addition to enrolling in the complimentary credit monitoring services offered by TTM, this letter provides information on steps you can take to monitor and protect your personal information. In general, it is a best practice to regularly review your credit reports and account statements to ensure that all activity and transactions are valid. Any questionable charges or inquiries should be reported immediately to the company producing the report or maintaining the account.

For More Information

For more information concerning this incident, please call 833-430-2161 toll-free. Representatives will be available between 8:00 AM and 8:00 PM CST, excluding holidays. When you call, reference your engagement number, which is [B######].

Sincerely,

TTM Technologies

Other Important Information

1. Enrolling in Identity Theft Protection

To help protect your identity, we are offering complimentary access to Experian IdentityWorks[SM] for .

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 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.

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 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** (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll: https://www.experianidworks.com/credit
- Provide your **activation code**: [Activation Code]

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 833-430-2161 by . Be prepared to provide engagement number [B#######] as proof of eligibility for the Identity Restoration services by Experian.

ADDITIONAL DETAILS REGARDING YOUR 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 ExtendCARE™:** 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.

2. Fraud Alerts

Whether or not you choose to enroll in the credit monitoring services offered by TTM, you may consider placing a fraud alert on your credit file. Fraud alerts help protect against the possibility of identity theft by providing a notice to creditors that an applicant for a new account may be the victim of identity theft. Fraud alerts notify credit grantors that they need to take additional steps to verify an applicant's identity. You can place a fraud alert on your credit report by filing a report through any one of the websites or calling any one of the toll-free numbers below. Once one of the credit agencies below confirms your fraud alert, they will notify the others.

Equifax
P.O. Box 105069
Atlanta, GA 30348
https://www.equifax.com/personal/credit-report-services/credit-fraud-alerts/
1-888-836-6351

Experian
P.O. Box 9554
Allen, TX 75013
https://www.experian.com/fraud/center.html
1-888-397-3742

TransUnion
PO Box 2000
Chester. PA 19016
https://www.transunion.com/fraudalerts
1-800-680-7289

3. Security Freezes

You may also consider requesting a "security freeze" from the three credit reporting agencies listed below. With certain exceptions, a security freeze prohibits credit reporting agencies from releasing your credit report or any information contained within it without your permission. If you choose to establish a security freeze, some creditors will not be able to access your credit report which may delay your ability to obtain credit. You may place a security freeze on your credit report by sending a request to one of the agencies listed below. To find out more about how to place a security freeze, you can use the following contact information:

Equifax Information Services LLC
P.O. Box 105788
Atlanta, GA 30348
https://www.equifax.com/personal/credit-report-services/credit-freeze/
1-888-298-0045

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

TransUnion
PO Box 2000
Chester. PA 19016
https://www.transunion.com/creditfreeze
1-800-909-8872

Unlike a fraud alert, a security freeze must be filed with each credit agency individually. To place a security freeze you will need to provide the agencies with personal identifying information to confirm your identity including your full name, date of birth, Social Security number, current and former addresses, and other information.

4. Obtaining a Free Credit Report

You are entitled under federal law to a free credit report every 12 months from each of the three major credit reporting companies. To request your free credit report, visit www.annualcreditreport.com or call 1-877-322-8228. Once you receive your credit reports, review them closely for any accounts you did not open or inquiries from creditors you did not authorize. If you have any questions or any information seems incorrect, contact the credit reporting companies at the contact information provided on the report.

5. Contact the U.S. Federal Trade Commission

If you find any suspicious activity on your credit reports or detect any unauthorized transactions in any of your financial accounts, you should immediately notify the appropriate credit agency or financial institution. If you identify any incidents of identity theft or fraud, immediately report your concerns to your local law enforcement authorities and the FTC.

You can obtain information from the FTC about fraud alerts and security freezes using the contact information below:

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

6. State Specific Information

Maryland Residents

You may obtain information about preventing identity theft from the Maryland Attorney General's Office: Maryland Office of Attorney General, Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202, 1-888-743-0023, www.marylandattorneygeneral.gov.

New York Residents

You may obtain information about preventing identity theft from the New York Attorney General's Office: Office of the Attorney General, The Capital, Albany, NY 12225-0341, 1-800-773-774, www.ag.ny.gov.

North Carolina Residents

You may obtain information about preventing identity theft from the North Carolina Attorney General's Office: Office of the Attorney General, 114 W Edenton St, Raleigh, NC 27603, 1-919-716-6400, https://ncdoj.gov/.

Oregon Residents

Oregon state law recommends that consumers report suspected identity theft to law enforcement, including the Oregon Attorney General and Federal Trade Commission. The Oregon Department of Justice can be reached: Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301, 1-877-877-9392, www.doj.state.or.us.

Rhode Island Residents

You may obtain information about preventing identity theft from the Rhode Island Attorney General's Office: RI Office of the Attorney General, 150 South Main Street, Providence, RI 02903, 1-401-274-4400, https://riag.ri.gov.

* 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.