MAYER | BROWN

CONFIDENTIAL TREATMENT REQUESTED

Mayer Brown LLP
1999 K Street, N.W.
Washington, DC 20006-1101
United States of America

T: +1 202 263 3000
F: +1 202 263 3300

mayerbrown.com

David Simon
Partner

December 30, 2022

BY EMAIL

New Hampshire Department of Justice
33 Capitol Street
Concord, NH 03301

Re: Wabtec Corporation – Notice of Data Event

Dear Sir or Madam:

We represent Wabtec Corporation ("Wabtec") and are writing to notify your Office of a recent event that may affect the security of certain personal information relating to three (3) New Hampshire residents. Please note this notice may be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, Wabtec does not waive any rights or defenses, including regarding the applicability of New Hampshire law, the applicability of the New Hampshire data breach notification statute, or personal jurisdiction.

Wabtec is a US-headquartered global provider of equipment, systems and services with a focus on the transportation sector and with affiliates around the globe. On June 26, 2022, Wabtec discovered that certain systems and data were encrypted, and subsequently determined the cause was malware. Shortly thereafter, Wabtec notified the Federal Bureau of Investigation and has cooperated with its investigation.

Wabtec quickly initiated incident response protocols and began containment efforts to further protect its systems. In addition, Wabtec promptly launched an investigation with the assistance of leading cybersecurity firms to assess the scope of the incident and mitigate any potential impact. The forensic investigation has since concluded, and the forensic investigation firm determined, based on available forensic evidence, that malware was introduced into certain systems as early as March 15, 2022. The forensic investigation did reveal that a certain amount of data was taken from certain Wabtec systems on June 26, 2022. On August 24, 2022, the attacker began posting data purportedly belonging to Wabtec on its leak site. The same day, Wabtec, via its forensic investigation firm, began downloading the posted data for review. The download process has been lengthy and is ongoing. There have been ongoing Distributed Denial of Service (DDoS) attacks to the attacker's leak site from which the stolen data is being downloaded, and the attacker implemented "mirror sites" (sites that host the same data but on a parallel structure), which are causing extreme delay in the download process. These mirror sites are also not available for certain periods of time during the day. As data is successfully downloaded, it is sent to a third-party data review firm to identify the individuals and the types of personal information impacted by the incident. All data obtained to date has been provided to the third-party data review team. The data review process is ongoing and involves a thorough and time-consuming review of all impacted data.

On November 23, 2022, Wabtec received the first round of data review results provided by the data review firm. The same day, Wabtec began analyzing the data and confirmed that personal data was impacted by the incident. The information impacted includes: name and Social Security number.

Notice to New Hampshire Residents

On December 30, 2022, Wabtec began providing written notice of this event to potentially affected individuals, which includes three (3) New Hampshire residents. Written notice is being provided in substantially the same form as the letter attached hereto as **Exhibit A**. Wabtec will continue to notify potentially affected individuals on a *rolling basis* as it continues to receive data review results from its third-party data review firm. Please know we will continue to keep this Office informed should additional New Hampshire residents be identified.

Other Steps Taken and To Be Taken

Upon discovery of the event, Wabtec moved quickly to investigate and respond to the incident, assess the security of its systems, and notify potentially impacted individuals, which it is doing on a continuous rolling basis. Wabtec is committed to, and takes very seriously its responsibility to safeguard all data entrusted to it. As part of Wabtec's ongoing commitment to the security of personal information in its care, it has taken additional steps to reinforce the integrity and security of its systems and operations, including implementing additional procedural safeguards. Wabtec will also notify applicable regulatory authorities, as required.

Wabtec is offering potentially impacted individuals with an offer of complimentary credit monitoring and identity restoration services for a period of twenty-four (24) months through Equifax. Additionally, Wabtec provided potentially affected individuals with guidance on how to protect against identity theft and fraud. Wabtec also provided potentially affected individuals with information on how to place a fraud alert and security freeze on one's credit file, the contact details for the national consumer reporting agencies, information on how to obtain a free credit report, a reminder to remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring free credit reports, and encouragement to contact the Federal Trade Commission, their state Attorney General, and law enforcement if there is any attempted or suspected identity theft or fraud.

Contact Information

Should you have any questions regarding this notification or other aspects of the data security event, please contact me at .

Very truly yours,

David Simon
Partner

Return Mail Processing Center
PO Box 6336
Portland, OR 97228-6336

<<Mail ID>>
<<Name 1>>
<<Name 2>>
<<Address 1>>
<<Address 2>>
<<Address 3>>
<<Address 4>>
<<Address 5>>
<<City>><<State>><<Zip>>
<<Country>>

<<Date>>

RE: Notice of Data Breach

Dear <<Name 1>>:

Wabtec Corporation ("Wabtec") is writing to advise you of a recent event that may impact personal information related to you. We write to provide you with information about the event, what we have done since discovering the event, and steps you can take to further safeguard your information, should you feel it appropriate to do so.

What Happened? On June 26, 2022, Wabtec became aware of unusual activity on its network and promptly began an internal investigation. It was subsequently determined that malware was introduced into certain systems as early as March 15, 2022. Wabtec, with the assistance of leading cybersecurity firms, assessed the scope of the incident to, among other things, determine if personal data may have been affected. Additionally, shortly after discovery of the event, Wabtec notified the Federal Bureau of Investigation.

The forensic investigation did reveal that certain systems containing sensitive information were subject to unauthorized access, and that a certain amount of data was taken from the Wabtec environment on June 26, 2022, and was later posted to the threat actor's leak site. Wabtec, with the assistance of data review specialists, has been working diligently to determine the types of information subject to unauthorized access and disclosure and to whom it relates. You are receiving this letter because, on November 23, 2022, Wabtec determined that your information may have been affected.

What Information Was Involved? Wabtec determined that your name and <<Breached Elements>> were contained among the files that were subject to unauthorized access and/or disclosure.

What We Are Doing. Wabtec is committed to, and takes very seriously its responsibility to safeguard all data entrusted to it. As part of Wabtec's ongoing commitment to the security of personal information in its care, it has taken additional steps to reinforce the integrity and security of its systems and operations, including implementing additional procedural safeguards. Wabtec is also notifying all applicable regulatory authorities, as required.

As an added precaution, we are also offering you access to twenty-four (24) months of complimentary credit monitoring and identity theft restoration services through Equifax. Individuals who wish to receive these services must enroll by following the attached enrollment instructions.

What You Can Do. We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your financial account statements and credit reports for any anomalies. We also encourage you to review the enclosed *Steps You Can Take to Protect Your Information* for additional guidance. You can also enroll to receive the complimentary services being offered to you.

For More Information. We understand that you may have additional questions that are not addressed in this letter. Please call 1-888-505-4784 Monday through Friday from 9:00 a.m. to 9:00 p.m. Eastern Time, except holidays, with any questions you may have.

Wabtec sincerely regrets any inconvenience this issue may have caused you.

Sincerely,

Wabtec Corporation

Steps You Can Take to Help Protect Your Personal Information

Enroll in Complimentary Credit Monitoring Services

As a safeguard, we have arranged for you to enroll, at no cost to you, in an online credit monitoring service for twenty-four months provided by Equifax, one of the three nationwide credit reporting companies. Due to privacy laws, we cannot register you directly.

To enroll in this service:

- Go directly to ***www.equifax.com/activate***
- Enter your unique Activation Code: <<Activation Code>> and then click "Submit" and follow the below four (4) steps:

1. **Register:**
   Complete the form with your contact information and click "Continue".
   If you already have a myEquifax account, click the 'Sign in here' link under the "Let's get started" header. Once you have successfully signed in, you will skip to the Checkout Page in Step 4
2. **Create Account:**
   Enter your email address, create a password, and accept the terms of use.
3. **Verify Identity:**
   To enroll in your product, we will ask you to complete our identity verification process.
4. **Checkout:**
   Upon successful verification of your identity, you will see the Checkout Page.
   Click 'Sign Me Up' to finish enrolling. The confirmation page shows your completed enrollment. Click "View My Product" to access the product features.

You can sign up for the online credit monitoring service anytime between now and <<Enrollment Deadline>>.

Key features of this offering include:

- Credit monitoring with email notifications of key changes to your Equifax credit report;
- Daily access to your Equifax credit report;
- WebScan notifications[1] when your personal information, such as Social Security Number, credit/debit card or bank account numbers are found on fraudulent Internet trading sites;
- Automatic fraud alerts[2], which encourages potential lenders to take extra steps to verify your identity before extending credit, plus blocked inquiry alerts and Equifax credit report lock[3];
- Identity Restoration to help restore your identity should you become a victim of identity theft, and a dedicated Identity Restoration Specialist to work on your behalf; and
- Up to $1,000,000 of identity theft insurance coverage for certain out of pocket expenses resulting from identity theft[4].

Monitor Your Accounts

We encourage you to remain vigilant against incidents of identity theft and fraud, to review your account statements, and to monitor your credit reports for suspicious activity. Under U.S., law you are entitled to one free credit report annually from each of the three major credit reporting bureaus. To order your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also contact the three major credit bureaus directly to request a free copy of your credit report.

---

[1] *WebScan searches for your Social Security Number, up to 5 passport numbers, up to 6 bank account numbers, up to 6 credit/debit card numbers, up to 6 email addresses, and up to 10 medical ID numbers. WebScan searches thousands of Internet sites where consumers' personal information is suspected of being bought and sold, and regularly adds new sites to the list of those it searches. However, the Internet addresses of these suspected Internet trading sites are not published and frequently change, so there is no guarantee that we are able to locate and search every possible Internet site where consumers' personal information is at risk of being traded.*

[2] *The Automatic Fraud Alert feature is made available to consumers by Equifax Information Services LLC and fulfilled on its behalf by Equifax Consumer Services LLC.*

[3] *Locking your Equifax credit report will prevent access to it by certain third parties. Locking your Equifax credit report will not prevent access to your credit report at any other credit reporting agency. Entities that may still have access to your Equifax credit report include companies like Equifax Global Consumer Solutions, which provide you with access to your credit report or credit score, or monitor your credit report as part of a subscription or similar service; companies that provide you with a copy of your credit report or credit score, upon your request; federal, state and local government agencies and courts in certain circumstances; companies using the information in connection with the underwriting of insurance, or for employment, tenant or background screening purposes; companies that have a current account or relationship with you, and collection agencies acting on behalf of those whom you owe; companies that authenticate a consumer's identity for purposes other than granting credit, or for investigating or preventing actual or potential fraud; and companies that wish to make pre-approved offers of credit or insurance to you. To opt out of such pre-approved offers, visit www.optoutprescreen.com*

[4] *The Identity Theft Insurance benefit is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company, under group or blanket policies issued to Equifax, Inc., or its respective affiliates for the benefit of its Members. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.*

Place a Security Freeze

You have the right to place a "security freeze" on your credit report, which will prohibit a consumer reporting agency from releasing information in your credit report without your express authorization. The security 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 security 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 security freeze on your credit report. Should you wish to place a security freeze, please contact the major consumer reporting agencies listed below:

Experian	**TransUnion**	**Equifax**
P.O. Box 9554	P.O. Box 160	P.O. Box 105788
Allen, TX 75013	Woodlyn, PA 19094	Atlanta, GA 30348-5788
1-888-397-3742	1-888-909-8872	1-800-685-1111
www.experian.com/freeze/center html	www.transunion.com/credit-freeze	www.equifax.com/personal/credit-report-services

To request a security freeze, you will need to provide the following information:

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. If you have moved in the past five (5) years, provide the addresses where you have lived over the prior 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, military identification, etc.);
7. 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.

Place a Fraud Alert

As an alternative to a security freeze, you have the right to place an initial or extended "fraud alert" on your 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 the agencies listed below:

Experian	**TransUnion**	**Equifax**
P.O. Box 9554	P.O. Box 2000	P.O. Box 105069
Allen, TX 75013	Chester, PA 19016	Atlanta, GA 30348
1-888-397-3742	1-800-680-7289	1-888-766-0008
www.experian.com/fraud/center.html	www.transunion.com/fraud-victim-resource/place-fraud-alert	www.equifax.com/personal/credit-report-services

Additional Information

You can learn more about identity theft, fraud alerts, security freezes, and the steps you can take to protect yourself, by contacting the consumer reporting agencies, the Federal Trade Commission, or your state Attorney General. The Federal Trade Commission can be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580, www.identitytheft.gov, 1-877-ID-THEFT (1-877-438-4338); 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 and your state Attorney General. This notice has not been delayed by law enforcement.

All US Residents: Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW Washington, DC 20580, www.consumer.gov/idtheft, 1-877-IDTHEFT (438-4338), TTY: 1-866-653-4261. **California Residents:** Visit the California Office of Privacy Protection (www.oag.ca.gov/privacy) for additional information on protection against identity theft. **Iowa residents**: You are advised to report any suspected identity theft to law enforcement or to the Iowa Attorney General. **Kentucky Residents:** Office of the Attorney General of Kentucky, 700 Capitol Avenue, Suite 118 Frankfort, Kentucky 40601**,** www.ag.ky.gov, Telephone: 1-502-696-5300. **Maryland Residents:** Office of the Attorney General of Maryland**,** Consumer Protection Division 200 St. Paul Place, Baltimore, MD 21202**,** www.oag.state.md.us/Consumer, Telephone: 1-888-743-0023. **New Mexico Residents**: You have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the 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 credit 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 a violator. You 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. You can review your rights pursuant to the Fair Credit Reporting Act by visiting 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. **New York Residents:** the Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; https://ag ny.gov/. **North Carolina Residents:** Office of the Attorney General of North Carolina**,** Consumer Protection Division, 9001 Mail Service Center Raleigh, NC 27699-9001, www.ncdoj.gov, Telephone: 1-919-716-6400, 877-566-7226 (toll free within NC). **Oregon Residents:** Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, www.doj.state.or.us/, Telephone: 877-877-9392. **Rhode Island Residents:** Office of the Attorney General, 150 South Main Street, Providence, Rhode Island 02903, www riag ri.gov, Telephone: 401-274-4400. Under Rhode Island law, you have the right to obtain any police report filed in regard to this incident. There are <<RI #>> Rhode Island residents impacted by this incident. **Washington D.C. Residents:** Office of Attorney General for the District of Columbia can be reached at: 400 6th St. NW, Washington, D.C. 20001; 1-202-442-9828; https://oag.dc.gov.