

Appendix

CSX learned on February 9, 2021 that a vulnerability in Accellion FTA, which CSX previously used to transfer large files, may have resulted in unauthorized access to some of its information. CSX had previously taken the Accellion FTA offline on January 5, 2021 as part of its planned transition to a new file transfer application. After learning of the potential unauthorized access to Accellion FTA, CSX contacted law enforcement, and launched an investigation.

Through its investigation, CSX learned that unauthorized parties exploited the vulnerability on the Accellion FTA and gained access to the software platform on December 25, 2020. While in the Accellion FTA, the unauthorized parties may have accessed or acquired some of the files that had been transferred through the platform.

As part of the ongoing investigation, CSX is working diligently to identify the files that may have been subject to unauthorized access as a result of the vulnerability in the Accellion FTA. On February 21, 2021, CSX determined that some of the files that may have been accessed by the unauthorized parties as a result of the vulnerability in the Accellion FTA may have contained information pertaining to some current, former, and retired employees, including their names and Social Security numbers.

Beginning on March 16, 2021, CSX will mail notification letters via United States Postal Service First-Class mail to 10 Maine residents in accordance with Me. Rev. Stat. Tit. 10, §1348. A copy of the notification letter is enclosed. CSX has established a toll-free, incident response call center to answer questions about the incident from notice letter recipients. CSX is also offering these individuals complimentary memberships to TransUnion, which include credit monitoring and fraud protection services.

To help prevent something like this from occurring in the future, CSX has permanently taken the Accellion FTA offline.



Return Mail Processing Center
P.O. 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>>

Dear <<Name 1>>:

CSX Transportation, Inc. is writing to notify you of a data security incident that occurred as a result of a vulnerability in Accellion, Inc.'s File Transfer Appliance software platform ("Accellion FTA") that may have involved some of your information. This notice explains the incident, measures we have taken, and steps you can take in response.

CSX learned on February 9, 2021 that a vulnerability in Accellion FTA, which CSX used to transfer large files, may have resulted in unauthorized access to some of its information. CSX had previously taken the Accellion FTA offline on January 5, 2021 as part of our planned transition to a new file transfer application. After learning of the potential unauthorized access to Accellion FTA, CSX contacted law enforcement, and launched an investigation.

Through our investigation, we learned that unauthorized parties exploited the vulnerability on the Accellion FTA and gained access to the software platform on December 25, 2020. While in the Accellion FTA, the unauthorized parties may have accessed or acquired some of the files that had been transferred through the platform.

As part of the investigation, CSX worked diligently to identify the files that may have been subject to unauthorized access as a result of the vulnerability in the Accellion FTA. On February 21, 2021, CSX determined that some of the files that may have been accessed by the unauthorized parties as a result of the vulnerability in the Accellion FTA may have contained some of your information. This information may have included your name and Social Security number.

We recommend you remain vigilant to the possibility of fraud by reviewing your financial account and payment card statements for any suspicious activity. You should immediately report any suspicious activity to your financial institution. As a precaution, we have secured the services of TransUnion® to offer you a complimentary one-year membership of TransUnion's myTrueIdentity. This product helps detect possible misuse of your information and provides you with identity protection support focused on immediate identification and resolution of identity theft. myTrueIdentity is completely free and enrolling in this program will not hurt your credit score. **For more information on myTrueIdentity, including instructions on how to activate your complimentary one-year membership, as well as some additional steps you can take to protect your information, please see the pages that follow this letter.**

We deeply regret any inconvenience or concern this may cause you. To help prevent something like this from happening in the future, we have taken the Accellion FTA offline permanently. If you have any questions about this incident, please call 855-654-0483, Monday through Friday, between 9:00 a.m. and 9:00 p.m., Eastern Time.

Sincerely,

Diana Sorfleet
Executive Vice President and Chief Administration Officer

Complimentary One-Year *myTrueIdentity* 3B Credit Monitoring Service

As a safeguard, we have arranged for you to enroll, at no cost to you, in an online, three-bureau credit monitoring service (*myTrueIdentity*) for one year provided by TransUnion Interactive, a subsidiary of TransUnion,® one of the three nationwide credit reporting companies.

How to Enroll: You can sign up online or via U.S. mail delivery

- To enroll in this service, go to the *myTrueIdentity* website at www.MyTrueIdentity.com and, in the space referenced as “Enter Activation Code,” enter the 12-letter Activation Code <<Insert Unique 12-letter Activation Code>> and follow the three steps to receive your credit monitoring service online within minutes.
- If you do not have access to the Internet and wish to enroll in a similar offline, paper-based, three-bureau credit monitoring service, via U.S. mail delivery, please call the TransUnion Fraud Response Services toll-free hotline at **1-855-288-5422**. When prompted, enter the six-digit telephone passcode <<Insert static six-digit Telephone Pass Code>> and follow the steps to enroll in the offline credit monitoring service, add an initial fraud alert to your credit file, or to speak to a TransUnion representative if you believe you may be a victim of identity theft.

You can sign up for the online or offline credit monitoring service anytime between now and <<Enrollment Deadline>>. Due to privacy laws, we cannot register you directly. Please note that credit monitoring services might not be available for individuals who do not have a credit file with TransUnion or an address in the United States (or its territories) and a valid Social Security number. Enrolling in this service will not affect your credit score.

ADDITIONAL DETAILS REGARDING YOUR 12-MONTH COMPLIMENTARY CREDIT MONITORING SERVICE:

- Once you are enrolled, you will be able to obtain one year of unlimited access to your TransUnion credit report and credit score.
- The daily three-bureau credit monitoring service will notify you if there are any critical changes to your credit files at TransUnion,® Experian,® and Equifax,® including fraud alerts, new inquiries, new accounts, new public records, late payments, changes of address, and more.
- The service also includes access to an identity restoration program that provides assistance in the event that your identity is compromised and up to \$1,000,000 in identity theft insurance with no deductible. (Policy limitations and exclusions may apply.)

ADDITIONAL STEPS YOU CAN TAKE

We remind you it is always advisable to be vigilant for incidents of fraud or identity theft by reviewing your account statements and free credit reports for any unauthorized activity. You may obtain a copy of your credit report, free of charge, once every 12 months from each of the three nationwide credit reporting companies. To order your annual free credit report, please visit www.annualcreditreport.com or call toll free at 1-877-322-8228. Contact information for the three nationwide credit reporting companies is as follows:

- *Equifax*, PO Box 740241, Atlanta, GA 30374, www.equifax.com, 1-800-685-1111
- *Experian*, PO Box 2002, Allen, TX 75013, www.experian.com, 1-888-397-3742
- *TransUnion*, PO Box 2000, Chester, PA 19016, www.transunion.com, 1-800-916-8800

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 the Federal Trade Commission and/or the Attorney General's office in your state. You can obtain information from these sources about steps an individual can take to avoid identity theft as well as information about fraud alerts and security freezes. You should also contact your local law enforcement authorities and file a police report. Obtain a copy of the police report in case you are asked to provide copies to creditors to correct your records. Contact information for the Federal Trade Commission is as follows:

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

Fraud Alerts: There are two types of general fraud alerts you can place on your credit report to put your creditors on notice that you may be a victim of fraud—an initial alert and an extended alert. You may ask that an initial fraud alert be placed on your credit report if you suspect you have been, or are about to be, a victim of identity theft. An initial fraud alert stays on your credit report for one year. You may have an extended alert placed on your credit report if you have already been a victim of identity theft with the appropriate documentary proof. An extended fraud alert stays on your credit report for seven years.

To place a fraud alert on your credit reports, contact one of the nationwide credit bureaus. A fraud alert is free. The credit bureau you contact must tell the other two, and all three will place an alert on their versions of your report.

For those in the military who want to protect their credit while deployed, an Active Duty Military Fraud Alert lasts for one year and can be renewed for the length of your deployment. The credit bureaus will also take you off their marketing lists for pre-screened credit card offers for two years, unless you ask them not to.

Credit or Security Freezes: You have the right to put a credit freeze, also known as a security freeze, on your credit file, free of charge, which makes it more difficult for identity thieves to open new accounts in your name. That's because most creditors need to see your credit report before they approve a new account. If they can't see your report, they may not extend the credit.

How do I place a freeze on my credit reports? There is no fee to place or lift a security freeze. Unlike a fraud alert, you must separately place a security freeze on your credit file at each credit reporting company. For information and instructions to place a security freeze, contact each of the credit reporting agencies at the addresses below:

- **Experian Security Freeze**, PO Box 9554, Allen, TX 75013, www.experian.com
- **TransUnion Security Freeze**, PO Box 2000, Chester, PA 19016, www.transunion.com
- **Equifax Security Freeze**, PO Box 105788, Atlanta, GA 30348, www.equifax.com

You'll need to supply your name, address, date of birth, Social Security number and other personal information. After receiving your freeze request, each credit bureau will provide you with a unique PIN (personal identification number) or password. Keep the PIN or password in a safe place. You will need it if you choose to lift the freeze.

How do I lift a freeze? A freeze remains in place until you ask the credit bureau to temporarily lift it or remove it altogether. If the request is made online or by phone, a credit bureau must lift a freeze within one hour. If the request is made by mail, then the bureau must lift the freeze no later than three business days after getting your request. If you opt for a temporary lift because you are applying for credit or a job, and you can find out which credit bureau the business will contact for your file, you can save some time by lifting the freeze only at that particular credit bureau. Otherwise, you need to make the request with all three credit bureaus.

CSX Transportation, Inc.'s mailing address is 500 Water Street, J-150, Jacksonville, Florida 32202 and its phone number is 1-800-633-4045.

Additional information for residents of the following states:

Maryland: You may contact and obtain information from your state attorney general at: *Maryland Attorney General's Office*, 200 St. Paul Place, Baltimore, MD 21202, 1-888-743-0023 / 1-410-576-6300, www.oag.state.md.us

New York: You may contact and obtain information from these state agencies: *New York Department of State Division of Consumer Protection*, One Commerce Plaza, 99 Washington Ave., Albany, NY 12231-0001, 518-474-8583 / 1-800-697-1220, <http://www.dos.ny.gov/consumerprotection>; and *New York State Office of the Attorney General*, The Capitol, Albany, NY 12224-0341, 1-800-771-7755, <https://ag.ny.gov>

North Carolina: You may contact and obtain information from your state attorney general at: *North Carolina Attorney General's Office*, 9001 Mail Service Centre, Raleigh, NC 27699, 1-919-716-6000 / 1-877-566-7226, www.ncdoj.gov

Rhode Island: This incident involves 11 Rhode Island residents. Under Rhode Island law, you have the right to file and obtain a copy of a police report. You also have the right to request a security freeze, as described above. You may contact and obtain information from your state attorney general at: *Rhode Island Attorney General's Office*, 150 South Main Street, Providence, RI 02903, 1-401-274-4400, www.riag.ri.gov

West Virginia: You have the right to ask that nationwide consumer reporting agencies place “fraud alerts” in your file to let potential creditors and others know that you may be a victim of identity theft, as described above. You also have a right to place a security freeze on your credit report, as described above.

A Summary of Your Rights Under the Fair Credit Reporting Act: The federal Fair Credit Reporting Act (FCRA) promotes the accuracy, fairness, and privacy of information in the files of consumer reporting agencies. There are many types of consumer reporting agencies, including credit bureaus and specialty agencies (such as agencies that sell information about check writing histories, medical records, and rental history records). Your major rights under the FCRA are summarized below. For more information, including information about additional rights, go to www.consumerfinance.gov/learnmore or write to: Consumer Financial Protection Bureau, 1700 G Street N.W., Washington, DC 20552.

- 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 have a 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.
- You may seek damages from violators.
- Identity theft victims and active duty military personnel have additional rights.