

## Appendix

H.N.S. completed an investigation into a security incident involving potential unauthorized access to data maintained on its systems. Upon discovering the incident, H.N.S. worked to quickly address the incident, launched an investigation, and a forensic investigator was engaged to assist. The investigation determined that some network systems were accessed by an unauthorized person between August 13, 2021 and September 3, 2021. The investigation was unable to precisely conclude what specific information was accessed. H.N.S. conducted a comprehensive review of the file sources that potentially may have been accessed and concluded that access to some personal information possibly occurred. H.N.S. determined on October 26, 2021 that the unauthorized person may have accessed the name, Social Security number, driver's license number, and/or medical information of eight Maine residents.

On November 24, 2021, H.N.S. will begin mailing notification letters to eight Maine residents in accordance with Me. Rev. Stat. Tit. 10, §1348, via United States First-Class mail. A copy of the notification letter is enclosed. H.N.S. is offering residents access to complimentary two-year subscriptions to credit monitoring, fraud consultation, and identity restoration services through Transunion. This service helps detect possible misuse of personal information and provides identity theft protection services focused on immediate identification and resolution of identity theft. A dedicated, toll-free call center has been established for individuals to call with questions regarding the incident.

To help prevent a similar incident from occurring in the future, H.N.S. reset employee passwords, blocked malicious IP addresses identified during the initial investigation, deployed endpoint monitoring protection throughout the network, we are also exploring implementation of other measures to help prevent unauthorized access to our network in the future.



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 <<Name1>>:

H.N.S. Management Company Incorporated (“H.N.S.”), the managing company for CTtransit, understands the importance of protecting information we maintain. We are writing to inform you of a data incident that may have involved some of your information. This notice explains the incident, measures we have taken, and some steps you may consider taking in response.

On September 3, 2021, certain H.N.S. network drives, telephones, and workstations became non-operational. We worked to quickly address the incident, launched an investigation, and a forensic investigator was engaged to assist. While this incident caused disruption, we were able to maintain normal operational capacity. Although a thorough review of the systems determined that some network systems were accessed by an unauthorized person between August 13, 2021 and September 3, 2021, the investigation was unable to precisely conclude what specific information was accessed. Therefore, H.N.S. conducted a comprehensive review of the file sources that potentially may have been accessed and concluded that access to some personal information possibly occurred. H.N.S. determined on October 26, 2021 that the unauthorized person may have accessed some of your personal information, including your Social Security number, driver’s license number, and/or medical information. Although the evidence that your specific personal information was accessed is not definitive, we are providing this notification in an abundance of caution.

We encourage you to remain vigilant by reviewing your credit report, bank, and other financial statements for any unauthorized activity. If you notice any unauthorized activity, you should immediately notify the relevant financial institution or the credit bureau that reported the activity. H.N.S. is also offering you access to complimentary identity theft prevention and credit monitoring services for two years. This service helps detect possible misuse of your personal information and provides you with identity theft protection services focused on immediate identification and resolution of identity theft. This service is completely free to you and enrolling in this program will not hurt your credit score. **For more information about TransUnion’s identity monitoring, including instructions on how to activate your complimentary two-year membership, please visit the below website:**

Visit [www.mytrueidentity.com](http://www.mytrueidentity.com) to activate and take advantage of your identity monitoring services.

*You have until <<Enrollment Deadline>> to activate your identity monitoring services.*

Membership Number: <<Activation Code>>

More information about steps you may consider taking to protect your personal information is attached. We have also established a dedicated call center to help answer any questions you may have about the incident. Please call 855-604-1648, Monday through Friday, between 9:00 a.m. and 9:00 p.m. Eastern Time for the most accurate, up-to-date information about the incident.

We regret any inconvenience or concern this incident may cause you. To help prevent something like this from happening in the future, we reset employee passwords, blocked malicious IP addresses identified during the initial investigation, and deployed endpoint monitoring protection throughout the network. We are also exploring implementation of other measures to help prevent unauthorized access to our network in the future.

Sincerely,

*Cole Pouliot*

Cole R. Pouliot  
General Manager



**Activation Code:**  
**<<Activation Code>>**

### **3-Bureau Credit Monitoring Product Offering: (Online and Offline)**

As a safeguard, we have arranged for you to enroll, at no cost to you, in an online 3-bureau credit monitoring service (*myTrueIdentity*) for 24 months provided by TransUnion Interactive, a subsidiary of TransUnion®, one of the three nationwide credit reporting companies.

To enroll in this service, go directly to the *myTrueIdentity* website at [www.mytrueidentity.com](http://www.mytrueidentity.com) and in the space referenced as “Enter Activation Code”, enter the following unique 12-letter Activation Code <<**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, 3-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 following 6-digit telephone pass code <<**Engagement Number**>> 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.

Once you are enrolled, you will be able to obtain 24 months of unlimited access to your TransUnion credit report and VantageScore® credit score by TransUnion. The daily 3-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, change of address and more. The service also includes the ability to lock and unlock your TransUnion credit report online, access to identity restoration services that provides assistance in the event your identity is compromised to help you restore your identity and up to \$1,000,000 in identity theft insurance with no deductible. (Policy limitations and exclusions may apply.)

You can sign up for the *myTrueIdentity* online 3-Bureau 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 credit files at TransUnion®, Experian® and Equifax®, or an address in the United States (or its territories) and a valid Social Security number, or are under the age of 18. Enrolling in this service will not affect your credit score.

If you have questions about your *myTrueIdentity* online credit monitoring benefits, need help with your online enrollment, or need help accessing your credit report, or passing identity verification, please contact the *myTrueIdentity* Customer Service Team toll-free at: 1-844-787-4607, Monday-Friday: 8am- 9pm, Saturday-Sunday: 8am-5pm Eastern time.

### **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](http://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](http://www.equifax.com), 1-800-685-1111
- *Experian*, PO Box 2002, Allen, TX 75013, [www.experian.com](http://www.experian.com), 1-888-397-3742
- *TransUnion*, PO Box 2000, Chester, PA 19016, [www.transunion.com](http://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](http://www.ftc.gov/idtheft)

## Fraud Alerts and Credit or Security Freezes:

**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](http://www.experian.com)
- **TransUnion Security Freeze**, PO Box 2000, Chester, PA 19016, [www.transunion.com](http://www.transunion.com)
- **Equifax Security Freeze**, PO Box 105788, Atlanta, GA 30348, [www.equifax.com](http://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.

You may contact H.N.S. Management Company Incorporated by mail at 100 Leibert Road, Hartford CT 06141 or by telephone at 1-844-930-1776.

### Additional information for residents of the following states:

**Connecticut:** You may contact and obtain information from your state attorney general at: *Connecticut Attorney General's Office*, 165 Capitol Ave, Hartford, CT 06106, 1-860-808-5318, [www.ct.gov/ag](http://www.ct.gov/ag).

**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](http://www.oag.state.md.us).

**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](http://www.ncdoj.gov).

**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>.

**Rhode Island:** On or about September 3, 2021, H.N.S. Management Company Incorporated discovered that an unauthorized person had accessed certain systems within the H.N.S. network. On October 26, 2021, H.N.S. learned that the personal information of Rhode Island residents was involved in the incident. This incident involves one individual in Rhode Island. 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.gov](http://www.riag.gov).