Quarles & Brady LLP

VIA EMAIL TO CONSUMER@AG.IOWA.GOV

September 21, 2021

Consumer Protection Division
Security Breach Notifications
Office of the Attorney General of Iowa
1305 E. Walnut Street
Des Moines, Iowa 50319-0106

Dear Sir or Madam:

Pursuant to Iowa Code § 715C.1 *et seq.*, this is to notify you about a security incident Navistar, Inc. ("Navistar") recently experienced and the steps we have taken in response.

On May 20, 2021, Navistar learned of a potential security incident affecting its information technology system ("IT System"). Upon learning of the security incident, Navistar launched an investigation and took immediate action in accordance with our cybersecurity response plan. Navistar conducted its investigation with the assistance of leading cybersecurity experts hired to evaluate and address the scope and impact of the incident.

On May 31, 2021, Navistar received a claim that certain data had been extracted from our IT System. In the course of our investigation, we were able to confirm that an unauthorized third party had accessed and taken certain data from our IT System. On August 20, 2021, we discovered that some of the data taken by the unauthorized third party contains personal information about a number of our current and former employees, as well as dependents, which may include participants in the Navistar, Inc. Health Plan or the Navistar, Inc. Retiree Health Benefit and Life Insurance Plan (collectively, the "Plan"), including information of 514 Iowa residents. Based on the information Navistar has at this time, we believe that this incident occurred prior to May 20, 2021.

The unauthorized third party accessed and took the following information from our IT System for the affected individuals: full name, address, date of birth, social security number and information related to participation in the Plan, such as information identifying certain of the individual's providers and prescriptions. Individuals will receive written notification of this incident postmarked no later than September 21, 2021. Copies of the template notices to individuals are attached. Please note that there are multiple template notices based on the recipient and affected data elements.

Although we are not aware at this time that any third party has made any use of the affected individual's information as a result of this incident, out of an abundance of caution, Navistar has arranged for affected individuals to receive free credit monitoring and identity theft protection for two (2) years through Experian.

As a covered entity under the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), Navistar, on behalf of the Plan, is required to notify the Secretary of Health and Human Services ("Secretary") of this incident. The Secretary will be notified in accordance with the timeframe required under HIPAA. We are also notifying the three largest nationwide consumer reporting agencies, including Equifax, Experian and TransUnion, of this incident.

In addition to our existing security measures, Navistar has taken a number of steps to enhance our security protocols and controls, technology, and training. Navistar also continues to assess further options to protect our IT System.

For further information and assistance, please contact me, Navistar's outside legal counsel, at 414-277-3038 or Linda.Emery@quarles.com.

Sincerely,

Linda C. Emery
Attorney at Law

QB\70135870.2

Return Mail Processing
PO Box 999
Suwanee, GA 30024

September 21, 2021

21 1 4063 **********AUTO**ALL FOR AADC 605
SAMPLE A. SAMPLE - L08
APT ABC
123 ANY ST
ANYTOWN, US 12345-6789

Dear Sample A. Sample,

In early July of 2021, you should have received a letter from Navistar via First Class mail notifying you of a security incident involving the personal information of certain current and former U.S. employees. That notice included steps we've taken in response to the incident as well as what can be done to protect against any potential harm. That notice also provided you with additional information on how to access two years of free credit monitoring and identity theft protection, although we are not aware at this time that any third party has made any use of the affected data as a result of this incident.

After sending the July notification, we have continued to investigate the security incident and worked around the clock with the assistance of leading cybersecurity experts to confirm the full scope of the incident. We have now completed our investigation.

As a result of our investigation, we determined that some individuals who should have received the notification in July of 2021 (which stated that their name, address, and social security number were affected) also had certain information related to their participation in the Navistar health plan affected in the same security incident. You are one of those individuals.

As a result, we've enclosed a second letter to notify you that certain additional information related to your participation in the health plan was also affected in this incident. To be clear, this second letter is a result of our work to thoroughly investigate the incident, and **not** the result of a second incident.

Additional details regarding this incident, how you were affected, and how we are working to support you are included in the enclosed letter. Because you already should have received information regarding identity theft protection and the opportunity to enroll in credit monitoring services in your first letter, we are not including that information here. However, in case you have not yet enrolled in the credit monitoring services, we have extended the enrollment period until December 31, 2021 to allow you additional time to take advantage of that offering.

On behalf of Navistar, I want to assure you that we take the security of our systems and data very seriously and regret any concern this situation may have caused. We appreciate your patience as we have worked to address this issue.

Sincerely,

Donna Dorsey
EVP, People & Culture
Navistar, Inc.

Return Mail Processing
PO Box 999
Suwanee, GA 30024

September 21, 2021

SAMPLE A. SAMPLE - L08
APT ABC
123 ANY ST
ANYTOWN, US 12345-6789

Notice of Data Breach

Dear Sample A. Sample,

Navistar, Inc. (”Navistar”) values the privacy of our current and former employees and uses physical, technical, and administrative measures to safeguard your personal information. Our records indicate you are a current or former participant in either the Navistar, Inc. Health Plan or the Navistar, Inc. Retiree Health Benefit and Life Insurance Plan (collectively, the “Plan”). We are writing to you to notify you about a security incident we recently experienced, which has impacted information related to your participation in the Plan. Below are details on the steps we are taking to address the situation.

WHAT HAPPENED?
On May 20, 2021, Navistar learned of a potential security incident affecting its information technology system (“IT System”). Upon learning of the security incident, Navistar launched an investigation and took immediate action in accordance with our cybersecurity response plan. Navistar conducted its investigation with the assistance of leading cybersecurity experts hired to evaluate and address the scope and impact of the incident.

On May 31, 2021, Navistar received a claim that certain data had been extracted from our IT System. In the course of our investigation, we were able to confirm that an unauthorized third party had accessed and taken certain data from our IT System, including data relating to participants in the Plan. On August 20, 2021, we discovered that some of the data taken by the unauthorized third party contains information relating to your participation in the Plan. Based on the information Navistar has at this time, we believe that this incident occurred prior to May 20, 2021.

WHAT INFORMATION WAS INVOLVED?
The data that was taken may have included your full name, address, date of birth, and information related to your participation in the Plan, such as information identifying certain of your providers and prescriptions.

WHAT ARE WE DOING?
We took immediate action to investigate the situation once we learned of the potential incident. Navistar has taken a number of steps to enhance our security protocols and controls, technology, and training. We continue to assess further options to protect our IT System.

WHAT CAN YOU DO?
We recommend that you remain vigilant for incidents of fraud and identity theft. You can review your account statements and monitor free credit reports. Promptly report any fraudulent activity or any suspected incidents of identity theft to your bank or other financial institution holding your accounts, as well as any appropriate authorities, such as your state attorney general and the Federal Trade Commission ("FTC").

The FTC and the Internal Revenue Service ("IRS") both generally recommend that individuals who believe that they may be at risk of taxpayer refund fraud should file their income taxes as early as possible. The IRS further suggests that a taxpayer who is an actual or potential victim of identity theft complete and submit to the IRS Form 14039 (Identity Theft Affidavit). Form 14039 is available at https://www.irs.gov/pub/irs-pdf/f14039.pdf. Upon receipt of this affidavit, the IRS may flag your taxpayer account to identify questionable activity.

On behalf of Navistar, I want to apologize for any concern this situation may have caused. We appreciate the patience all our current and former employees have demonstrated as we have worked to address this issue.

FOR MORE INFORMATION.
For more information and assistance, please contact (855) 387-4540 Monday through Friday 8 am – 10 pm CST, Saturday and Sunday 10 am – 7 pm CST (excluding major U.S. holidays). Please be prepared to provide engagement number **B018458**.

Sincerely,

Donna Dorsey
EVP, People & Culture
Navistar, Inc.

Attachment 1

ADDITIONAL INFORMATION ON CREDIT MONITORING & IDENTITY THEFT

Individuals are advised to remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring free credit reports and to promptly report any fraudulent activity or any suspected incidents of identity theft to proper law enforcement authorities, including the police and your state's attorney general as well as the Federal Trade Commission.

The following are some resources:

Federal Trade Commission ("FTC")
www.ftc.gov/idtheft
1-877-ID-THEFT (1-877-438-4338)

Federal Trade Commission
600 Pennsylvania Avenue, NW
Washington, DC 20580

Take Charge: Fighting Back Against Identity Theft
This is a comprehensive guide from the FTC to help you guard against and deal with identity theft https://www.identitytheft.gov/.

Credit Bureaus
You may obtain a free copy of your credit report from each of the three major credit reporting agencies once every 12 months by visiting www.annualcreditreport.com, calling 1-877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. You can print a copy of the request form at www.annualcreditreport.com/manualRequestForm.action

Alternatively, you may elect to purchase a copy of your credit report by contacting one of the three national credit reporting agencies. Contact information for the three national credit reporting agencies for the purpose of requesting a copy of your credit report or for general inquiries is as follows:

Equifax	**Experian**	**TransUnion**
1-800-685-1111 www.equifax.com/CreditReport Assistance P.O. Box 740241 Atlanta, GA 30374	1-888-397-3742 www.experian.com P.O. Box 4500 Allen, TX 75013	1-800-888-4213 www.transunion.com/fraud P.O. Box 1000 Chester, PA 19016

You can obtain additional information from the FTC and the nationwide credit reporting agencies about placing a security freeze on your credit files and fraud alerts. A security freeze is a free tool that lets you restrict access to your credit report, which in turn makes it more difficult for identity thieves to open new accounts in your name. To place a security freeze on your credit files, contact each of the nationwide credit bureaus using the contact information listed above. You will need to supply your name, address, date of birth, social security number, and other personal information. You may want to consider placing a fraud alert on

your credit report. An initial fraud alert is free and will stay on your credit file for at least 90 days. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any accounts in your name. To place a fraud alert on your credit report, contact any of the three credit reporting agencies using the contact information listed above.

FOR MARYLAND RESIDENTS

You can obtain information about preventing identity theft from the FTC or:

Maryland Attorney General:

Visit the Maryland Office of the Attorney General, Identity Theft Unit at:
http://www.marylandattorneygeneral.gov/Pages/IdentityTheft/default.aspx
or call 410-576-6491
or write to this address:
Maryland Office of the Attorney General
Identity Theft Unit
16th Floor
200 St. Paul Place
Baltimore, MD 21202

FOR NORTH CAROLINA RESIDENTS

You can obtain information about preventing identity theft from the FTC or:

North Carolina Attorney General:

Visit the North Carolina Office of the Attorney General at:
www.ncdoj.gov or call 1-877-566-7226
or write to this address:
Attorney General's Office
9001 Mail Service Center
Raleigh, NC 27699-9001

FOR RHODE ISLAND RESIDENTS

Eight (8) individuals in Rhode Island were affected by this incident. You may obtain information about preventing identity theft from:

Rhode Island Attorney General:

Visit the Rhode Island Office of the Attorney General at:
www.riag.ri.gov, or call (401) 274-4400
or write to this address:
Rhode Island Office of the Attorney General
Consumer Protection Unit
150 South Main Street
Providence, RI 02903

FOR WASHINGTON D.C. RESIDENTS

You can obtain information about preventing identity theft from the FTC or the following:

Washington D.C. Attorney General:

Visit the Washington Office of the Attorney General (OAG) at:
https://oag.dc.gov/, or call the OAG's Office of Consumer Protection at 202-442-9828
or write to this address:
Office of the Attorney General
400 6th Street, NW
Washington, DC 20001

Return Mail Processing
PO Box 999
Suwanee, GA 30024

September 21, 2021

244 3 55383 **********AUTO**ALL FOR AADC 890
SAMPLE A. SAMPLE - L07
APT ABC
123 ANY ST
ANYTOWN, US 12345-6789

Notice of Data Breach

Dear Sample A. Sample,

Navistar, Inc. ("Navistar") is writing to you because our records indicate that you are or were a dependent of a current or former Navistar employee.

Navistar values the privacy of our current and former employees and their dependents, and uses physical, technical, and administrative measures to safeguard your personal information. We are writing to notify you about a security incident we recently experienced, which has impacted your personal information. Below are details on the steps we are taking to address the situation, as well as what we are doing to support affected individuals.

WHAT HAPPENED?
On May 20, 2021, Navistar learned of a potential security incident affecting its information technology system ("IT System"). Upon learning of the security incident, Navistar launched an investigation and took immediate action in accordance with our cybersecurity response plan. Navistar conducted its investigation with the assistance of leading cybersecurity experts hired to evaluate and address the scope and impact of the incident.

On May 31, 2021, Navistar received a claim that certain data had been extracted from our IT System. In the course of our investigation, we were able to confirm that an unauthorized third party had accessed and taken certain data from our IT System. This included data containing personal information about dependents of current and former employees. On August 20, 2021, we discovered that some of the data taken by the unauthorized third party contains your personal information. Based on the information Navistar has at this time, we believe that this incident occurred prior to May 20, 2021.

WHAT INFORMATION WAS INVOLVED?
The data that was taken may have included your full name, address, date of birth, and social security number.

WHAT ARE WE DOING?
We took immediate action to investigate the situation once we learned of the potential incident. Navistar has taken a number of steps to enhance our security protocols and controls, technology, and training. We continue to assess further options to protect our IT System.

Although we are not aware at this time that any third party has made any use of data as a result of this incident, out of an abundance of caution, we are providing you with access to free credit monitoring and identity theft protection for two years through Experian**.** Enrollment instructions and details for these free services are further outlined on Attachment 1.

WHAT CAN YOU DO?

In addition to using the credit monitoring and identity theft protection described above, we recommend that you remain vigilant for incidents of fraud and identity theft. You can review your account statements and monitor free credit reports. Promptly report any fraudulent activity or any suspected incidents of identity theft to your bank or other financial institution holding your accounts, as well as any appropriate authorities, such as your state attorney general and the Federal Trade Commission ("FTC").

The FTC and the Internal Revenue Service ("IRS") both generally recommend that individuals who believe that they may be at risk of taxpayer refund fraud should file their income taxes as early as possible. The IRS further suggests that a taxpayer who is an actual or potential victim of identity theft complete and submit to the IRS Form 14039 (Identity Theft Affidavit). Form 14039 is available at https://www.irs.gov/pub/irs-pdf/f14039.pdf. Upon receipt of this affidavit, the IRS may flag your taxpayer account to identify questionable activity.

On behalf of Navistar, I want to apologize for any concern this situation may have caused. We appreciate your patience as we have worked to address this issue.

FOR MORE INFORMATION.

For more information and assistance, please contact (855) 387-4540 Monday through Friday 8 am – 10 pm CST, Saturday and Sunday 10 am – 7 pm CST (excluding major U.S. holidays).

Sincerely,

Donna Dorsey
EVP, People & Culture
Navistar, Inc.

Attachment 1

CREDIT MONITORING & IDENTITY THEFT PROTECTION SERVICES

Credit Monitoring Services Offer:

We have retained Experian to assist us in providing you access to Experian IdentityWorks[SM], its credit-monitoring service. Using Experian IdentityWorks, you can monitor your personal information. Experian IdentityWorks provides you with superior identity detection and resolution of identity theft.

How to Enroll in Experian IdentityWorks and Activate Your Membership:

You may enroll in and activate your complimentary two (2) year membership in Experian IdentityWorks by taking the following steps:

- **Visit the Experian IdentityWorks website** to enroll at: https://www.experianidworks.com/3bcredit
- **Activation Code.** Provide your **activation code**: **ABCDEFGHI**
- **Enroll by**: **December 31, 2021** (Your code will not work after this date.)
- **No Credit Card Required.** You do not need a credit card to enroll in Experian IdentityWorks.

What if I Have Questions or Need Help Enrolling:

If you have questions about Experian IdentityWorks or would like an alternative to enrolling online, please contact Experian's customer care team at (855) 387-4540 **by December 31, 2021.** Please be prepared to provide engagement number **B018456** as proof of eligibility.

Can You Provide Me More Details Regarding My Membership?:

Once you enroll in Experian IdentityWorks, you can contact Experian **immediately** regarding any fraud issues, and have access to the following features once you enroll:

- **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, Equifax and Transunion files 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[TM]**: 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.

What If I Believe That My Personal Information Has Been Used Without My Consent?

Even if you do not enroll in Experian IdentityWorks, you are still automatically eligible to use Experian's Identity Restoration Services. Please note that this offer is available to you for two years from the date of this letter and does not require any action on your part at this time.

If you believe there was a fraudulent use of your personal information 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, an Experian Identity Restoration agent is available to work with you to investigate and resolve each incident of fraud that occurred (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).

The Terms and Conditions for this offer are located at www.ExperianIDWorks.com/restoration. You will also find self-help tips and information about identity protection at this site.

What Else Can I Do to Protect My Personal Information?

There are additional actions you can consider taking to reduce the chances of identity theft or fraud on your account(s). Please refer to www.ExperianIDWorks.com/restoration for this information.

ADDITIONAL INFORMATION ON CREDIT MONITORING & IDENTITY THEFT

Individuals are advised to remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring free credit reports and to promptly report any fraudulent activity or any suspected incidents of identity theft to proper law enforcement authorities, including the police and your state's attorney general as well as the Federal Trade Commission.

The following are some resources:

Federal Trade Commission ("FTC")
www.ftc.gov/idtheft
1-877-ID-THEFT (1-877-438-4338)

Federal Trade Commission
600 Pennsylvania Avenue, NW
Washington, DC 20580

Take Charge: Fighting Back Against Identity Theft
This is a comprehensive guide from the FTC to help you guard against and deal with identity theft https://www.identitytheft.gov/.

Credit Bureaus
You may obtain a free copy of your credit report from each of the three major credit reporting agencies once every 12 months by visiting www.annualcreditreport.com, calling 1-877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. You can print a copy of the request form at www.annualcreditreport.com/manualRequestForm.action

Alternatively, you may elect to purchase a copy of your credit report by contacting one of the three national credit reporting agencies. Contact information for the three national credit reporting agencies for the purpose of requesting a copy of your credit report or for general inquiries is as follows:

Equifax	**Experian**	**TransUnion**
1-800-685-1111 www.equifax.com/CreditReport Assistance P.O. Box 740241 Atlanta, GA 30374	1-888-397-3742 www.experian.com P.O. Box 4500 Allen, TX 75013	1-800-888-4213 www.transunion.com/fraud P.O. Box 1000 Chester, PA 19016

You can obtain additional information from the FTC and the nationwide credit reporting agencies about placing a security freeze on your credit files and fraud alerts. A security freeze is a free tool that lets you restrict access to your credit report, which in turn makes it more difficult for identity thieves to open new accounts in your name. To place a security freeze on your credit files, contact each of the nationwide credit bureaus using the contact information listed above. You will need to supply your name, address, date of birth, social security number, and other personal information. You may want to consider placing a fraud alert on your credit report. An initial fraud alert is free and will stay on your credit file for at least 90 days. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any accounts in your name. To place a fraud alert on your credit report, contact any of the three credit reporting agencies using the contact information listed above.

FOR MARYLAND RESIDENTS

You can obtain information about preventing identity theft from the FTC or:

Maryland Attorney General:

Visit the Maryland Office of the Attorney General, Identity Theft Unit at:
http://www.marylandattorneygeneral.gov/Pages/IdentityTheft/default.aspx
or call 410-576-6491
or write to this address:
Maryland Office of the Attorney General
Identity Theft Unit
16th Floor
200 St. Paul Place
Baltimore, MD 21202

FOR NORTH CAROLINA RESIDENTS

You can obtain information about preventing identity theft from the FTC or:

North Carolina Attorney General:

Visit the North Carolina Office of the Attorney General at:
www.ncdoj.gov or call 1-877-566-7226
or write to this address:
Attorney General's Office
9001 Mail Service Center
Raleigh, NC 27699-9001

FOR RHODE ISLAND RESIDENTS

Eight (8) individuals in Rhode Island were affected by this incident. You may obtain information about preventing identity theft from:

Rhode Island Attorney General:

Visit the Rhode Island Office of the Attorney General at:
www.riag.ri.gov, or call (401) 274-4400
or write to this address:
Rhode Island Office of the Attorney General
Consumer Protection Unit
150 South Main Street
Providence, RI 02903

FOR WASHINGTON D.C. RESIDENTS

You can obtain information about preventing identity theft from the FTC or the following:

Washington D.C. Attorney General:

Visit the Washington Office of the Attorney General (OAG) at:
https://oag.dc.gov/, or call the OAG's Office of Consumer Protection at 202-442-9828
or write to this address:
Office of the Attorney General
400 6th Street, NW
Washington, DC 20001

Return Mail Processing
PO Box 999
Suwanee, GA 30024

September 21, 2021

247 2 55866 **********AUTO**ALL FOR AADC 956
SAMPLE A. SAMPLE - L06
APT ABC
123 ANY ST
ANYTOWN, US 12345-6789

Notice of Data Breach

Dear Sample A. Sample,

Navistar, Inc. ("Navistar") is writing to you because our records indicate that you are a current or former participant in either the Navistar, Inc. Health Plan or the Navistar, Inc. Retiree Health Benefit and Life Insurance Plan (collectively, the "Plan").

Navistar values the privacy of the current and former participants in our health and welfare benefit plans and uses physical, technical, and administrative measures to safeguard your personal information. We are writing to notify you about a security incident we recently experienced, which has impacted your personal information. Below are details on the steps we are taking to address the situation, as well as what we are doing to support affected individuals.

WHAT HAPPENED?
On May 20, 2021, Navistar learned of a potential security incident affecting its information technology system ("IT System"). Upon learning of the security incident, Navistar launched an investigation and took immediate action in accordance with our cybersecurity response plan. Navistar conducted its investigation with the assistance of leading cybersecurity experts hired to evaluate and address the scope and impact of the incident.

On May 31, 2021, Navistar received a claim that certain data had been extracted from our IT System. In the course of our investigation, we were able to confirm that an unauthorized third party had accessed and taken certain data from our IT System, including data containing personal information about certain participants in the Plan. On August 20, 2021, we discovered that some of the data taken by the unauthorized third party contains your personal information. Based on the information Navistar has at this time, we believe that this incident occurred prior to May 20, 2021.

WHAT INFORMATION WAS INVOLVED?
The data that was taken may have included your full name, address, date of birth, social security number, and information related to your participation in the Plan, such as information identifying certain of your providers and prescriptions.

WHAT ARE WE DOING?
We took immediate action to investigate the situation once we learned of the potential incident. Navistar has

taken a number of steps to enhance our security protocols and controls, technology, and training. We continue to assess further options to protect our IT System.

Although we are not aware at this time that any third party has made any use of data as a result of this incident, out of an abundance of caution, we are providing you with access to free credit monitoring and identity theft protection for two years through Experian**.** Enrollment instructions and details for these free services are further outlined on Attachment 1.

WHAT CAN YOU DO?
In addition to using the credit monitoring and identity theft protection described above, we recommend that you remain vigilant for incidents of fraud and identity theft. You can review your account statements and monitor free credit reports. Promptly report any fraudulent activity or any suspected incidents of identity theft to your bank or other financial institution holding your accounts, as well as any appropriate authorities, such as your state attorney general and the Federal Trade Commission ("FTC").

The FTC and the Internal Revenue Service ("IRS") both generally recommend that individuals who believe that they may be at risk of taxpayer refund fraud should file their income taxes as early as possible. The IRS further suggests that a taxpayer who is an actual or potential victim of identity theft complete and submit to the IRS Form 14039 (Identity Theft Affidavit). Form 14039 is available at https://www.irs.gov/pub/irs-pdf/f14039.pdf. Upon receipt of this affidavit, the IRS may flag your taxpayer account to identify questionable activity.

On behalf of Navistar, I want to apologize for any concern this situation may have caused. We appreciate your patience as we have worked to address this issue.

FOR MORE INFORMATION.
For more information and assistance, please contact (855) 387-4540 Monday through Friday 8 am – 10 pm CST, Saturday and Sunday 10 am – 7 pm CST (excluding major U.S. holidays).

Sincerely,

Donna Dorsey
EVP, People & Culture
Navistar, Inc.

Attachment 1

CREDIT MONITORING & IDENTITY THEFT PROTECTION SERVICES

Credit Monitoring Services Offer:

We have retained Experian to assist us in providing you access to Experian IdentityWorks[SM], its credit-monitoring service. Using Experian IdentityWorks, you can monitor your personal information. Experian IdentityWorks provides you with superior identity detection and resolution of identity theft.

How to Enroll in Experian IdentityWorks and Activate Your Membership:

You may enroll in and activate your complimentary two (2) year membership in Experian IdentityWorks by taking the following steps:

- **Visit the Experian IdentityWorks website** to enroll at: https://www.experianidworks.com/3bcredit
- **Activation Code.** Provide your **activation code**: **ABCDEFGHI**
- **Enroll by**: **December 31, 2021** (Your code will not work after this date.)
- **No Credit Card Required.** You do not need a credit card to enroll in Experian IdentityWorks.

What if I Have Questions or Need Help Enrolling:

If you have questions about Experian IdentityWorks or would like an alternative to enrolling online, please contact Experian's customer care team at (855) 387-4540 **by December 31, 2021.** Please be prepared to provide engagement number **B018456** as proof of eligibility.

Can You Provide Me More Details Regarding My Membership?:

Once you enroll in Experian IdentityWorks, you can contact Experian **immediately** regarding any fraud issues, and have access to the following features once you enroll:

- **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, Equifax and Transunion files 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[TM]**: 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.

What If I Believe That My Personal Information Has Been Used Without My Consent?

Even if you do not enroll in Experian IdentityWorks, you are still automatically eligible to use Experian's Identity Restoration Services. Please note that this offer is available to you for two years from the date of this letter and does not require any action on your part at this time.

If you believe there was a fraudulent use of your personal information 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, an Experian Identity Restoration agent is available to work with you to investigate and resolve each incident of fraud that occurred (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).

The Terms and Conditions for this offer are located at www.ExperianIDWorks.com/restoration. You will also find self-help tips and information about identity protection at this site.

What Else Can I Do to Protect My Personal Information?

There are additional actions you can consider taking to reduce the chances of identity theft or fraud on your account(s). Please refer to www.ExperianIDWorks.com/restoration for this information.

ADDITIONAL INFORMATION ON CREDIT MONITORING & IDENTITY THEFT

Individuals are advised to remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring free credit reports and to promptly report any fraudulent activity or any suspected incidents of identity theft to proper law enforcement authorities, including the police and your state's attorney general as well as the Federal Trade Commission.

The following are some resources:

Federal Trade Commission ("FTC")
www.ftc.gov/idtheft
1-877-ID-THEFT (1-877-438-4338)

Federal Trade Commission
600 Pennsylvania Avenue, NW
Washington, DC 20580

Take Charge: Fighting Back Against Identity Theft
This is a comprehensive guide from the FTC to help you guard against and deal with identity theft https://www.identitytheft.gov/.

Credit Bureaus
You may obtain a free copy of your credit report from each of the three major credit reporting agencies once every 12 months by visiting www.annualcreditreport.com, calling 1-877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. You can print a copy of the request form at www.annualcreditreport.com/manualRequestForm.action

Alternatively, you may elect to purchase a copy of your credit report by contacting one of the three national credit reporting agencies. Contact information for the three national credit reporting agencies for the purpose of requesting a copy of your credit report or for general inquiries is as follows:

Equifax	**Experian**	**TransUnion**
1-800-685-1111 www.equifax.com/CreditReport Assistance P.O. Box 740241 Atlanta, GA 30374	1-888-397-3742 www.experian.com P.O. Box 4500 Allen, TX 75013	1-800-888-4213 www.transunion.com/fraud P.O. Box 1000 Chester, PA 19016

You can obtain additional information from the FTC and the nationwide credit reporting agencies about placing a security freeze on your credit files and fraud alerts. A security freeze is a free tool that lets you restrict access to your credit report, which in turn makes it more difficult for identity thieves to open new accounts in your name. To place a security freeze on your credit files, contact each of the nationwide credit bureaus using the contact information listed above. You will need to supply your name, address, date of birth, social security number, and other personal information. You may want to consider placing a fraud alert on your credit report. An initial fraud alert is free and will stay on your credit file for at least 90 days. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any accounts in your name. To place a fraud alert on your credit report, contact any of the three credit reporting agencies using the contact information listed above.

FOR MARYLAND RESIDENTS

You can obtain information about preventing identity theft from the FTC or:

Maryland Attorney General:

Visit the Maryland Office of the Attorney General, Identity Theft Unit at:
http://www.marylandattorneygeneral.gov/Pages/IdentityTheft/default.aspx
or call 410-576-6491
or write to this address:
Maryland Office of the Attorney General
Identity Theft Unit
16th Floor
200 St. Paul Place
Baltimore, MD 21202

FOR NORTH CAROLINA RESIDENTS

You can obtain information about preventing identity theft from the FTC or:

North Carolina Attorney General:

Visit the North Carolina Office of the Attorney General at:
www.ncdoj.gov or call 1-877-566-7226
or write to this address:
Attorney General's Office
9001 Mail Service Center
Raleigh, NC 27699-9001

FOR RHODE ISLAND RESIDENTS

Eight (8) individuals in Rhode Island were affected by this incident. You may obtain information about preventing identity theft from:

Rhode Island Attorney General:

Visit the Rhode Island Office of the Attorney General at:
www.riag.ri.gov, or call (401) 274-4400
or write to this address:
Rhode Island Office of the Attorney General
Consumer Protection Unit
150 South Main Street
Providence, RI 02903

FOR WASHINGTON D.C. RESIDENTS

You can obtain information about preventing identity theft from the FTC or the following:

Washington D.C. Attorney General:

Visit the Washington Office of the Attorney General (OAG) at:
https://oag.dc.gov/, or call the OAG's Office of Consumer Protection at 202-442-9828
or write to this address:
Office of the Attorney General
400 6th Street, NW
Washington, DC 20001

Return Mail Processing
PO Box 999
Suwanee, GA 30024

September 21, 2021

247 2 55916 **********AUTO**ALL FOR AADC 956
SAMPLE A. SAMPLE - L05
APT ABC
123 ANY ST
ANYTOWN, US 12345-6789

Notice of Data Breach

Dear Sample A. Sample,

Navistar, Inc. ("Navistar") is writing to you because our records indicate that you are a current or former participant in either the Navistar, Inc. Health Plan or the Navistar, Inc. Retiree Health Benefit and Life Insurance Plan (collectively, the "Plan").

Navistar values the privacy of the current and former participants in our health and welfare benefit plans and uses physical, technical, and administrative measures to safeguard your personal information. We are writing to notify you about a security incident we recently experienced, which has impacted information related to your participation in the Plan. Below are details on the steps we are taking to address the situation, as well as what we are doing to support affected individuals.

WHAT HAPPENED?
On May 20, 2021, Navistar learned of a potential security incident affecting its information technology system ("IT System"). Upon learning of the security incident, Navistar launched an investigation and took immediate action in accordance with our cybersecurity response plan. Navistar conducted its investigation with the assistance of leading cybersecurity experts hired to evaluate and address the scope and impact of the incident.

On May 31, 2021, Navistar received a claim that certain data had been extracted from our IT System. In the course of our investigation, we were able to confirm that an unauthorized third party had accessed and taken certain data from our IT System, including data relating to participants in the Plan. On August 20, 2021, we discovered that some of the data taken by the unauthorized third party contains information relating to your participation in the Plan. Based on the information Navistar has at this time, we believe that this incident occurred prior to May 20, 2021.

WHAT INFORMATION WAS INVOLVED?
The data that was taken may have included your full name, address, date of birth, and information related to your participation in the Plan, such as information identifying certain of your providers and prescriptions.

WHAT ARE WE DOING?
We took immediate action to investigate the situation once we learned of the potential incident. Navistar has taken a number of steps to enhance our security protocols and controls, technology, and training. We continue to assess further options to protect our IT System.

Although we are not aware at this time that any third party has made any use of data as a result of this incident, out of an abundance of caution, we are providing you with access to free credit monitoring and identity theft protection for two years through Experian**.** Enrollment instructions and details for these free services are further outlined on Attachment 1.

WHAT CAN YOU DO?

In addition to using the credit monitoring and identity theft protection described above, we recommend that you remain vigilant for incidents of fraud and identity theft. You can review your account statements and monitor free credit reports. Promptly report any fraudulent activity or any suspected incidents of identity theft to your bank or other financial institution holding your accounts, as well as any appropriate authorities, such as your state attorney general and the Federal Trade Commission ("FTC").

The FTC and the Internal Revenue Service ("IRS") both generally recommend that individuals who believe that they may be at risk of taxpayer refund fraud should file their income taxes as early as possible. The IRS further suggests that a taxpayer who is an actual or potential victim of identity theft complete and submit to the IRS Form 14039 (Identity Theft Affidavit). Form 14039 is available at https://www.irs.gov/pub/irs-pdf/f14039.pdf. Upon receipt of this affidavit, the IRS may flag your taxpayer account to identify questionable activity.

On behalf of Navistar, I want to apologize for any concern this situation may have caused. We appreciate your patience as we have worked to address this issue.

FOR MORE INFORMATION.

For more information and assistance, please contact (855) 387-4540 Monday through Friday 8 am – 10 pm CST, Saturday and Sunday 10 am – 7 pm CST (excluding major U.S. holidays).

Sincerely,

Donna Dorsey
EVP, People & Culture
Navistar, Inc.

Attachment 1

CREDIT MONITORING & IDENTITY THEFT PROTECTION SERVICES

Credit Monitoring Services Offer:

We have retained Experian to assist us in providing you access to Experian IdentityWorks[SM], its credit-monitoring service. Using Experian IdentityWorks, you can monitor your personal information. Experian IdentityWorks provides you with superior identity detection and resolution of identity theft.

How to Enroll in Experian IdentityWorks and Activate Your Membership:

You may enroll in and activate your complimentary two (2) year membership in Experian IdentityWorks by taking the following steps:

- **Visit the Experian IdentityWorks website** to enroll at: https://www.experianidworks.com/3bcredit
- **Activation Code.** Provide your **activation code**: **ABCDEFGHI**
- **Enroll by**: **December 31, 2021** (Your code will not work after this date.)
- **No Credit Card Required.** You do not need a credit card to enroll in Experian IdentityWorks.

What if I Have Questions or Need Help Enrolling:

If you have questions about Experian IdentityWorks or would like an alternative to enrolling online, please contact Experian's customer care team at (855) 387-4540 **by December 31, 2021.** Please be prepared to provide engagement number **B018456** as proof of eligibility.

Can You Provide Me More Details Regarding My Membership?:

Once you enroll in Experian IdentityWorks, you can contact Experian **immediately** regarding any fraud issues, and have access to the following features once you enroll:

- **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, Equifax and Transunion files 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[TM]**: 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.

What If I Believe That My Personal Information Has Been Used Without My Consent?

Even if you do not enroll in Experian IdentityWorks, you are still automatically eligible to use Experian's Identity Restoration Services. Please note that this offer is available to you for two years from the date of this letter and does not require any action on your part at this time.

If you believe there was a fraudulent use of your personal information 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, an Experian Identity Restoration agent is available to work with you to investigate and resolve each incident of fraud that occurred (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).

The Terms and Conditions for this offer are located at www.ExperianIDWorks.com/restoration. You will also find self-help tips and information about identity protection at this site.

What Else Can I Do to Protect My Personal Information?

There are additional actions you can consider taking to reduce the chances of identity theft or fraud on your account(s). Please refer to www.ExperianIDWorks.com/restoration for this information.

ADDITIONAL INFORMATION ON CREDIT MONITORING & IDENTITY THEFT

Individuals are advised to remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring free credit reports and to promptly report any fraudulent activity or any suspected incidents of identity theft to proper law enforcement authorities, including the police and your state's attorney general as well as the Federal Trade Commission.

The following are some resources:

Federal Trade Commission ("FTC")
www.ftc.gov/idtheft
1-877-ID-THEFT (1-877-438-4338)

Federal Trade Commission
600 Pennsylvania Avenue, NW
Washington, DC 20580

Take Charge: Fighting Back Against Identity Theft
This is a comprehensive guide from the FTC to help you guard against and deal with identity theft https://www.identitytheft.gov/.

Credit Bureaus
You may obtain a free copy of your credit report from each of the three major credit reporting agencies once every 12 months by visiting www.annualcreditreport.com, calling 1-877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. You can print a copy of the request form at www.annualcreditreport.com/manualRequestForm.action

Alternatively, you may elect to purchase a copy of your credit report by contacting one of the three national credit reporting agencies. Contact information for the three national credit reporting agencies for the purpose of requesting a copy of your credit report or for general inquiries is as follows:

Equifax	**Experian**	**TransUnion**
1-800-685-1111 www.equifax.com/CreditReport Assistance P.O. Box 740241 Atlanta, GA 30374	1-888-397-3742 www.experian.com P.O. Box 4500 Allen, TX 75013	1-800-888-4213 www.transunion.com/fraud P.O. Box 1000 Chester, PA 19016

You can obtain additional information from the FTC and the nationwide credit reporting agencies about placing a security freeze on your credit files and fraud alerts. A security freeze is a free tool that lets you restrict access to your credit report, which in turn makes it more difficult for identity thieves to open new accounts in your name. To place a security freeze on your credit files, contact each of the nationwide credit bureaus using the contact information listed above. You will need to supply your name, address, date of birth, social security number, and other personal information. You may want to consider placing a fraud alert on your credit report. An initial fraud alert is free and will stay on your credit file for at least 90 days. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any accounts in your name. To place a fraud alert on your credit report, contact any of the three credit reporting agencies using the contact information listed above.

FOR MARYLAND RESIDENTS

You can obtain information about preventing identity theft from the FTC or:

Maryland Attorney General:

Visit the Maryland Office of the Attorney General, Identity Theft Unit at:
http://www.marylandattorneygeneral.gov/Pages/IdentityTheft/default.aspx
or call 410-576-6491
or write to this address:
Maryland Office of the Attorney General
Identity Theft Unit
16th Floor
200 St. Paul Place
Baltimore, MD 21202

FOR NORTH CAROLINA RESIDENTS

You can obtain information about preventing identity theft from the FTC or:

North Carolina Attorney General:

Visit the North Carolina Office of the Attorney General at:
www.ncdoj.gov or call 1-877-566-7226
or write to this address:
Attorney General's Office
9001 Mail Service Center
Raleigh, NC 27699-9001

FOR RHODE ISLAND RESIDENTS

Eight (8) individuals in Rhode Island were affected by this incident. You may obtain information about preventing identity theft from:

Rhode Island Attorney General:

Visit the Rhode Island Office of the Attorney General at:
www.riag.ri.gov, or call (401) 274-4400
or write to this address:
Rhode Island Office of the Attorney General
Consumer Protection Unit
150 South Main Street
Providence, RI 02903

FOR WASHINGTON D.C. RESIDENTS

You can obtain information about preventing identity theft from the FTC or the following:

Washington D.C. Attorney General:

Visit the Washington Office of the Attorney General (OAG) at:
https://oag.dc.gov/, or call the OAG's Office of Consumer Protection at 202-442-9828
or write to this address:
Office of the Attorney General
400 6th Street, NW
Washington, DC 20001

Return Mail Processing
PO Box 999
Suwanee, GA 30024

September 21, 2021

247 2 55915 **********AUTO**ALL FOR AADC 956
SAMPLE A. SAMPLE - L04
APT ABC
123 ANY ST
ANYTOWN, US 12345-6789

Notice of Data Breach

Dear Sample A. Sample,

Navistar, Inc. ("Navistar") values the privacy of our current and former employees and uses physical, technical, and administrative measures to safeguard your personal information. We are writing to notify you about a security incident we recently experienced, which has impacted your personal information. Below are details on the steps we are taking to address the situation, as well as what we are doing to support affected individuals.

WHAT HAPPENED?
On May 20, 2021, Navistar learned of a potential security incident affecting its information technology system ("IT System"). Upon learning of the security incident, Navistar launched an investigation and took immediate action in accordance with our cybersecurity response plan. Navistar conducted its investigation with the assistance of leading cybersecurity experts hired to evaluate and address the scope and impact of the incident.

On May 31, 2021, Navistar received a claim that certain data had been extracted from our IT System. In the course of our investigation, we were able to confirm that an unauthorized third party had accessed and taken certain data from our IT System, including data containing personal information about some of our current and former employees. On August 20, 2021, we discovered that some of the data taken by the unauthorized third party contains your personal information. Based on the information Navistar has at this time, we believe that this incident occurred prior to May 20, 2021.

WHAT INFORMATION WAS INVOLVED?
The data that was taken may have included your full name, address, date of birth, and social security number.

WHAT ARE WE DOING?
We took immediate action to investigate the situation once we learned of the potential incident. Navistar has taken a number of steps to enhance our security protocols and controls, technology, and training. We continue to assess further options to protect our IT System.

Although we are not aware at this time that any third party has made any use of current or former employee data as a result of this incident, out of an abundance of caution, we are providing you with access to free credit monitoring and identity theft protection for two years through Experian**.** Enrollment instructions and details for these free services are further outlined on Attachment 1.

WHAT CAN YOU DO?
In addition to using the credit monitoring and identity theft protection described above, we recommend that you remain vigilant for incidents of fraud and identity theft. You can review your account statements and monitor free credit reports. Promptly report any fraudulent activity or any suspected incidents of identity theft to your bank or other financial institution holding your accounts, as well as any appropriate authorities, such as your state attorney general and the Federal Trade Commission ("FTC").

The FTC and the Internal Revenue Service ("IRS") both generally recommend that individuals who believe that they may be at risk of taxpayer refund fraud should file their income taxes as early as possible. The IRS further suggests that a taxpayer who is an actual or potential victim of identity theft complete and submit to the IRS Form 14039 (Identity Theft Affidavit). Form 14039 is available at https://www.irs.gov/pub/irs-pdf/f14039.pdf. Upon receipt of this affidavit, the IRS may flag your taxpayer account to identify questionable activity.

On behalf of Navistar, I want to apologize for any concern this situation may have caused. We appreciate the patience all our current and former employees have demonstrated as we have worked to address this issue.

FOR MORE INFORMATION.
For more information and assistance, please contact (855) 387-4540 Monday through Friday 8 am – 10 pm CST, Saturday and Sunday 10 am – 7 pm CST (excluding major U.S. holidays).

Sincerely,

Donna Dorsey
EVP, People & Culture
Navistar, Inc.

Attachment 1

CREDIT MONITORING & IDENTITY THEFT PROTECTION SERVICES

Credit Monitoring Services Offer:

We have retained Experian to assist us in providing you access to Experian IdentityWorks[SM], its credit-monitoring service. Using Experian IdentityWorks, you can monitor your personal information. Experian IdentityWorks provides you with superior identity detection and resolution of identity theft.

How to Enroll in Experian IdentityWorks and Activate Your Membership:

You may enroll in and activate your complimentary two (2) year membership in Experian IdentityWorks by taking the following steps:

- **Visit the Experian IdentityWorks website** to enroll at: https://www.experianidworks.com/3bcredit
- **Activation Code.** Provide your **activation code**: **ABCDEFGHI**
- **Enroll by**: **December 31, 2021** (Your code will not work after this date.)
- **No Credit Card Required.** You do not need a credit card to enroll in Experian IdentityWorks.

What if I Have Questions or Need Help Enrolling:

If you have questions about Experian IdentityWorks or would like an alternative to enrolling online, please contact Experian's customer care team at (855) 387-4540 **by December 31, 2021.** Please be prepared to provide engagement number **B018456** as proof of eligibility.

Can You Provide Me More Details Regarding My Membership?:

Once you enroll in Experian IdentityWorks, you can contact Experian **immediately** regarding any fraud issues, and have access to the following features once you enroll:

- **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, Equifax and Transunion files 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[TM]**: 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.

What If I Believe That My Personal Information Has Been Used Without My Consent?

Even if you do not enroll in Experian IdentityWorks, you are still automatically eligible to use Experian's Identity Restoration Services. Please note that this offer is available to you for two years from the date of this letter and does not require any action on your part at this time.

If you believe there was a fraudulent use of your personal information 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, an Experian Identity Restoration agent is available to work with you to investigate and resolve each incident of fraud that occurred (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).

The Terms and Conditions for this offer are located at www.ExperianIDWorks.com/restoration. You will also find self-help tips and information about identity protection at this site.

What Else Can I Do to Protect My Personal Information?

There are additional actions you can consider taking to reduce the chances of identity theft or fraud on your account(s). Please refer to www.ExperianIDWorks.com/restoration for this information.

ADDITIONAL INFORMATION ON CREDIT MONITORING & IDENTITY THEFT

Individuals are advised to remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring free credit reports and to promptly report any fraudulent activity or any suspected incidents of identity theft to proper law enforcement authorities, including the police and your state's attorney general as well as the Federal Trade Commission.

The following are some resources:

Federal Trade Commission ("FTC")
www.ftc.gov/idtheft
1-877-ID-THEFT (1-877-438-4338)

Federal Trade Commission
600 Pennsylvania Avenue, NW
Washington, DC 20580

Take Charge: Fighting Back Against Identity Theft
This is a comprehensive guide from the FTC to help you guard against and deal with identity theft https://www.identitytheft.gov/.

Credit Bureaus
You may obtain a free copy of your credit report from each of the three major credit reporting agencies once every 12 months by visiting www.annualcreditreport.com, calling 1-877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. You can print a copy of the request form at www.annualcreditreport.com/manualRequestForm.action

Alternatively, you may elect to purchase a copy of your credit report by contacting one of the three national credit reporting agencies. Contact information for the three national credit reporting agencies for the purpose of requesting a copy of your credit report or for general inquiries is as follows:

Equifax	**Experian**	**TransUnion**
1-800-685-1111 www.equifax.com/CreditReport Assistance P.O. Box 740241 Atlanta, GA 30374	1-888-397-3742 www.experian.com P.O. Box 4500 Allen, TX 75013	1-800-888-4213 www.transunion.com/fraud P.O. Box 1000 Chester, PA 19016

You can obtain additional information from the FTC and the nationwide credit reporting agencies about placing a security freeze on your credit files and fraud alerts. A security freeze is a free tool that lets you restrict access to your credit report, which in turn makes it more difficult for identity thieves to open new accounts in your name. To place a security freeze on your credit files, contact each of the nationwide credit bureaus using the contact information listed above. You will need to supply your name, address, date of birth, social security number, and other personal information. You may want to consider placing a fraud alert on your credit report. An initial fraud alert is free and will stay on your credit file for at least 90 days. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any accounts in your name. To place a fraud alert on your credit report, contact any of the three credit reporting agencies using the contact information listed above.

FOR MARYLAND RESIDENTS

You can obtain information about preventing identity theft from the FTC or:

Maryland Attorney General:

Visit the Maryland Office of the Attorney General, Identity Theft Unit at:
http://www.marylandattorneygeneral.gov/Pages/IdentityTheft/default.aspx
or call 410-576-6491
or write to this address:
Maryland Office of the Attorney General
Identity Theft Unit
16th Floor
200 St. Paul Place
Baltimore, MD 21202

FOR NORTH CAROLINA RESIDENTS

You can obtain information about preventing identity theft from the FTC or:

North Carolina Attorney General:

Visit the North Carolina Office of the Attorney General at:
www.ncdoj.gov or call 1-877-566-7226
or write to this address:
Attorney General's Office
9001 Mail Service Center
Raleigh, NC 27699-9001

FOR RHODE ISLAND RESIDENTS

Eight (8) individuals in Rhode Island were affected by this incident. You may obtain information about preventing identity theft from:

Rhode Island Attorney General:

Visit the Rhode Island Office of the Attorney General at:
www.riag.ri.gov, or call (401) 274-4400
or write to this address:
Rhode Island Office of the Attorney General
Consumer Protection Unit
150 South Main Street
Providence, RI 02903

FOR WASHINGTON D.C. RESIDENTS

You can obtain information about preventing identity theft from the FTC or the following:

Washington D.C. Attorney General:

Visit the Washington Office of the Attorney General (OAG) at:
https://oag.dc.gov/, or call the OAG's Office of Consumer Protection at 202-442-9828
or write to this address:
Office of the Attorney General
400 6th Street, NW
Washington, DC 20001

Return Mail Processing
PO Box 999
Suwanee, GA 30024

September 21, 2021

247 2 55917 **********AUTO**ALL FOR AADC 956
SAMPLE A. SAMPLE - L03
APT ABC
123 ANY ST
ANYTOWN, US 12345-6789

Notice of Data Breach

Dear Sample A. Sample,

Navistar, Inc. ("Navistar") values the privacy of our current and former employees and uses physical, technical, and administrative measures to safeguard your personal information. Our records indicate you are also a current or former participant in either the Navistar, Inc. Health Plan or the Navistar, Inc. Retiree Health Benefit and Life Insurance Plan (collectively, the "Plan"). We are writing to you to notify you about a security incident we recently experienced, which has impacted your personal information. Below are details on the steps we are taking to address the situation, as well as what we are doing to support affected individuals.

WHAT HAPPENED?
On May 20, 2021, Navistar learned of a potential security incident affecting its information technology system ("IT System"). Upon learning of the security incident, Navistar launched an investigation and took immediate action in accordance with our cybersecurity response plan. Navistar conducted its investigation with the assistance of leading cybersecurity experts hired to evaluate and address the scope and impact of the incident.

On May 31, 2021, Navistar received a claim that certain data had been extracted from our IT System. In the course of our investigation, we were able to confirm that an unauthorized third party had accessed and taken certain data from our IT System, including data containing personal information about some of our current and former employees that are or were participants in the Plan. On August 20, 2021, we discovered that some of the data taken by the unauthorized third party contains your personal information. Based on the information Navistar has at this time, we believe that this incident occurred prior to May 20, 2021.

WHAT INFORMATION WAS INVOLVED?
The data that was taken may have included your full name, address, date of birth, social security number, and information related to your participation in the Plan, such as information identifying certain of your providers and prescriptions.

WHAT ARE WE DOING?
We took immediate action to investigate the situation once we learned of the potential incident. Navistar has taken a number of steps to enhance our security protocols and controls, technology, and training. We continue to assess further options to protect our IT System.

Although we are not aware at this time that any third party has made any use of current or former employee data as a result of this incident, out of an abundance of caution, we are providing you with access to free credit monitoring and identity theft protection for two years through Experian**.** Enrollment instructions and details for these free services are further outlined on Attachment 1.

WHAT CAN YOU DO?

In addition to using the credit monitoring and identity theft protection described above, we recommend that you remain vigilant for incidents of fraud and identity theft. You can review your account statements and monitor free credit reports. Promptly report any fraudulent activity or any suspected incidents of identity theft to your bank or other financial institution holding your accounts, as well as any appropriate authorities, such as your state attorney general and the Federal Trade Commission ("FTC").

The FTC and the Internal Revenue Service ("IRS") both generally recommend that individuals who believe that they may be at risk of taxpayer refund fraud should file their income taxes as early as possible. The IRS further suggests that a taxpayer who is an actual or potential victim of identity theft complete and submit to the IRS Form 14039 (Identity Theft Affidavit). Form 14039 is available at https://www.irs.gov/pub/irs-pdf/f14039.pdf. Upon receipt of this affidavit, the IRS may flag your taxpayer account to identify questionable activity.

On behalf of Navistar, I want to apologize for any concern this situation may have caused. We appreciate the patience all our current and former employees have demonstrated as we have worked to address this issue.

FOR MORE INFORMATION.

For more information and assistance, please contact (855) 387-4540 Monday through Friday 8 am – 10 pm CST, Saturday and Sunday 10 am – 7 pm CST (excluding major U.S. holidays).

Sincerely,

Donna Dorsey
EVP, People & Culture
Navistar, Inc.

Attachment 1

CREDIT MONITORING & IDENTITY THEFT PROTECTION SERVICES

Credit Monitoring Services Offer:

We have retained Experian to assist us in providing you access to Experian IdentityWorks[SM], its credit-monitoring service. Using Experian IdentityWorks, you can monitor your personal information. Experian IdentityWorks provides you with superior identity detection and resolution of identity theft.

How to Enroll in Experian IdentityWorks and Activate Your Membership:

You may enroll in and activate your complimentary two (2) year membership in Experian IdentityWorks by taking the following steps:

- **Visit the Experian IdentityWorks website** to enroll at: https://www.experianidworks.com/3bcredit
- **Activation Code.** Provide your **activation code**: **ABCDEFGHI**
- **Enroll by**: **December 31, 2021** (Your code will not work after this date.)
- **No Credit Card Required.** You do not need a credit card to enroll in Experian IdentityWorks.

What if I Have Questions or Need Help Enrolling:

If you have questions about Experian IdentityWorks or would like an alternative to enrolling online, please contact Experian's customer care team at (855) 387-4540 **by December 31, 2021.** Please be prepared to provide engagement number **B018456** as proof of eligibility.

Can You Provide Me More Details Regarding My Membership?:

Once you enroll in Experian IdentityWorks, you can contact Experian **immediately** regarding any fraud issues, and have access to the following features once you enroll:

- **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, Equifax and Transunion files 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[TM]**: 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.

What If I Believe That My Personal Information Has Been Used Without My Consent?

Even if you do not enroll in Experian IdentityWorks, you are still automatically eligible to use Experian's Identity Restoration Services. Please note that this offer is available to you for two years from the date of this letter and does not require any action on your part at this time.

If you believe there was a fraudulent use of your personal information 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, an Experian Identity Restoration agent is available to work with you to investigate and resolve each incident of fraud that occurred (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).

The Terms and Conditions for this offer are located at www.ExperianIDWorks.com/restoration. You will also find self-help tips and information about identity protection at this site.

What Else Can I Do to Protect My Personal Information?

There are additional actions you can consider taking to reduce the chances of identity theft or fraud on your account(s). Please refer to www.ExperianIDWorks.com/restoration for this information.

ADDITIONAL INFORMATION ON CREDIT MONITORING & IDENTITY THEFT

Individuals are advised to remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring free credit reports and to promptly report any fraudulent activity or any suspected incidents of identity theft to proper law enforcement authorities, including the police and your state's attorney general as well as the Federal Trade Commission.

The following are some resources:

Federal Trade Commission ("FTC")
www.ftc.gov/idtheft
1-877-ID-THEFT (1-877-438-4338)

Federal Trade Commission
600 Pennsylvania Avenue, NW
Washington, DC 20580

Take Charge: Fighting Back Against Identity Theft
This is a comprehensive guide from the FTC to help you guard against and deal with identity theft https://www.identitytheft.gov/.

Credit Bureaus
You may obtain a free copy of your credit report from each of the three major credit reporting agencies once every 12 months by visiting www.annualcreditreport.com, calling 1-877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. You can print a copy of the request form at www.annualcreditreport.com/manualRequestForm.action

Alternatively, you may elect to purchase a copy of your credit report by contacting one of the three national credit reporting agencies. Contact information for the three national credit reporting agencies for the purpose of requesting a copy of your credit report or for general inquiries is as follows:

Equifax	**Experian**	**TransUnion**
1-800-685-1111 www.equifax.com/CreditReport Assistance P.O. Box 740241 Atlanta, GA 30374	1-888-397-3742 www.experian.com P.O. Box 4500 Allen, TX 75013	1-800-888-4213 www.transunion.com/fraud P.O. Box 1000 Chester, PA 19016

You can obtain additional information from the FTC and the nationwide credit reporting agencies about placing a security freeze on your credit files and fraud alerts. A security freeze is a free tool that lets you restrict access to your credit report, which in turn makes it more difficult for identity thieves to open new accounts in your name. To place a security freeze on your credit files, contact each of the nationwide credit bureaus using the contact information listed above. You will need to supply your name, address, date of birth, social security number, and other personal information. You may want to consider placing a fraud alert on your credit report. An initial fraud alert is free and will stay on your credit file for at least 90 days. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any accounts in your name. To place a fraud alert on your credit report, contact any of the three credit reporting agencies using the contact information listed above.

FOR MARYLAND RESIDENTS

You can obtain information about preventing identity theft from the FTC or:

Maryland Attorney General:

Visit the Maryland Office of the Attorney General, Identity Theft Unit at:
http://www.marylandattorneygeneral.gov/Pages/IdentityTheft/default.aspx
or call 410-576-6491
or write to this address:
Maryland Office of the Attorney General
Identity Theft Unit
16th Floor
200 St. Paul Place
Baltimore, MD 21202

FOR NORTH CAROLINA RESIDENTS

You can obtain information about preventing identity theft from the FTC or:

North Carolina Attorney General:

Visit the North Carolina Office of the Attorney General at:
www.ncdoj.gov or call 1-877-566-7226
or write to this address:
Attorney General's Office
9001 Mail Service Center
Raleigh, NC 27699-9001

FOR RHODE ISLAND RESIDENTS

Eight (8) individuals in Rhode Island were affected by this incident. You may obtain information about preventing identity theft from:

Rhode Island Attorney General:

Visit the Rhode Island Office of the Attorney General at:
www.riag.ri.gov, or call (401) 274-4400
or write to this address:
Rhode Island Office of the Attorney General
Consumer Protection Unit
150 South Main Street
Providence, RI 02903

FOR WASHINGTON D.C. RESIDENTS

You can obtain information about preventing identity theft from the FTC or the following:

Washington D.C. Attorney General:

Visit the Washington Office of the Attorney General (OAG) at:
https://oag.dc.gov/, or call the OAG's Office of Consumer Protection at 202-442-9828
or write to this address:
Office of the Attorney General
400 6th Street, NW
Washington, DC 20001

Return Mail Processing
PO Box 999
Suwanee, GA 30024

September 21, 2021

245 3 55588 **********AUTO**ALL FOR AADC 970
SAMPLE A. SAMPLE - L02
APT ABC
123 ANY ST
ANYTOWN, US 12345-6789

Notice of Data Breach

Dear Sample A. Sample,

Navistar, Inc. (”Navistar”) values the privacy of our current and former employees and uses physical, technical, and administrative measures to safeguard your personal information. Our records indicate you are also a current or former participant in either the Navistar, Inc. Health Plan or the Navistar, Inc. Retiree Health Benefit and Life Insurance Plan (collectively, the “Plan”). We are writing to you to notify you about a security incident we recently experienced, which has impacted information related to your participation in the Plan. Below are details on the steps we are taking to address the situation, as well as what we are doing to support affected individuals.

WHAT HAPPENED?
On May 20, 2021, Navistar learned of a potential security incident affecting its information technology system (“IT System”). Upon learning of the security incident, Navistar launched an investigation and took immediate action in accordance with our cybersecurity response plan. Navistar conducted its investigation with the assistance of leading cybersecurity experts hired to evaluate and address the scope and impact of the incident.

On May 31, 2021, Navistar received a claim that certain data had been extracted from our IT System. In the course of our investigation, we were able to confirm that an unauthorized third party had accessed and taken certain data from our IT System, including data relating to participants in the Plan. On August 20, 2021, we discovered that some of the data taken by the unauthorized third party contains information relating to your participation on the Plan. Based on the information Navistar has at this time, we believe that this incident occurred prior to May 20, 2021.

WHAT INFORMATION WAS INVOLVED?
The data that was taken may have included your full name, address, date of birth, and information related to your participation in the Plan, such as information identifying certain of your providers and prescriptions.

WHAT ARE WE DOING?
We took immediate action to investigate the situation once we learned of the potential incident. Navistar has taken a number of steps to enhance our security protocols and controls, technology, and training. We continue to assess further options to protect our IT System.

Although we are not aware at this time that any third party has made any use of current or former employee data as a result of this incident, out of an abundance of caution, we are providing you with access to free credit monitoring and identity theft protection for two years through Experian**.** Enrollment instructions and details for these free services are further outlined on Attachment 1.

WHAT CAN YOU DO?

In addition to using the credit monitoring and identity theft protection described above, we recommend that you remain vigilant for incidents of fraud and identity theft. You can review your account statements and monitor free credit reports. Promptly report any fraudulent activity or any suspected incidents of identity theft to your bank or other financial institution holding your accounts, as well as any appropriate authorities, such as your state attorney general and the Federal Trade Commission ("FTC").

The FTC and the Internal Revenue Service ("IRS") both generally recommend that individuals who believe that they may be at risk of taxpayer refund fraud should file their income taxes as early as possible. The IRS further suggests that a taxpayer who is an actual or potential victim of identity theft complete and submit to the IRS Form 14039 (Identity Theft Affidavit). Form 14039 is available at https://www.irs.gov/pub/irs-pdf/f14039.pdf. Upon receipt of this affidavit, the IRS may flag your taxpayer account to identify questionable activity.

On behalf of Navistar, I want to apologize for any concern this situation may have caused. We appreciate the patience all our current and former employees have demonstrated as we have worked to address this issue.

FOR MORE INFORMATION.

For more information and assistance, please contact (855) 387-4540 Monday through Friday 8 am – 10 pm CST, Saturday and Sunday 10 am – 7 pm CST (excluding major U.S. holidays).

Sincerely,

Donna Dorsey
EVP, People & Culture
Navistar, Inc.

Attachment 1

CREDIT MONITORING & IDENTITY THEFT PROTECTION SERVICES

Credit Monitoring Services Offer:

We have retained Experian to assist us in providing you access to Experian IdentityWorks[SM], its credit-monitoring service. Using Experian IdentityWorks, you can monitor your personal information. Experian IdentityWorks provides you with superior identity detection and resolution of identity theft.

How to Enroll in Experian IdentityWorks and Activate Your Membership:

You may enroll in and activate your complimentary two (2) year membership in Experian IdentityWorks by taking the following steps:

- **Visit the Experian IdentityWorks website** to enroll at: https://www.experianidworks.com/3bcredit
- **Activation Code.** Provide your **activation code**: **ABCDEFGHI**
- **Enroll by**: **December 31, 2021** (Your code will not work after this date.)
- **No Credit Card Required.** You do not need a credit card to enroll in Experian IdentityWorks.

What if I Have Questions or Need Help Enrolling:

If you have questions about Experian IdentityWorks or would like an alternative to enrolling online, please contact Experian's customer care team at (855) 387-4540 **by December 31, 2021.** Please be prepared to provide engagement number **B018456** as proof of eligibility.

Can You Provide Me More Details Regarding My Membership?:

Once you enroll in Experian IdentityWorks, you can contact Experian **immediately** regarding any fraud issues, and have access to the following features once you enroll:

- **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, Equifax and Transunion files 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[TM]**: 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.

What If I Believe That My Personal Information Has Been Used Without My Consent?

Even if you do not enroll in Experian IdentityWorks, you are still automatically eligible to use Experian's Identity Restoration Services. Please note that this offer is available to you for two years from the date of this letter and does not require any action on your part at this time.

If you believe there was a fraudulent use of your personal information 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, an Experian Identity Restoration agent is available to work with you to investigate and resolve each incident of fraud that occurred (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).

The Terms and Conditions for this offer are located at www.ExperianIDWorks.com/restoration. You will also find self-help tips and information about identity protection at this site.

What Else Can I Do to Protect My Personal Information?

There are additional actions you can consider taking to reduce the chances of identity theft or fraud on your account(s). Please refer to www.ExperianIDWorks.com/restoration for this information.

ADDITIONAL INFORMATION ON CREDIT MONITORING & IDENTITY THEFT

Individuals are advised to remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring free credit reports and to promptly report any fraudulent activity or any suspected incidents of identity theft to proper law enforcement authorities, including the police and your state's attorney general as well as the Federal Trade Commission.

The following are some resources:

Federal Trade Commission ("FTC")
www.ftc.gov/idtheft
1-877-ID-THEFT (1-877-438-4338)

Federal Trade Commission
600 Pennsylvania Avenue, NW
Washington, DC 20580

Take Charge: Fighting Back Against Identity Theft
This is a comprehensive guide from the FTC to help you guard against and deal with identity theft https://www.identitytheft.gov/.

Credit Bureaus
You may obtain a free copy of your credit report from each of the three major credit reporting agencies once every 12 months by visiting www.annualcreditreport.com, calling 1-877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. You can print a copy of the request form at www.annualcreditreport.com/manualRequestForm.action

Alternatively, you may elect to purchase a copy of your credit report by contacting one of the three national credit reporting agencies. Contact information for the three national credit reporting agencies for the purpose of requesting a copy of your credit report or for general inquiries is as follows:

Equifax	**Experian**	**TransUnion**
1-800-685-1111 www.equifax.com/CreditReport Assistance P.O. Box 740241 Atlanta, GA 30374	1-888-397-3742 www.experian.com P.O. Box 4500 Allen, TX 75013	1-800-888-4213 www.transunion.com/fraud P.O. Box 1000 Chester, PA 19016

You can obtain additional information from the FTC and the nationwide credit reporting agencies about placing a security freeze on your credit files and fraud alerts. A security freeze is a free tool that lets you restrict access to your credit report, which in turn makes it more difficult for identity thieves to open new accounts in your name. To place a security freeze on your credit files, contact each of the nationwide credit bureaus using the contact information listed above. You will need to supply your name, address, date of birth, social security number, and other personal information. You may want to consider placing a fraud alert on your credit report. An initial fraud alert is free and will stay on your credit file for at least 90 days. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any accounts in your name. To place a fraud alert on your credit report, contact any of the three credit reporting agencies using the contact information listed above.

FOR MARYLAND RESIDENTS

You can obtain information about preventing identity theft from the FTC or:

Maryland Attorney General:

Visit the Maryland Office of the Attorney General, Identity Theft Unit at:

http://www.marylandattorneygeneral.gov/Pages/IdentityTheft/default.aspx

or call 410-576-6491

or write to this address:

Maryland Office of the Attorney General
Identity Theft Unit
16th Floor
200 St. Paul Place
Baltimore, MD 21202

FOR NORTH CAROLINA RESIDENTS

You can obtain information about preventing identity theft from the FTC or:

North Carolina Attorney General:

Visit the North Carolina Office of the Attorney General at:

www.ncdoj.gov or call 1-877-566-7226

or write to this address:

Attorney General's Office
9001 Mail Service Center
Raleigh, NC 27699-9001

FOR RHODE ISLAND RESIDENTS

Eight (8) individuals in Rhode Island were affected by this incident. You may obtain information about preventing identity theft from:

Rhode Island Attorney General:

Visit the Rhode Island Office of the Attorney General at:

www.riag.ri.gov, or call (401) 274-4400

or write to this address:

Rhode Island Office of the Attorney General
Consumer Protection Unit
150 South Main Street
Providence, RI 02903

FOR WASHINGTON D.C. RESIDENTS

You can obtain information about preventing identity theft from the FTC or the following:

Washington D.C. Attorney General:

Visit the Washington Office of the Attorney General (OAG) at:

https://oag.dc.gov/, or call the OAG's Office of Consumer Protection at 202-442-9828

or write to this address:

Office of the Attorney General
400 6th Street, NW
Washington, DC 20001