TOYOTA
TOYOTA INDUSTRIES GROUP
Processing Center ● P.O. BOX 141578 ● Austin, TX 78714

Toyota Industries North America, Inc.
3030 Barker Drive, Columbus, IN 47201

00008
R82690M

JOHN Q. SAMPLE
1234 MAIN STREET
ANYTOWN US 12345-6789

September 28, 2018

VIA First Class Mail

Please read this entire letter

Dear John Sample:

Toyota Industries North America, Inc. ("TINA") is writing to notify you about a data security incident we recently experienced and the steps we are taking to address the incident. TINA provides shared services to your employer and/or health and welfare benefit plan. Although we are not aware at this time of any actual harm to any individuals as a result of this situation, the incident may have potentially exposed your personal information to third parties. We recognize the concern this may cause, and we want to inform you of the steps we have taken and provide you information on steps you can take to further protect your personal information.

More information is below, but if you have any immediate questions, you can contact our call center at 1-855-725-5778 (toll free) from 8 a.m. to 8 p.m. Central Time Monday through Saturday.

WHAT HAPPENED?
On August 30, 2018, we discovered that an unauthorized third party may have accessed our email system through a process called "phishing," where a third-party bad actor was disguised in order to appear as though it was a known source requesting authorized access to information. This email phishing attack occurred on or around August 15, 2018, and may have allowed the unauthorized third party to access a small number of email accounts. After becoming aware of this incident, we took prompt action to contain the threat and engaged information security experts to secure our system and help ensure that the unauthorized third party no longer had access. We also obtained legal assistance and began a review of the incident, which included contacting technology experts to determine what, if any, information may have been accessed.

At this point, we are not aware of any misuse of your information, and to date, we have no evidence that this data was removed from our system.

WHAT INFORMATION WAS INVOLVED?
The information that the unauthorized party may have accessed may have included: full name, home address, date of birth, phone number, financial account information, social security number, photograph of social security card, driver's license number, photograph of driver's license, email address, photograph of birth certificate, photograph of passport, treatment information, prescription information, diagnoses, health plan beneficiary number, and portal username, password and security question(s).

WHAT ARE WE DOING?
We took action to investigate the incident once it was discovered, and promptly engaged legal and information security experts to assist in the investigation. In addition to security measures already in place, TINA is also reviewing additional options to enhance our training, technology and security practices to reduce the risk of a similar issue occurring in the future, including requiring multifactor authentication, and implementing real-time security monitoring enhancements.

We are alerting our self-funded health plans' third party administrator, and notifying the three largest nationwide consumer reporting agencies, Equifax, Experian, and TransUnion, of the incident.

Again, although we are not aware at this time of any actual harm to any individuals as a result of this situation, TINA has arranged for you to receive complimentary credit monitoring and identity theft protection for one year (if you desire to obtain such protection) through AllClear ID, as further outlined on Attachment 1.

WHAT YOU CAN DO.
Besides using the credit monitoring and identity theft protection described above, we recommend that you remain vigilant for incidents of fraud and identity theft by reviewing your account statements and monitoring free credit reports to detect errors resulting from the security incident. Promptly report any fraudulent activity or any suspected incidents of identity theft to your financial institutions or company with which the account is maintained, as well as applicable authorities, including local law enforcement, your state attorney general and the Federal Trade Commission ("FTC").

Additionally, 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, in addition to the above-described steps, file their income taxes as soon 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.

We recommend that you be alert for "phishing" scams going forward. These scams take various forms and may appear as if they are from TINA or another familiar person or company. TINA will not email or call you regarding this incident to ask for your personal information. We also suggest that you are cautious when opening emails, clicking on links, responding to requests for entering network credentials, or giving personal information over the phone to anyone claiming to be from TINA.

FOR MORE INFORMATION.
TINA has a strong commitment to protect your personal information, and we apologize for any concern this situation has caused. For further information and assistance, please contact our call center at 1-855-725-5778 (toll free) from 8 a.m. to 8 p.m. Central Time Monday through Saturday.

Sincerely,

Jennifer M. Triplett

Jennifer M. Triplett
Senior Counsel, Toyota Industries North America, Inc.

ATTACHMENT 1
OTHER IMPORTANT INFORMATION

CREDIT MONITORING & IDENTITY THEFT PROTECTION SERVICES

As an added precaution, we have arranged to have AllClear ID protect your identity for 12 months at no cost to you. The following identity protection services start on the date of this notice and you can use them at any time during the next 12 months.

AllClear Identity Repair: This service is automatically available to you with no enrollment required. If a problem arises, simply call 1-855-725-5778 and a dedicated investigator will help recover financial losses, restore your credit and make sure your identity is returned to its proper condition.

AllClear Fraud Alerts with Credit Monitoring: This service offers the ability to set, renew, and remove 90-day fraud alerts on your credit file to help protect you from credit fraud. In addition, it provides credit monitoring services, a once annual credit score and credit report, and a $1 million identity theft insurance policy. To enroll in this service, you will need to provide your personal information to AllClear ID. You may sign up online at enroll.allclearid.com or by phone by calling 1-855-725-5778 using the following redemption code: Redemption Code.

Please note: Following enrollment, additional steps are required by you in order to activate your phone alerts and fraud alerts, and to pull your credit score and credit file. Additional steps may also be required in order to activate your monitoring options.

ADDITIONAL INFORMATION ON CREDIT MONITORING & IDENTITY THEFT

You can obtain information from these sources about preventing identify theft:

Federal Trade Commission
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.

You may also decide to purchase a copy of your credit report by contacting one of the three national credit reporting agencies listed here:

Equifax	**Experian**	**TransUnion**
1-800-685-1111	1-888-397-3742	1-800-888-4213
www.equifax.com/CreditReport Assistance	www.experian.com	www.transunion.com/fraud
P.O. Box 740241	P.O. Box 2002	P.O. Box 1000
Atlanta, GA 30374	Allen, TX 75013	Chester, PA 19016

You can obtain additional information from the FTC and national credit reporting agencies about placing a security freeze on your credit files and fraud alerts. 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.

ADDENDUM

FOR NORTH CAROLINA RESIDENTS

You can obtain information from these sources about preventing identify 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 MARYLAND RESIDENTS

You can obtain information from these sources about preventing identify 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 1-410-576-6491
or write to this address:
Maryland Office of the Attorney General
Identity Theft Unit
16th Floor
200 St. Paul Place
Baltimore, MD 21202

FOR NEW MEXICO RESIDENTS

The federal Fair Credit Reporting Act (FCRA) promotes the accuracy, fairness, and privacy of information in the files of consumer reporting agencies. There are many types of consumer reporting agencies, including credit bureaus and specialty agencies (such as agencies that sell information about check writing histories, medical records, and rental history records). A summary of your major rights under the FCRA is available at: https://www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf. For more information, including information about additional rights, go to www.ftc.gov/credit or write to: Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.