TOYOTA

Allison H. Cohen
Managing Counsel

Toyota Motor Sales, U.S.A., Inc.
19001 South Western Avenue
Torrance, CA 90501
310 468-7737
310 381-4430 Fax

November 21, 2008

Attorney General's Office
Attn: Mary Gould, Legal Assistant
Consumer Protection Bureau
33 Capitol Street
Concord, NH 03301

Dear Ms. Gould:

I am writing on behalf of Toyota Motor Sales, USA, Inc. ("Toyota") to inform you of a security breach affecting 23 New Hampshire residents.

On November 6, 2008, Express Scripts, Toyota's pharmacy benefits manager, informed Toyota that an unknown person or persons had made an extortionate threat to disclose Express Script's members' personal information, including the name, Social Security number and date of birth to identity thieves unless Express Scripts paid a ransom. At that time, Express Scripts advised Toyota that it did not believe personal information about Toyota members was involved.

Early the following week, Toyota received a similar threat directly, apparently from the same extortionist. The extortionists identified 188 current and former Toyota associates' name, social security number and date of birth held by Express Scripts. Additionally, they suggested that they possessed similar information for "most" other current and former Toyota associates and their covered dependents. The FBI is investigating the incident.

Toyota has worked diligently to determine the identity of the Company's employees who are affected by this criminal incident. Toyota sent informal e-mail notice to affected employees on November 14, 2008 and will mail the formal notice of security breach on November 20 and 21, 2008. A copy of the letter that will be sent to affected New Hampshire residents is attached.

If you have any questions concerning the matters discussed above, please do not hesitate to call me at 310-468-7737.

Very truly yours,

Allison Hoff Cohen
Managing Counsel

November 20, 2008

Re: Call to Action: Important Notice of Security Breach

Dear Associate and Covered Dependent:

This letter is intended for all Toyota associates who are eligible under the Express Scripts, Inc. Pharmacy Benefits Program offered in connection with the Toyota Motor Sales, USA, Inc. sponsored Aetna medical insurance plans. The information in this letter applies to all Toyota associates and eligible dependents currently covered or who previously had coverage anytime between 2006 and the present date.

Toyota recognizes the importance of safeguarding associates' personal information. To that end, Toyota has taken steps to safeguard that information. Even the most rigorous safeguards, however, cannot guarantee protection against criminal conduct.

Express Scripts, Toyota's pharmacy benefits manager, was victimized by such conduct. More specifically, Express Scripts recently informed Toyota that it had received a letter from an unknown person or persons demanding money from the company. The person(s) threatened to expose a portion of the company's members' records containing personal information, including Social Security numbers and possibly prescription information, to identity thieves if the extortion threat was not met. At that time, Express Scripts advised Toyota that it did not believe personal information about Toyota members was involved. An FBI investigation is underway.

Last week Toyota Motor Sales, U.S.A., Inc. received a similar threat apparently from the same criminals. The extortionists identified 188 current and former Toyota associates' name, social security number and date of birth held by Express Scripts. At this time, we are unsure whether other personal information is also at risk. Additionally, they also suggested that they possessed similar information for other current and former Toyota associates and their covered dependents. Toyota has already notified the 188 associates of the breach and we are working with these associates to assist them in connection with fraud prevention. Toyota also notified the FBI agents involved with the Express Scripts investigation.

We believe that there is some risk, based on the threat contained in extortionists' letter, that you or your dependents' personal information could be misused. Therefore, we believe you should consider taking action to protect your identity even though, at this time, we have received no evidence that there has been any attempt to misuse your personal information or that of your covered dependents.

Express Scripts, through its vendor Kroll, Inc., is offering fraud prevention assistance in connection with this incident (please see enclosed information). The Fraud Prevention Steps You Can Take enclosed with this letter will also be available on **ToyotaVision** at http://tv/toyotavision/. You may also obtain information through the Express Scripts website at www.esisupports.com We recommend that you take action promptly.

We are sincerely sorry for any inconvenience that this incident may cause you.

Sincerely,

TMS Human Resources Department

Fraud Prevention Steps You Can Take

1. **Place Fraud Alerts**. You can place an initial 90-day fraud alert at one of the three major credit bureaus by phone or at the website(s). A fraud alert tells creditors to follow certain procedures, including contacting you, before they open any new accounts or change your existing accounts. Placing a fraud alert can protect you, but also may delay you when you seek to obtain credit. The contact information for all three bureaus are:

Credit Bureaus

Equifax Fraud Reporting	Experian Fraud Reporting	TransUnion Fraud Reporting
(800) 525-6285	(888) 397-3742	(800) 680-7289
P.O. Box 740241	P.O. Box 9532	Fraud Victim Assistance Division
Atlanta, GA 30374-0241	Allen, TX 75013	P.O. Box 6790
www.fraudalert.equifax.com	www.experian.com	Fullerton, CA 92834-6790

It is necessary to contact only ONE of these bureaus and use only ONE of these methods. As soon as one of the three bureaus confirms your fraud alert, the others are notified to place alerts on their records as well. You will receive confirmation letters in the mail and will then be able to order a credit report from each of the three credit bureaus, free of charge, for your review.

2. **Security Freeze.** An alternative to the Fraud Alert is the **Security Freeze (also called a "Credit Freeze")**. You may want to consider **placing a** Security **Freeze** with the three national credit bureaus. There may be costs associated with this process. Kroll can provide you with information related to placing a security freeze on your credit report. You can also find more information about security freezes at:

- ☐ Equifax Freeze: www.equifax.com/cs7/Satellite?c=EFX_Page_C&childpagename=CP%2FEFX_Page_C%2FGetcreditCP&cid=1182376319357&p=1182376320319&packedargs=locale%3Den_cp&pagename=EFX%2FWrapper
- ☐ Transunion Freeze: http://www.transunion.com/corporate/personal/fraudIdentityTheft/preventing/securityFreeze.page
- ☐ Experian Freeze: http://www.experian.com/consumer/security_freeze.html

3. **Review Your Credit Reports**. Periodically check your credit report to ensure that all your information is correct. Checking your credit report periodically can help you spot problems and address them quickly. Under federal law, you also are entitled every 12 months to one free copy of your credit report from each of the three major credit reporting companies. To obtain a free annual credit report yourself, go to www.annualcreditreport.com or call 877-322-8228. You may wish to stagger your requests so that you receive a free report from one of the three credit bureaus every four months. In addition, placing a fraud alert entitles you to a free credit report.

4. **Review Your Account Statements.** You should carefully review for suspicious activity the statements that you receive from credit card companies, banks, utilities and other service providers. Close any compromised accounts.

5. Contact Law Enforcement. If you find suspicious activity on your credit reports or have reason to believe your information is being misused contact your local law enforcement agency and file a police report. Get a copy of the report when it becomes available to you and retain it for further use, as many creditors want the information it contains to absolve you of potential fraudulent debts. Please note that in order to file a crime report or incident report with law enforcement for identity theft, you will likely need to provide some kind of proof that you have been a victim. A police report is often required to dispute fraudulent items.

6. Contact Kroll, Inc. You can contact **Kroll** at **866-795-9350**, **Monday through Friday, 8AM to 5PM (CT)** to gain additional information about this event and to talk with representatives from **Kroll** about appropriate steps to place fraud alerts or security freezes.

7. Contact Kroll if you see suspicious activity. If you discover any suspicious items in your credit reports or account statements, notify **Kroll** immediately after notifying law enforcement by calling **866-795-9350.**

8. Additional Information. You can obtain additional information about steps you can take to avoid identity theft from the following:

Identity Theft Clearinghouse
Federal Trade Commission
600 Pennsylvania Avenue, NW
Washington, DC 20580
http://www.ftc.gov/bcp/edu/microsites/idtheft/
(877) IDTHEFT (438-4338)
TDD: (202) 326-2502

California Office of Information Security and Privacy Protection
http://www.oispp.ca.gov/consumer_privacy/identitytheft.asp