

Christine N. Czuprynski
Direct Dial: 248-220-1360
E-mail: cczuprynski@mcdonaldhopkins.com

P 1.248.646.5070
F 1.248.646.5075

June 30, 2022

VIA EMAIL (Idtheft@oag.state.md.us)

Office of the Maryland Attorney General
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202

Re: Richmond Ford, LLC – Incident Notification

Dear Sir or Madam:

McDonald Hopkins PLC represents Richmond Ford, LLC (“Richmond Ford”). I am writing to provide notification of an incident at Richmond Ford that may affect the security of personal information of five (5) Maryland residents. By providing this notice, Richmond Ford does not waive any rights or defenses regarding the applicability of Maryland law or personal jurisdiction.

On June 2, 2022, Richmond Ford discovered that an unauthorized party obtained access to one employee email account between March 21, 2022 and March 29, 2022. Upon learning of this issue, Richmond Ford secured the account and commenced a prompt and thorough investigation. As part of their investigation, Richmond Ford worked very closely with external cybersecurity professionals. After an extensive forensic investigation and manual document review, Richmond Ford discovered that the account accessed contained some personal information including residents’ full name, Social Security number, driver’s license number, and financial account information.

Richmond Ford has no indication that any of the information has been misused. Nevertheless, out of an abundance of caution, Richmond Ford wanted to inform you (and the affected residents) of the incident and to explain the steps that it is taking to help safeguard the affected residents against identity fraud. Richmond Ford is providing the affected residents with written notification of this incident commencing on or about July 1, 2022 in substantially the same form as the letter attached hereto. Richmond Ford is also offering the affected residents complimentary one-year membership with a credit monitoring service if their Social Security number was found to be contained within the one employee account accessed. Richmond Ford will also advise the affected residents to always remain vigilant in reviewing financial account statements for fraudulent or irregular activity on a regular basis. Richmond Ford will advise the affected residents about the process for placing a fraud alert and/or security freeze on their credit files and obtaining free credit reports. The affected residents are also being provided with the contact information for the consumer reporting agencies the Federal Trade Commission, and the Maryland Attorney General.

June 28, 2022

Page 2

At Richmond Ford, protecting the privacy of personal information is a top priority. Richmond Ford is committed to maintaining the privacy of personal information in its possession and has taken many precautions to safeguard it. Richmond Ford continually evaluates and modifies its practices and internal controls to enhance the security and privacy of personal information.

Should you have any questions concerning this notification, please contact me at (248) 220-1360 or cczuprynski@mcdonaldhopkins.com. Thank you for your cooperation.

Very truly yours,

A handwritten signature in black ink, appearing to read "Christine N. Czuprynski", written in a cursive style.

Christine N. Czuprynski

Encl.

Richmond Ford
10300 SW Greenburg Rd. Suite 570
Portland, OR 97223



To Enroll, Please Call:
1-800-939-4170

Or Visit:

<https://app.idx.us/account-creation/protect>

Enrollment Code: <<XXXXXXXXXX>>

<<Name 1>> <<Name 2>>
<<Address 1>> <<Address 2>>
<<City>>, <<State>> <<Zip>>

July 1, 2022

IMPORTANT INFORMATION
PLEASE REVIEW CAREFULLY

Dear <<Name1>>:

The privacy and security of your personal information is of the utmost importance to Richmond Ford, LLC ("Richmond Ford"). We are writing with important information regarding a recent data security incident that may have involved some of your information. We want to provide you with information about the incident, tell you about the services that we are providing to you, and let you know that we continue to take significant measures to protect your information.

What Happened?

We recently learned that an unauthorized party obtained access to one employee email account.

What We Are Doing.

Upon learning of this issue, we secured the account and commenced a prompt and thorough investigation. As part of our investigation, we have worked very closely with external cybersecurity professionals. After an extensive forensic investigation and manual document review, we discovered on June 2, 2022 that the email account that was accessed between March 21, 2022 and March 29, 2022 contained some of your personal information.

What Information Was Involved.

The accessed account contained some of your personal information, specifically your <<variable text>>.

What You Can Do.

We have no evidence that any of your information has been misused. Nevertheless, out of an abundance of caution, we want to make you aware of the incident. To protect you and your information, however, we are providing you with 12 months of free credit monitoring and identity theft protection services through IDX. IDX identity protection services includes: 12 months of credit and CyberScan monitoring, a \$1,000,000 insurance reimbursement policy, and fully managed id theft recovery services. With this protection, IDX will help you resolve issues if your identity is compromised.

This letter also provides other precautionary measures you can take to protect your personal information, including placing a fraud alert and security freeze on your credit files, and obtaining a free credit report. Additionally, you should always remain vigilant in reviewing your financial account statements and credit reports for fraudulent or irregular activity on a regular basis.

For More Information.

Please accept our apologies that this incident occurred. We remain fully committed to maintaining the privacy of personal information in our possession and have taken many precautions to safeguard it. We continually evaluate and modify our practices to enhance the security and privacy of your personal information.

If you have any further questions regarding this incident, please call our dedicated and confidential toll-free response line that we have set up to respond to questions at 1-800-939-4170. The response line is available Monday through Friday, 9:00 a.m. to 9:00 p.m. Eastern Time.

Sincerely,

Ron Kody, President
Richmond Ford, LLC
4600 W. Broad Street
Richmond, VA 23230

– OTHER IMPORTANT INFORMATION –

1. **Enrolling in Complimentary 12-Month Credit Monitoring.**

Activate IDX Identity Protection Membership Now in Three Easy Steps

1. ENROLL by: **October 1, 2022** (Your code will not work after this date.)
2. VISIT the **IDX website** to enroll: <https://app.idx.us/account-creation/protect>
3. PROVIDE the **Enrollment Code**: <<**Code**>>

Activate the credit monitoring provided as part of your IDX identity protection membership. The monitoring included in the membership must be activated to be effective. Note: You must have established credit and access to a computer and the internet to use this service. If you need assistance, IDX will be able to assist you.

If you have questions about the product or if you would like to enroll over the phone, please contact IDX at 1-800-939-4170.

2. **Placing a Fraud Alert on Your Credit File.**

Whether or not you choose to use the complimentary 12 month credit monitoring services, we recommend that you place an initial one year “fraud alert” on your credit files, at no charge. A fraud alert tells creditors to contact you personally before they open any new accounts. To place a fraud alert, call any one of the three major credit bureaus at the numbers listed below. As soon as one credit bureau confirms your fraud alert, they will notify the others.

Equifax

P.O. Box 105069
Atlanta, GA 30348-5069
<https://www.equifax.com/personal/credit-report-services/credit-fraud-alerts/>
(800) 525-6285

Experian

P.O. Box 9554
Allen, TX 75013
<https://www.experian.com/fraud/center.html>
(888) 397-3742

TransUnion

Fraud Victim Assistance
Department
P.O. Box 2000
Chester, PA 19016-2000
<https://www.transunion.com/fraud-alerts>
(800) 680-7289

3. **Placing a Security Freeze on Your Credit File.**

If you are very concerned about becoming a victim of fraud or identity theft, you may request a “security freeze” be placed on your credit file, at no charge. A security freeze prohibits, with certain specific exceptions, the consumer reporting agencies from releasing your credit report or any information from it without your express authorization. You may place a security freeze on your credit report by contacting all three nationwide credit reporting companies at the numbers below and following the stated directions or by sending a request in writing, by mail, to all three credit reporting companies:

Equifax Security Freeze

P.O. Box 105788
Atlanta, GA 30348-5788
<https://www.equifax.com/personal/credit-report-services/credit-freeze/>
(888)-298-0045

Experian Security Freeze

P.O. Box 9554
Allen, TX 75013
<http://experian.com/freeze>
(888) 397-3742

TransUnion Security Freeze

P.O. Box 160
Woodlyn, PA 19094
<https://www.transunion.com/credit-freeze>
(888) 909-8872

In order to place the security freeze, you’ll need to supply your name, address, date of birth, Social Security number and other personal information. After receiving your freeze request, each credit reporting company will send you a confirmation letter containing a unique PIN (personal identification number) or password. Keep the PIN or password in a safe place. You will need it if you choose to lift the freeze.

If you do place a security freeze *prior* to enrolling in the credit monitoring service as described above, you will need to remove the freeze in order to sign up for the credit monitoring service. After you sign up for the credit monitoring service, you may refreeze your credit file.

4. **Obtaining a Free Credit Report.**

Under federal law, you are entitled to one free credit report every 12 months from each of the above three major nationwide credit reporting companies. Call **1-877-322-8228** or request your free credit reports online at **www.annualcreditreport.com**. Once you receive your credit reports, review them for discrepancies. Identify any accounts you did not open or inquiries from creditors that you did not authorize. Verify all information is correct. If you have questions or notice incorrect information, contact the credit reporting company.

5. **Additional Helpful Resources.**

Even if you do not find any suspicious activity on your initial credit reports, the Federal Trade Commission (FTC) recommends that you check your credit reports periodically. Checking your credit report periodically can help you spot problems and address them quickly.

If you find suspicious activity on your credit reports or have reason to believe your information is being misused, call your local law enforcement agency and file a police report. Be sure to obtain a copy of the police report, as many creditors will want the information it contains to absolve you of the fraudulent debts. You may also file a complaint with the FTC by contacting them on the web at www.ftc.gov/idtheft, by phone at 1-877-IDTHEFT (1-877-438-4338), or by mail at Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580. Your complaint will be added to the FTC's Identity Theft Data Clearinghouse, where it will be accessible to law enforcement for their investigations. In addition, you may obtain information from the FTC about fraud alerts and security freezes.

If your personal information has been used to file a false tax return, to open an account or to attempt to open an account in your name or to commit fraud or other crimes against you, you may file a police report in the city in which you currently reside.

If this letter states that your financial information was impacted, we recommend that you contact your financial institution to inquire about steps to take to protect your account, including whether you should close your account or obtain a new account number.

Maryland Residents: You may obtain information about avoiding identity theft from the Maryland Attorney General's Office: Office of the Attorney General of Maryland, Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202, www.oag.state.md.us/Consumer, Telephone: 1-888-743-0023.

New York Residents: You may obtain information about preventing identity theft from the New York Attorney General's Office: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; <https://ag.ny.gov/consumer-frauds-bureau/identity-theft>; Telephone: 1-800-771-7755.

North Carolina Residents: You may obtain information about preventing identity theft from the North Carolina Attorney General's Office: Office of the Attorney General of North Carolina, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001, www.ncdoj.gov/, Telephone: 1-877-566-7226.