

November 2, 2023

VIA E-MAIL (IDTheft@oag.state.md.us)

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

Re: Data Incident Notification

Dear Sir or Madam:

We are writing to notify your office of a data security incident affecting 2 Maryland residents. We are submitting this notice as counsel for Detroit Chassis LLC (“DCP”), whose mailing address is 6501 Lynch Road, Detroit, MI 48234.

DCP was subject to a sophisticated cybersecurity attack on or about March 12, 2023 (the “Incident”). With assistance from third-party experts, DCP took immediate steps to secure its systems and investigate the nature and scope of the Incident. As part of its extensive investigation, DCP has been working diligently to identify any personal information that may have been subject to unauthorized access or acquisition as a result of the Incident. On or about September 25, 2023, its investigation concluded. DCP has been reviewing the investigation results and determined certain information located in an email server in the process of being decommissioned may have been impacted, which contained personal information related to 2 Maryland residents. While DCP believes there is a reasonable basis to conclude this information was not subject to unauthorized acquisition, DCP was unable to rule it out. DCP has not found any evidence that personal information was misused as a result of the Incident. The categories of personal information involved in the Incident for the Maryland residents are names, social security numbers, financial account information, and health insurance numbers.

Out of an abundance of caution, and in accordance with applicable law, DCP will provide notice to the affected Maryland residents, in the forms enclosed as Exhibit A, so that they can take steps to minimize the risk that their information will be misused.

DCP treats all sensitive information in a confidential manner and is proactive in the careful handling of such information. Since the Incident, DCP has augmented its cybersecurity environment to reduce the risk of a future event including implementing end point detection, periodic vulnerability scanning and reporting, resetting all administrator passwords, and restricting externally exposed remote desktop services or implemented MFA to secure them.

DCP will continue to monitor this situation and will update you on any significant developments. If you require any additional information on this matter, please contact me.¹

¹ Please note that DCP is not, by submitting this letter, agreeing to the jurisdiction of State of Maryland, nor waiving its right to challenge jurisdiction in any subsequent actions.

Office of the Attorney General

November 2, 2023

Page 2

Sincerely,

JACKSON LEWIS P.C.

/s/ Mary T. Costigan

Mary T. Costigan

Enclosure.

EXHIBIT “A”

November 2, 2023

Incident Notice

Dear _____,

What Happened

We are writing to notify you that Detroit Chassis LLC (“DCP”) was subject to a sophisticated cybersecurity attack on or about March 12, 2023 (the “Incident”). With assistance from third-party experts, we took immediate steps to secure our systems and investigate the nature and scope of the Incident. As part of our extensive investigation, we have been working diligently to identify any personally identifiable information (“PII”) or protected health information (“PHI”) that may have been subject to unauthorized access or acquisition as a result of the Incident. On or about September 25, 2023, our investigation concluded. We have been reviewing the investigation results and determined certain information located in an email server in the process of being decommissioned may have been impacted. While we believe there is a reasonable basis to conclude this information was not subject to unauthorized acquisition, we were unable to rule it out.

What Information Was Involved

The Incident may have impacted some of the following categories of PII or PHI related to you: name, address, date of birth, Social Security number, driver’s license, financial account information, passport number, credit card number, state identification number, username and access information for a non-financial account, medical information, health insurance number or information related to your DCP prescription benefits plan. However, we have not found any evidence that your information has been used to commit fraud or identity theft.

What We Are Doing

Out of an abundance of caution, and in accordance with applicable law, we are providing this notice so you can take any precautionary steps you deem necessary to minimize the potential misuse of your information.

As an added precaution, we have arranged for TransUnion to provide you 12 months of free credit monitoring, a \$1,000,000 identity theft insurance policy, and identity restoration services. To enroll, please visit www.firstwatchid.com or call 877-817-0173. Your enrollment code is _____. To receive these services, please be sure to enroll by January 31, 2024.

We endeavor to treat all sensitive information in a confidential manner and are proactive in the careful handling of such information. Since the Incident, we have augmented our cybersecurity environment to reduce the risk of a future event.

What You Can Do

In addition to enrolling in the credit monitoring services discussed above, consider taking some of the precautionary steps on the attached sheet.

For More Information

If you have questions or concerns, please call our dedicated assistance line at 888-562-5906, 9:00 a.m. – 5:30 p.m., Eastern Time. We sincerely apologize for this situation and any concern or inconvenience it may cause you.

Sincerely,

Michael Guthrie
Co-Chairman
Detroit Chassis LLC

Additional Steps and Resources To Protect Your Personal Information

We recommend you remain vigilant and consider taking the following steps to protect your personal information:

1. Contact the nationwide credit-reporting agencies as soon as possible to:
 - Add a fraud alert statement to your credit file at all three national credit-reporting agencies: Equifax, Experian, and TransUnion. You only need to contact one of the three agencies listed below; your request will be shared with the other two agencies. This fraud alert will remain on your credit file for 90 days.
 - You can also receive information from these agencies about avoiding identity theft, such as by placing a “security freeze” on your credit accounts. Credit reporting agencies may charge a \$5.30 fee to place or remove a security freeze, unless you provide proof that you are a victim of identity theft, in which case there is no fee. In your request, you also must include: (i) a copy of either the police report or case number documenting the identity theft, if you are a victim of identity theft; (ii) your full name (including middle initial as well as Jr., Sr., II, III, etc.), address, Social Security number, and date of birth; (iii) if you have moved in the past five years, the address of each residence you lived at during that time period; (iv) proof of current address, such as a current utility bill or phone bill; (v) a photocopy of a government issued identification card (state driver's license or ID card, military identification, etc.); and, if applicable, (vi) payment by check, money order, or credit card (Visa, Master Card, American Express, or Discover cards only.)
 - Remove your name from mailing lists of pre-approved offers of credit for approximately six months.
 - Receive and carefully review a free copy of your credit report by going to www.annualcreditreport.com.

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

2. Carefully review all bills and credit card statements you receive to see if there are items you did not contract for or purchase. Also review all of your bank account statements frequently for checks, purchases, or deductions not made by you. Note that even if you do not find suspicious activity initially, you should continue to check this information periodically since identity thieves sometimes hold on to stolen personal information before using it.
3. The Federal Trade Commission (“FTC”) offers consumer assistance and educational materials relating to identity theft, privacy issues, and how to avoid identity theft, such as by setting up fraud alerts or placing a “security freeze” on your credit accounts. The FTC can be contacted either by visiting www.ftc.gov, www.consumer.gov/idtheft, or by calling (877) 438-4338.

If you suspect or know that you are the victim of identity theft, you should contact local law enforcement or the attorney general, and you can also contact the Fraud Department of the FTC, which will collect all information and make it available to law enforcement agencies. The FTC can be contacted at the website or phone number above, or at the mailing address below:

Federal Trade Commission
Consumer Response Center
600 Pennsylvania Avenue
NW Washington, DC 20580

4. *For Iowa Residents:* You may contact law enforcement or the Iowa Attorney General’s Office to report suspected incidents of identity Theft: Office of the Attorney General of Iowa, Consumer Protection

Division, Hoover State Office Building, 1305 East Walnut Street, Des Moines, IA 50319, (515) 281-5164, www.iowaattorneygeneral.gov.

5. *For Maryland Residents:* You can obtain information about steps you can take to help prevent identity theft from the Maryland Attorney General, 200 St. Paul Place, Baltimore, MD 21202, (888) 743-0023, marylandattorneygeneral.gov.
6. *For New York Residents:* You may also contact the following state agencies for information regarding security breach response and identity theft prevention and protection information: 1) New York Attorney General, (212) 416-8433 or <https://ag.ny.gov/internet/resource-center>; or 2) NYS Department of State's Division of Consumer Protection, (800) 697-1220 or <https://dos.ny.gov/consumer-protection>.
7. *For North Carolina Residents:* You can obtain information about steps you can take to help prevent identity theft from the North Carolina Attorney General at: 9001 Mail Service Center, Raleigh, NC 27699, 1-877566-7226, www.ncdoj.gov.
8. *For Oregon Residents:* You may obtain information about preventing identity theft from the Oregon Attorney General's Office at: Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, (877) 877-9392, www.doj.state.or.us/.
9. *For New Mexico Residents:* You have rights under the federal Fair Credit Reporting Act (FCRA). These include, among others, the right to know what is in your file; to dispute incomplete or inaccurate information; and to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information. For more information about the FCRA, please visit https://files.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf or www.ftc.gov. In addition, New Mexico consumers may obtain a security freeze on your credit report to protect your privacy and ensure that credit is not granted in your name without your knowledge. You may submit a declaration of removal to remove information placed in your credit report as a result of being a victim of identity theft. You have a right to place a security freeze on your credit report or submit a declaration of removal pursuant to the Fair Credit Reporting and Identity Security Act. For more information about New Mexico consumers obtaining a security freeze, go to https://www.ffnm.org/_/kcms-doc/1254/38712/Credit-Freeze-Q-A-New-Mexico-Sept-2017.pdf.

November 2, 2023

Incident Notice

Dear _____,

What Happened

We are writing to notify you that Detroit Chassis LLC (“DCP”) was subject to a sophisticated cybersecurity attack on or about March 12, 2023 (the “Incident”). With assistance from third-party experts, we took immediate steps to secure our systems and investigate the nature and scope of the Incident. As part of our extensive investigation, we have been working diligently to identify any personally identifiable information (“PII”) or protected health information (“PHI”) that may have been subject to unauthorized access or acquisition as a result of the Incident. On or about September 25, 2023, our investigation concluded. We have been reviewing the investigation results and determined certain information located in an email server in the process of being decommissioned may have been impacted. While we believe there is a reasonable basis to conclude this information was not subject to unauthorized acquisition, we were unable to rule it out.

What Information Was Involved

The Incident may have impacted some of the following categories of PII or PHI related to you: name, address, date of birth, Social Security number, driver’s license, financial account information, passport number, credit card number, state identification number, username and access information for a non-financial account, medical information, health insurance number or information related to your DCP prescription benefits plan. However, we have not found any evidence that your information has been used to commit fraud or identity theft.

What We Are Doing

Out of an abundance of caution, and in accordance with applicable law, we are providing this notice to you so that you can take steps to minimize the risk that your information will be misused.

We endeavor to treat all sensitive information in a confidential manner and are proactive in the careful handling of such information. Since the Incident, we have augmented our cybersecurity environment to reduce the risk of a future event.

What You Can Do

The attached sheet describes precautionary steps you can take to protect your identity, credit, and personal information.

For More Information

If you have questions or concerns, please call our dedicated assistance line at 888-562-5906, 9:00 a.m. – 5:30 p.m., Eastern Time. We sincerely apologize for this situation and any concern or inconvenience it may cause you.

Sincerely,

Michael Guthrie
Co-Chairman
Detroit Chassis LLC

Additional Steps and Resources To Protect Your Personal Information

We recommend you remain vigilant and consider taking the following steps to protect your personal information:

1. Contact the nationwide credit-reporting agencies as soon as possible to:
 - Add a fraud alert statement to your credit file at all three national credit-reporting agencies: Equifax, Experian, and TransUnion. You only need to contact one of the three agencies listed below; your request will be shared with the other two agencies. This fraud alert will remain on your credit file for 90 days.
 - You can also receive information from these agencies about avoiding identity theft, such as by placing a “security freeze” on your credit accounts.
 - Remove your name from mailing lists of pre-approved offers of credit for approximately six months.
 - Receive and carefully review a free copy of your credit report by going to www.annualcreditreport.com.

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

2. Carefully review all bills and credit card statements you receive to see if there are items you did not contract for or purchase. Also review all of your bank account statements frequently for checks, purchases, or deductions not made by you. Note that even if you do not find suspicious activity initially, you should continue to check this information periodically since identity thieves sometimes hold on to stolen personal information before using it.
3. The Federal Trade Commission (“FTC”) offers consumer assistance and educational materials relating to identity theft, privacy issues, and how to avoid identity theft, such as by setting up fraud alerts or placing a “security freeze” on your credit accounts. The FTC can be contacted either by visiting www.ftc.gov, www.consumer.gov/idtheft, or by calling (877) 438-4338. If you suspect or know that you are the victim of identity theft, you should contact local law enforcement or the attorney general, and you can also contact the Fraud Department of the FTC, which will collect all information and make it available to law enforcement agencies. The FTC can be contacted at the website or phone number above, or at the mailing address below:

Federal Trade Commission
Consumer Response Center
600 Pennsylvania Avenue
NW Washington, DC 20580
4. *For Iowa Residents:* You may contact law enforcement or the Iowa Attorney General’s Office to report suspected incidents of identity Theft: Office of the Attorney General of Iowa, Consumer Protection Division, Hoover State Office Building, 1305 East Walnut Street, Des Moines, IA 50319, (515) 281-5164, www.iowaattorneygeneral.gov.
5. *For Maryland Residents:* You can obtain information about steps you can take to help prevent identity theft from the Maryland Attorney General, 200 St. Paul Place, Baltimore, MD 21202, (888) 743-0023, marylandattorneygeneral.gov.
6. *For New York Residents:* You may also contact the following state agencies for information regarding security breach response and identity theft prevention and protection information: 1) New York Attorney General, (212) 416-8433 or <https://ag.ny.gov/internet/resource-center>; or 2) NYS Department of State’s Division of Consumer Protection, (800) 697-1220 or <https://dos.ny.gov/consumer-protection>.

7. *For North Carolina Residents:* You can obtain information about steps you can take to help prevent identity theft from the North Carolina Attorney General at: 9001 Mail Service Center, Raleigh, NC 27699, 1-877566-7226, www.ncdoj.gov.
8. *For Oregon Residents:* You may obtain information about preventing identity theft from the Oregon Attorney General's Office at: Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, (877) 877-9392, www.doj.state.or.us/.
9. *For New Mexico Residents:* You have rights under the federal Fair Credit Reporting Act (FCRA). These include, among others, the right to know what is in your file; to dispute incomplete or inaccurate information; and to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information. For more information about the FCRA, please visit https://files.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf or www.ftc.gov. In addition, New Mexico consumers may obtain a security freeze on your credit report to protect your privacy and ensure that credit is not granted in your name without your knowledge. You may submit a declaration of removal to remove information placed in your credit report as a result of being a victim of identity theft. You have a right to place a security freeze on your credit report or submit a declaration of removal pursuant to the Fair Credit Reporting and Identity Security Act. For more information about New Mexico consumers obtaining a security freeze, go to https://www.ffnm.org/_kcms-doc/1254/38712/Credit-Freeze-Q-A-New-Mexico-Sept-2017.pdf.