



150 N. Riverside Plaza, Suite 3000, Chicago, IL 60606 • (312) 819-1900

June 5, 2024

Bruce A. Radke
312-463-6211 Direct
312-819-1910 Fax
bradke@polsinelli.com

VIA E-MAIL (IDTHEFT@OAG.STATE.MD.US)

Office of the Attorney General
Attn: Jeff Karberg, Administrator of the Identity Theft Program
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202

Re: Notification of a Potential Data Security Incident

Dear Mr. Karberg:

We represent Drive Sally, LLC (“Drive Sally”), 2209 Queens Plz N, Long Island City, New York 11101, in connection with an incident that may have involved the personal information of Maryland residents. Drive Sally is reporting the incident pursuant to MD. CODE ANN., COM. LAW § 14-3504(H). This notice will be supplemented, if necessary, with any new significant facts discovered subsequent to its submission. While Drive Sally is notifying you of this incident, Drive Sally does not waive any rights or defenses relating to the incident, this notice, or the applicability of Maryland law on personal jurisdiction.

NATURE OF THE INCIDENT

On May 1, 2024, Drive Sally learned that an unauthorized third party gained access to its staging database and potentially acquired certain files contained in that database. Upon becoming aware of the situation, Drive Sally promptly initiated an internal investigation to determine the nature and scope of the incident, notified law enforcement, and took steps to contain the unauthorized access. Drive Sally’s investigation determined that an unknown, unauthorized third party gained access to its staging database between April 30, 2024 and May 1, 2024, and during that time, acquired certain files. Drive Sally concluded that the unauthorized access was limited to its staging database due to a misconfiguration of the database settings, which was leveraged by the unauthorized third party.

Drive Sally conducted a review of the potentially acquired files to determine if they contained any personal information. Drive Sally recently completed its review and determined that the potentially acquired files contained some personal information that varied by the individual but included their



June 5, 2024

Page 2

names, dates of birth, and driver's license numbers. At this time, Drive Sally is not aware of any fraud or identity theft to any individual as a result of this incident.

NOTICE TO THE MARYLAND RESIDENTS

Drive Sally determined that the incident involved the unauthorized access to, and acquisition of personal information belonging to five (5) Maryland residents. Drive Sally is notifying the individuals today, June 5, 2024, via email correspondence. The notification letter includes information on ways the individuals can protect themselves against potential fraud and identity theft, as well as a dedicated website they can visit if they have any questions regarding the incident. Enclosed is a copy of the notice that is being sent to the Maryland residents.

STEPS TAKEN RELATING TO THE INCIDENT

Upon learning of the incident, Drive Sally promptly initiated an investigation, prevented further unauthorized access to its database, and notified law enforcement. Drive Sally has taken steps to reduce the risk of this type of incident occurring in the future, including enhancing its technical security measures. As discussed above, Drive Sally is notifying the potentially involved individuals and providing them with information on how they can protect themselves against fraudulent activity and identity theft.

CONTACT INFORMATION

Please do not hesitate to contact me if you have any questions or if I can provide you with any further information concerning this matter.

Very truly yours,

A handwritten signature in black ink, appearing to read 'Bruce A. Radke'.

Bruce A. Radke

Enclosures



Dear: <<Name1>>

RE: NOTICE OF DATA BREACH

Drive Sally, LLC values and respects the privacy of your information, which is why we are writing to advise you of a recent incident that may have involved some of your personal information stored in our systems. At this time, we have no reason to believe that your personal information has been misused for the purpose of committing fraud or identity theft. Nonetheless, we are writing to advise you about the incident and to provide you with guidance on what you can do to protect yourself, should you feel it is appropriate to do so.

What Happened? On May 1, 2024, we learned that an unknown, unauthorized third party accessed our computer systems, specifically our staging database. Upon discovery, we promptly contained the incident, initiated an investigation, and notified law enforcement. Our investigation determined that the unauthorized third party acquired certain files from our staging database between April 30, 2024 and May 1, 2024.

What Information Was Involved? Based on the investigation results, we conducted a review of the involved files, and recently determined that they contained some personal information. The type of information varied by the individual but may have included your name, driver's license number, and/or date of birth.

What We Are Doing. In addition to the steps described above, we have taken steps to reduce the risk of this type of incident occurring in the future, including enhancing our technical security measures.

What You Can Do. While we have no evidence that your personal information has been misused, we encourage you to find more information on steps to protect yourself against identity theft or fraud in the enclosed *Additional Important Information* sheet.

For More Information. We value the trust you place in us to protect the privacy and security of your personal information and apologize for any inconvenience this incident might cause. For further information about the incident, please visit

[REDACTED URL]

Sincerely,

Drive Sally, LLC

Additional Important Information

As a precautionary measure, we recommend that you remain vigilant to protect against potential fraud and/or identity theft by, among other things, reviewing your account statements and monitoring credit reports closely. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained. You should also 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 ("FTC").

You may wish to review the tips provided by the FTC on fraud alerts, security/credit freezes and steps you can take to avoid identity theft. For more information and to contact the FTC, please visit www.ftc.gov/idtheft or call 1-877-ID-THEFT (1-877-438-4338). You may also contact the FTC at Federal Trade Commission, 600 Pennsylvania Avenue, NW, Washington, DC 20580.

Under Massachusetts law, you have the right to obtain any police report filed in regard to this incident. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it.

The District of Columbia and Massachusetts law also allow consumers to place a security freeze on their credit reports. A security freeze can be placed without any charge. A security freeze prohibits a credit reporting agency from releasing any information from a consumer's credit report without written authorization. However, please be aware that placing a security freeze on your credit report may delay, interfere with, or prevent the timely approval of any requests you make for new loans, credit mortgages, employment, housing or other services.

Credit and Security Freezes: By law, you have the right to place a security freeze on your credit report, you must send a written request to each of the three major consumer reporting agencies by regular, certified or overnight mail at the addresses below or, if available, comply with the consumer reporting agencies' online security freeze request procedures:

Equifax Security Freeze

1-888-298-0045

<https://www.equifax.com/personal/credit-report-services/credit-freeze/>

P.O. Box 105788

Atlanta, GA 30348

Experian Security Freeze

1-888-397-3742

<https://www.experian.com/freeze/center.html>

P.O. Box 9554

Allen, TX 75013

TransUnion Security Freeze

1-888-909-8872

<https://www.transunion.com/credit-freeze>

P.O. Box 160

Woodlyn, PA 19094

In order to request a security freeze, you may need to provide the following information:

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security Number;
3. Date of birth;
4. If you have moved in the past five (5) years, provide the addresses where you have lived over the prior five years;
5. Proof of current address such as a current utility bill or telephone bill;
6. A legible photocopy of a government issued identification card (state driver's license or ID card, military identification, etc.); and
7. If you are a victim of identity theft, include a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft.

The credit reporting agencies have three (3) business days after receiving your request to place a security freeze on your credit report. The credit bureaus must also send written confirmation to you within five (5) business days and provide you with a unique personal identification number (PIN) or password, or both that can be used by you to authorize the removal or lifting of the security freeze.

To lift the security freeze in order to allow a specific entity or individual access to your credit report, you must call or send a written request to the credit reporting agencies by mail or, if available, comply with the consumer reporting agencies' online procedures for lifting a security freeze, and include proper identification (name, address, and social security number) and the PIN number or password provided to you when you placed the security freeze as well as the identities of those entities or individuals you would like to receive your credit report or the specific period of time you want the credit report

available. The credit reporting agencies have three (3) business days after receiving your request to lift the security freeze for those identified entities or for the specified period of time.

To remove the security freeze, you must send a written request to each of the three credit bureaus by mail or, if available, comply with the consumer reporting agencies' online procedures for removing a security freeze, and include proper identification (name, address, and social security number) and the PIN number or password provided to you when you placed the security freeze. The credit bureaus have three (3) business days after receiving your request to remove the security freeze.

Credit Reports: By law, you may obtain a free copy of your credit report once every 12 months from each of the three national credit reporting agencies. The three national credit reporting agencies have also agreed to provide free weekly online credit reports. You can obtain your free credit report by visiting www.annualcreditreport.com, by calling toll-free 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 <https://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
1-866-349-5191
www.equifax.com
P.O. Box 740241
Atlanta, GA 30374

Experian
1-888-397-3742
www.experian.com
P.O. Box 2002
Allen, TX 75013

TransUnion
1-800-888-4213
www.transunion.com
P.O. Box 1000
Chester, PA 19016

Fraud Alerts: You may want to consider placing a fraud alert on your credit report. A fraud alert is free and will stay on your credit report for one (1) year. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any new accounts in your name. To place a fraud alert on your credit report, contact any of the three national credit reporting agencies using the contact information listed above. Additional information is available at www.annualcreditreport.com.

This notification was not delayed by law enforcement.

District of Columbia Residents: District of Columbia residents can contact the Office of the Attorney general to obtain information about steps to take to avoid identity theft from the Office of the Attorney General for the District of Columbia at 441 4th Street, NW, Washington, DC 20001, 202-727-3400, oag@dc.gov, <https://oag.dc.gov/>. The District of Columbia law also allows consumers to place a security freeze on their credit reports without any charge.

Iowa Residents: Iowa residents can contact the Office of the Attorney general to obtain information about steps to take to avoid identity theft from the Iowa Attorney General's office at: Office of the Attorney General of Iowa, Hoover State Office Building, 1305 E. Walnut Street, Des Moines IA 50319, 515-281-5164.

Maryland Residents: Maryland residents can contact the Office of the Attorney General to obtain information about steps you can take to avoid identity theft from the Maryland Attorney General's office at: Office of the Attorney General, 200 St. Paul Place, Baltimore, MD 21202, (888) 743-0023, <http://www.marylandattorneygeneral.gov/>.

New York State Residents: New York residents can obtain information about preventing identity theft from the New York Attorney General's Office at: Office of the Attorney General for the State of New York, Bureau of Consumer Frauds & Protection, The Capitol, Albany, New York 12224-0341; <https://ag.ny.gov/consumer-frauds/identity-theft>; (800) 771-7755.

North Carolina Residents: North Carolina residents can obtain information about preventing identity theft from the North Carolina Attorney General's Office at: North Carolina Attorney General's Office, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001; 877-5-NO-SCAM (Toll-free within North Carolina); 919-716-6000; www.ncdoj.gov.

Oregon Residents: Oregon residents are advised to report any suspected identity theft to law enforcement, including the Federal Trade Commission and the Oregon Attorney General. Oregon residents can contact the Oregon Attorney General at 1162 Court St. NE, Salem, OR 97301-4096; 503-378-4400; <https://www.doj.state.or.us/>.

Rhode Island Residents: We believe that this incident affected 1 Rhode Island resident. Rhode Island residents can contact the Office of the Attorney general at: Rhode Island Office of the Attorney General, 150 South Main Street, Providence, RI 02903, (401) 274-4400, www.riag.ri.gov. You have the right to obtain any police report filed in regard to this incident. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it.