

Dominic A. Paluzzi
Direct Dial: 248.220.1356
E-mail: dpaluzzi@mcdonaldhopkins.com

March 24, 2025

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

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

Re: D&S Insurance Agency, Inc. – Incident Notification

To Whom It May Concern:

McDonald Hopkins, PLC represents D&S Insurance Agency, Inc. (“D&S”), located at 5015 Canyon Crest Dr., Suite 207, Riverside, California 92507, regarding a recent security incident. I am writing to provide notification of an incident at D&S that may affect the security of the personal information of approximately one (1) Maryland resident. By providing this notice, D&S does not waive any rights or defenses regarding the applicability of Maryland law or personal jurisdiction.

D&S learned that an unauthorized individual obtained access to two (2) employee email accounts. Upon learning of this issue, D&S immediately launched an investigation in consultation with outside cybersecurity professionals who regularly investigate and analyze these types of situations to analyze the extent of any compromise of the email accounts and the security of the emails and attachments contained within it. After an extensive forensic investigation and manual review, on February 26, 2025, D&S discovered that between February 21, 2024 and March 14, 2024, certain impacted files containing personal information may have been subject to unauthorized access or acquisition. The potentially impacted information includes full names, dates of birth, Social Security numbers, driver’s license number, financial account information, health insurance information, and/or medical information. The data elements impacted for each individual is subject to variance and may not include all data elements listed.

To date, D&S is not aware of any reports of identity fraud or financial fraud as a direct result of this incident. Nevertheless, out of an abundance of caution, D&S wanted to inform you (and the affected resident) of the incident and to explain the steps that it is taking to help safeguard the affected resident against identity fraud. D&S is providing the affected resident with notification of this incident, commencing on March 24, 2025. The notice will be in substantially the same form as the letter attached hereto. D&S will provide individuals whose Social Security

March 24, 2025

Page 2

numbers were impacted by this incident with a complementary 12-month membership of credit monitoring.

Further, D&S is advising the affected resident to always remain vigilant in reviewing financial account statements and credit reports for fraudulent or irregular activity on a regular basis. D&S is also advising the affected resident about the process for placing a fraud alert and/or security freeze on their credit files and obtaining free credit reports. Additionally, the affected resident is being provided with the contact information for the consumer reporting agencies and the Federal Trade Commission.

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

If you have any questions or wish to discuss this event further, please do not hesitate to call me on my direct dial (248) 220-1356 or email me at dpaluzzi@mcdonaldhopkins.com.

Sincerely,



Dominic A. Paluzzi

Encl.



March 24, 2025

Dear [REDACTED],

The privacy and security of the personal information we maintain is of the utmost importance to D&S Insurance Agency, Inc. ("D&S"). We are writing with important information regarding a data security incident that may have impacted some of your information. As such, 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 help protect your information.

What Happened?

D&S learned that an unauthorized individual obtained access to two (2) employee email accounts.

What D&S Is Doing?

Upon learning of this issue, we immediately launched an investigation in consultation with outside cybersecurity professionals who regularly investigate and analyze these types of situations to analyze the extent of any compromise of the email accounts and the security of the emails and attachments contained within it. After an extensive forensic investigation and manual review, on February 26, 2025, we discovered that, between February 21, 2024 and March 14, 2024, certain impacted files containing personal information may have been subject to unauthorized access or acquisition.

What Information Was Involved?

The impacted email accounts contained some of your personal information, specifically your [REDACTED]

What You Can Do?

To date, we have no knowledge that your information has been or will be misused as a direct result of this incident. However, out of an abundance of caution to help protect you from potential misuse of your information, we are offering a complimentary [REDACTED] month membership for identity monitoring. For more information on how to help safeguard your information and credit monitoring, including instructions on how to activate your complimentary membership, please see the additional information provided in this letter.

This letter also provides other precautionary measures you can take to help 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, explanation of benefits statements, and credit reports for fraudulent or irregular activity on a regular basis.

For More Information

Please accept our apologies that this incident occurred. D&S is committed to maintaining the privacy of personal information in our possession and have taken many precautions to safeguard it. D&S continually evaluates and modifies its practices and internal controls to enhance the security and privacy of your personal information.

If you have any further questions regarding this incident, please call the dedicated, confidential toll-free response line we have set up to respond to questions at [REDACTED]. The response line is staffed with professionals familiar with this incident and knowledgeable. The response line is available between the hours of [REDACTED], Monday through Friday, excluding holidays.

Sincerely,

D&S Insurance Agency, Inc.

5015 Canyon Crest Dr., Suite 207
Riverside, California 92507

– OTHER IMPORTANT INFORMATION –

1. Activating Complimentary Identity Monitoring.

To help relieve concerns and restore confidence following this incident, we have secured the services of Kroll to provide identity monitoring at no cost to you for [REDACTED] months. Kroll is a global leader in risk mitigation and response, and their team has extensive experience helping people who have sustained an unintentional exposure of confidential data. Your identity monitoring services include Credit Monitoring, Fraud Consultation, and Identity Theft Restoration.

Visit [REDACTED] to activate and take advantage of your identity monitoring services.

You have until [REDACTED] to activate your identity monitoring services.

Membership Number: [REDACTED]

For more information about Kroll and your Identity Monitoring services, you can visit info.krollmonitoring.com.



TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES

You have been provided with access to the following services from Kroll:

Single Bureau Credit Monitoring

You will receive alerts when there are changes to your credit data—for instance, when a new line of credit is applied for in your name. If you do not recognize the activity, you'll have the option to call a Kroll fraud specialist, who will be able to help you determine if it is an indicator of identity theft.

Fraud Consultation

You have unlimited access to consultation with a Kroll fraud specialist. Support includes showing you the most effective ways to protect your identity, explaining your rights and protections under the law, assistance with fraud alerts, and interpreting how personal information is accessed and used, including investigating suspicious activity that could be tied to an identity theft event.

Identity Theft Restoration

If you become a victim of identity theft, an experienced Kroll licensed investigator will work on your behalf to resolve related issues. You will have access to a dedicated investigator who understands your issues and can do most of the work for you. Your investigator will be able to dig deep to uncover the scope of the identity theft, and then work to resolve it.

Kroll's activation website is only compatible with the current version or one version earlier of Chrome, Firefox, Safari and Edge.

To receive credit services, you must be over the age of 18 and have established credit in the U.S., have a Social Security number in your name, and have a U.S. residential address associated with your credit file.

2. Placing a Fraud Alert on Your Credit File.

We recommend that you place an initial one (1) 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 anyone (1) of the three (3) 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. Consider 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 (3) 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 (3) 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 (1) free credit report every twelve (12) months from each of the above three (3) 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 this notice letter states that your financial account information and/or credit or debit card 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.

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.

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, www.iowaattorneygeneral.gov, Telephone: 515-281-5164.

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, <https://www.marylandattorneygeneral.gov/>, Telephone: 888-743-0023.

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: 877-566-7226 (Toll-free within North Carolina), 919-716-6000.

New Jersey Residents: You may obtain information about preventing identity theft from the New State Police: P.O. Box 7068, West Trenton, NJ 08628; <https://nj.gov/njsp/tech/identity.html>; Telephone: 609-882-2000.

Oregon Residents: You may obtain information about preventing identity theft from the Oregon Attorney General's Office: Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, www.doj.state.or.us/, Telephone: 877-877-9392.