JOSEPH SALVO
JSALVO@GRSM.COM
DIRECT DIAL: (212) 453-0725

JOHN T. MILLS
JTMILLS@GRSM.COM
DIRECT DIAL: (212) 453-0778

GRSM50
GORDON REES SCULLY MANSUKHANI
YOUR 50 STATE LAW FIRM™

ATTORNEYS AT LAW
1 BATTERY PARK PLAZA, 28TH FLOOR
NEW YORK, NY 10004
WWW.GRSM.COM

July 17, 2024

VIA ELECTRONIC MAIL (IDTHEFT@OAG.STATE.MD.US)
Office of the Attorney General
Security Breach Notification
220 St. Paul Place, 25th Floor
Baltimore, Maryland 21202

Re: Notification of Data Security Incident
Our File No.: 1288070

To Whom It May Concern:

Our client, Dell & Dean, PLLC ("Dell & Dean"), understands the importance of protecting personal information and is making this notification to your Office in accordance with applicable law following a recent data security incident.

On September 29, 2022, Dell & Dean became aware of a data security incident that impacted its server infrastructure and took its systems offline. Dell & Dean immediately undertook efforts to restore its servers and undertook additional affirmative steps to safeguard the security of data maintained on its systems. Dell & Dean also simultaneously retained a forensic investigation firm to determine the nature of the security compromise and identify any individuals whose information may have been compromised.

The forensic investigation determined that access to Dell & Dean's systems occurred on approximately September 28, 2022 through September 29, 2022. The investigation also identified certain files that may have been accessed or acquired in connection with the incident. In continuing its thorough investigation, Dell & Dean undertook a comprehensive manual review process to review these files and identify the specific individuals with personal information contained therein. This comprehensive manual review process concluded on or about May 30, 2024.

In an abundance of caution, Dell & Dean is providing notification to all individuals with personal information contained within the files that may have been accessed and/or acquired in connection with the incident. Dell & Dean has obtained confirmation to the best of its ability that the information is no longer in possession of the third party(ies) associated with this incident, and it is entirely possible that any specific personal information *was not compromised* as a result of the incident.

Dell & Dean is providing notification of the incident via U.S. mail in accordance with applicable law beginning on July 17, 2024, including twelve (12) Maryland residents. A sample copy of the notification letter is attached. As noted in the attachment, Dell & Dean has included in the notification an offer to provide complimentary credit monitoring and identity theft protection services to the potentially impacted individuals. Additionally, Dell & Dean has established a toll-free call center to answer any questions that the potentially impacted individuals may have regarding the incident, as well as to assist the potentially impacted individuals in enrolling in the credit monitoring and identity theft protection services.

As stated above, following the data security incident, Dell & Dean immediately undertook efforts to restore its servers, and also undertook additional affirmative steps to safeguard the security of data maintained on it systems. Dell & Dean retained a forensic investigation firm to thoroughly investigate the incident. At all relevant times, Dell & Dean maintained and continues to maintain comprehensive policies and procedures to protect the information maintained on its servers and systems, including a written information security management policy. Please be advised that Dell & Dean is continuing to work closely with leading security experts to identify and implement measures to further strengthen the security of their systems to help prevent this from happening in the future.

Should you have any questions or require additional information, please do not hesitate to contact me.

Best regards,

GORDON REES SCULLY MANSUKHANI, LLP

/s/ John Mills

Joseph Salvo, Esq.
John T. Mills, Esq.

Enclosures

Dell & Dean, PLLC
Secure Processing Center
P.O. Box 3826
Suwanee, GA 30024

<<Full Name>>
<<Address 1>>
<<Address 2>>
<<Address 3>>
<<City>>, <<State>> <<Zip>>
<<Country>>
***Postal IMB Barcode

<<Date>>

NOTICE OF DATA BREACH

Dear <<Full Name>>:

Dell & Dean, PLLC ("Dell & Dean") values your business and understands the importance of protecting your information. We are sending you this notice to inform you that it recently identified and addressed a security incident that may have involved your personal information. This notice describes the incident, outlines the measures that we have taken in response, and advises you on steps you can take to further protect your information.

What Happened? On September 29, 2022, Dell & Dean became aware of a data security incident that impacted its server infrastructure and took its systems offline. We immediately undertook efforts to restore our servers and undertook additional affirmative steps to safeguard the security of data maintained on it systems. We also simultaneously retained a forensic investigation firm to determine the nature of the security compromise and identify any individuals whose information may have been compromised.

What Information Was Involved? The forensic investigation determined that access to Dell & Dean's systems occurred on approximately September 28, 2022 through September 29, 2022. The investigation also identified certain files that may have been accessed or acquired in connection with the incident. In continuing its thorough investigation, we undertook a comprehensive manual review process to review these files and identify the specific individuals with personal information contained therein. This comprehensive manual review process concluded on or about May 30, 2024.

In an abundance of caution, Dell & Dean is providing this notification to you as your personal information may have been accessed and/or acquired in connection with the incident, including <<Data Elements>><<Variable data 1>><<Variable data 2>><<Variable data 3>>. We have obtained confirmation to the best of our ability that the information is no longer in possession of the third party(ies) associated with this incident, and it is entirely possible that your specific personal information *was not compromised* as a result of the incident.

What We Are Doing. As stated above, following the data security incident, Dell & Dean immediately undertook efforts to restore its servers, and also undertook additional affirmative steps to safeguard the security of data maintained on it systems. We retained a forensic investigation firm to thoroughly investigate the incident. Please be advised that we are continuing to work closely with leading security experts to identify and implement measures to further strengthen the security of their systems to help prevent this from happening in the future.

FREE CREDIT MONITORING/INSURANCE: Additionally, we are offering you a free <<CM Duration>>-month membership to Equifax Credit Watch Gold credit monitoring service. This product helps detect possible misuse of your personal information and provides you with identity protection services focused on immediate identification and resolution of identity theft. **This product also includes various features such as up to $1,000,000 in identity theft insurance with no deductible, subject to policy limitations and exclusions. Equifax Credit Watch Gold is completely free to you** and enrolling in this program will not hurt your credit score. For more information on identity theft protection and Equifax Credit Watch Gold, including instructions on how to activate your complimentary <<CM Duration>>-month membership, please see the additional information attached to this letter. ***TO TAKE ADVANTAGE OF THE FREE CREDIT MONITORING OFFER, YOU MUST ENROLL BY <<ENROLLMEN DEADLINE>>.***

What You Can Do. We are aware of how important your personal information is to you. We encourage you to protect yourself from potential harm associated with this incident by enrolling in the credit monitoring service, closely monitoring all mail, email, or other contact from individuals not known to you personally, and to avoid answering questions or providing additional information to such unknown individuals. We also remind you to remain vigilant for incidents of fraud or identity theft by reviewing account statements, explanation of benefits statements, and credit reports for unauthorized activity, and to report any such activity or any suspicious contact whatsoever to law enforcement if warranted.

For More Information. For further information on steps you can take to prevent against possible fraud or identity theft, please see the attachments to this letter. Dell & Dean understands the importance of protecting your personal information, and deeply regrets any concern this may have caused to you. **Should you have any questions and would like further information regarding the information contained in this letter, please do not hesitate to contact 1-888-326-0764**.

Sincerely,

Joseph G. Dell
Managing Partner, Dell & Dean, PLLC

Attachment 1: Protecting Yourself

We remind you to remain vigilant for incidents of fraud or identity theft by reviewing account statements and credit reports for unauthorized activity. **Residents of the United States are entitled to one free credit report annually from each of the three major credit reporting agencies.** To order your free credit reports, visit www.annualcreditreport.com or call toll-free (877) 322-8228. 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 incidence of identity theft to proper law enforcement authorities, your state attorney general, and/or the Federal Trade Commission.

You may want to consider placing a fraud alert on your credit report. There are two types of fraud alerts you can place on your credit report to put your creditors on notice that you may be a victim of fraud – an initial alert and an extended alert.

- **Initial Alert:** You may ask that an initial alert be placed on your credit report if you suspect you have been, or are about to be, a victim of identity theft. A fraud alert does not impact your ability to get a loan or credit, but rather alerts a business that your personal information may have been compromised and requires the business to verify your identity before issuing you credit. Although this may cause some delay if you are applying for credit, it may protect against someone else obtaining credit in your name. An initial fraud alert stays on your credit report for at least 90 days
- **Extended Alert:** You may have an extended alert placed on your credit report if you have already been a victim of identity theft with the appropriate documentary proof. An extended fraud alert stays on your credit report for seven years. You can place a fraud alert on your credit report by contacting any of the three national credit reporting agencies. The agency that you contacted must notify the other two agencies.

Additionally, you have the right to put a **credit freeze**, also known as a security freeze, on your credit file, free of charge, so that no new credit can be opened in your name without the use of a PIN number that is issued to you when you initiate a freeze. A security freeze is designed to prevent potential credit grantors from accessing your credit report without your consent. If you place a security freeze, potential creditors and other third parties will not be able to access your credit report unless you temporarily lift the freeze. Therefore, using a security freeze may delay your ability to obtain credit. There is no fee to place or lift a security freeze. However, unlike a fraud alert, you must separately place a security freeze on your credit file at each of the three national credit reporting agencies. 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.

Below are the toll-free numbers and addresses for the three largest credit reporting agencies:

Equifax	Experian	TransUnion
P.O. Box 74021	P.O. Box 2002	P.O. Box 1000
Atlanta, GA 30374	Allen, TX 75013	Chester, PA 19016
1-800-685-1111	1-888-397-3742	1-800-916-8800
www.equifax.com	www.experian.com	www.transunion.com

Below is the toll-free number, address and website address for the Federal Trade Commission, which you may contact to obtain further information on how to protect yourself from identity theft and how to repair identity theft:

Federal Trade Commission
Consumer Response Center
600 Pennsylvania Avenue, NW
Washington, DC 20580
1-877-IDTHEFT (438-4338)
www.ftc.gov/idtheft

For residents of District of Columbia, Maryland, Rhode Island, and North Carolina: You can obtain information from the Offices of the Attorney General and the Federal Trade Commission about fraud alerts, security freezes, and steps you can take toward preventing identity theft.

Maryland Office of the Attorney General
Consumer Protection Division
200 St. Paul Place
Baltimore, MD 21202
1-888-743-0023
www.oag.state.md.us

Rhode Island Office of the Attorney General
Consumer Protection
150 South Main Street
Providence, RI 02903
1-401-274-4400
www.riag.ri.gov

District of Columbia Office of the Attorney General
Office of Consumer Protection
400 6th Street, NW
Washington, DC 20001
1-202-442-9828
www.oag.dc.gov

North Carolina Office of the Attorney General
Consumer Protection Division
9001 Mail Service Center
Raleigh, NC 27699-9001
1-877-566-7226
www.ncdoj.com

For residents of Massachusetts and Rhode Island: It is required by state law that you are informed of your right to obtain a police report if you are a victim of identity theft.

*FAIR CREDIT REPORTING ACT***.** You also have rights under the federal Fair Credit Reporting Act, which promotes the accuracy, fairness, and privacy of information in the files of consumer reporting agencies. The FTC has published a list of the primary rights created by the FCRA (https://www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf), and that article refers individuals seeking more information to visit www.ftc.gov/credit. The FTC's list includes the following FCRA rights: (1) To receive a copy of your credit report, which must contain all the information in your file at the time of your request; (2) To receive a free copy of your credit report, at your request, once every 12 months from each of the nationwide credit reporting companies – Equifax, Experian, and TransUnion; (3) To receive a free credit report if a company takes adverse action against you (e.g. denying your application for credit, insurance, or employment), and you ask for your report within 60 days of receiving notice of the action. The notice will give you the name, address, and phone number of the credit reporting company. You are also entitled to one free report a year if you're unemployed and plan to look for a job within 60 days; if you are on welfare; or if your report is inaccurate because of fraud, including identity theft; (4) To ask for a credit score; (5) To dispute incomplete or inaccurate information; (6) To obtain corrections to your report or delete inaccurate, incomplete, or unverifiable information; (7) Consumer reporting agencies may not report outdated negative information; (8) To restrict access to your file and to require consent from you for reports to be provided to employer; (9) To limit "prescreened" offers of credit and insurance you receive based on information in your credit report; and (10) To seek damages from violators. Note - Identity theft victims and active duty military personnel have additional rights.

<<Full Name>>
Enter your Activation Code: *<<ACTIVATION CODE>>*
Enrollment Deadline: *<<ENROLLMENT DEADLINE>>*

Equifax Credit Watch™ Gold

*Note: You must be over age 18 with a credit file to take advantage of the product

Key Features

- Credit monitoring with email notifications of key changes to your Equifax credit report
- Daily access to your Equifax credit report
- WebScan notifications[1] when your personal information, such as Social Security Number, credit/debit card or bank account numbers are found on fraudulent Internet trading sites
- Automatic fraud alerts[2], which encourages potential lenders to take extra steps to verify your identity before extending credit, plus blocked inquiry alerts and Equifax credit report lock[3]
- Identity Restoration to help restore your identity should you become a victim of identity theft, and a dedicated Identity Restoration Specialist to work on your behalf
- Up to $1,000,000 of identity theft insurance coverage for certain out of pocket expenses resulting from identity theft[4]

Enrollment Instructions

Go to ***www.equifax.com/activate***
Enter your unique Activation Code of ***<<ACTIVATION CODE>>*** then click “Submit” and follow these 4 steps:

1. **Register:**
   Complete the form with your contact information and click “Continue”.
   If you already have a myEquifax account, click the ‘Sign in here’ link under the “Let’s get started” header.
   Once you have successfully signed in, you will skip to the Checkout Page in Step 4
2. **Create Account:**
   Enter your email address, create a password, and accept the terms of use.
3. **Verify Identity:**
   To enroll in your product, we will ask you to complete our identity verification process.
4. **Checkout:**
   Upon successful verification of your identity, you will see the Checkout Page.
   Click ‘Sign Me Up’ to finish enrolling.

You’re done!
The confirmation page shows your completed enrollment.
Click “View My Product” to access the product features.

[1] WebScan searches for your Social Security Number, up to 5 passport numbers, up to 6 bank account numbers, up to 6 credit/debit card numbers, up to 6 email addresses, and up to 10 medical ID numbers. WebScan searches thousands of Internet sites where consumers' personal information is suspected of being bought and sold, and regularly adds new sites to the list of those it searches. However, the Internet addresses of these suspected Internet trading sites are not published and frequently change, so there is no guarantee that we are able to locate and search every possible Internet site where consumers' personal information is at risk of being traded. [2] The Automatic Fraud Alert feature is made available to consumers by Equifax Information Services LLC and fulfilled on its behalf by Equifax Consumer Services LLC. [3] Locking your Equifax credit report will prevent access to it by certain third parties. Locking your Equifax credit report will not prevent access to your credit report at any other credit reporting agency. Entities that may still have access to your Equifax credit report include: companies like Equifax Global Consumer Solutions, which provide you with access to your credit report or credit score, or monitor your credit report as part of a subscription or similar service; companies that provide you with a copy of your credit report or credit score, upon your request; federal, state and local government agencies and courts in certain circumstances; companies using the information in connection with the underwriting of insurance, or for employment, tenant or background screening purposes; companies that have a current account or relationship with you, and collection agencies acting on behalf of those whom you owe; companies that authenticate a consumer's identity for purposes other than granting credit, or for investigating or preventing actual or potential fraud; and companies that wish to make pre-approved offers of credit or insurance to you. To opt out of such pre-approved offers, visit www.optoutprescreen.com [4] The Identity Theft Insurance benefit is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company, under group or blanket policies issued to Equifax, Inc., or its respective affiliates for the benefit of its Members. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.