DRM DOWNS RACHLIN MARTIN
199 Main Street
P.O. Box 190
Burlington, Vermont 05402-0190

September 6, 2024

«First_Name» «Last_Name» «Suffix»
«Address 1» «Address 2»
«City», «State» «Postal Code»

NOTICE OF SECURITY INCIDENT

Dear «First Name» «Last Name» «Suffix»:

Downs Rachlin Martin PLLC ("DRM") writes to inform you of an event that may affect the privacy of some of your personal information. DRM was provided your information by Dartmouth Hitchcock Medical Center ("DHMC") so that DRM could provide legal services to DHMC. Although we are unaware of any identity theft or fraud in relation to the event, we are providing you with information about the event, our response, and additional measures you can take to help protect your information, should you feel it appropriate to do so.

What Happened? DRM recently learned that a laptop being used by an attorney was stolen out of a car. We quickly reported the incident to law enforcement and began an investigation into the information potentially stored on the laptop at the time of the theft. We then undertook a comprehensive and time-intensive review of the data at risk to determine if any sensitive information could be affected and to whom it relates. During this review, we received notice from DRM's security software that the laptop's wipe command initiated on April 7, 2024, creating the possibility (though not absolute certainty) that the data was destroyed. In an abundance of caution, we continued the review of the data at risk through data privacy specialists. On July 8, 2024, we notified DHMC of the event and offered to provide notice to potentially impacted individuals. DHMC later agreed to this offer.

What Information Was Involved? Our investigation determined that the laptop **may** have contained the following types of personal information: your «Unique Identifier». At this time, DRM has received no indication of any attempted or actual misuse of your personal information.

What We Are Doing. The confidentiality, privacy, and security of information in our care is among our highest priorities. Upon learning of the theft, we quickly reported it to law enforcement and commenced an investigation into the nature and scope of the incident. We quickly activated software safeguards to ensure that if the laptop were to come back online, its data would be automatically wiped. We also reinforced with our staff the importance of safeguarding information in our possession, and worked with data privacy specialists to assist in the response. Additionally, we undertook a robust effort to recreate the information potentially contained on the stolen laptop to ensure we could notify any potentially impacted individuals, including you, in order to take steps to best protect the information, should you feel it appropriate to do so.

What You Can Do. We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your account statements and monitoring your free credit reports for suspicious activity and to detect errors. Please also review the information contained in the enclosed *STEPS YOU CAN TAKE TO PROTECT PERSONAL INFORMATION*.

For More Information. We understand that you may have questions about this event that are not addressed in this letter. If you have additional questions, please write to us at P.O. Box 190, Burlington, Vermont 05402 or email us at info@drm.com. We take this event very seriously and sincerely regret any inconvenience or concern this event may cause you.

Sincerely,

William J. Dodge
Managing Partner & CEO

STEPS YOU CAN TAKE TO PROTECT PERSONAL INFORMATION

Monitor Your Accounts

Under U.S. law, a consumer is entitled to one (1) free credit report annually from each of the three (3) major credit reporting bureaus, Equifax, Experian, and TransUnion. To order a free credit report, visit http://www.annualcreditreport.com or call, toll-free, 1 (877) 322-8228. Consumers may also directly contact the three (3) major credit reporting bureaus listed below to request a free copy of their credit report.

Consumers have the right to place an initial or extended "fraud alert" on a credit file at no cost. An initial fraud alert is a one (1) year alert that is placed on a consumer's credit file. Upon seeing a fraud alert display on a consumer's credit file, a business is required to take steps to verify the consumer's identity before extending new credit. If consumers are the victim of identity theft, they are entitled to an extended fraud alert, which is a fraud alert lasting seven (7) years. Should consumers wish to place a fraud alert, please contact any of the three (3) major credit reporting bureaus listed below.

As an alternative to a fraud alert, consumers have the right to place a "credit freeze" on a credit report, which will prohibit a credit bureau from releasing information in the credit report without the consumer's express authorization. The credit freeze is designed to prevent credit, loans, and services from being approved in a consumer's name without consent. However, consumers should be aware that using a credit freeze to take control over who gets access to the personal and financial information in their credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application they make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, consumers cannot be charged to place or lift a credit freeze on their credit report. To request a credit freeze, individuals may need to provide some or all of the following information:

1. Full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. Addresses for the prior two (2) to five (5) 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, etc.); and
7. A copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft if they are a victim of identity theft.

Should consumers wish to place a credit freeze or fraud alert, please contact the three (3) major credit reporting bureaus listed below:

Equifax	Experian	TransUnion
https://www.equifax.com/personal/credit-report-services/	https://www.experian.com/help/	https://www.transunion.com/credit-help/
1 (888) 298-0045	1 (888) 397-3742	1 (800) 916-8800
Equifax Fraud Alert, P.O. Box 105069 Atlanta, GA 30348-5069	Experian Fraud Alert, P.O. Box 9554, Allen, TX 75013	TransUnion Fraud Alert, P.O. Box 2000, Chester, PA 19016
Equifax Credit Freeze, P.O. Box 105788 Atlanta, GA 30348-5788	Experian Credit Freeze, P.O. Box 9554, Allen, TX 75013	TransUnion Credit Freeze, P.O. Box 160, Woodlyn, PA 19094

Additional Information

Consumers may further educate themselves regarding identity theft, fraud alerts, credit freezes, and the steps they can take to protect their personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or their state Attorney General. The Federal Trade Commission may be reached at: 600 Pennsylvania Avenue NW, Washington, D.C. 20580; https://www.identitytheft.gov; 1 (877) ID-THEFT (1 (877) 438-4338); and TTY: 1 (866) 653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. Consumers can obtain further information on how to file such a complaint by way of the contact information

listed above. Consumers have the right to file a police report if they ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, consumers will likely need to provide some proof that they have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement, the relevant state Attorney General, and the Federal Trade Commission. This notice has not been delayed by law enforcement.