

STATE OF NEW HAMPSHIRE
DEPT OF JUSTICE
2019 MAY 31 PM 12:36

SKADDEN, ARPS, SLATE, MEAGHER & FLOM LLP

155 N. WACKER DR.
CHICAGO, IL 60606

TEL: (312) 407-0700

FAX: (312) 407-0411

WWW.SKADDEN.COM

FIRM/AFFILIATE OFFICES

BOSTON
CHICAGO
HOUSTON
LOS ANGELES
NEW YORK
PALO ALTO
WILMINGTON

BEIJING
BRUSSELS
FRANKFURT
HONG KONG
LONDON
MOSCOW
MUNICH
PARIS
SÃO PAULO
SEOUL
SHANGHAI
SINGAPORE
TOKYO
TORONTO

May 28, 2019

Via U.S. Mail

New Hampshire Department of Justice
Office of the Attorney General
33 Capitol Street,
Concord, NH 03301

Dear Attorney General:

We write to inform you that Mediant Communications Inc., 3 Columbus Cir. #2110, New York, NY 10019, will be sending notices to New Hampshire residents advising them of a data breach incident.

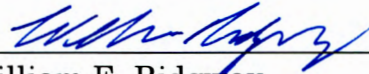
On April 1, 2019, an unknown malicious party obtained unauthorized access to four Mediant business email accounts by exploiting a vulnerability in the third party email software used by Mediant. On that same day, following the discovery of the unauthorized access, Mediant disconnected the affected email server from its system and commenced an investigation to understand the nature and scope of the incident. During this investigation, on April 16, 2019, Mediant learned that personal information of consumers, including name, address, email address, phone number, Social Security Number/tax identification number, and/or financial account number, was accessed by the malicious party. Mediant received such information from its customers or their transfer agents while providing mailing, document processing, and/or proxy services related to the consumers' ownership of certain securities. Following a detailed review of the emails affected, on May 10, 2019, Mediant determined that 504 New Hampshire residents were affected by the incident.

Mediant has reported the matter to law enforcement but is not aware of a pending investigation at this time. Mediant has also taken steps to strengthen the security of its systems—such as remediating the vulnerability in the current email system, implementing targeted network access restrictions, updating network monitoring systems, requiring affected employees to change their passwords, and accelerating planned improvements to its email system—and will take further steps as appropriate to safeguard such information. Mediant will also be reviewing its written information security program to determine if any updates to the program are appropriate. For the convenience of New Hampshire residents, Mediant has

arranged to make credit monitoring and identity repair services available to them at no cost for two years.

The formal notice will be sent to the affected residents via U.S. Mail on May 31, 2019. A copy of the consumer notice template is attached. Please contact me if you have any questions.

Sincerely,



William E. Ridgway
Counsel to Mediant Communications Inc.
155 N. Wacker Dr.
Chicago, IL 60606
312-407-0449
William.ridgway@skadden.com

Enclosure

Return Mail Processing
PO Box 470
Claysburg, PA 16625-0470

<<Name>>
<<Address>>
<<City>><<State>><<Zip>>
<<Country>>

<<Date>>

Re: Notice of Data Breach

Dear <<Name>>,

We write to inform you of an issue involving some of your personal information.

What Happened? Mediant Communications Inc., 3 Columbus Cir. #2110, New York, NY 10019, provides many mutual funds and public companies, including real estate investment trusts, with mailing and document processing services as well as services in connection with their annual and special shareholder meetings, including the distribution of proxy materials, coordination of votes, and tabulation of voting results. Mutual funds and public companies hire proxy agents such as Mediant in connection with their shareholder meetings as a matter of standard practice. Mediant received your information while providing its services to entities related to your ownership of certain securities including: <<securities list>>.

On April 1, 2019, a malicious party obtained access to certain Mediant business email accounts. Following the discovery of the unauthorized access on April 1, 2019, the affected email server was disconnected from our system, and an investigation was commenced to understand the nature and scope of the incident. This investigation determined that the unauthorized party gained access to certain investor information from a number of mutual funds and companies, including investors of the companies noted above. On May 10, 2019, we determined that your personal information was among the information impacted.

We first informed the companies noted above of these events within the last two weeks. None of the noted companies' systems were involved in the incident, and none of these companies were otherwise at fault in the incident.

What Information Was Involved? The following personal information was involved in the incident: your name, address, <<data elements>>.

What We Are Doing. We are taking this incident very seriously. We have taken steps to strengthen our protection of personal information, including updating our network security controls and email system, and we will continue to closely monitor and take further steps as appropriate to safeguard such information. We have reported the matter to law enforcement, but this notice has not been delayed because of law enforcement investigation.

In addition, we are offering credit monitoring for a period of 24 months at no cost to you. To take advantage of this offer:

- Ensure that you enroll by: [enrollment end date] (Your code will not work after this date.)
- Visit the Experian IdentityWorks website to enroll: www.experianidworks.com/credit
- Provide your activation code: <<activation code>>

If you have questions about the product, need assistance with identity restoration, or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at 866-362-1769 by [enrollment end date]. Be prepared to provide engagement number [engagement #] as proof of eligibility for the identity restoration services by Experian.

Return Mail Processing
PO Box 470
Claysburg, PA 16625-0470

What You Can Do. It is always a good practice to be vigilant and closely review or monitor your financial accounts, statements, credit reports and other financial information for any evidence of unusual activity, fraudulent charges or signs of identity theft. Please see the attachment for additional information that may be helpful to you.

For More Information. If you have any questions regarding the content of this notice, please contact us at 866-362-1769 between the hours of 9:00am – 5:00pm PST Monday through Friday.

Sincerely,

William Lauricella
Chief Financial Officer

Return Mail Processing
PO Box 470
Claysburg, PA 16625-0470

ADDITIONAL INFORMATION

Please note that you can contact the Federal Trade Commission (“FTC”) and the national consumer reporting agencies for more information on fraud alerts, security freezes and other steps you can take to avoid identity theft:

Equifax, P.O. Box 105788, Atlanta, Georgia 30348, 1-877-478-7625, www.equifax.com

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

TransUnion, P.O. Box 2000, Chester, PA 19016, 1-800-680-7289, www.transunion.com

Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, D.C. 20580, 1-877-FTC-HELP (382-4357), www.ftc.gov/idtheft

You may obtain a free copy of your credit report online at www.annualcreditreport.com, by calling toll-free 1-877-322-8228, or by mailing an Annual Credit Report Request Form (available at www.annualcreditreport.com) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281. You may also purchase a copy of your credit report by contacting one or more of the three national credit reporting agencies listed above.

Additional information about security freezes is included below. Please also note that you can report any suspected incidents of identity theft to law enforcement, your state’s attorney general and the FTC. In certain states, you may also obtain any police report filed about this issue. You also have other rights under the Fair Credit Reporting Act (“FCRA”). For further information about your rights under the FCRA, please visit https://files.consumerfinance.gov/f/201410_cfpb_summary_your-rights-under-fcra.pdf.

Additional Information for Maryland Residents. You can obtain information from the Maryland Office of the Attorney General about steps you can take to prevent identity theft. You can contact the MD Office of the AG at:

Maryland Office of the Attorney General
Consumer Protection Division
200 St. Paul Place
Baltimore, MD 21202
888-743-0023 (toll-free in Maryland)
410-576-6300
www.marylandattorneygeneral.gov

Additional Information for North Carolina Residents. You can obtain information from the North Carolina Attorney General’s Office about steps you can take to prevent identity theft. You can contact the office of the NC AG’s Office at:

North Carolina Attorney General’s Office
9001 Mail Service Center
Raleigh, NC 27699-9001
877-566-7226 (toll-free in North Carolina)
919-716-6400
www.ncdoj.gov

Return Mail Processing
PO Box 470
Claysburg, PA 16625-0470

Additional Information for Rhode Island Residents. You can obtain information from the Rhode Island Office of the Attorney General about steps you can take to prevent identity theft. You can contact the office of the RI AG at:

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

Additional Information About Security Freezes. You also have a right to place a “security freeze” on your credit report at no charge, which will prohibit a consumer reporting agency from releasing information in your credit report without your express authorization. The security freeze is designed to prevent credit, loans and services from being approved in your name without your consent. However, you should be aware that using a security freeze to take control over who gets access to the personal and financial information in your credit report may delay, interfere with or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. In addition, a security freeze does not apply to a person or entity, or its affiliates, or collection agencies acting on behalf of the person or entity, with which you have an existing account that requests information in your credit report for the purposes of reviewing or collecting the account. Reviewing the account includes activities related to account maintenance, monitoring, credit line increases, and account upgrades and enhancements.

If you wish to place a security freeze on your credit file, you must separately place a security freeze on your credit file at each credit reporting agency. In order to place a security freeze, you may need to provide 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 five years; (5) Proof of current address; and (6) A legible copy of a government issued identification card. You can contact each credit reporting agency below for details on what information each company requires and to place a security freeze on your credit file:

Equifax Security Freeze
P.O. Box 105788
Atlanta, GA 30348
800-349-9960
www.equifax.com

Experian Security Freeze
P.O. Box 9554
Allen, TX 75013
888-397-3742
www.experian.com

TransUnion
P.O. Box 160
Woodlyn, PA 19094
888-909-8872
www.transunion.com

Return Mail Processing
PO Box 470
Claysburg, PA 16625-0470

Additional Information About Credit Monitoring.

A credit card is **not** required for enrollment in Experian IdentityWorks.

You can contact Experian **immediately** regarding any fraud issues, and have access to the following features once you enroll in Experian IdentityWorks:

- **Experian credit report at signup:** See what information is associated with your credit file. Daily credit reports are available for online members only.*
- **Credit Monitoring:** Actively monitors Experian file for indicators of fraud.
- **Identity Restoration:** Identity Restoration agents are immediately available to help you address credit and non-credit related fraud.
- **Experian IdentityWorks ExtendCARE™:** You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- **Up to \$1 Million Identity Theft Insurance**:** Provides coverage for certain costs and unauthorized electronic fund transfers.

If you believe there was fraudulent use of your information and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent at 866-362-1769. If, after discussing your situation with an agent, it is determined that Identity Restoration support is needed, then an Experian Identity Restoration agent is available to work with you to investigate and resolve each incident of fraud that occurred (including, as appropriate, helping you with contacting credit grantors to dispute charges and close accounts; assisting you in placing a freeze on your credit file with the three major credit bureaus; and assisting you with contacting government agencies to help restore your identity to its proper condition).

Please note that this Identity Restoration support is available to you for two years from the date of this letter and does not require any action on your part at this time. The Terms and Conditions for this offer are located at www.ExperianIDWorks.com/restoration. You will also find self-help tips and information about identity protection at this site.

* Offline members will be eligible to call for additional reports quarterly after enrolling

** Identity theft insurance is underwritten by insurance company subsidiaries or affiliates of American International Group, Inc. (AIG). The description herein is a summary and intended for informational purposes only and does not include all terms, conditions and exclusions of the policies described. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions