

Cynthia J. Larose
617 348 1732
cjarose@mintz.com



One Financial Center
Boston, MA 02111
617 542 6000
mintz.com

August 30, 2022

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

Attorney General Brian E. Frosh
ATTN: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202

Re: Reporting of Security Incident Pursuant to Maryland Code. § 14-3505

Dear Attorney General Frosh:

We are writing on behalf of Mediacom Communications Corporation (the "Company") to advise you of an incident that may affect the security of personal information relating to approximately 21 Maryland residents. By providing this notice, the Company does not waive any rights or defenses regarding the applicability of Maryland law or personal jurisdiction.

On or about July 18, 2022, an unknown third party apparently exploited a technical bug which enabled it to bypass the Company's security procedures and change passwords for customers' Mediacom ID used to provide customers with access to their Mediacom online account and Mediacom email account. The Company detected the intrusion on or about August 17, 2022 and promptly changed customer passwords to a random complex 16-character password unknown to anyone, including Mediacom. Any further password changes were blocked except for those made directly by the customer through a call to a Mediacom customer service representative. The Company also took technical steps to ensure that the exploit could not be used in the future.

No sensitive customer personal information, such as Social Security numbers, driver's license numbers, or financial information, was stored in the customer's Mediacom online account. However, the malicious actor had the ability to view billing statements, view and edit contact information, and access customers' Mediacom email account.

The Company is taking this incident very seriously, and has taken a number of steps to strengthen the protection of personal information and mitigate risk to protect from further types of attacks, including extending its implementation of multi-factor authentication. The Company will also continue to further improve security across the Company networks and protect from unauthorized access or similar criminal activity in the future.

The Company is not aware of any fraudulent use of personal information of the affected Illinois residents at this time. The Company will send the attached notices to affected Maryland residents on August 31, 2022. Letter #1 will be sent to 6 Maryland residents whose Mediacom email account was not logged into between July 18, 2022 and August 17, 2022, and Letter #2 will be sent to 15 Maryland residents whose Mediacom email account was logged into between July 18, 2022 and August 17, 2022. For those accounts that were apparently logged into, we have no evidence that emails were downloaded or otherwise exfiltrated from the Mediacom email account.

MINTZ

Office of Attorney General
August 30, 2022
Page 2



Please contact the undersigned at cjlarose@mintz.com or 617-348-1732 should you need further information or have any additional questions.

Sincerely,

A handwritten signature in black ink, appearing to read 'Cynthia J. Larose'. The signature is fluid and cursive, with the first name 'Cynthia' and last name 'Larose' being clearly legible.

Cynthia J. Larose
Member

Attachments



1 Mediacom Way
Mediacom Park, NY 10918

[DATE]

[CUSTOMER NAME]
[CUSTOMER ADDRESS]
[City State]

RE: NOTICE OF SECURITY INCIDENT

Dear [Customer Name]:

The Internet is a wonderful resource, but it also presents certain privacy and security risks to users, including “virus” infections, “ransomware” attacks, identity theft, unauthorized access to computer files or email accounts (“hacking”) and other malicious acts by intruders. Mediacom takes customer privacy and security very seriously and devotes significant resources to identify and deal with threats.

While no one can detect and safeguard against all risks, if we become aware that a privacy or security incident has occurred despite our preventative efforts, we are committed to taking appropriate action, which includes alerting customers who may be impacted, as soon as we become aware of an issue. We are providing this notice regarding a recent security incident to all affected customers regardless of any legal requirement to do so.

On or about July 18, 2022, an unknown third party exploited a technical “bug” and changed the password for your Mediacom ID, which is used to provide you access to your Mediacom online account and Mediacom email account. While this incident did not affect many customers, (less than 1% of our customer accounts), you are receiving this notice as our research indicates you have been impacted. No sensitive personal information, such as your social security number, driver’s license number or financial information, is stored in your Mediacom online account but the third party had the ability to view billing statements, view and edit contact information (name, address, phone number) and access your Mediacom email account.

While the malicious actor took measures to hide this activity, we detected the intrusion on or about August 17, 2022. Once we became aware, we promptly changed your password to a random complex 16-character password unknown to anyone, including Mediacom, to protect your account. We also blocked any further password changes, except for those made by you directly through one of our customer service representatives, and took steps to ensure the exploit could not be used in the future.

A system activity review shows that between July 18, 2022, and August 17, 2022, your Mediacom email account was not logged into, and we have no evidence that emails were downloaded or otherwise removed from your Mediacom email account.

We recommend that you scan your computer, phone, tablet and other devices that you may have used to access your Mediacom account for viruses and malware using the security software already installed or which you download from a reputable, well-known security company. If the scan identifies suspicious software, delete it and restart your device.

LETTER #1

If you are a current active Mediacom customer, please do the following:

- If you have not done so already, call Mediacom at 844-381-5578 to change your password from the one we created after the incident to one you select; you will be required to set-up two-factor authentication with either a cell-phone number or landline.
- Review your online account information to make sure information such as contact phone numbers or email addresses are correct, and that no information has been modified (except for those changes you may have made).

In addition, consider taking all or at least some of the actions recommended or suggested by the Federal Trade Commission at <https://consumer.ftc.gov/articles/how-recover-your-hacked-email-or-social-media-account> under the caption “What To Do Once You’re Back in Your Account” or by the Center for Internet Security at <https://www.cisecurity.org/insights/newsletter/compromised-email-account-heres-what-to-do> under the caption “What to Do if Your Email Account is Compromised.”

Mediacom regrets the inconvenience that this criminal act by an unauthorized third-party may cause you. If you have any questions about this matter, please call 844-381-5578.

Thank you for your continued loyalty to Mediacom.

Sincerely,

Mediacom Customer Service



1 Mediacom Way
Mediacom Park, NY 10918

[DATE]

[CUSTOMER NAME]
[CUSTOMER ADDRESS]
[City State]

RE: NOTICE OF SECURITY INCIDENT

Dear [Customer Name]:

The Internet is a wonderful resource, but it also presents certain privacy and security risks to users, including “virus” infections, “ransomware” attacks, identity theft, unauthorized access to computer files or email accounts (“hacking”) and other malicious acts by intruders. Mediacom takes customer privacy and security very seriously and devotes significant resources to identify and deal with threats.

While no one can detect and safeguard against all risks, if we become aware that a privacy or security incident has occurred despite our preventative efforts, we are committed to taking appropriate action, which includes alerting customers who may be impacted, as soon as we become aware of an issue. We are providing this notice regarding a recent security incident to all affected customers regardless of any legal requirement to do so.

On or about July 18, 2022, an unknown third party exploited a technical “bug” and changed the password for your Mediacom ID, which is used to provide you access to your Mediacom online account and Mediacom email account. While this incident did not affect many customers, (less than 1% of our customer accounts), you are receiving this notice as our research indicates you have been impacted. No sensitive personal information, such as your social security number, driver’s license number or financial information, is stored in your Mediacom online account but the third party had the ability to view billing statements, view and edit contact information (name, address, phone number) and access your Mediacom email account.

While the malicious actor took measures to hide this activity, we detected the intrusion on or about August 17, 2022. Once we became aware, we promptly changed your password to a random complex 16-character password unknown to anyone, including Mediacom, to protect your account. We also blocked any further password changes, except for those made by you directly through one of our customer service representatives, and took steps to ensure the exploit could not be used in the future.

A system activity review shows that between July 18, 2022, and August 17, 2022, your Mediacom email account was logged into but we have no evidence that emails were downloaded or otherwise removed from your Mediacom email account.

We recommend that you scan your computer, phone, tablet and other devices that you may have used to access your Mediacom account for viruses and malware using the security software already installed or which you download

LETTER #2

from a reputable, well-known security company. If the scan identifies suspicious software, delete it and restart your device.

If you are a current active Mediacom customer, please do the following:

- If you have not done so already, call Mediacom at 844-381-5578 to change your password from the one we created after the incident to one you select; you will be required to set-up two-factor authentication with either a cell-phone number or landline.
- Review your online account information to make sure information such as contact phone numbers or email addresses are correct, and that no information has been modified (except for those changes you may have made).

In addition, consider taking all or at least some of the actions recommended or suggested by the Federal Trade Commission at <https://consumer.ftc.gov/articles/how-recover-your-hacked-email-or-social-media-account> under the caption “What To Do Once You’re Back in Your Account” or by the Center for Internet Security at <https://www.cisecurity.org/insights/newsletter/compromised-email-account-heres-what-to-do> under the caption “What to Do if Your Email Account is Compromised.”

Mediacom deeply regrets the inconvenience that this criminal act by an unauthorized third-party may cause you. If you have any questions about this matter, please call 844-381-5578.

Thank you for your continued loyalty to Mediacom.

Sincerely,

Mediacom Customer Service