

October 30, 2017

Jonathan G. Cedarbaum

+1 202 663 6315 (t)
+1 202 663 6363 (f)
jonathan.cedarbaum@wilmerhale.com

Attorney General Gordon MacDonald
Office of the Attorney General
Attn: Security Breach Notification
33 Capitol Street
Concord, NH 03301

RECEIVED
NOV 02 2017
CONSUMER PROTECTION

Re: Data Security Incident Notification

Dear Attorney General MacDonald:

We write on behalf of our client, Home Box Office, Inc. (the "Company") to advise you of a cyber incident that impacted the personal information (as defined under New Hampshire law) of fewer than ten residents of the State of New Hampshire.

On Sunday, July 23, 2017, the Company was contacted by an individual (the "attacker") claiming among other things that he had gained unauthorized access to Company data. Upon confirmation that the attacker was in possession of confidential Company data, counsel to the Company retained Mandiant, a forensic data specialist, to assist with the situation and to perform a forensic analysis. The Company also notified the Federal Bureau of Investigation.

Extensive investigation and analysis have been required to review and catalogue the material which was stolen. While the investigation and analysis remain ongoing, based on the investigation to date, the Company has determined that the attacker had unauthorized access for a limited period of time to certain portions of the Company's corporate information technology network, including the following types of personal information from residents of New Hampshire: Social Security Number.

The Company is offering all impacted individuals the AllClear Credit Monitoring Service for 12 months at no cost to the individual, which includes identity theft monitoring and a \$1 million identity theft insurance policy. In addition, in accordance with New Hampshire law, formal notification to impacted residents is being provided beginning on or about October 31, 2017, by sending a letter via United States Mail in substantially the same form as the example attached hereto.

The Company immediately made changes to decrease the chance of a similar occurrence in the future, including implementing additional security measures, internal controls, and safeguards. To the best of the Company's knowledge, based on the investigation to date and following

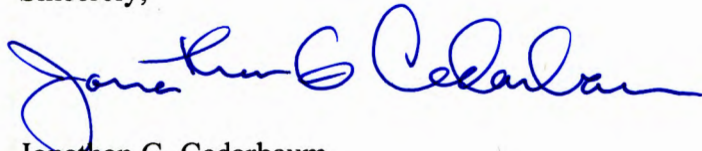
October 30, 2017

Page 2

ongoing remediation efforts, there has been no unauthorized access by the attacker to the Company's network since July 26, 2017.

If you have any questions, please do not hesitate to contact me.

Sincerely,

A handwritten signature in blue ink, appearing to read "Jonathan G. Cedarbaum". The signature is fluid and cursive, with the first name "Jonathan" being more prominent and the last name "Cedarbaum" following in a similar style.

Jonathan G. Cedarbaum

Encl.



Processing Center • P.O. BOX 141578 • Austin, TX 78714



00001
JOHN Q. SAMPLE
1234 MAIN STREET
ANYTOWN US 12345-6789

October 31, 2017

NOTICE OF DATA BREACH

Dear John Sample:

I am writing to notify you of a cyber incident involving Home Box Office, Inc.'s ("HBO") information technology network and to inform you that we have determined that your personal information was compromised during this incident. The privacy and protection of your information is a matter we take very seriously. HBO deeply regrets the inconvenience this may cause, and we recommend that you closely review the information provided in this letter for some steps that you may take to protect yourself against potential misuse of your information.

What Happened

In late July 2017, HBO became aware of an incident in which an unauthorized third party claimed to have accessed HBO's information technology network. We began investigating the incident as soon as we became aware of the potential breach. Our investigation has revealed that an unauthorized third party illegally accessed HBO's network, including some personally identifiable information about you.

What Information Was Involved

Though the investigation is still underway, we have determined that the information involved in this incident included the following types of your personally identifiable information: [Personal Information Categories].

What We Are Doing

We have worked swiftly to respond to the incident and we are cooperating with law enforcement. We are also making changes to decrease the chance of a similar occurrence in the future, including implementing additional security measures, internal controls, and safeguards. To the best of HBO's knowledge, based on the investigation to date, the earliest evidence of identified attacker access to HBO systems occurred on May 15, 2017, and there has been no unauthorized access by the attacker to HBO's network since July 26, 2017.

We are also providing free identity theft prevention and mitigation services from AllClear ID, including credit monitoring, for twelve (12) months to you because your personal information was exposed by the incident.

As a precautionary measure, you may enroll in the AllClear Credit Monitoring service at no cost to you. These services include identity theft monitoring and a \$1 million identity theft insurance policy. To obtain these services, and learn how to enroll, visit [REDACTED].



01-02-1-00

If you need identity repair assistance, the team at AllClear ID is ready and standing by to assist you. There is no action required on your part at this time. If a problem arises, simply call 1-855-742-6218 and a dedicated investigator will work with you.

If you have additional questions about the services, the AllClear ID call center is available to respond to your questions and to assist you Monday through Saturday, 8 a.m. to 8 p.m. Central Time at 1-855-742-6218. You may also email AllClear ID's support center at support@allclearid.com.

What You Can Do

Monitor Your Accounts

You should remain vigilant for incidents of fraud, identity theft, and errors by regularly reviewing your account statements and monitoring free credit reports. If you discover any suspicious or unusual activity on your accounts, be sure to report it immediately to your financial institutions, as major credit card companies have rules that restrict them from requiring you to pay for fraudulent charges that are timely reported.

In addition, you are encouraged to contact the Federal Trade Commission (FTC), or law enforcement to report incidents of suspected identity theft or to learn about steps you can take to protect yourself from identity theft. You can contact the FTC at:

Federal Trade Commission
600 Pennsylvania Avenue, NW
Washington, DC 20580
(877) IDTHEFT (438-4338)
www.identitytheft.gov

If you find that your information has been misused, the FTC encourages you to file a complaint with the FTC and to take these additional steps: (1) close the accounts that you have confirmed or believe have been tampered with or opened fraudulently; and (2) file and keep a copy of a local police report as evidence of the identity theft crime.

Obtain Your Credit Reports

You should also monitor your credit reports. You may periodically obtain credit reports from each nationwide consumer reporting agency. If you discover inaccurate information or a fraudulent transaction on your credit report, you have the right to request that the consumer reporting agency delete that information from your credit report file.

In addition, under federal law, you are entitled to one free copy of your credit report every 12 months from each of the three nationwide consumer reporting agencies. You may obtain a free copy of your credit report by going to www.AnnualCreditReport.com or by calling (877) 322-8228. You also may complete the Annual Credit Report Request Form available from the FTC at <https://www.consumer.ftc.gov/articles/pdf-0093-annual-report-request-form.pdf>, and mail it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. You may also contact any of the three major consumer reporting agencies to request a copy of your credit report.

Place a Fraud Alert or Security Freeze on Your Credit File

In addition, you may obtain information from the FTC and the consumer reporting agencies about fraud alerts and security freezes. A fraud alert can make it more difficult for someone to get credit in your name because it tells creditors to follow certain procedures to protect you, but it also may delay your ability to obtain credit. If you suspect you may be a victim of identity theft, you may place a fraud alert in your file by calling just one of the three nationwide consumer reporting agencies listed below. As soon as that agency processes your fraud alert, it will notify the other two agencies, which then must also place fraud alerts in your file. An initial fraud alert will

last 90 days. An extended alert stays on your file for seven years. To place either of these alerts, a consumer reporting agency will require you to provide appropriate proof of your identity, which may include your Social Security number. If you ask for an extended alert, you will have to provide an identity theft report.

Also, you can contact the nationwide consumer reporting agencies regarding if and how you may place a security freeze on your credit report. A security freeze prohibits a consumer reporting agency from releasing information from your credit report without your prior written authorization, which makes it more difficult for unauthorized parties to open new accounts in your name. However, please be aware that placing a security freeze on your credit report may delay, interfere with, or prevent the timely approval of any requests you make for new loans, credit mortgages, employment, housing or other services. The consumer reporting agencies have three (3) business days after receiving your request to place a security freeze on your credit report. You may be charged to place or lift a security freeze. Unlike a fraud alert, you must separately place a credit freeze on your credit file at each credit reporting company.

You may contact the nationwide consumer reporting agencies at:

Equifax
P.O. Box 105788
Atlanta, GA 30348
(800) 525-6285
www.equifax.com


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

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

Change Your Passwords

If the information affected included your user credentials for an online account, you should change those account settings or take other appropriate steps to protect those online accounts. You should also take steps appropriate to protect all online accounts which use the same user name or email address and password or security question and answer. If you discover any suspicious or unusual activity on your accounts, be sure to report it immediately to your financial institutions.

For More Information

Again, we apologize for any inconvenience caused by this incident. If you have any questions regarding this incident or if you desire further information or assistance please contact AllClear ID Monday through Saturday, 8 a.m. to 8 p.m. Central Time at 1-855-742-6218 or visit .

Sincerely,



Home Box Office, Inc.



IF YOU ARE AN OREGON RESIDENT:

You may report suspected identity theft and obtain information about preventing identity theft from the Oregon Attorney General's Office. This office can be reached at:

Oregon Department of Justice
1162 Court Street NE
Salem, OR 97301-4096
(503) 378-4400
www.doj.state.or.us