Akin Gump
STRAUSS HAUER & FELD LLP

MICHELLE A. REED
+1 214.969.2713/fax: +1 214.969.4343
mreed@akingump.com

February 5, 2020

VIA EMAIL

New Hampshire Office of the Attorney General
Consumer Protection and Antitrust Bureau
33 Capitol Street
Concord, NH 03301
DOJ-CPB@doj.nh.gov

Re: Notice of Data Breach at Altice USA, Inc.

To the New Hampshire Office of the Attorney General:

We are contacting you on behalf of our client, Altice USA, Inc. ("Altice" or "Altice USA"), about a data security incident that occurred on November 4, 2019 to January 2020 and involved the personal information of 13 residents of New Hampshire. The affected New Hampshire residents will be notified of this security incident on February 6, 2020, after your office has received this notification. Please note that in submitting this notice, Altice does not waive any rights or defenses regarding the applicability of New Hampshire law or personal jurisdiction.

What Happened

Altice USA is a communications and media company headquartered at One Court Square, Long Island City, NY 11101. On November 13, 2019, Altice became aware of unusual activity in certain employee email accounts that are held in the cloud in an Office365 platform. Altice immediately launched an investigation to determine what happened and ultimately learned that an unauthorized third party gained access to certain Altice USA employees' email account credentials through a phishing incident. The unauthorized third party then used the stolen credentials to remotely access and, in some instances, download the employees' mailbox contents. In the case of 18 individuals, the unauthorized third party used the credentials to change their direct deposit information. Those individuals were previously notified and had their paychecks promptly reissued.

Upon identifying this incident through Altice's internal controls, Altice secured the email accounts and immediately launched an investigation. As part of its investigation, Altice conducted an in depth review of the email accounts to determine if personal information was

contained in the email accounts. At this point, Altice has determined that the potentially exposed personal information in this incident may have included some combination of the following: name, address, employment information, Social Security number, date of birth, driver's license number. The affected individuals are being notified because their personal information was present in the email accounts.

Altice diligently conducted its investigation into this incident, notified law enforcement, and took steps to identify and remediate the security issue after learning of the email intrusion. Altice retained an expert computer forensics firm to conduct a thorough investigation of the incident and determine additional security measures designed to prevent incidents of this kind in the future. Altice maintains a Written Information Security Program and has a developed Incident Response Plan, which was activated in response to the incident.

Altice also contacted a third-party, Kroll, who assisted with identifying locations for the impacted individuals and who gathered relevant contact information into a consistent format for notification. This investigation was a time-consuming process, but Altice believed it was necessary to ensure appropriate precautions and that next steps were taken.

Steps to Protect Your State Residents

Altice is providing all potentially affected New Hampshire residents with written notice of the incident via U.S. Mail on or about February 6, 2020, after our notice to you. A copy of that notice is attached, excluding any identifying information. Altice is also providing access to free identity theft protection, credit monitoring, identity theft consultation and restoration for one year for affected individuals, and information on how to protect against identity theft and fraud.

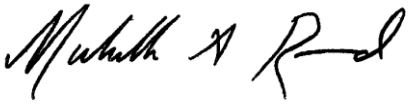
Altice has implemented additional security measures that include, but are not limited to:

- having reset passwords for all compromised accounts to prevent further unauthorized access;
- conducting additional mandatory education to help employees recognize and avoid phishing emails;
- revising internal policies and practices to strengthen our internal security standards; and
- strengthening email system security controls and protocols.

Altice also is working to implement multi-factor authentication and other enhanced authentication protocols.

If you have any further questions regarding this incident, please do not hesitate to contact me either by telephone at (214) 969-2713, or by email at mreed@akingump.com.

Sincerely,



Michelle A. Reed

Enclosure

<<Date>> (Format: Month Day, Year)

<<first_name>> <<middle_name>> <<last_name>> <<suffix>>
<<address_1>>
<<address_2>>
<<city>>, <<state_province>> <<postal_code>>
<<country >>

Notice of Data Breach

Dear <<first_name>> <<middle_name>> <<last_name>> <<suffix>>,

Altice USA takes seriously our commitment to protecting your personal information. Unfortunately, we are contacting you about an email phishing incident that may have involved some of your personal information<<b2b_text_3 (as a former employee of Altice USA, its subsidiaries or predecessor companies Cablevision and Suddenlink)>>. We regret that this incident occurred and apologize for any inconvenience or concern it may cause you. While we have no information at this time that would indicate that your personal information has been misused, below please find details about the incident, information about the complimentary identity and credit monitoring resources we are providing, and additional steps you can take to protect your information.

What happened?

In November 2019, an unauthorized third party gained access to certain Altice USA employees' email account credentials through a phishing incident. The unauthorized third party then used the stolen credentials to remotely access and, in some instances, download the employees' mailbox contents. Upon identifying this incident through our internal controls, we secured the email accounts, engaged an expert computer forensics firm to assist with our investigation, and notified law enforcement.

What information was involved?

During our investigation, we learned in January 2020 that one of the downloaded mailboxes contained a password protected report that contained personal information, including name, employment information, Social Security number, date of birth and, in some instances, driver's license number. <<b2b_text_4 (As a current employee, your personal information was included in this report. / As a former employee, your personal information was included in this report.)>>

What we are doing.

In November 2019 after learning about the phishing incident, we retained an expert computer forensics firm to support our efforts to contain the incident, and to determine the scope of the incident. We also informed federal law enforcement agencies about the incident. While the investigation is ongoing, we continue taking steps to prevent similar situations from happening in the future, including:

- having reset passwords for all compromised accounts to prevent further unauthorized access;
- conducting additional mandatory education to help employees recognize and avoid phishing emails;
- revising internal policies and practices to strengthen our internal security standards; and
- strengthening email system security controls and protocols.

Although we have no evidence that any of your information from this report has been misused to date, in an abundance of caution and to help relieve concerns following this incident, we have secured the services of Experian to provide complimentary identity and credit monitoring services. You are eligible to enroll in Experian IdentityWorks℠ Credit 3B for a period of one year, free of cost. Identity monitoring services available to you include:

- **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, Equifax and Transunion files for indicators of fraud.
- **Experian IdentityWorks Extend CARE™:** Identity Restoration specialists are immediately available to help 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). **NOTE:** this service is immediately available to you and does not require any action on your part. You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired. Be prepared to provide engagement number **<<b2b_text_2 (Engagement Number)>>** as proof of eligibility for the identity restoration services by Experian.
- **$1 Million Identity Theft Insurance**:** Provides coverage for certain costs and unauthorized electronic fund transfers.

All you need to do to take advantage of these services is contact Experian to enroll. Activate IdentityWorks Credit 3B Now in Three Easy Steps

1. ENROLL by: **<<b2b_text_1 (Date as Month Day, Year) >>** (Your code will not work after this date.)
2. VISIT the Experian IdentityWorks website to enroll: **www.experianidworks.com/3bcredit**
3. PROVIDE the Activation Code: **<<Member ID>>**

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 877-288-8057. Your activation code expires at **11:59pm on <<b2b_text_1 (Date as Month Day, Year) >>** and will not work after this date. A credit card is not required for enrollment in Experian IdentityWorks Credit 3B. If you have any questions about IdentityWorks, need help understanding something on your credit report, or suspect that an item on your credit report may be fraudulent, please contact Experian's customer care team at 877-288-8057.

What you can do.

Please review the enclosed "Additional Resources" document which describes additional steps you can take to help protect yourself, including recommendations by the Federal Trade Commission regarding identity theft protection and details on how to place a fraud alert or a security freeze on your credit file.

<<b2b_text_5 (It's also important to always stay vigilant when reviewing emails – in the workplace or on personal email)>> <<b2b_text_6 (– which is why we have a 24/7 employee resource via chat on our internal Service Central or IT Service Desk via phone in case employees have questions or want to verify a communication.)>>

For more information.

Protecting your information remains important to us. If you have any questions please contact our dedicated call center at 1-844-902-2038 between 9:00 a.m. and 6:30 p.m. Eastern Time, Monday through Friday. We regret any inconvenience or concern this may have caused and are continuing to take steps to demonstrate our ongoing commitment to the security of your information.

Sincerely,

Colleen Schmidt
Executive Vice President, Human Resources
Altice USA

* 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.

ADDITIONAL RESOURCES

Contact information for the three nationwide credit reporting agencies is:

Equifax, PO Box 740241, Atlanta, GA 30374, www.equifax.com, 1-800-685-1111

Experian, PO Box 2104, Allen, TX 75013, www.experian.com, 1-888-397-3742

TransUnion, PO Box 2000, Chester, PA 19022, www.transunion.com, 1-800-888-4213

Free Credit Report. It is recommended that you remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring your credit report for unauthorized activity. You may obtain a copy of your credit report, free of charge, once every 12 months from each of the three nationwide credit reporting agencies.

To order your annual free credit report please visit **www.annualcreditreport.com** or call toll free at **1-877-322-8228**.

You can also order your annual free credit report by mailing a completed Annual Credit Report Request Form (available from the U.S. Federal Trade Commission's ("FTC") website at www.consumer.ftc.gov) to:

Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281.

For Colorado, Georgia, Maine, Maryland, Massachusetts, New Jersey, Puerto Rico, and Vermont residents: You may obtain one or more (depending on the state) additional copies of your credit report, free of charge. You must contact each of the credit reporting agencies directly to obtain such additional report(s).

Fraud Alert. You may place a fraud alert in your file by calling one of the three nationwide credit reporting agencies above. A fraud alert tells creditors to follow certain procedures, including contacting you before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit.

Security Freeze. You have the ability to place a security freeze on your credit report.

A security freeze is intended to prevent credit, loans and services from being approved in your name without your consent. To place a security freeze on your credit report, you may be able to use an online process, an automated telephone line, or a written request to any of the three credit reporting agencies listed above. The following information must be included when requesting a security freeze (note that if you are requesting a credit report for your spouse, this information must be provided for him/her as well): (1) full name, with middle initial and any suffixes; (2) Social Security number; (3) date of birth; (4) current address and any previous addresses for the past five years; and (5) any applicable incident report or complaint with a law enforcement agency or the Registry of Motor Vehicles. The request must also include a copy of a government-issued identification card and a copy of a recent utility bill or bank or insurance statement. It is essential that each copy be legible, display your name and current mailing address, and the date of issue.

Federal Trade Commission and State Attorneys General Offices. If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should immediately contact the Federal Trade Commission and/or the Attorney General's office in your home state. You may also contact these agencies for information on how to prevent or avoid identity theft.

You may contact the **Federal Trade Commission**, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580, www.ftc.gov/bcp/edu/microsites/idtheft/, 1-877-IDTHEFT (438-4338).

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

For North Carolina residents: You may contact the North Carolina Office of the Attorney General, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001, www.ncdoj.gov, 1-877-566-7226.

For New York residents, the Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; https://ag.ny.gov/; 1-800-771-7755.

For Connecticut residents: You may contact the Connecticut Office of the Attorney General, 55 Elm Street, Hartford, CT 06106; www.ct.gov/ag; 1-860-808-5318.

For Massachusetts residents: You may contact the Office of the Massachusetts Attorney General, One Ashburton Place, Boston, MA 02108; www.mass.gov/ago/contact-us.html; 1-617-727-8400.

Reporting of identity theft and obtaining a police report.

For Iowa residents: You are advised to report any suspected identity theft to law enforcement or to the Iowa Attorney General.

For Massachusetts residents: You have the right to obtain a police report if you are a victim of identity theft.

For Oregon residents: You are advised to report any suspected identity theft to law enforcement, the Federal Trade Commission, and the Oregon Attorney General.