KILPATRICK TOWNSEND
ATTORNEYS AT LAW

KILPATRICK TOWNSEND & STOCKTON LLP
www.kilpatricktownsend.com

Suite 2800, 1100 Peachtree Street NE
Atlanta, GA 30309-4528
t 404 815 6500 f 404 815 6555

direct dial 404 815 6004
JNeiditz@kilpatricktownsend.com

May 19, 2017

BY ELECTRONIC MAIL doj-cpb@doj.nh.gov

Attorney General Gordon MacDonald
Office of the Attorney General
Attn: Consumer Protection and Antitrust Bureau
33 Capitol Street
Concord, NH 03301

Re: Breach Notification

Dear Attorney Gordon MacDonald:

I am sending this letter on behalf of AT&T pursuant to N.H. Rev. Stat. §§ 359-C:19 et seq. AT&T monitors the security of its online services using state-of-the-art tools that help to detect indicators of unauthorized access. On May 5th, AT&T determined that one of those tools detected an issue involving the drivers' license numbers of up to 78 residents of New Hampshire. It appears that unauthorized person(s) gained access to the ID and password combinations associated with the online accounts of some of those AT&T wireless customers from a source outside of AT&T, likely through malware or phishing. Each driver's license number was displayed on a single page within these accounts. The display of such numbers is contrary to AT&T's standard practice. These instances of unauthorized access likely occurred between January 25th and April 20th.

AT&T promptly locked online access to all known impacted accounts, and assured that drivers' license numbers are no longer displayed in AT&T online accounts, in keeping with AT&T standard practice. AT&T will offer credit and other monitoring, insurance and identity restoration services to all potentially impacted customers in accordance with the attached letter, which will be mailed to each of them on Monday, May 22nd.

Please let me know if you need any additional information.

Sincerely,

Jon Neiditz

Jon Neiditz

cc: AT&T

AT&T

[DATE]

[NAME]
[ADDRESS]
[CITY], [STATE] [ZIP]-[ZIP+4]

RE: Notice of Data Breach

Dear [NAME]:

AT&T's commitments to customer privacy and data security are top priorities, and we take those commitments very seriously. AT&T monitors the security of its online services using state-of-the-art tools that help to detect unusual patterns than may be indicators of unauthorized access. One of those tools may have found an issue involving your personal information and we are letting you know.

What Happened
Our monitoring shows that an unauthorized person may have acquired your att.com ID and password and used these credentials to access your online account. We have found nothing to suggest that the ID and password combinations were obtained from AT&T; they were likely obtained from another source and/or through malware or phishing (discussed below). Your online account was potentially accessed between January 25th and April 20th, 2017.

What Information Was Involved
The potential unauthorized account access may have included a single page on which your driver's license number was visible. Your mobile service and device were not affected.

What Are We Doing
AT&T moved quickly to block the unauthorized activity. For many of you, we already locked your online Access ID. We will continue to monitor your AT&T online account to help protect your information.

As a courtesy, we are offering you one year of free credit monitoring – and access to your credit report – with CSID. **While we have already arranged for payment, you must enroll to start the service.** The attached page provides details about the service, as well as instructions on how to enroll online using the CSID PIN code at the top of this letter. If you have questions or concerns, please contact CSID at 877.274.5554 where specialists are ready to assist you.

What You Can Do
You may have previously received one or more communications from us notifying you that we locked your online Access ID. If you have not already done so please reset your password online at att.com. You can also add an extra security passcode to your account or unlock your Access ID by calling 877.285.3194.

Scammers use many ways to steal your private information such as usernames, passwords, and credit card information. Two common methods are through "malware" or a "phishing" scam.

Malware is malicious software that may have been downloaded to your computer. It records keystrokes and is often spread through email attachments or hidden within what appears to be legitimate programs. Phishing is a trick used to gather information through fake emails, text messages and websites. Scammers usually provide links to web pages that are disguised to look identical to a legitimate site in order to trick victims to provide their private information. AT&T does not solicit sensitive personal information through email or text messages.

You may also want to consider contacting the major credit reporting agencies to place a fraud alert on your credit report, and to learn about identity theft programs offered by the Federal Trade Commission. Details on how to contact the credit reporting agencies and FTC can also be found on the attached pages.

Thank you,

Deno Hairston
AVP – AT&T Digital Experience
CSID ProtectorSM

After you complete registration for CSID's service, that AT&T is providing for you at no charge, you will have increased visibility into any possible fraudulent activity so you can respond more quickly if such activity is detected. You will also have an insurance policy of up to $1,000,000 in coverage should you experience identity theft, and an Identity Restoration team to guide you through the recovery process. You must complete registration before [MM/DD/YYYY-90 days from date of letter] to take advantage of CSID Protector Service.

Enrollment is conducted online at www.CSID.com/attcustomercare or by calling CSID at 877.274.5554 using your CSID "PIN Code" shown at the top of the first page of this letter. This PIN Code can only be used once and cannot be transferred to another individual. Once you have provided your PIN Code, you will be prompted to answer a few security questions to authenticate your identity: previous addresses, names of creditors and payment amounts.
Should you have any questions regarding the service or the sign-up process, please contact CSID's Customer Care Center at 877.274.5554, 24 hours per day, or e-mail support@CSID.com. Once you have enrolled and set your User Name and Password, you will return to CSID's page to log in and access your personal information on future visits.

CSID Protector Includes:

- **Single Bureau Credit Report and Monitoring:** Includes credit inquiries, delinquencies, judgments and liens, bankruptcies, new loans and more.
- **Court Record Monitoring**: Looks for actions that might fraudulently link your name, birth date and/or Social Security number to criminal and court records.
- **Public Records Search:** Looks for names and addresses affiliated with your Social Security number, address history and any changes to the same.
- **Non-Credit Loans:** Searches for short-term, high-interest payday loan activity that doesn't require a credit inquiry.
- **Internet Surveillance:** Monitors Web sites, chat rooms and bulletin boards for criminal selling or trading of your personal information online using CSID's CyberAgent® technology.
- **ID Theft Insurance:** $1,000,000 insurance policy with $0 deductible.
- **Restoration Services:** Full-service Identity Theft Restoration experts will act on your behalf to restore your credit and identity while you get on with your life.
- **Social Media Monitoring:** CSID's Social Media Monitoring alerts you of privacy and reputational risks on the four major social networks - Facebook, Twitter, LinkedIn and Instagram.
- **Bank Account/Financial Account Takeover:** Financial Account Takeover alerts you if your personal information has been used to open a new credit card, apply for a new credit card, open a new bank account, or make changes to an existing bank account.
- **Change of Address:** This service reports if your mail has been redirected through the US Postal Service.
- **SSN Trace:** CSID's Social Security Number Trace service provides you with a report of all names and aliases associated with your Social Security number, and notifies you if a new one is added.

Fraud Alerts
In addition to completing CSID Protector registration, AT&T strongly suggests that you contact the fraud departments of any one of the three major credit reporting agencies and let them know you may have potentially experienced identity theft. That agency will notify the other two. Through that process, a "fraud alert" will automatically be placed in each of your three credit reports to notify creditors not to issue new credit in your name without gaining your permission. Contact:

Equifax	Experian	TransUnion™
P.O. Box 740241	P.O. Box 2002	P.O. Box 6790
Atlanta GA 30374	Allen, TX 75013	Fullerton, CA 92834
877.478.7625	888.397.3742	800.680.7289
www.fraudalerts.equifax.com	www.experian.com	www.transunion.com

We also encourage you to carefully review your credit report(s). Look for accounts you did not open and inquiries from creditors that you did not initiate. Also review your personal information for accuracy, such as home address and Social Security number. If you see anything you do not understand or that is inaccurate, call the credit reporting agency at the telephone number on the report. If you find suspicious activity on your credit reports or bank account, call your local police or sheriff's office and file a police report of identity theft. Get a copy of the police report. You may need copies of the police report to clear your personal records. You can also request information from the agencies about the option of placing a security freeze on your credit reports.

Learn about the FTC's identity theft programs at www.ftc.gov/bcp/edu/microsites/idtheft or call the FTC's toll-free Identity Theft helpline: 877.ID.THEFT (877.438.4338); TTY: 866.653.4261. The FTC is headquartered at 600 Pennsylvania Avenue, NW Washington, DC 20580.

Credit Freezes: You may have the right to put a credit freeze, also known as a security freeze, on your credit file, so that no new credit can be opened in your name without the use of a PIN number that is issued to you when you initiate a freeze. A credit freeze is designed to prevent potential credit grantors from accessing your credit report without your consent. If you place a credit freeze, potential creditors and other third parties will not be able to get access to your credit report unless you temporarily lift the freeze. Therefore, using a credit freeze may delay your ability to obtain credit. In addition, you may incur fees to place, lift and/or remove a credit freeze. Credit freeze laws vary from state to state. The cost of placing, temporarily lifting, and removing a credit freeze also varies by state, generally $5 to $20 per action at each credit reporting company. Unlike a fraud alert, you must separately

place a credit freeze on your credit file at each credit reporting company. Since the instructions for how to establish a credit freeze differ from state to state, please contact the three major credit reporting companies as specified below to find out more information:

Equifax	Experian	TransUnion, LLC
P.O. Box 105788	P.O. Box 9554	P.O. Box 2000
Atlanta GA 30348	Allen, TX 75013	Chester, PA 19022-2000
www.equifax.com	www.experian.com	www.transunion.com

You can obtain more information about fraud alerts and credit freezes by contacting the FTC or one of the national credit reporting agencies listed above.