[redacted]

[redacted]

April 20, 2015

Via Email and UPS
The Honorable Attorney General Joseph Foster
New Hampshire Department of Justice
33 Capitol St.
Concord, NH 03301
DOJ-CPB@doj.nh.gov

**Re: Privacy Incident**

Dear Attorney General Foster:

At the conclusion of its investigation, on or about June 5, 2014, AT&T notified you and all affected New Hampshire customers regarding a data breach that occurred in Mexico. As you may have recently heard, AT&T and the FCC entered into a Consent Decree relating to that Mexico breach, as well as to data breaches at vendor call centers in Colombia and the Philippines that involved the same type of suspicious activity. These incidents occurred at different call centers and involved different vendor employees, but the purpose of each appears to have been the same, *i.e.*, to obtain customers' names, telephone numbers and the last four digits of their social security numbers for the purpose of obtaining a device unlock code. We have concluded the investigations regarding certain vendor call center data breaches in Colombia and the Philippines, and hereby provide you with information regarding those incidents.

Our investigation of the Colombia and Philippines breaches revealed that approximately 80 total New Hampshire residents were affected, 17 of whom *may* have had their full social security number accessed. Attached are sample notifications we will send to all of the New Hampshire residents affected by the Colombia and Philippines breaches, with an offer of free credit monitoring services for one year.

As we shared with the FCC, AT&T has determined that a small number of vendor employees' inappropriately accessed AT&T customer accounts in an apparent effort to obtain codes that are used to "unlock" recycled AT&T mobile phones so that those devices can be activated with other telecommunications providers. Because AT&T devices are programed to our network, the device must be recalibrated to another network when it changes carriers. Prior to December 2014, AT&T only provided unlock codes to current and former customers. Limited customer information, including the information referenced above, was necessary to request and obtain such a code.

It is important to note that this activity did not impact the devices of the customers whose accounts were accessed. And while any misuse of customer information is serious, **we have no reason to believe that the information was used for any other purpose, including for identity theft or financial fraud against our customers.** Indeed, for the majority of customers, no sensitive personal information was visible when the account was accessed by the vendor employees. And although full social security numbers were accessible for 17 New Hampshire residents, we have no evidence that full social security numbers were acquired or used for any inappropriate purpose.

Protecting customer privacy is critically important to us. AT&T has taken steps to mitigate the possibility of similar incidents occurring in the future, including changing its device unlock policy so that

customer information is no longer needed to obtain a device unlock code. This change in policy eliminates the incentive to misuse customer information to obtain an unlock code. We also are enhancing our existing security measures and developing new security measures to help prevent these types of situations in the future, including as outlined in the Consent Decree. Moreover, we are terminating vendor sites where these incidents occurred, as appropriate.

If you have any questions regarding this matter, please contact me.

Sincerely,

[redacted]

Enclosure

[Date]

CSID PIN code: [XXXXXXXXXX]

[Name]
[Address]
[City], [State] [Zip]

***Re: Important Notice – Privacy Incident***

Dear [Name]:

AT&T's commitments to customer privacy and data security are top priorities, and we take those commitments very seriously. As part of an ongoing investigation, we determined that your account was accessed without authorization in violation of AT&T's privacy and security policies between February and July, 2014. AT&T believes your account was accessed as part of an effort to request codes that allow phones programmed for the AT&T Network to be used on other networks. **This activity did not affect your AT&T mobile device(s).** While there is no evidence that information related to telecommunications services that you purchase from AT&T, known as Customer Proprietary Network Information or CPNI (e.g., type of service or quantity of service), has been acquired, AT&T is offering you one year of free credit-monitoring. We have also confirmed that no sensitive personal information was accessed or acquired such as Social Security Number or Credit Card Information.

As noted above, to help address any inconvenience this may cause, 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 about this CSID offering, please contact CSID at 877.274.5554 where specialists are ready to assist you.

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 page.

To strengthen your account security, we recommend that if you currently have a passcode on your account, you change it. If you do not have a passcode on your account, we recommend you add one. The passcode will be required when you speak with an AT&T representative on the phone or in a retail store, or to access your account online. You can change or add a passcode online at att.com or by calling the number below. AT&T has also changed policies and strengthened operations to mitigate the possibility of similar incidents occurring in the future.

Protecting customer privacy is critical to AT&T and we value your business. If you have any questions, please contact us at 800.438.5678 (select option 1, then option 2), weekdays between 8 a.m. and 6 p.m. (Eastern time).

Sincerely,

Peter F. Diaz
Director – Consumer Centers Sales & Service

**CSID Protector℠**

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. AT&T encourages you to complete registration as quickly as possible before September 30, 2015 to take advantage of CSID Protector Service.

Enrollment is conducted online at www.CSID.com/attcustomercare1 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.

**Fraud Alerts**

In addition to completing CSID Protector enrollment, 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. You can also request information from the agencies about the option of placing a security freeze on your credit reports. Contact:

| Equifax | Experian | TransUnion™ |
|---|---|---|
| P.O. Box 740241<br>Atlanta GA 30374<br>To report fraud call:<br>877.478.7625<br>Website: www.fraudalerts.equifax.com | P.O. Box 2002<br>Allen, TX 75013<br>To report fraud call:<br>888.397.3742<br>Website: www.experian.com | Post Office Box 6790<br>Fullerton, CA 92834<br>To report fraud call:<br>800.680.7289<br>Website: 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.

**Learn about the FTC's identity theft programs at http://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.**

at&t

[Date]

CSID PIN code: [XXXXXXXXXX]

[Name]
[Address]
[City], [State] [Zip]

***Re: Important Notice – Privacy Incident***

Dear [Name]:

AT&T's commitments to customer privacy and data security are top priorities, and we take those commitments very seriously. As part of an ongoing investigation, we determined that your account was accessed without authorization in violation of AT&T's privacy and security policies between February and July, 2014. AT&T believes your account was accessed as part of an effort to request codes that allow phones programmed for the AT&T Network to be used on other networks. **This activity did not affect your AT&T mobile device(s).** While there is no evidence that your Social Security Number or information related to telecommunications services that you purchase from AT&T, known as Customer Proprietary Network Information or CPNI (e.g., type of service or quantity of service), has been acquired, such information was contained in the system accessed and thus AT&T is offering you one year of free credit-monitoring.

As noted above, to help address any inconvenience this may cause, 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 about this CSID offering, please contact CSID at 877.274.5554 where specialists are ready to assist you.

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 page.

To strengthen your account security, we recommend that if you currently have a passcode on your account, you change it. If you do not have a passcode on your account, we recommend you add one. The passcode will be required when you speak with an AT&T representative on the phone or in a retail store, or to access your account online. You can change or add a passcode online at att.com or by calling the number below. AT&T has also changed policies and strengthened operations to mitigate the possibility of similar incidents occurring in the future.

Protecting customer privacy is critical to AT&T and we value your business. If you have any questions, please contact us at 800.438.5678 (select option 1, then option 2), weekdays between 8 a.m. and 6 p.m. (Eastern time).

Sincerely,

Peter F. Diaz
Director – Consumer Centers Sales & Service

**CSID Protector℠**

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. AT&T encourages you to complete registration as quickly as possible before September 30, 2015 to take advantage of CSID Protector Service.

Enrollment is conducted online at www.CSID.com/attcustomercare1 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.

## Fraud Alerts

In addition to completing CSID Protector enrollment, 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. You can also request information from the agencies about the option of placing a security freeze on your credit reports. Contact:

| Equifax | Experian | TransUnion™ |
|---|---|---|
| P.O. Box 740241<br>Atlanta GA 30374<br>To report fraud call:<br>877.478.7625<br>Website: www.fraudalerts.equifax.com | P.O. Box 2002<br>Allen, TX 75013<br>To report fraud call:<br>888.397.3742<br>Website: www.experian.com | Post Office Box 6790<br>Fullerton, CA 92834<br>To report fraud call:<br>800.680.7289<br>Website: 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.

**Learn about the FTC's identity theft programs at http://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.**