at&t

*Jennifer Shasha Kay*
*General Attorney*

AT&T Services, Inc.
150 West Flagler Street
Suite 1910
Miami, FL 33130

T: (305) 347-5332
F: (305) 375-0209
Jennifer.kay@att.com

June 5, 2014

Attorney General Joseph Foster
New Hampshire Department of Justice
33 Capitol Street
Concord, New Hampshire, 03301

Re: Data Security Incident

Dear Attorney General Foster:

Pursuant to New Hampshire Rev. Stat. Ann. Section 359-C:20, this letter is to notify you of a breach of security of personal information impacting one resident of New Hampshire.

AT&T recently determined that employees of one of our call center service providers violated our strict privacy and security guidelines by accessing AT&T customer accounts without authorization. Our investigation revealed that between April 9 and 21, 2014, these individuals accessed the account of one New Hampshire resident, enabling them to view the resident's social security number and possibly date of birth, as well as Customer Proprietary Network Information ("CPNI"). AT&T believes these individuals accessed the account as part of an effort to request codes from AT&T that are used to "unlock" AT&T mobile phones in the secondary mobile phone market so that those devices can then be activated with other telecommunications providers. This activity did not impact the New Hampshire resident's AT&T device(s) and the service provider terminated the employment of these individuals in connection with this incident.

Pursuant to New Hampshire law and FCC regulations, AT&T plans to notify the one New Hampshire resident of this incident on or about June 10, 2014, using the form attached and will offer free credit monitoring services for one year. AT&T notified the FBI of the CPNI breach on May 20, 2014.

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

Sincerely,

Jennifer S. Kay

Enclosure

cc: Nancy J. Hertel, Esq., AT&T Legal Department

13075 Manchester Rd.
Des Peres, MO 63131

[Date] CSID PIN code: [XXXXXXXXXX]

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

***Re: Important Notice – Misuse of Personal Identifying Information and Access to CPNI***

Dear [Name]:

AT&T's commitments to customer privacy and data security are top priorities, and we take these commitments very seriously. We recently determined that employees of one of our service providers violated our strict privacy and security guidelines by accessing your account without authorization between April 9 and 21, 2014, and, while doing so, would have been able to view your social security number and possibly your date of birth. AT&T believes the employees accessed your account as part of an effort to request codes from AT&T that are used to "unlock" AT&T mobile phones in the secondary mobile phone market so that those devices can then be activated with other telecommunications providers. **There is no impact to your AT&T mobile device(s) in connection with this activity.**

Additionally, while in your account, these individuals would also have been able to view your Customer Proprietary Network Information (CPNI) without proper authorization. CPNI is information related to the telecommunications services you purchase from us. On behalf of AT&T, please accept my sincere apology for this incident. Simply stated, this is not the way we conduct business, and as a result, our service provider has notified us that these individuals no longer work for them. AT&T and the service provider are also taking additional steps to mitigate the possibility of similar incidents occurring in the future, including further restricting access to sensitive personal information.

To help address any inconvenience this may cause, we're taking the following steps:

1) 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; and,

2) We have notified federal law enforcement concerning the unauthorized access of your CPNI as required by the Federal Communications Commission regulations. Our report to law enforcement does not contain specific information about your CPNI; only that the unauthorized access occurred.

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.

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.

Once again, please accept my apology for this incident. 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,

Brian E. Woolverton
Director – Consumer Centers Sales & Service

 WTM-CM

**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, 2014 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.

**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. Contact:

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