

Telephone: (425) 383-5687 Fax: (425) 383-6290

PLEASE SUBMIT THIS FORM TO ALL THREE (3) STATE AGENCIES as follows:

Fax this form to:

CPB:
Security Breach Notification-
Fax: 518-474-2474

NYS Office of Cyber Security and Critical Infrastructure Coordination (CSCIC):

30 South Pearl St.
Floor P2
Albany, NY 12207
Fax: 518-474-9090

and also **Fax & Mail** this form to:

Attorney General:

Asst. Attorney General in Charge
Bureau of Consumer Frauds
120 Broadway - 3rd Floor
New York, NY 10271
Fax: 212-416-6003

Reporting Form
For Business, Individual or NY State Entity reporting a
"Breach of the Security of the System"
Pursuant to the Information Security Breach
and Notification Act (General Business Law §889-aa;
State Technology Law §208)

Name of Business, Individual or State Entity T-Mobile USA, Inc.
Date of Discovery of Breach: September 29, 2006
Estimated Number of Affected Individuals: 45,000
Date of Notification to Affected Individuals: October 14, 2006
Manner of Notification: written notice
 electronic notice (email)
 telephone notice

Are you requesting substitute notice? Yes No (If yes, attach justification)

Content of Notification to Affected Individuals: Describe what happened in general terms and what kind of information was involved. Please attach copy of Notice.

 While recently traveling on business, a T-Mobile employee's laptop which may have contained certain sensitive employee information, was lost. The loss of this laptop occurred after the luggage containing the laptop was placed into checked baggage, sometime after the Transportation Security Administration performed an inspection of the bag. On September 29th, the T-Mobile employee informed the internal investigation team that this laptop *may have contained* employee Social Security number information, together with names, addresses and salary information. From computer back-up files, it cannot be ascertained for certain whether Social Security number information was *actually* included on the laptop. Nonetheless, out of an abundance of caution, we are notifying our employees who may have been affected by this potential breach in the security of their personal information. Nonetheless, out of an abundance of caution, we intend to send the enclosed notification on October 14, 2006, to 45,000 of our employees, including 923 employees who are New York residents, who may have been affected by this potential breach.

Name of Business or Individual Contact Person: Pamela
Henderson
Title: Corporate Counsel for Privacy
Telephone number: (425) 383-5687
Email: Pamela.Henderson3@T-Mobile.com

Dated: October 13, 2006
Submitted by: Pamela
Henderson
Title: Corporate Counsel for
Privacy
Address: 12920 SE 38th Street, Bellevue, WA 98006
Email: Pamela.Henderson3@T-Mobile.com



T-Mobile USA, Inc.
12920 SE 38th Street, Bellevue, WA 98006

October 14, 2006

Re: INCD2006-10-00358

Dear T-Mobile Employee:

I am writing to inform you about the loss of a T-Mobile laptop that contained certain sensitive employee information. While recently traveling on business, an employee from the Human Resources department checked his luggage, which included his laptop, at the airport. When the employee picked up his luggage at the destination airport, the laptop was missing. At the time this occurred, it was promptly reported to T-Mobile, the airline, the local police department, and to the Transportation Security Administration (the "TSA"), and an investigation was initiated.

Despite our exhaustive efforts and investigations with the TSA, the airports, and the airlines, the laptop has not yet been located. We continue to take aggressive steps to locate and recover and will keep you informed of any important changes or developments.

What You Need To Know

We have no reason to believe that any employee information has been improperly accessed. As with all T-Mobile laptops, this laptop and its contents are protected by a security logon and password.

In conducting our investigation, we have learned that the laptop may have contained certain sensitive employee information including data such as name, address, home phone number, Social Security number, date of birth, and compensation information. There is no indication that credit card information, driver's license numbers, or customer information was on the laptop.

Most importantly, I want to express our deep regret and apology for this incident. We take very seriously the protection of your personal information. Human Resources has a very specific policy about the storage of sensitive information on laptops that unfortunately was not followed in this case. We are treating this seriously, and have taken, and will continue to take, additional steps to ensure sensitive data is protected.

Precautionary Measures In Place

We are taking specific precautionary steps to help protect you. We have partnered with Experian[®] to provide you with a full year of a credit monitoring service at no cost to you, which also includes unlimited access to your credit report. Again, we have no reason to believe your information has been improperly accessed or impacted. This is merely a precautionary measure we are taking to further protect the integrity of your personal data.

This credit monitoring service, "Credit ManagerSM" will identify and notify you of any key changes that may be a sign of Identity Theft. Your complimentary benefits under this protection plan will include:

- Unlimited access to your Experian Credit Report and Credit Score
- Monitoring of your Experian Credit Report EVERY DAY
- Email or SMS Text alerts when key changes are identified
- Identity Theft insurance [up to \$50,000] provided by Virginia Surety Company, Inc.
- Identity Theft assistance from dedicated Fraud Resolution Representatives
- Membership expires one year after activation

To obtain your Credit ManagerSM benefits, please visit <http://partner.consumerinfo.com/tmobile> and enter the code provided below, *disregarding any pricing information*. You will not be charged for this service, and you will be instructed on how to initiate your online membership. Your personal reference code is: [insert code]. You must activate your credit monitoring service within 180 days from the date of this letter.

For further information about this incident, please visit the T-Mobile OneVoice Intranet site at <http://onevoice.internal.t-mobile.com/laptop> . The information on the site may help to answer any questions you have regarding this incident. If, after visiting OneVoice, you still have additional questions, please contact 1-877- 213-1050.

Again, we sincerely apologize for this unfortunate incident and fully recognize the trust you put in our organization. We will continue to do our utmost to maintain that trust.

Sincerely,



Manny Sousa
Senior Vice President, Human Resources and Chief People Officer
T-Mobile USA