U.S. Cellular

June 27, 2017

Sent via UPS OVERNIGHT

The Honorable Attorney General Joseph Foster
New Hampshire Department of Justice
33 Capitol St.
Concord, NH 03301

Dear Attorney General Foster,

On behalf of United States Cellular Corporation ("U.S. Cellular"), I wish to provide your office with notice under New Hampshire's data breach law.

Unauthorized individuals attempted to access U.S. Cellular's online user accounts starting in April 2017 by trying various login and password combinations using automated attacks. U.S. Cellular suspects this activity was due to large breaches at other companies (not associated with the U.S. Cellular website), in which user login names and passwords were stolen. At present, all indications are that the U.S. Cellular database of customer user names and passwords remains safe and that our cyber defenses repelled the majority of the attacks.

Unfortunately, it has become evident that some online user accounts were accessed by unauthorized individuals and that information contained in the accounts included the customer's name, Social Security Number, address, and cellular telephone number(s) as well as information about the customer's wireless services including the service plan, usage and billing statements.

U.S. Cellular estimates that approximately 1,852 customers were affected by this incident. On June 27, 2017, U.S. Cellular began notifying the approximately 47 New Hampshire residents who may have been affected by this incident. As a precautionary measure, U.S. Cellular is providing 12 months of free credit monitoring and identity theft insurance to individuals who may have been affected by this incident, as described in the attached notice template enclosed with this letter.

U.S. Cellular has encouraged its customers to change their passwords and instituted additional technical controls on its website to further protect customer information. We take this incident very seriously and have notified law enforcement and the Federal Communications Commission.

If you have any questions or need further information, please do not hesitate to contact me.

Respectfully submitted,

Barbara Kern

Barbara Kern
Director - Privacy and Senior Counsel
(773) 399-4109

U.S. Cellular

June , 2017

[customer name]
[customer address]

RE: U.S. Cellular Account #

Notice Of Data Breach

Dear [customer's first name],

U.S. Cellular values you as a customer and is committed to protecting your privacy. We take this responsibility seriously and it is for this reason that **we need to share with you information regarding a recent incident.**

What happened?

We recently detected some unusual activity concerning your My Account login. Unauthorized individuals began using login and password combinations in April 2017 on My Account and we have been monitoring our systems. This type of attack indicates that the hackers obtained user names and passwords from a third-party source and attempted to confirm the validity of the login information by using them on My Account. It appears that your My Account has been accessed by hackers as a result of this attack. U.S. Cellular has found no evidence that U.S. Cellular's systems were the source of the login and password combinations used by the unauthorized individuals.

What Information Was Involved?

As indicated above, your user name and password which were used to access your My Account have been compromised. Your My Account contains your Social Security number, name, address, and cellular telephone number(s) as well as information about your wireless services including your service plan, usage and billing statements known as Customer Proprietary Network Information ("CPNI"). If you stored payment information in My Account, such as credit card information, the information is masked and only the last four digits are visible.

If you are a former customer, once you have cancelled your service, My Account allows access only to the Billing & Payments page which includes billing statements for the previous 16 months.

What is U.S. Cellular Doing?

If you are a current U.S. Cellular customer, we expired your password to protect your information, and when you login to your account again (if you have not already), you will have to choose a different password. If you are a former customer, we have disabled your My Account so that login is no longer enabled. U.S. Cellular has introduced additional technical controls to protect My Account from unauthorized access. Additionally, U.S. Cellular reported the incident to law enforcement in accordance with the requirements of the Federal Communications Commission as well as certain state agencies.

What You Can Do

We encourage you to **reset your My Account password** by visiting My Account, dialing 611 from your U.S. Cellular phone (always a free call), calling 1-888-944-9400, or visiting your nearest U.S. Cellular retail store and presenting a valid government issued photo ID.

If you are a former customer, we have already disabled your account from being accessed and no further action is required.

We are also offering you credit monitoring services for 12 months. Included is the instruction sheet with your unique activation code for Equifax® Credit Watch™ Gold with 3-in-1 Credit Monitoring. Your unique activation code is [insert code]. **You have until December 31, 2017 to activate this code before it expires.**

Other Important Information

This situation presents an opportunity to increase the level of security on your account as well as other accounts to ensure that your information is protected. To the extent you have used the same user name and password for other online accounts, you should consider updating those user names and passwords. With regard to your U.S. Cellular account, in the interests of caution, you should consider changing your PIN on your account by visiting a U.S. Cellular retail store or contacting Customer Service at 1-888-944-9400.

We would also like to take this opportunity to encourage you to remain vigilant about reviewing your account statements and monitoring your other online accounts and credit reports over the next 12 months. Promptly report any incidents of suspected identity theft to your credit card company and the credit bureaus. Contact information for the three credit bureaus is included below.

We also have included an attachment listing additional steps you may wish to consider taking at any time if you ever suspect that you may have been the victim of identity theft. We offer this out of an abundance of caution so that you have information that may be helpful to you.

We apologize for this incident and any inconvenience it may have caused. Your confidence in our ability to safeguard your personal information and your peace of mind are very important to us.

Sincerely,

cc:

Important Identity Theft Information: Additional Steps You Can Take to Protect Your Identity

The following are additional steps you may wish to take to protect your identity.

Review Your Accounts and Credit Reports

Regularly review statements from your accounts and periodically obtain your credit report from one or more of the national credit reporting companies.

You may obtain a free copy of your credit report online at www.annualcreditreport.com by calling toll free 1.877.322.8228, or by mailing an Annual Credit Report Request Form (available at www.annualcreditreport.com) to: Annual Credit Report Request Service. P.O. Box 105281, Atlanta, GA, 30348-5281. You may also purchase a copy of your credit report by contacting one or more of the three national credit reporting agencies listed below.

- **Equifax**, P.O. Box 740241, Atlanta, Georgia 30374-0241. 1.800.685.1111. www.equifax.com
- **Experian**, P.O. Box 9532, Allen, TX 75013, 1.888.397.3742. www.experian.com
- **TransUnion**, 2 Baldwin Place, P.O. Box 1000, Chester, PA 19016. 1.800.916.8800. www.transunion.com

Consider Placing a Fraud Alert

You may wish to consider contacting the fraud department of the three major credit bureaus to request that a "fraud alert" be placed on your file. A fraud alert notifies potential lenders to verify your identification before extending credit in your name.

Equifax:	Report Fraud:	1.800.766.0008
Experian:	Report Fraud:	1.888.397.3742
TransUnion:	Report Fraud:	1.800.680.7289

Security Freeze for Credit Reporting Agencies

You may wish to request a security freeze on your credit reports. A security freeze prohibits a credit reporting agency from releasing any information from a consumer's credit report without written authorization. However, please be aware that placing a security freeze on your credit report may delay, interfere with, or prevent the timely approval of any requests you make for new loans, credit mortgages, employment, housing or other services. If you have been a victim of identity theft, and you provide the credit reporting agency with a valid police report, it cannot charge you to place, lift or remove a security freeze. In all other cases, a credit reporting agency may charge you up to $10.00, (or in certain states no more than $5.00), each to place, temporarily lift, or permanently remove a security freeze.

To place a security freeze on your credit report, you must send a written request to each of the three major consumer reporting agencies by regular, certified or overnight mail at the following addresses:

- Equifax Security Freeze, P.O. Box 105788, Atlanta, GA 30348
- Experian Security Freeze, P.O. Box 9554, Allen, TX 75013

- TransUnion Security Freeze, Fraud Victim Assistance Department, 2 Baldwin Place, P.O. Box 1000, Chester, PA 19016

To request a security freeze, you will need to provide the following:

- Your full name (including middle initial, Jr., Sr., Roman numerals, etc.),
- Social Security number
- Date of birth
- Address(es) where you have lived over the prior five years
- Proof of current address such as a current utility bill
- A photocopy of a government-issued ID card
- If you are a victim of identity theft, include a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft
- If you are not a victim of identity theft, include payment by check, money order, or credit card (Visa, MasterCard, American Express or Discover only). Don't send cash through the mail.

The credit reporting agencies have three business days after receiving your request to place a security freeze on your credit report. The credit bureaus must also send written confirmation to you within five business days and provide you with a unique personal identification number (PIN) or password, or both that can be used by you to authorize the removal or lifting of the security freeze.

To lift the freeze to allow a specific entity or individual access to your credit report, you must call or send a written request to the credit reporting agencies by mail and include (1) proper identification (name, address, and Social Security number), (2) the PIN number or password provided to you when you placed the security freeze; and (3) the identities of those entities or individuals you would like to receive your credit report or the specific period of time you want the credit report available. The credit reporting agencies have three business days after receiving your request to lift the security freeze for those identified entities or for the specified period of time.

To remove the security freeze all together, you must send a written request to each of the three credit bureaus by mail and include proper identification (name, address, and Social Security number) and the PIN number or password provided to you when you placed the security freeze. The credit bureaus have three business days after receiving your request to remove the security freeze.

Suggestions if You Are a Victim of Identity Theft

- File a police report. Get a copy of the report to submit to your creditors and others that may require proof of a crime.
- Contact the U.S. Federal Trade Commission (FTC). The FTC provides useful information to identity theft victims and maintains a database of identity theft cases for use by law enforcement agencies. File a report with the FTC by calling the FTC's Identity Theft Hotline: 1- 877-IDTHEFT (438-4338); online at http://www.ftc.gov/idtheft; or by mail at Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Ave., N.W., Washington, D.C. 20580. Also request a copy of the publication, "Take Charge: Fighting Back Against Identity Theft" from http://www.ftc.gov/bcp/edu/pubs/consumer/idtheft/idt04.pdf.

- Keep a record of your contacts. Start a file with copies of your credit reports, the police reports, any correspondence, and copies of disputed bills. It is also helpful to keep a log of your conversations with creditors, law enforcement officials, and other relevant parties.

Take Steps to Avoid Identity Theft

Further information can be obtained from the FTC about steps to take to avoid identity theft through the following paths: http://www.ftc.gov/idtheft; calling 1-877-IDTHEFT (438-4338); or write to Consumer Response Center, Federal Trade Commission, 600 Pennsylvania Ave., N.W., Washington, D.C. 20580.

Maryland residents can learn more about preventing identity theft from the Maryland Office of the Attorney General, by visiting their web site at http://www.oag.state.md.us/idtheft/index.htm, calling the Identity Theft Unit at 410.567.6491, or requesting more information at the Identity Theft Unit, 200 St. Paul Place, 16th Floor, Baltimore, MD 21202.

North Carolina residents can learn more about preventing identity theft from the North Carolina Office of the Attorney General, by visiting their web site at http://www.ncdoj.gov/Help-for-Victims/ID-Theft-Victims.aspx, calling 919.716.6400 or requesting more information from the North Carolina Attorney General's Office, 9001 Mail Service Center Raleigh, NC 27699-9001.

Vermont residents may learn helpful information about fighting identity theft, placing a security freeze, and obtaining a free copy of your credit report on the Vermont Attorney General's website at http://www.atg.state.vt.us.

EQUIFAX®

Activation Code: **INSERT Credit Monitoring Code**

About the Equifax Credit Watch™ Gold with 3-in-1 Monitoring identity theft protection product

Equifax Credit Watch will provide you with an "early warning system" to changes to your credit file and help you to understand the content of your credit file at the three major credit-reporting agencies. Note: You must be over age 18 with a credit file in order to take advantage of the product.

Equifax Credit Watch provides you with the following key features and benefits:

- Comprehensive credit file monitoring and automated alerts of key changes to your **Equifax, Experian**, and **TransUnion** credit reports [3]
- Wireless alerts and customizable alerts available (available online only)
- One 3-in-1 Credit Report and access to your Equifax Credit Report™
- Up to $1 million in identity theft insurance [1] with $0 deductible, at no additional cost to you
- 24 by 7 live agent Customer Service to assist you in understanding the content of your Equifax credit information, to provide personalized identity theft victim assistance and in initiating an investigation of inaccurate information.
- 90 day Fraud Alert [2] placement with automatic renewal functionality* (available online only)

How to Enroll: You can sign up online or over the phone

To sign up online for **online delivery** go to www.myservices.equifax.com/tri

1. Welcome Page: Enter the Activation Code provided at the top of this page in the "Activation Code" box and click the "Submit" button.
2. Register: Complete the form with your contact information (name, gender, home address, date of birth, Social Security Number and telephone number) and click the "Continue" button.
3. Create Account: Complete the form with your email address, create a User Name and Password, check the box to accept the Terms of Use and click the "Continue" button.
4. Verify ID: The system will then ask you up to four security questions to verify your identity. Please answer the questions and click the "Submit Order" button.
5. Order Confirmation: This page shows you your completed enrollment. Please click the "View My Product" button to access the product features.

To sign up for **US Mail delivery**, dial 1-866-937-8432 for access to the Equifax Credit Watch automated enrollment process. Note that all credit reports and alerts will be sent to you via US Mail only.

1. Activation Code: You will be asked to enter your enrollment code as provided at the top of this letter.
2. Customer Information: You will be asked to enter your home telephone number, home address, name, date of birth and Social Security Number.
3. Permissible Purpose: You will be asked to provide Equifax with your permission to access your credit file and to monitor your file. Without your agreement, Equifax cannot process your enrollment.
4. Order Confirmation: Equifax will provide a confirmation number with an explanation that you will receive your Fulfillment Kit via the US Mail (when Equifax is able to verify your identity) or a Customer Care letter with further instructions (if your identity can not be verified using the information provided). Please allow up to 10 business days to receive this information.

Directions for placing a Fraud Alert

A fraud alert is a consumer statement added to your credit report. This statement alerts creditors of possible fraudulent activity within your report as well as requests that they contact you prior to establishing any accounts in your name. Once the fraud alert is added to your credit report, all creditors should contact you prior to establishing any account in your name. To place a fraud alert on your credit file, visit: www.fraudalerts.equifax.com or you may contact the Equifax auto fraud line at 1-877-478-7625, and follow the simple prompts. Once the fraud alert has been placed with Equifax, a notification will be sent to the other two credit reporting agencies, Experian and Trans Union, on your behalf.

1 - Identity Theft Insurance underwritten by insurance company subsidiaries or affiliates of American International Group, Inc. 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.. This product is not intended for minors (under 18 years of age)

2 - The Automatic Fraud Alert feature made available to consumers by Equifax Information Services LLC and fulfilled on its behalf by Equifax Consumer Services LLC

3 - Credit monitoring from Experian® and Transunion® will take several days to begin