U.S. Cellular

October 24, 2017

Sent via UPS Overnight

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

Dear Attorney General Foster:

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

As we previously disclosed on June 27, 2017 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.

In our first notice, we explained that there was evidence that some online user accounts were accessed by unauthorized individuals and that information contained in the accounts included the customer's name, address, and cellular telephone number(s) as well as information about the customer's wireless services including the service plan, usage and billing statements, and for some user accounts, customers' Social Security numbers. In the course of conducting additional investigation relating to the incident, we discovered that ACH information, consisting of bank account numbers and routing numbers, also may have been exposed. While there is no direct evidence of exfiltration, we are notifying potentially impacted individuals out of an abundance of caution. U.S. Cellular is offering 12 months of credit monitoring services as a precautionary measure.

Accordingly, U.S. Cellular will be providing an updated notice to all individuals affected by this incident. Since we last contacted your office, we conducted a third-party address check for the customer notice letters, and determined that there approximately 62 individuals within New Hampshire, which is 15 more than we previously notified you.

We have also become aware of an error in the formulation of the original mailing list and determined that we actually provided notice to only a portion of these individuals that we intended to notify. Therefore, on October 24, 2017, we will be providing a second notice letter to all individuals whose ACH information was affected, and will be providing a comprehensive notice to all individuals that did not receive the initial letter. We have attached an updated sample notice letter. Consistent with our previous estimate, U.S. Cellular estimates that approximately 1,852 customers were affected by this incident.

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

Respectfully submitted,

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

U.S. Cellular

October 24, 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 notified you that we had detected some unusual activity concerning your My Account login and that it appeared that your My Account had been accessed by hackers as a result of an attack. The facts about the attack and our successful response to stop the attack are unchanged.

As we previously explained, 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 indicated that the hackers had 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.

What Information Was Involved?

We recently learned that bank account and routing numbers for direct deposit may have been accessible during this attack. Although this information initially appeared to be obfuscated, it has come to our attention that it may have been possible for a hacker to view this information.

We had previously notified you that your user name and password may have been used to access your My Account information, including 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"). We would like to reiterate that 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.

Out of an abundance of caution, we are offering a complimentary one-year membership of Experian IdentityWorks^{SM} Credit 3B. This product helps detect possible misuse of your personal information and provides you with identity protection services focused on immediate identification and resolution of identity theft. IdentityWorks Credit 3B is completely free to you and enrolling in this program will not hurt your credit score. For more information on identity theft prevention and IdentityWorks Credit 3B, including instructions on how to activate your complimentary one-year membership, please see the additional information provided in this letter.

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.

While we don't believe that the information available in My Account could lead to identity theft, 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: File

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:	1.888.766.0008
Experian:	Report Fraud:	1.888.397.3742
TransUnion:	Report Fraud:	1.800.916.8800

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 such as Massachusetts, 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.

You have rights under the federal Fair Credit Reporting Act (FCRA). These include, among others, the right to know what is in your file; to dispute incomplete or inaccurate information; and to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information. For more information about the FCRA, please visit www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf or www.ftc.gov.

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 (1.877.438.4338); 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 (1.877.438.4338); or write to Consumer Response Center, Federal Trade Commission, 600 Pennsylvania Ave., N.W., Washington, D.C. 20580.

Iowa residents may contact law enforcement or the Iowa Attorney General's Office to report suspected incidents of identity theft. This office can be reached at: Office of the Attorney General, Hoover State Office Building, 1305 E. Walnut Street, Des Moines, IA 50319, www.iowaattorneygeneral.gov, (515) 281-5164.

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 1.410.567.6491, or requesting more information at the Identity Theft Unit, 200 St. Paul Place, 16th Floor, Baltimore, MD 21202.

Massachusetts residents are reminded that you have the right to obtain a police report and request a security freeze as described above. The consumer reporting agencies may charge you a fee of up to $5 to place a security freeze on your account, and may require that you provide certain personal information (such as your name, Social Security Number, date of birth and address) and proper identification (such as a copy of a government-issued ID card and a bill or statement) prior to honoring your request. There is no charge, however, to place, lift or remove a security freeze if you have been a victim of identity theft and you provide the consumer reporting agencies with a valid police report.

New Mexico residents are reminded that you have the right to obtain a police report and request a security freeze as described above and you have rights under the Fair Credit Reporting Act as described above.

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 1.919.716.6400 or requesting more information from the North Carolina Attorney General's Office, 9001 Mail Service Center Raleigh, NC 27699-9001.

Oregon residents may obtain information about preventing identity theft from the Oregon Attorney General's Office. This office can be reached by mail at Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, online at www.doj.state.or.us, by phone at (503) 378-4400.

Rhode Island residents are reminded that you have the right to obtain a police report and request a security freeze as described above. The consumer reporting agencies may charge you a small fee to place a security freeze on your account, and may require that you provide certain personal information (such as your name, Social Security Number, date of birth and address) and proper identification (such as a copy of a government-issued ID card and a bill or statement) prior to honoring your request. There is no charge, however, to place, lift or remove a security freeze if you have been a victim of identity theft and you provide the consumer reporting agencies with a valid police report. Residents can learn more by contacting the Rhode Island Office of the Attorney General by phone at 1.410.274.4400 or by mail at 150 South Main Street, Providence, Rhode Island 02903.

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.

To help protect your identity, we are offering a **complimentary** one-year membership of Experian IdentityWorks[SM] Credit 3B. This product helps detect possible misuse of your personal information and provides you with superior identity protection support focused on immediate identification and resolution of identity theft.

Activate IdentityWorks Credit 3B Now in Three Easy Steps

1. ENROLL by: **January 31, 2018** (Your code will not work after this date.)
2. VISIT the **Experian IdentityWorks website** to enroll: https://www.experianidworks.com/3bcreditone
3. PROVIDE the **Activation Code**: **[INSERT CODE]**

If you have questions about the product, need assistance with identity restoration or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at 877-288-8057. Be prepared to provide engagement number **DB03832** as proof of eligibility for the identity restoration services by Experian.

ADDITIONAL DETAILS REGARDING YOUR 12-MONTH EXPERIAN IDENTITYWORKS CREDIT 3B MEMBERSHIP:

A credit card is **not** required for enrollment in Experian IdentityWorks Credit 3B.

You can contact Experian **immediately without needing to enroll in the product** regarding any fraud issues. Identity Restoration specialists are available to help you address credit and non-credit related fraud.

Once you enroll in Experian IdentityWorks, you will have access to the following additional features:

- **Experian credit report at signup:** See what information is associated with your credit file. Daily credit reports are available for online members only.*
- **Credit Monitoring:** Actively monitors Experian, Equifax and Transunion files for indicators of fraud.
- **Experian IdentityWorks ExtendCARE**[TM]: You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- **$1 Million Identity Theft Insurance**:** Provides coverage for certain costs and unauthorized electronic fund transfers.

Activate your membership today at https://www.experianidworks.com/3bcreditone
or call 877-288-8057 to register with the activation code above.

What you can do to protect your information: There are additional actions you can consider taking to reduce the chances of identity theft or fraud on your account(s). Please refer to www.ExperianIDWorks.com/restoration for this information. If you have any questions about IdentityWorks, need help understanding something on your credit report or suspect that an item on your credit report may be fraudulent, please contact Experian's customer care team at 877-288-8057.

* Offline members will be eligible to call for additional reports quarterly after enrolling.

** Identity theft insurance is underwritten by insurance company subsidiaries or affiliates of American International Group, Inc. (AIG). 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.