



STATE OF NH
DEPT OF JUSTICE

2021 JAN 25 PM 1:29

January 22, 2021

Sent Via UPS DELIVERY

Consumer Protection Bureau
Office of the Attorney General
33 Capitol Street
Concord, NH 03301

Dear Attorney General MacDonald,

On behalf of USCC Services, LLC (d/b/a UScellular), I wish to provide your office with notice under New Hampshire's data breach law.

On January 6, 2021, pursuant to a customer complaint of unauthorized porting of a wireless number, UScellular detected a data security incident in which unauthorized individuals gained access to wireless customer accounts that contain personal information. An employee in a retail store was successfully scammed by an unauthorized individual and downloaded software onto a store computer. Since the employee was already logged into the customer retail management ("CRM") system, the downloaded software allowed the unauthorized individual to remotely access the store computer and enter the CRM system under the employee's credentials. Based on our investigation, we believe that the incident occurred on January 4, 2021.

Information in customer accounts include name, address, PIN code and cellular telephone number(s) as well as information about wireless services including service plan, usage and billing statements. Sensitive personal information, such as Social Security number and credit card information, is masked within the CRM system.

Upon discovery of the incident, UScellular immediately removed the computer with the downloaded software from accessing the internet and then permanently removed it from use in the retail store. The login credentials for every employee impacted in this incident at that retail store were reset. In addition, UScellular immediately changed the impacted customers' PIN and security question/answer.

UScellular determined that approximately 276 customers were affected by this incident. On January 22, 2021, UScellular began notifying the twenty-three (23) New Hampshire residents who may have been affected by this incident. The customer notification letter is attached which explains how impacted customers can establish new PIN and security question/answer and encourages them to remain vigilant and contact UScellular if they have concerns about the validity of a communication that appears to be from us.

We take this incident very seriously and have reported the incident to law enforcement in accordance with the requirements of the Federal Communications Commission as well as certain state agencies.

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

Respectfully submitted,

Danielle Denkmann

Danielle Denkmann
Counsel, Legal and Regulatory Affairs
(773) 399-7529



January 21, 2021

[customer name]
[customer address]

RE: UScellular Account #

Notice of Data Breach

Dear [customer's first name],

UScellular 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 and the steps that UScellular is taking to safeguard your personal information.

What happened?

On January 6, 2021, we detected a data security incident in which unauthorized individuals may have gained access to your wireless customer account and wireless phone number. A few employees in retail stores were successfully scammed by unauthorized individuals and downloaded software onto a store computer. Since the employee was already logged into the customer retail management ("CRM") system, the downloaded software allowed the unauthorized individual to remotely access the store computer and enter the CRM system under the employee's credentials. We believe the incident occurred on January 4, 2021.

What Information Was Involved?

As indicated above, your customer account was impacted in this incident. Information in your customer account includes your name, address, PIN code 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"). Your sensitive personal information, such as Social Security number and credit card information, is masked within the CRM system. At this time, we have no indication that there has been unauthorized access to your UScellular online user account ("My Account").

What is UScellular Doing?

We took immediate measures to prevent this information from being accessed in the future by this unauthorized individual to prevent fraudulent activity on your account. We immediately removed the computer with the downloaded software from accessing the internet and then permanently removed it from use in the retail store. We also had the login credentials for employees impacted in this incident at that retail store reset. Also, we immediately changed your and your Authorized Contacts' PIN and security question/answer. Additionally, UScellular reported the incident to law enforcement in

accordance with the requirements of the Federal Communications Commission as well as certain state agencies.

To establish a new PIN and security question/answer, you must contact us. When you do so, you will be asked to establish a new PIN and security question/answer. You may also establish a new PIN and security question/answer for each of your Authorized Contacts, or you may have your Authorized Contacts contact us separately to establish their PIN and security question/answer.

What You Can Do

You should also remain vigilant against phishing schemes, and if you have any concerns about the validity of a communication that appears to be from us, you can contact Customer Service at 1-888-944-9400. This is the Federal Trade Commission's page to help you recognize a phishing scam. <https://www.consumer.ftc.gov/articles/how-recognize-and-avoid-phishing-scams#recognize>.

If you have any concerns about your online account, out of an abundance of caution, you can always reset your My Account password by visiting My Account. You must also contact us to change your PIN on your UScellular My Account and your security question/answer. You are encouraged to create a strong PIN by avoiding sequences, repetition, and mirroring personal information, such as social security numbers or date of birth. Please note that neither you or your Authorized Contacts will be able to discuss account information over the phone with us until you or your Authorized Contacts establish new PINs and security questions/answers. You or your Authorized Contacts may contact us by dialing 611 from your UScellular phone (always a free call), calling 1-888-944-9400, or visiting your nearest UScellular retail store and presenting a valid government issued photo ID.

Other Important Information

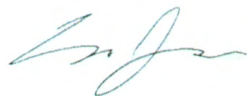
This situation presents an opportunity to increase the level of security on your account as well as other accounts to ensure that your information is protected. To the extent that you have used the same user name and passwords for other online accounts, you should consider updating those user names and passwords.

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 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,



Eric Jagher
Senior Vice President, Retail Sales and Operations

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 at 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, GA 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 customer’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 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/idtheft04.pdf>.
- Keep a record of your contacts. Start a file with copies of your credit reports, the police reports, and 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.

- Oregon residents report to state Attorney General. Oregon residents who suspect they have been the victim of identity theft should file a report with the Oregon Attorney General at 877-877-9392.

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.

North Carolina residents can learn more about preventing identity theft from the North Carolina Office of the Attorney General, by visiting their website at <https://ncdoj.gov/protecting-consumers/protecting-your-identity/>, calling 919-716-6000, or requesting more information from the North Carolina Attorney General's Office, 9001 Mail Service, Raleigh, NC 27699-9001.

Oregon residents may learn helpful information about reporting suspected identity theft from the Oregon office of the Attorney General, by visiting their website at <https://www.doj.state.or.us/consumer-protection/> or calling 877-877-9392.