November 9, 2022

[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 October 31, 2022, we detected a data security incident in which unauthorized individuals may have illegally gained accessed to a retail store's billing system which allowed the individuals to view certain information regarding your wireless customer account. The incident occurred between October 29, 2022 through October 31, 2022.

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 billing 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 type of incident in the future, as well as took measures to prevent fraudulent activity on your account. We immediately reset the login credentials for impacted employees, and we changed your and your Authorized Contacts' PIN and security question/answer. Lastly, 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 888-944-9400. This is the Federal Trade Commission's page to help you recognized 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 **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 username and passwords for other online accounts, you should consider updating those usernames 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.

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,

Barbara Kern
Sr. Director, Privacy and Legal Affairs

cc: File