Dear Robert,

We are sorry to hear about the recent breach of security in your mobile communications and are happy to be able to work with you to resolve this issue so that sensitive information cannot unintentionally be sent to people outside of your choosing. We have developed an encryption system that will allow text messages that are sent from company cellular phones to be encrypted so that if someone were to intercept or see the text message in its coded form it would appear to just be garbled gibberish. We have limited the encryption key so that it can be processed by most mobile devices and will output a message with equal character length to the message that is sent to avoid unnecessary charges from sending multiple messages.

We would like to introduce you to a form of the encryption method commonly known as the Vigenère Cipher. The general idea is that first an encryption key of length 4 is chosen; this will be done by the program that is being designed by your engineers and not manually. A key length 4 means that 4 numbers (from 0-25) are chosen randomly by our program and placed in sequence. For example 2 16 4 20. We choose from 0-25 to represent how far each letter will be shifted forward in the alphabet. Through this encryption method we will move the 1st, 5th, 9th… and every 4th letter thereafter forward in the alphabet by the amount shown in the first space of the encryption key (in our example 2). We will then move the 2nd, 6th, 10th, and again every 4th letter thereafter forward in the alphabet in the same manner (in our example 16). We will then move the rest of the letters forward according to the specific encryption key given. The output is sent in all capital letters, and the receiving mobile device electronically receives the encryption key and will decrypt the message for that specific device only. For the sake of a simple example, if we wanted to send the text message “The dog ran” and we used our example encryption key (2 16 4 20), we would take “t”, “o”, and “n” and move them all forward two
letters in the alphabet. “Vhe dQg raP”. We apply the process for the second number in our encryption key and the output is “VXe dQW raP”. We apply the process for the remaining two numbers in our encryption key and the output is “VXI XQW VUP”. As shown, the text appears meaningless to any potential observer, and in addition it is difficult to deduce the encryption key because there are $26^4$ or about half of a million possible keys.

This encryption system will allow you to send messages securely without the fear of other parties that might accidentally receive such information being able to utilize it. By using this form of the Vigenère Cipher you will be able to send and receive encrypted text messages via mobile devices, by moving each letter of the message being sent forward in the alphabet by a certain amount. These keys are easily generated and can be decrypted by the computer program that is being developed by your engineers. In this way we are happy to help ensure that confidential information cannot accidentally be sent to unauthorized persons.