Group B

09/10/15

From the best IMC team: [redacted]

To: ORCAI

The Sasquatch Cipher

We were sorry to hear about the potential disaster that could happen to your company with sensitive information being sent to wrong recipients. However, we were excited at the opportunity to create a completely unique and practically unbreakable cipher for your company in order to ensure security of this important information. In fact, this cipher is so good, it is easier to spot Sasquatch than it is to crack the cipher; hence the name.

First we will explain the key to the cipher. The key has two components that are separated by a period (i.e. 123.1, the first component being "123" and the second component being "1"). First, we will address the first component of the key.

The first part of the key will be given as any random number that is up to 9, unique digits composed of integers 1 to 9. For example: "123", "47892", or "159". Remember, the first part of the key cannot consist of any repeated integers such as "115," "3345," or "777777."

Next, we use each digit of the first part of the selected key, in order, one at a time, and assign them to the first few letters of the alphabet. Example: for the key whose first part "742," we assign A-7, B-4, C-2. Next, we proceed to go back to the next smallest integer and assign it to the next letter. So we return to our example and we would assign D-1. We simply count upwards, and assign each integer to the next letter. Remember however, once an integer has already been assigned to a letter, you may not use that integer again. Simply skip it and use the next highest integer. Thus in our example, E-3 (since C-2), F-5, G-6, and so on and so forth until

you reach the letter Z. We will then assign the next highest integer to [ ] (space, being able to have spaces between the words in our plain-text message).

Example: Key is 485.3 (NOTE: we have only covered the "485" component of our key)

A-4, B-8, C-5, D-1, E-2, F-3, G-6, H-7, I-9, J-10, K-11, L-12, M-13, N-14, O-15, P-16, Q-17, R-18, S-19, T-20, U-21, V-22, W-23, X-24, Y-25, Z-26, [ ]-27.

We can then express a phrase by assigning each letter and space to its' corresponding number and separating each number by a period in order to keep the order.

Example (using the key above):

plaintext: Josh Bundy should not be confused with Ted Bundy.

after assigning plaintext to integers:

10.15.19.7.27.8.21.14.1.25.27.19.7.15.21.12.1.27.14.15.20.27.8.2.27.5.15.14.3.21.19.2.1.27.23.9.20.7.27.20.2.1.27.8.21.14.1.25

Once we have assigned each plaintext letter to a corresponding number, we use the second component of our cipher key. We will proceed to send each number through a quadratic equation in the form of x^2+b, the second component of our key representing b in the equation. In the example above, the second component of our key is "3" so the equation through which we will send each number is x^2+3.

Example (continuing from above)

final ciphertext:

103.228.364.52.732.67.444.199.4.628.732.364.52.228.444.147.4.732.199.228.403.732.67.7.732.28.228.199.12.444.364.7.4.732.532.84.403.52.732.403.7.4.732.67.444.199.4.628

Thus, once we have a ciphertext and the key, in order to decipher the message we would go backwards, taking the inverse of the equation and assigning each letter of the alphabet to its' corresponding number, based on the first component of the key.

We can assure you that this cipher is very secure and will help your company succeed in all of their endeavors by keeping their trade secrets and important information safe and in the right hands. Good luck!