Recently, our debit cards have been subjected to brute force attacks. Our fraud monitoring system is doing its job and flagging these attempts, trying to prevent future fraudulent activity from occurring.

It is important to note that **your account and personal information have not been compromised** and we are working diligently to correct this issue. If you have any questions on brute force attacks, please read the FAQs below or call us at 402-391-5838 or 712-242-1055 to speak with a representative. After hours, please call the fraud department number, 833-462-0798

What is happening?

The fraudsters have found a partial number associated with the credit union's debit card batch and they are using this partial number along with random numerical strings to guess at full card numbers, expiration dates, and 3-digit security codes. **The fraudsters do not have the cardholder's name, phone**

number, address, or PIN. They are simply trying to guess at card numbers and expiration dates to find a match.

What is a brute force attack?

Brute force attacks are typically small fraudulent transactions, often under $30.00, where the attacker will keep running different card numbers until it comes back approved. The fraudsters are trying to guess card numbers and expiration dates in addition to the 3-digit security code or the cardholder's ZIP code. They start with one random card number and keep incrementing the card numbers, looking for a match based on the guesses. The fraudsters perform a flood of thousands of random attempts, looking for just one success.

Why am I getting a phone call or text about possible fraud?

Our fraud monitoring system sees the suspicious attempts and follows up with a text or call the cardholder just to be sure it really is not a legitimate transaction. This just means that our fraud monitoring system has done its job to prevent fraudulent activity from occurring. It is not very likely the fraudsters will try again on that card once the transaction has been blocked. They will likely move on to guess other card numbers looking for a successful match.

Is a brute force attack a card compromise?

No. The card numbers in the attacks were **not obtained from a compromise.** The fraudsters are simply guessing card numbers and the card expiration dates. If a fraudulent transaction did post to your account, we would recommend replacing your debit card to avoid further fraud attempts. Otherwise, if you have not seen any fraudulent transaction attempts, there is little risk for you to keep that same card.

What happens when there is a successful fraud transaction hit?

When the fraudsters get a successful hit on a debit card, they try to use that card information to make large internet purchases before the bank and the account owner notice the activity.

What should I do next?

Review your recent activity and if you see anything that is suspicious, please contact us immediately.