The media recently announced that a hacker gained access to more than 100 million Capital One customer accounts and credit card applications earlier this year. Not too long ago, Equifax was in the hot seat as well. With more breaches surfacing, we consider this a great opportunity to remind everyone of how stolen cardholder information is used to commit fraud. Below are some tips to keep your information safe – even when dealing with someone you may think is from MMFCU.

- A text alert from us warning of suspicious activity on your card will NEVER include a link to be clicked. Never click on a link in a text message that is supposedly from us. A valid notification will provide information about the suspect transaction and ask the cardholder to reply to the text message with answers such as 'yes', 'no', 'help', or 'stop'. It will never include a link.

- A text alert in relation to debit card transactions or online/mobile banking transactions will always be from a 5-digit number and NOT a 10-digit number resembling a phone number. Text caller IDs will be 37268 for debit card transactions and 454545 for online/mobile banking related items.

- A phone call from MMFCU's automated system will only include a request for your zip code, and no other personal information, unless you confirm that a transaction is fraudulent. If you confirm that a transaction is fraudulent, you are transferred to an agent who will ask questions to confirm that you are the actual cardholder before going through your transactions with you. If at any point you are uncertain about questions being asked or the call itself, hang up and call us directly. If a call is received by the cardholder, claiming to be our call center and asking to verify transactions, no information should have to be provided by the cardholder other than their zip code, and a 'yes' or 'no' to the transaction provided.

- We will NEVER ask you for your PIN or the 3-digit security code on the back of your card. Don't give them out to anyone, no matter what they say. Hang up and call us directly. Fraudsters will often ask cardholders to verify fake transactions. When the cardholder says no, they did not perform those transactions, the fraudster then says that their card will be blocked, a new card will be issued, and that they need the card's PIN to put it on the new card. Many people believe this and provide their PIN. The 3-digit CV2 code on the back of the card will allow a fraudster to conduct card-not-present transactions.

- Regularly check your account online or through our mobile app to see if there are any suspicious transactions that have occurred, but especially If you are unsure about a call or text message you've received. If anything looks amiss, call us directly for assistance.

- If you have received a voicemail or a text-message from us and are unsure about responding to it, call us directly for assistance.