Sound
FEDERAL CREDIT UNION

Cardholder Fraud Education

We want to remind everyone how stolen cardholder information is used to commit fraud. We have included tips below about keeping information safe — even when dealing with someone you think is from a financial institution. Fraudsters have become increasingly adept at getting cardholders to share the information they need to commit fraud by posing as financial institution call center agents, or by sending text messages that look like they are coming from a financial institution, warning of suspicious transaction activities. They are also known to call in to call centers posing as cardholders requesting changes to card information and parameters. Fraudsters use information stolen through data breaches (at health insurance providers, reward program providers, credit bureaus, merchant terminals, and social media sites, to mention just a few recent ones) as well as through malware programs deployed on personal computers and other sources. Stolen personally identifiable information (PII) is combined with stolen card information, resulting in sufficient information to create profiles that fraudsters can use to position themselves as the actual cardholders.

To avoid compromising personal information, note this information:

• A text alert from Fiserv to cardholders warning of suspicious activity on their card will NEVER include a link to be clicked. Cardholders should never click on a link in a text message that is supposedly from Fiserv. A valid notification from Fiserv 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,' and will never include a link.

• A text alert from Fiserv will always be from a 5-digit number and NOT a 10-digit number resembling a phone number. Text caller IDs will be 20733 if you use the standard call center, or 37268 if you use the premium call center.

• A phone call from Fiserv's automated dialer will only include a request for a cardholder's Zip code, and no other personal information, unless they confirm that a transaction is fraudulent. Only then will they be transferred to an agent who will ask questions to confirm their identity before going through their transactions. If at any point a cardholder is uncertain about questions being asked or the call itself, hang up and call Sound directly. If a cardholder receives a call claiming to be the Fiserv call center, 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.

• Fiserv will NEVER ask for the PIN or the 3-digit security code on the back of a card.

• Posing as call center agents, 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 on the new card. Many people believe this and provide their PIN.

• Regularly check your account(s) online for suspicious transactions, but especially if unsure about a call or text message received. If anything looks amiss, call Sound directly for assistance.

• If a cardholder has received a voice or a text message from Fiserv's fraud call center and is unsure about responding to it, call Sound directly for assistance.

If you have any questions please give us a call at 1.833.SoundFCU (1.833.768.6332) and we'll be happy to help.