We are aware that some of our local merchants have reported that the ever-present identity thieves have been at work around the area. As always we encourage our members and the general public to stay alert to how you use your debit and credit cards. Here are some smart tips from ftc.gov:

Limit what you carry. Take only the ID, credit cards, and debit cards you need. Leave your Social Security card at home. If you've got a Medicare card, make a copy to carry and blot out all but the last four digits on it.

Know the deal with public Wi-Fi. Many cafés, hotels, airports, and other public places offer wireless networks — or Wi-Fi — you can use to get online. Two things to remember:

- **Wi-Fi hotspots often aren't secure.** If you connect to a public Wi-Fi network and send information through websites or mobile apps, the info might be accessed by someone it's not meant for. If you use a public Wi-Fi network, send information only to sites that are fully encrypted and avoid using apps that require personal or financial information. Researchers have found many mobile apps don't encrypt information properly.
- **That Wi-Fi network might not belong to the hotel or airport.** Scammers sometimes set up their own "free networks" with names similar to or the same as the real ones. Check to make sure you're using the authorized network before you connect.

Protect your smartphone. Use a password or pin, and report a stolen smartphone — first to local law enforcement authorities, and then to your wireless provider. In coordination with the Federal Communications Commission (FCC), the major wireless service providers have a stolen phone database that lets them know a phone was stolen and allows remote "bricking" so the phone can't be activated on a wireless network without your permission. Find tips specific to your operating system with the FCC Smartphone Security Checker at fcc.gov.

ATMs and gas stations may have skimming devices. Scammers use cameras, keypad overlays, and skimming devices — like a realistic-looking card reader placed over the factory-installed card reader on an ATM or gas pump — to capture the information from your card's magnetic strip without your knowledge and get your PIN.

Watch that laptop. If you travel with a laptop, keep a close eye on it — especially through the shuffle of airport security — and consider carrying it in something less obvious than a laptop case.

For our Bronco members – If you're ever concerned with any of your Bronco accounts or services, please feel free to call any of the following: during business hours call 757.569.6000; after hours for debit cards call 800.554.8969, after hours for credit cards call 800-325-3678.