

Prevent fraud this back-to-school season

Back-to-school season means more purchases, often by students using the credit and debit cards given to them by their parents. As your account holders send their children off to school, give them these tips to help avoid both real and “friendly fraud” on their accounts.

Be cautious of public Wi-Fi, computers and chargers

- Advise students to avoid public networks and computers whenever possible and to be mindful of the information they enter if they must be used. If students don't have access to a private network, suggest they use a virtual private network when entering sensitive information which is often provided to students through their school.
- Tell family members not to use public charging stations, even if they're in a seemingly secure area like the student union or library. Fraudsters can tamper with these stations and use them to collect information.

Protect important numbers and passwords

- Help students memorize numbers like PINs, credit and debit card numbers, driver's license number and Social Security number rather than writing them down or storing them on a device. The more places these numbers are stored, the greater the risk of being stolen.
- Tell them to use a different strong, unique password for each of their accounts. If a fraudster hacks their social media account, they won't also have the password to access their university or online banking account.
- Have them switch up their responses to security questions by creating fake answers that only they know. Because information like pet names, hometown or a parent's maiden name are now more easily accessible online, these answers don't always provide security.
- Make sure your student uses an access password on their phone. This prevents unwanted or unauthorized access to information your student may store there.

Monitor activity and beware of “friendly fraud”

- When a student is using a card in their parent's name, both parties should sign up to receive alerts for that card, like those available if you're using SHAZAM BOLT\$. Contact your financial institution for a similar service.
- “Friendly fraud” can occur when a friend or family member makes a purchase on your account without your knowledge. When you give your child a card in your name, have them check in with you whenever they make a purchase so true fraudulent charges can be identified. In the end, it's your responsibility to ensure your child isn't using your card to make any unwanted purchases.

While these tips are great for students, they're helpful practices for all cardholders. Implement these steps today to protect your accounts from fraud — friendly or otherwise.