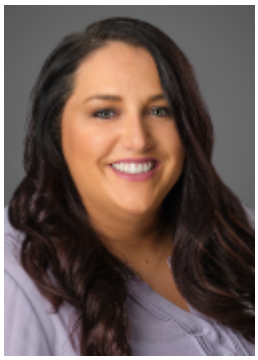

Back-to-School Scams

Helpful Tips to Protect Members

By Savanna Osborne, Certified Fraud Examiner (CFE), Analyst, Compliance

August 17, 2022

Back-to-school season is around the corner, and for some, it's already well underway! As students begin returning to school, it is important to remain vigilant and be aware of the various back-to-school scams that malicious actors are conducting during this time of year. We encourage you to review the different types of scams below and share them with your members.

With technology being a key to any classroom – especially since the pandemic – many students and parents are looking to buy new laptops and tablets. But beware of the scammers!

The best things to do are:

- Shop reputable retailers.
- Beware of deals that seem "too good to be true." This is especially true if the seller is offering a hard-to-find item for cheap given the technology shortages we are currently experiencing.
- If the brand or retailer typically does not have sales, proceed with caution when you see a sale price and make sure to research the website before purchasing
- Amazon and eBay often have third-party sellers.

In addition, beware of back-to-school giveaways! Again, if it sounds "too good to be true," it is probably a scam. Most email giveaways will request the victim to visit a website where you will then be asked to provide your email address to claim your prize. However, once you

provide your information, you will begin receiving countless emails, texts and robocalls, with no giveaway prize.

IRS scams happen all the time, but they are even more common right before the start of a new school year. Scammers will impersonate an IRS agent, calling college-bound students to inform them of their failure to pay student taxes, making it seem like this will restrict their access to attending college and cause them to potentially face jail time.
Rest assured that:

- There are no “student taxes”.
- IRS agents will not initiate contact with a taxpayer through phone calls.
- IRS agents will not demand payment via prepaid debit cards or wire transfers.

Schooling is expensive and tuition continues to increase, whether it’s private school or college. That’s why scholarship scams are so prevalent. The victim will typically receive an email or text offering a free scholarship in exchange for paying a redemption or disbursement fee. This is a scam! Legitimate scholarships do not require you to pay a fee and also do not solicit applications.
Another related technique is paying a small fee for government student loans or financial aid. There is no fee to apply for government student loans or financial aid. Rather, you can apply for free help at **FAFSA® Application | Federal Student Aid**.
Want to erase all student debt loans? This is a scam! Scammers will email or text students and parents promising to reduce or erase student debt altogether for a small fee. After the victim wires the funds, the scammer will disappear, and the victim is out the fee money and is stuck with the student loan responsibility.

Additionally, the scammers may even ask for personal or financial information to begin the loan-forgiveness process. Once the scammer receives this personal information, they will use it to their benefit (i.e., take out loans, apply for credit cards, access the victim’s bank account(s), or use the credit card to make fraudulent purchases).
What to do in these situations:

- RESEARCH! Do not work with private loan companies promising to help eliminate or reduce your student loans. Instead, find a reputable loan provider to help create a payment plan with a more attainable interest rate and monthly fee.
- Do not pay a fee for debt relief. Legitimate companies do not charge you for these services.

Beware of fake test-prep companies! Scammers will send emails to parents of students claiming their child ordered test-prep materials. They will then request a credit card to

process payment for the order. The victim's child never ordered these materials and now the fraudster has access to your credit card to make unauthorized charges.

What to do in these situations:

- Do not give your credit card information to any individual or company that calls, texts or emails with a payment request. Call the company's customer service number found on a reputable website to confirm the order before proceeding.
- Research any company claiming to be a test-prep company by entering their name and "scam" or "complaint" in the search engine to verify there are no reports of fraudulent behavior.

Beware of parking meters utilizing QR codes for payment. This has been a huge lure for fraudsters, especially on college campuses. After the QR code is scanned, it redirects users to a website for payment where they are prompted to enter their credit card information and it will display an approved message. However, they now have access to your credit card information and will begin making unauthorized payments.

What to do in this situation:

- Don't scan QR codes from people you don't know.
- Confirm who you are sending/receiving the code from.
- Check for tampering.

Flying back to college? Beware of fake text or email cancellations! Recently, there has been an uptick in flight cancellations, so of course fraudsters have found a way to use this to their advantage. They will send an email or text message stating the flight has been cancelled and to call the number provided. When calling that number, the caller will be instructed to rebook their flight for a fee to make sure the flight is not cancelled or changed. However, the flight was never cancelled, so they are out the fee and the fraudster made some easy money.

What to do in these situations:

- Double check your email or text and make sure it matches your flight details.
- Call the phone number on your original confirmation link from when you booked the flight.

For additional fraud prevention tips and information, feel free to contact Alloya's Compliance Department at **compliance@alloyacorp.org**.