Top Ten Student Fraud Prevention Tips

1. Get your free credit report at **annualcreditreport.com.** Each year you may receive 1 free creditreport from each of the 3 credit reporting agencies (TransUnion, Equifax or Experian). Upon receipt, check for unauthorized accounts, inquiries and unknown addresses.
2. Register to access your Social Security benefits statement at www.ssa.gov. Upon receipt, reviewyour estimated benefits and earnings record. You should also ensure no one is using your Social Security number for employment or other benefits.
3. Know who you are paying, via person to person payments, i.e., Zelle, Venmo, etc. Pay and receive money only with people you know. Don't pay strangers with P2P (Person to Person).Most "person to person" transactions are instantaneous and irreversible.
4. Do not pay for merchandise online or via the phone using a debit card. Debit cards are vulnerable because they are linked to a bank account. You have a far better chance of resolvinga fraudulent transaction when paying with a credit card rather than with a debit card. Also do not provide your debit/credit card numbers over the phone, via emails or on websites unless you initiated the call or order.
5. Keep thorough records. If your laptop is stolen, can you provide a full description to the police?Write down your computer's make, model, color and most importantly the unique serial number, which acts as a key identifier, much like the vehicle identification number (VIN) on a car. You might also need this information to file an insurance claim.
6. Do not use an ATM machine if you notice wires or a skimming device attached to where you insert your card. Also, cover the keypad with your hand, a hat or other piece of clothing wheninputting pin numbers. Notify the bank or local police if you observe device(s) attached to theATM.
7. Do not make a debit card purchase without first verifying the account balance. Most financial institutions will allow the transaction to process through even when you don't have enough funds to cover the charge. This will result in penalties and unnecessary fees.
8. Don't assume an email or phone call is authentic. Just because someone knows your basic information (such as your name, date of birth and address), it doesn't mean the email or phonecall is legit. Criminals will use a range of social engineering techniques to get your personal identifiable information.
9. When leaving bars or restaurants late at night do not accept a ride from a person who purportsto be employed by a well-known private car service or transportation network company unlessyou initiated the call for service. In the past, fraudsters have driven students to secluded areasand robbed them. In other cases intoxicated customers were driven to ATM machines and forced to withdraw funds from their accounts.
10. Do not offer to deposit a check into your account if requested by an unknown individual. The individual may claim they do not have an account and offer a sob story. You are financially responsible for all Items deposited into your account. Do not provide your account log on credentials to anyone. If you do, they can deposit stolen or counterfeit checks into your account. The bank will hold you financially responsible.

Trust Your Gut — If something just feels wrong, it probably is.