PREVENTION OF IDENTITY THEFT IN A COLLEGE ENVIRONMENT

It has been reported that students today are five (5) times more likely to suffer from identity theft than the general public. Identity thieves can use your personal information and commit various crimes. Some of the methods thieves use to obtain your personal information are mail theft, email fraud, website spoofing, telemarketing fraud and burglary. Thieves can then use your information for unauthorized financial transactions, medical services, or in any interaction with the police. Therefore, students, faculty and staff need to take adequate precautions to protect nonpublic personal information as shown below:

- E-mail should never be used to transfer personal and/or confidential information such as your name, birth date, Social Security Number (SSN), credit card or bank account numbers, tax return information, a driver's license number or other personal information that is not available to the general public. The same is true for other end-user messaging technologies (instant messaging, chat, etc.).
- Don't carry your Social Security card, passport, or birth certificate with you, except when necessary. Keep this data in a secure location.
- Never include your SSN on personal checks and only release your SSN when absolutely necessary.
- Don't respond to unsolicited requests for personal information (your name, birthdate, SSN, credit card or bank account number) by phone, mail, or online.
- Beware of anyone standing too close behind you when you are using your credit card or writing a check.
- Never leave your wallet or purse in an unsecure location when you are not present.
- Don't leave your wallet, purse, computer or anything of value in your vehicle where it would be visible to the public, even if your vehicle is locked.
- Protect your important papers and documents containing personal information such as tax returns, credit cards, applications for credit cards, and other similar documents.
- Payment card data should be treated as confidential information and should not be retained in paper format at any place where you are conducting business or purchasing any items.
- Inquire at business locations where credit cards are used if the business complies with the PCI DSS security requirements.
- Don't use WiFi for financial transactions, since you usually don't know if the network is secure.
- Limit the information you share on social media, and limit access to your account(s) by adjusting the privacy settings on your social network sites so people you don't know cannot view your information or post material on your page.
- Never download attachments or click on links in an email or other social media site unless you are positive they are legitimate.
- Be sure and install security software and anti-malware software on all of your electronic devices and keep them current.
- Shred papers with personal information that you do not need to keep.
- Examine your bank account statements and credit card bills monthly to ensure that your accounts have no unauthorized charges. If they do, contact your banking institution immediately.
- Report all suspected theft of information or security breaches to Campus Police and/or the Business Office as soon as possible.