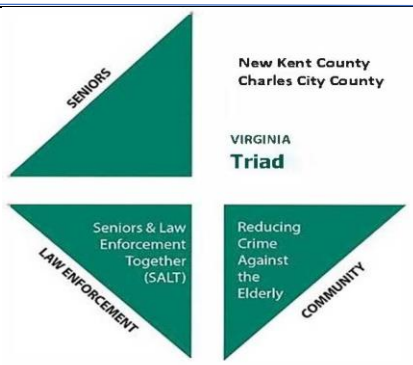

Chickahominy Area Triad

Scam/Fraud Alert Bulletin #21

Be Aware, Be Smart, Stay Protected

Serving the Counties of New Kent and Charles City, VA.

Type	Synopsis of Reported Incidents
Fraud: SCAM:	The victim advised that she and her husband had been on Facebook Marketplace and had found an advertisement for a Honda CRV that was for sale. She used her husband's Facebook account and began speaking with a subject who identified herself as Brianna A. Wade from Gary, West Virginia. According to the victim, "Brianna" had gone to the same school in West Virginia as the victim's husband, so they felt that they knew each other a little bit. The victim said she and "Brianna" started speaking on Facebook on June 11th, and "Brianna" advised that there were a lot of people wanting the Honda CRV so she would need the victim to make a deposit of $1500.00 on the vehicle for to hold the vehicle for the victim. The victim was provided two different phone numbers for her to place the down payment. The First phone number was 480-697-0103, which came back with a name of Mrina Yoladnez Duran, and the second phone number was 217-413-5700, which returned to a Karen Jefferies. The victim had asked for the title of the vehicle to verify that "Brianna" was the owner of the vehicle, but "Brianna" kept making excuses and trying to get more money from the victim. "Brianna" even became hostile and advised that she would have the victim deported if she did not pay more money and that she needed $200.00 more in order to send her a refund. The victim began to research about this advertisement on Facebook and found other individuals had discovered that this was a scam.
Fraud: SCAM	The victim received a phone call from (808) 425-2209 claiming to be in the fraud department with Walmart. The

	victim was advised that there was an attempted purchase for $483.50 on his Walmart debit card. They then advised the victim that they would send him a text with a number, and he would have to provide the number to confirm his identity. The victim received the text and provided the number. He was then advised that they would conduct a fraud investigation. Shortly after the phone call, the victim received a text message stating that his Walmart account had been changed and to contact them if it was not him. He used the phone number on the back of his debit card and contacted the actual Walmart fraud division. During this interaction with Walmart, it was discovered that there had been an attempt to purchase merchandise totaling $483.50, however it had been unsuccessful. It was further learned there had been an electronic transfer of $500 which was successful. He told them he did not make the transfer and they froze his account.
Fraud: SCAM	The victim received an email stating it was from the computer security company McAfee and they had taken $500 from his checking account for the annual service fee. The victim called the phone number attached to the email to inform them he did not use their service and he wants his money back. The victim spoke to "Daryl White" who offered to assist with the return of the victim's money, but instead accidentally transferred $15,000 to the victim's account. "Daryl" stated he needed the money back today and directed the victim to purchase Apple cards to pay the money back. The victim was advised that until the money was returned, his account would be locked and infected with a computer with a virus. The victim purchased $4,000 worth of Apple cards and sent them to "Daryl". Luckily, with the assistance of a family member, the victim stopped communicating with "Daryl" and put a "freeze" on all financial accounts.
Fraud: SCAM	The victim noticed purchases on her Apple account that she did not recognize. She went online and selected the first link she saw which said it was for Apple support. The website was Apples-help-centercare.b-cdn.net and the phone number she eventually called was (833) 211-0525. She related that she

	spoke with someone who told her there was fraudulent activity coming from New Mexico and Louisiana. The Apple support representative also told the victim that there were multiple apps on her phone that were not secure, and she needed to give them access to her phone which she did. The Apple support representative then told her the fraudulent purchases were happening again and they were trying to take $2,400 from her account and in order to block this transaction she needed to go to a website called LibertyX and put in some information that would give her a 6-digit code. The victim followed their directions and then the Apple support representative directed her to an ATM at the Chatham Heights CVS. Once there the victim was instructed to put her card into the ATM and access the LibertyX portal. She said the ATM had access to the bitcoin transfer from the LibertyX website. She said she was apprehensive about putting her card in the ATM and the Apple support representative told her it was not going to take money from her. She then put her card in the ATM with the LibertyX and the 6-digit code. She said the Apple support representative told her he needed to put her on hold to get some information for her and then the call disconnected. She said the money was in fact taken from her account and when she tried to call the Apple support service back, they answered but when she asked for her money back, they hung up on her.
Fraud: SCAM	The victim advised he was looking for an after-retirement job online. He set up a job search account on May 7, 2024. The victim was contacted by the subject identifying himself as "James Podwell" who contacted the victim by text message. "Podwell" advised him he would pay the victim a year's worth of wages all in advance. The victim was not aware of what the job entailed, but advised he would work for "Podwell". The victim received payment by check for the amount of $34,567.00, and the check had a business name of Trans Payment LLC on it. The victim was suspicious that there was something wrong with the check and asked his bank to investigate the validity of the check. The bank held the check

	and a couple of days later, the bank contacted the victim advising him that the check was fraudulent

NOTE: The reported occurrences depicted in this bulletin are true. **They did not occur within the Counties of New Kent or Charles City, Virginia.** However, they were reported to a Northern Virginia Sheriff's Department or the Better Business Bureau (BBB) within the past month. Stay alert, do not become a victim, as you can see it can be costly and do not think that it couldn't happen to you.

Meta: Chickahominy Area Triad Scam Warriors
www.chickahominytriad.org

Meta: Chickahominy Area Triad