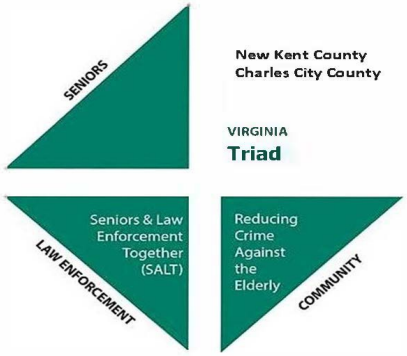

Chickahominy Area Triad

Scam/Fraud Alert Bulletin #17

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 received a call from a male who identified himself as Mr. Frank Leek. This individual stated he was with the Amazon fraud department and asked if she had ordered a computer and had it shipped to an address in New York. She stated she told him she had not, so he informed her that her Amazon account had been hacked. "Frank" then went on to tell the victim that her bank accounts had been hacked, and two (2) properties in Texas had been rented using her financial and identity information. The caller insisted the victim empty her bank accounts to avoid having the money stolen. The victim stated she became suspicious and wanted to verify their identities. She stated "Frank" conferenced in another male who identified himself as the Inspector General of Baltimore and they directed the victim to a county website with a picture and a name that matched the name he had given, so the victim felt she could trust him. "Frank and the IG" then instructed her to purchase three (3) $500 Apple iTunes gift cards and send pictures of the cards and the numbers along with a photo of the receipts. The victim complied and was promised this would help verify if her accounts had been hacked and that a member of the IG's office would meet her at her bank to reimburse her for the $1,500. After sending the iTunes codes, a different number called the victim stating they were with the Border Patrol. The victim states they claimed to have intercepted a package at the border containing $96,000 in cash and six (6) various passports containing her information. It was for this reason the caller urged the victim to empty her IRA/retirement

	accounts for safekeeping. She stated she called her broker, but he didn't answer so she called a friend who helped her realize this had all been a scam.
Fraud: SCAM	The victim advised that she was contacted by someone pretending to be with Exotic Travelers. The suspect advised the victim if they paid a current debt they would give her a free vacation. When she did not receive a free trip, she contacted the real Exotic Travelers who informed her that she had been scammed.
Fraud: SCAM	The victim received a call from "Danielle Lamb" who claimed to be with Publisher Clearing House, advising the victim she had won a $7.5 million giveaway. However, she would have to pay $1,750 for the processing fee and then she would receive the check for $7.5 million. The victim was then contacted by a "George William" who worked with "Danielle" and was going to walk the victim through the process to make the processing fee payment. "George" had the victim drive to Walmart and purchase two (2) Vanilla gift cards for $500 each. She was then instructed to provide "George" the numbers on the back, which she did. Fortunately, the victim locked her keys in her car and had to call her spouse for assistance. When her husband found out what was happening, he immediately had the victim disconnect from the call and explained this had been a scam.
Fraud: SCAM	The victim "googled" the Apple customer service phone number online and called. During the call the victim was advised to enter her social security number, name, and date of birth. She was then advised to obtain Target gift cards to provide to the caller for them to repair her phone. The victim advised to obtain two (2) $250 cards, one (1) $350 card, and an additional $200 card and provided the card information to the subject over the phone and never heard back from them.
Fraud: SCAM	The victim stated that someone intercepted ordered blank checks that had been mailed to him. Soon after, on January 15th, 2024, he got a letter from a bank stating that someone

	had opened an account using his name. The scammer then attempted to cash the two (2) of the checks that had been stolen from the victim, one for $6,169.77 and another for $2,492.70. Due to the fraud procedures in place at the bank, the victim sustained no monetary loss.
Fraud: SCAM	The victim was contacted telephonically by an unknown individual pretending to be his bank, (a common telephone scam). This scammer asked for his social security number and bank information, which the victim provided. The victim was later contacted by his bank and informed that there was suspicious activity on his account. In addition, he also was contacted by CashApp and informed that there was an account attached to his bank, but under a different name. Due to fraud procedures in place at the victims' bank and CashApp, the victim sustained no monetary loss.
Fraud: SCAM	The victim was contacted by someone claiming to be with her bank. The victim proceeded to give the caller her credit card information. Shortly afterward, $17,000 from the victim's account was routed overseas.
Fraud: SCAM	The victim saw an ad on Facebook for employment with "HCA Healthcare". It was posted allegedly by "Beckie Michele Napier". The victim stated the ad claimed that the company would pay off any employee's credit card debt to allow the newly employed individual to focus strictly on their work. The victim was interviewed allegedly by "Leslie Renee Ferguson". The victim was informed that she had passed the interview, and the victim was offered a position. The victim was instructed to create an ID.me account and provided the login info to "Leslie". "Leslie" then asked for the limits on all of the victim's credit cards and asked for photos of all statements. "Leslie" then provided the victim with the routing number and account numbers for the victim to use to pay off her credit card debt. Afterwards, "Leslie" then instructed the victim to purchase a $500 gift card, at which time the victim became suspicious and contacted the Sheriff's Office
Fraud: SCAM	Victim received text messages from Navy Federal sending him codes to sign into his account. He said shortly after he

	received a call from a number he recognized as Navy Federal. They began to ask him questions about his account. They knew the last four digits of his accounts and started to ask him security questions. He said he didn't recognize the questions they were asking as his specific security questions. He said the caller now started to set up new security questions which he later learned was what was used to gain access to his account. He said he got disconnected twice before calling Navy Federal himself and they told him he had been scammed; the caller was spoofing the number. In total, the victim lost $3,180.

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, don't become a victim, as you can see it can be costly and don't think that it couldn't happen to you.

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

Meta: Chickahominy Area Triad