Testimony of Catherine Taylor, AARP Rhode Island
In support of House Bill 5121
House Innovation, Internet, and Technology Committee
February 11, 2025

Chairwoman Baginski and Members of the Innovation, Internet, and Technology Committee:

AARP is a nonpartisan, social mission organization with 38 million members nationwide and nearly 125,000 members here in Rhode Island. We advocate on behalf of issues that impact older adults, and we appreciate the opportunity to offer our support to establishing guidelines for the operation of virtual currency (crypto) ATMs through House Bill 5121, sponsored by Chairwoman Casimiro.

Fraud criminals steal billions of dollars from unsuspecting consumers every year. The impact on victims and their families can be financially and emotionally devastating, especially for older adults. The recent growth in fraud has been meteoric. The Federal Trade Commission (FTC) revealed their estimates of under-reporting in a 2023 report, suggesting that rather than $9 billion reported stolen through fraud in 2022, it was likely closer to $137.4 billion. A recent survey from AARP shows that 42% of adults—that's 141 million people - have had money or sensitive information stolen through fraud. Nine in 10 US adults now believe fraud can happen to anyone – and the biggest worry they have about fraud is of it happening to them.

Education is an important part of the solution. Research suggests that, if you know about a specific scam, you're 80% less likely to engage with it. But we cannot educate our way out of the fraud epidemic our country is experiencing. Addressing fraud requires a whole of society approach. Together, educators, policymakers, law enforcement and industry can turn the tide against the criminals who hold the power right now. We can disrupt their business model, protect millions of consumers, and keep billions of dollars in savings accounts and in our economy.

The AARP Fraud Watch Network hotline is a free resource, manned by trained fraud specialists and volunteers, that field thousands of calls each month. These trained specialists provide information about current scams, offer support and guidance, and connect victims with others who have also been victimized. Over the past few years more and more of the calls to our hotline include stories involving Crypto ATM machines. Here are a few of those stories…

Sincerely,

Catherine Taylor, State Director, AARP Rhode Island.

AARP Fraud Watch Network: Stories of Virtual Currency Kiosk Fraud

AARP's Fraud Watch Network is sharing recent stories from across the United States of older Americans who have been victimized by fraud involving virtual currency kiosks. Callers to the Fraud Watch Network Helpline shared their personal experiences on how they were victimized. Criminals in many different types of scams exploit virtual currency kiosks as a method for receiving payment. These machines may be attractive to criminals because they are not yet well-understood by the public, because larger amounts of money can be transferred compared to other payment methods (like gift cards), and because virtual currency transactions are irreversible. These scams are disproportionately impacting older Americans.

Business Impersonation Scams

• Mable, a 79-year-old, searched a number for Netflix online and instead of finding a legitimate Netflix number, found herself in touch with Netflix impersonators who scammed her. Mable sent over $250,000 via a virtual currency kiosk. She also purchased gold bars and cashier's checks to be picked up by what turned out to be a government impersonator. This is a huge loss and she has contacted the police and local media hoping it will help her some way.

• Barbara, a 77-year-old, has a granddaughter who was notified by what appeared to be Facebook that her bank account information was compromised. The granddaughter searched for a Facebook phone number and called the number at the top of the search results. She was instructed to take her money out of her bank account and put it in a virtual currency kiosk. The scammer then wanted the account number, supposedly to make sure she got her money back. The granddaughter withdrew her money and deposited it. The money disappeared and the bank has said there is nothing that they can do.

Government Impersonation Scams

• Nadine, a 66-year-old, has a sister who has multiple sclerosis and lost $40,000 to a government grant imposter scheme she found on Facebook. The sister cannot get around very well, so the scammers had an Uber pick her up. She deposited her life savings into a virtual currency kiosk. They took personal information from her as 2 well. She is devastated by this since this was all the money she had and there is no way to recover it.

• Robert, a 77-year-old, reported that his wife received a call about owing taxes, and she transferred $30,000 to via a virtual currency kiosk to the "IRS". Then Robert's wife and daughter knew someone from their church Facebook group who was a "Bitcoin broker" and told them they could help them invest to make up for their previous losses. They "invested" another

$30,000 with this person in Bitcoin. The “broker” coached them through the transactions through a Facebook page. Now the page has disappeared the church won't help with information. They are worried about how the losses will affect their finances and future.

• Linda is a 60-year-old woman who received an email claiming the FBI and United Nations had agreed to reimburse people who lost money to a previous scam, but that she needed to pay $100 to start the process. She paid the scammers using Bitcoin via a virtual currency kiosk, and then received a message saying they needed another $600 the next day. She had previously lost her savings in another scam, including her 401(k) and thought the person impersonating the FBI was going to help her recover it. Her friends and family no longer wish to associate with her because she borrowed money from them, and she is too embarrassed to say what happened to the money.

Tech Support Scams

• Betty, an 81-year-old in, was online when her computer froze with a Microsoft popup and she called what turned out to be Microsoft impersonators. She withdrew all her money and put it all in a virtual currency kiosk. She lost over $5,000 in total. She put a credit freeze on her account. The DMV put a law enforcement stop on her license. She is hoping there may be a way to recover some of her money since she lives on a very tight budget.

• Stephanie, a 73-year-old woman, was struggling with a computer issue and Googled Geek Squad in an effort to receive some support. Unfortunately, she reached a Geek Squad impostor who accessed her computer, conducted a fake refund scam, and convinced Stephanie to send them money though a virtual currency kiosk. The scammer berated her and threated her continuously throughout the course of the 3 scam to the point she was afraid to report it to anyone until she reached out to the Fraud Watch Network.

• Ricky, a 96-year-old man from was reading the news on his iPad when he received a pop-up claiming to be from Microsoft. He called the number shown in the pop-up message thinking it was truly Microsoft. After an elaborate and lengthy conversation with a Microsoft impostor (who accessed his computer), he was convinced to drive to the bank, empty out his bank account, and deposit the money in the nearest virtual currency kiosk. He was told not to speak to anyone while he did this.

• Susan, a 64-year-old in got a pop-up message on her computer from Microsoft. She called the number in the alert and a scammer told her they would need to remote into her computer to fix a problem, which she allowed them to do. The criminal then pretended to transfer her to a fake “FTC agent.” The criminal told her that her accounts were being used by several criminals and she needed to withdraw her money from her bank to protect it. Susan sent $3,500 in gift cards, a $40,000 cashier's check, and $18,000 deposited into a virtual currency kiosk. She is worried about her future due to the huge money loss.

• Elaine, a 76-year-old woman was devastated after losing her husband and trying to sort through legal affairs after his death. She googled the Apple Support number in an attempt to secure his Apple accounts, but unfortunately, the number she called was an Apple impostor. The

criminal convinced her she was the victim of identity theft, then convinced her to take $30,000 out of her bank account and deposit into a virtual currency kiosk. Now she is out of the money while also recovering from the loss of her husband.

• Sally, an 81-year-old woman, was reading her daily horoscope on an astrology website and clicked a button to finish reading the rest of the article. When she did this, she received a pop-up message that her claimed computer was infected with a virus. Sally called the number and provided them access to her computer. The criminals were able to obtain her SSN, DL, and banking information. Sally drove to her bank, withdrew the money, and put it into a virtual currency kiosk. Sally feels unsafe and violated at the amount of information they stole from here. They even forced her to take a selfie. Now she is without the money and her sense of security.

• Christina, a 78-year-old woman, purchased an HP printer. When she tried to connect this printer to her computer, she was struggling to get it to work, so reached out to a number online she thought was HP. Upon speaking to a customer support representative, who was really a scammer, she was convinced to take $40,000 from her bank account and transfer it via a virtual currency kiosk. She attempted to contact the bank and the kiosk company as soon as she realized it was a scam but has been unable to return the money, which she worked all her life for.

Romance Scams

• Toni is a 69-year-old single woman from who became the victim of an investment scam after forming an online romantic relationship via Facebook. She was convinced by her alleged love interest to put this “investment money” into a virtual currency kiosk. She soon realized the scammer’s true intentions but is now living without the hard-earned money she had accumulated during her working life.