AARP Vermont

To: Senate Finance Committee
From: Colin Hilliard (chilliard@aarp.org | 802-238-5693)
Advocacy Director, AARP Vermont
Re: S.129 - Regulation of virtual-currency kiosk operators
Date: April 1, 2025

Chair Cummings and Members of the Senate Finance Committee:

My name is Colin Hilliard, Advocacy Director of AARP Vermont. AARP is a nonpartisan, social mission organization with an age 50+ membership of nearly 38 million nationwide and 110,000 members here in Vermont. We advocate on issues that impact older adults and appreciate the opportunity to testify on virtual-currency kiosk regulations in S.129.

AARP has supported legislative efforts to bring consumer protections to virtual currency transactions especially at virtual currency kiosks. Robust consumer protections help safeguard older Vermonters' financial well-being by ensuring transparency, fairness, and accountability. We believe strong protections against fraud are needed as cryptocurrency used as a payment for scams is a fast-growing problem.

As written, S.129 would weaken existing consumer protections that help prevent fraud, particularly through the increase in the daily transaction limit. It would also end the moratorium on new virtual currency kiosk operators without any refund provisions for fraudulent transactions. Refund requirements are a vital consumer protection that has been enacted in states like Connecticut and Nebraska.

The impact of fraud on victims and their families is wide reaching and can be financially and emotionally devastating, especially for older adults. The recent growth in fraud is staggering. 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.

According to the FBI, cryptocurrency ATM schemes have increased too, particularly among older adults. Of the more than 5,500 complaints involving cryptocurrency kiosks reported to the agency's Internet Crime Complaint Center in 2023 (the latest data available), almost half came from people over 60. Of the roughly $189 million of losses involved in the complaints, $124 million belonged to those over 60.

Below are several recommendations to strengthen the bill, as well as real stories from callers to the AARP Fraud Watch Network Helpline who shared their personal experiences on how they were victimized:

Section 2577 (a) Daily transaction limits: We supported enactmenting the $1000 daily transaction limit for all customers as it protects victims from large losses and limits the use of kiosks for criminal activity.

Recommendation: Keep the $1000 daily transaction limit in place.

Section 2577 (a) "New customer" definition: While some victims may realize they have been the victim of fraud within 72 hours, many others will not. There are many types of scams, such as investment or romance scams, that go on for many weeks or even months. AARP believes that 30 days is a more reasonable time frame for someone to be considered a new customer. Below, please find language we would like to see amended:

New Customer. "New customer" means an individual who has never previously transacted with the virtual currency kiosk operator. The new customer shall remain defined as such during the thirty (30) day period after the first virtual currency kiosk transaction with the virtual currency kiosk operator.

Existing customer. "Existing customer" means an individual who transacts with the virtual currency kiosk operator following the thirty (30) day period after the first virtual currency kiosk transaction with the virtual currency kiosk operator. For the avoidance of doubt, Existing customer includes any customer that is not a New customer.

Section 2577 Refund Provisions: We would like to see a refund provision added in cases of fraud. Several states (including Connecticut and Minnesota) already require refunds for customers of virtual currency kiosks who are victims of fraud.

Below, please find the language we would like to see added:

a. **Refunds for new customers.** Upon the request of a customer, a virtual currency kiosk operator shall issue a refund to a new customer for the full amount of all transactions made within the thirty (30) day new customer time period. In order to receive a refund under this section, a new customer shall have been fraudulently induced to engage in the virtual currency transactions, shall have contacted both the virtual currency kiosk operator and a government or law enforcement entity to inform them of the fraudulent nature of the transaction agency within ninety (90) days of the last transaction to occur during the thirty (30) day new customer time period. In addition, such customer shall have submitted proof of the fraud incident, such as a police report or sworn declaration detailing the fraudulent nature of the transaction or transactions.
b. **Refunds for existing customers**. A virtual currency kiosk operator shall issue a refund to an existing customer for the full amount of all transaction fees upon the request of an existing customer. In order to receive a refund under this section, a customer must have been fraudulently induced to engage in the virtual currency transactions, shall have contacted the virtual currency kiosk operator and a government or law enforcement agency to inform them of the fraudulent nature of the transaction within ninety (90) days of the transaction, and shall have submitted proof of the fraudulent incident, such as either a police report or sworn declaration detailing the fraudulent nature of the transaction.

Recommendation: Transactions based on fraudulent activity should be refunded to the victim.

Section 2507 Receipts: Receipts are an important part of investigations by law enforcement. We would like to have receipts required at virtual currency kiosks in the language chosen by the customer. Receipts should be physical where possible. In addition, all receipts should have information of who to contact when fraud is suspected as well as all other transaction information.

Recommendation: Require receipts for every transaction, in physical form where possible, and law enforcement contact information on all receipts.

Section 2507 (f) Disclosures: Disclosures are an important part of consumer and fraud protection. We support the statute's inclusion of disclosures but would suggest the addition of language acknowledging that many victims of fraud are operating under duress and disclosures cannot be used to affect or prevent a fraud victim's ability to be eligible for a refund. Below, please find the language we would like to see added to this section:

The disclosures in this section are intended to serve as warnings to users who may be conducting a virtual currency kiosk transaction as a result of a scam. The Legislature recognizes that many victims of fraud are operating under duress and may lack the ability to understand and appreciate these disclosures while under the influence of a scam. The disclosures in this section cannot be used to affect or prevent a fraud victim's ability to be eligible for a refund as described in this chapter or otherwise.

Recommendation: Add acknowledgment that the disclosures in this section cannot be used to affect or prevent a fraud victim's ability to be eligible for a refund.

Sincerely,

Colin Hilliard
Advocacy Director, AARP Vermont

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 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 pop-up 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 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.

*****

AARP Fraud Watch Network Helpline: 877-908-3360

Our toll-free service is available Monday through Friday, 8 a.m. to 8 p.m. ET

AARP's Fraud Watch Network™ Helpline is a free resource for AARP members and nonmembers alike. Trained fraud specialists and volunteers field thousands of calls each month. Get guidance you can trust, free of judgment.

Have you or a loved one been targeted by a scam?

If you or a loved one has been targeted by a scam or fraud, you are not alone. Our fraud specialists provide free support and guidance on what to do next.