AARP Vermont

To: Chair Marcotte, Vice Chair Granning and Members of the House Committee on Commerce and Economic Development

From: Colin Hilliard (chilliard@aarp.org | 802-238-5693) Advocacy Director, AARP Vermont

Re: **H. 648 Draft 1.3 - Crypto Kiosks**

Date: May 12, 2026

Dear Chair Marcotte, Vice Chair Granning and Members of the House Committee on Commerce and Economic Development,

AARP Vermont appreciates the opportunity to comment on the amendment to H.648, An act relating to banking, insurance, and securities. AARP is the nation's largest nonprofit, non-partisan organization dedicated to empowering Americans 50 and older to choose how they live as they age. On behalf of the nearly 38 million members nationwide and 110,000 members here in Vermont, we want to **express our support for the changes to Sec. 11. 8 V.S.A. § 2507 banning crypto kiosks in Draft 1.3.**

While anyone can be the victim of a scam, older Vermonters have a lifetime savings to lose and are the frequent targets of romance scams, government impersonation scams, and more. The impact of fraud on victims and their families is wide reaching and can be financially and emotionally devastating, especially for older adults.

As the scale and sophistication of fraud perpetrated through cryptocurrency kiosks increases, data of reported complaints and losses continue to grow, states are increasingly adopting bans, and older voters are overwhelmingly supportive of stronger protections.

Crypto Kiosk fraud complaints and losses are growing

In April, the FBI released its new 2025 IC3 (Internet Crime Complaint Center) Report. The report found:

- 13,460 complaints, totaling $389m in losses in 2025
- 23 % increase in complaints from 2024
- 58% increase in losses from 2024.
- Americans 60 + reported 6,188, a 131% increase YoY.
- Americans 60+ reported losses over $250m, a 140% increase YoY.
- ***Because crypto kiosk fraud is vastly underreported, these numbers only tell part of the story.***

The FBI has not provided state-specific crypto kiosk fraud report/loss data for 2025. A full breakdown of losses and complaints by age group can be found on pg. 3.

More states are acting, with 3 bans passed this year.

States are increasingly taking action to protect consumers from crypto kiosk-related scams. To date, 29 states have passed legislation. Indiana, Tennessee, and Minnesota have both passed full bans into law this year. Massachusetts and Hawaii are also contemplating bans.

Minnesota passed consumer protections in 2024 that are very similar to those passed in Vermont last session with H.137 (Act 23). Minnesota has over 350 licensed kiosks in the state. Despite these protections, the Minnesota Dept. Of Commerce found that 2025 was “the worst on record”, with 70 cases and more than $540,000 lost. The average reported loss was nearly $6,800 (House Commerece Finance and Policy Committee Hearing 2/26/26, 25:00).

Written testimony from law enforcement in MN demonstrated the harm they were seeing in thier communities. In Faribault, MN, a population of ~24k with 6 kiosks, the Chief of Police reported that since 2024 they've seen $500k in reported losses with avg victim age of 68. The chief noted "while these measures (protections passed in 2024) were a positive first step, our investigations demonstrate that fraud continues at significant levels (Faribault, MN Chief of Police Letter).

Older Americans want lawmakers to implement better protections against cryptocurrency kiosk fraud

A February 2026 AARP survey found that an overwhelming majority of older adults (92%) think laws designed to protect consumers from crypto-kiosk-related fraud and scams are important. More than 8 in 10 perceive such laws as ways to support responsible growth of cryptocurrency, not barriers to innovation. Additionally, only a quarter of older adults (25%) say they would feel somewhat or very confident that they would know what steps to take to try to get their money back, such as whom to contact for help or how to report the incident, if they experienced a crypto scam or fraud.

AARP’s approach to cryptocurrency kiosks has been measured and evidence-driven. When these machines first began appearing, we did not call for bans—we worked with states, including here in Vermont, to put thoughtful consumer protections in place. Those protections were important. But experience since then has made something clear: the presence of the kiosks themselves continues to create an entry point for fraud. Criminals and bad actors consistently find ways to work around limits, disclosures, and other safeguards.

The issue is no longer whether protections are in place—it is whether those protections can ever keep pace with how these scams operate. In many states, the answer has increasingly been no. That is why AARP is now supporting stronger policy options, including bans.

In conclusion, given the alarming rise in fraud perpetrated through cryptocurrency kiosks, we have serious concerns about what an influx in new kiosks could mean for Vermonters. The state law enacted in 2025 was a step forward, but it falls far short of addressing the scale and sophistication of this growing threat. These machines continue to serve as easy targets for criminals, putting consumers—especially older adults—at significant financial risk.

Sincerely,

Colin Hilliard
Associate State Director – Advocacy and Outreach, AARP Vermont

FBI Internet Crime Complaint Center (IC3) Annual Report Data

2025 Annual Report

2025_IC3 Report.pdf

Cryptocurrency ATMs/Kiosks

13,460 Complaints; $389 million in Losses

23% Increase in Complaints from 2024
58% Increase in Losses from 2024

The FBI Warns of Fraudulent Schemes Leveraging Cryptocurrency ATMs and QR Codes to Facilitate Payment

Crypto ATM/Kiosk Use Reported by Age Group

Age Group	Count	Losses
Under 20	58	$124,013
20 - 29	825	$6,474,240
30 - 39	1,275	$10,936,943
40 - 49	1,472	$20,826,227
50 – 59	1,524	$44,584,724
60+	6,188	$257,466,130

2024 Annual Report

2024_IC3Report.pdf

Cryptocurrency ATMs/Kiosks

10,956 Complaints; $246.7 Million in Losses

99% Increase in Complaints from 2023
31% Increase in Losses from 2023

The FBI Warns of Fraudulent Schemes Leveraging Cryptocurrency ATMs and QR Codes to Facilitate Payment

REPORTS of CRYPTO ATM/KIOSK USE by AGE GROUP

Age Group	Count	Losses
Under 20	7	$51,913
20 - 29	280	$3,739,620
30 - 39	361	$4,241,387
40 - 49	319	$3,621,774
50 – 59	349	$5,523,230
Over 60	2,674	$107,206,251

CRIME TYPES MOST ASSOCIATED WITH CRYPTO ATM USE

	Count	Losses		Count	Losses
Extortion	4,189	$5,601,953	Government Impersonation	1,786	$44,587,335
Tech Support	3,037	$107,429,709	Investment	606	$38,090,269

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.