Pennsylvania Senate Joint Public Hearing
Banking & Insurance Committee
and
Communications & Technology Committee

Hearing Room 1 – North Office Building
Wednesday, April 8, 2026

AARP Pennsylvania Testimony
Teresa Osborne
State Advocacy Director

My name is Teresa Osborne, and I serve as the State Advocacy Director for AARP Pennsylvania. I am honored to testify on behalf of AARP, which advocates for nearly 5 million Pennsylvanians age 50 and older and their families. Thank you to the members of the Senate Banking and Insurance Committee and Senate Communications and Technology Committee for convening this important hearing on consumer protections related to virtual currency kiosks. AARP has a long history of educating consumers, supporting fraud victims, and advancing effective fraud detection and prevention across industries. We look forward to working with you to advance policy solutions that protect consumers and prevent fraud.

Fraud has surged dramatically over the past five years. According to data from the Federal Trade Commission (FTC), Americans reported $12.8 billion stolen through fraud in 2024 alone. In Pennsylvania, 83,755 residents reported fraud losses totaling $373.3 million. But these figures capture only a fraction of the harm. In a December 2025 report to Congress, the FTC acknowledged widespread, under-reporting and, using its own estimates, concluded that actual fraud losses in 2024 were closer to $196 billion nationwide. Of that total, the FTC estimated $81.5 billion in losses were borne by older adults – losses that too often devastate retirement security and financial independence.

Fraud criminals know no demographic bounds. They target people of all ages, education levels, and incomes. But when older adults are victimized, the consequences are too often profound and life-altering. Older adults are more likely to have accumulated a lifetime of savings and housing wealth – and too often, the scammers steal everything. Victims are left emotionally and financially devastated, families are torn apart, and many people who were once financially prepared for a secure retirement are instead forced to rely on already-strained local, state, and federal safety nets.

The tactics used by fraud criminals range from old-fashioned schemes – like stealing your mail - to highly sophisticated attacks, including data breaches at banks, retailers, and other companies that store sensitive consumer information. Scammers often impersonate government agencies, utility companies, financial institutions, or major technology firms to trick people into revealing their personal information. Others rely on phishing emails and messages that infect devices with data-harvesting malware. Stolen information is then bought and sold on the dark web and through apps, allowing criminals to then refine their schemes and more precisely target their victims.

Fraudsters exploit every communication channels - phone calls, emails, text messages, social media, online ads and pop-up messages, fraudulent apps, mail, and even in-person interactions. In short, there is no form of communication that criminals have not made dangerous. And until we collectively recognize that fraud victims are crime victims - and that they are not responsible for becoming targeted - we will continue to fall short in confronting this crime for the serious and pervasive threat it is.

AARP has seen an alarming increase in criminals using cryptocurrency kiosks to steal Americans' hard-earned money. These machines - also known as "crypto ATMs," "bitcoin ATMs," "BTMs," or "virtual currency kiosks" – are increasingly common, appearing in supermarkets, convenience stores, gas stations, bars, and restaurants across our communities.

While cryptocurrency kiosks can be used for legitimate transactions, such as sending money to digital wallets, scammers are increasingly exploiting these machines to commit fraud. The way these scams work is that criminals – often impersonating government officials or trusted businesses – create a false sense of urgency and instruct individuals to withdraw large amounts of cash and deposit it into a crypto kiosk. That cash is then immediately transferred to a digital wallet controlled by the criminal.

Today, there are more than 30,000 crypto kiosks nationwide that allow users to insert cash and send it to a digital wallet anywhere in the world. Transactions take only minutes, and once completed, the money is nearly impossible to recover – making these kiosks an attractive tool for fraudsters. Moreover, because crypto kiosks are largely unregulated at the state level compared to traditional financial institutions - such as banks and other money service businesses - they lack comparable fraud protections. As a result, criminals are using crypto kiosks to steal hundreds of millions of dollars from Americans each year.

Older adults are disproportionately affected by fraud and scams involving cryptocurrency kiosks. In 2025, the FBIs Internet Crime Complaint Center (IC3) reported $389 million stolen through crypto kiosk scams – an alarming increase from just over $189 million in reported losses in 2023. And we know from Federal Trade Commission analysis that these figures represent only the tip of the iceberg. More than one in five cryptocurrency complaints came from people age 60 and older. In fact, more than 201,000 complaints were filed by older adults (60+) in 2025 - a 37 percent increase from the prior year – resulting in losses exceeding $7.4 billion, a 54 percent increase from the prior year.

AARP is not opposed to cryptocurrency. We simply want safeguards in place to protect consumers from criminals who exploit these machines. We are committed to empowering people with information about crypto kiosk scams and what to do if they are targeted. In fact, throughout this month of April – recognized by AARP as Fraud Prevention Month – we are showing up in communities across the Commonwealth with free, fraud prevention events to give people practical tools to recognize scams, how to stop them, and know where to turn for help. For example, as I join you here in the Capitol today, AARP Pennsylvania volunteers and staff are hosting a Scam Jam in Lehigh County, where nearly 100 participants are learning about fraud through interactive activities – like Fraud Bingo - and hearing from their local district attorney's office, area agency on aging, and a federal credit union. At the same time, volunteers from our Fraud Speakers Bureau – known as the Consumer Issues Task Force - are delivering fraud presentations today in Bedford, Montgomery, and Beaver counties. In addition to educating consumers and supporting fraud victims through the AARP Fraud Watch Network, we are advocating for stronger consumer protections that will deter criminals from leveraging cryptocurrency kiosks in their schemes.

Which brings us to today's discussion of Senate Bill 1015. We commend Senator Pennycuick for introducing this legislation and for highlighting the need for Pennsylvania to join 22 other states in adopting common sense consumer protections for the growing number of virtual currency kiosks operating across all sixty-seven counties of the Commonwealth. AARP supports several provisions in the bill, including licensing, consumer disclosures, fraud warnings, receipts, live customer service, anti-fraud, and exploitation policies, blockchain analytics, and reporting to the Department of Banking and Securities. However, we believe the bill must be strengthened through amendments to include transaction limits, fee caps, mandatory transaction delays or holds for new users, user identification, and training requirements, and a refund or remediation mechanism for individuals who promptly report fraud.

There is a myth that transaction limits do not reduce fraud. The evidence shows otherwise. Law enforcement testimony demonstrates that transaction limits dramatically reduce fraud and related criminal activity. After one state enacted daily transaction limits, fraud tied to a cryptocurrency kiosk operator dropped to just one percent of the prior year's level. Law enforcement also reported reductions in the use of kiosks for escort services linked to human trafficking after limits took effect. Because fraud losses through kiosks are rarely recoverable, prevention - not after-the-fact reporting – is the most effective protection. The bottom line is clear: transaction limits work because they stop large losses before they occur.

There is another myth that low daily transaction limits interfere with the filing of Suspicious Activity Reports – commonly referred to as SARs. That claim that SARs "cannot be filed" under $2,000 is false. The Code of Federal Regulations - 31 CFR 1022.320 - makes clear that operators may file SARs on *any amount* and the $2,000 is simply the threshold at which reporting becomes mandatory. If a cryptocurrency business chooses not to file SARs below $2000, that is a business decision – not a legal limitation. The other threshold often cited is $10,000, which triggers Currency Transaction Reports – or CTRs. SARs and CTRs primarily support federal investigations and are often not directly accessible to state or local law enforcement, nor do they help victims recover stolen funds. Allowing higher transaction limits simply allows victims to lose more money, more quickly, with little chance of recovery. The bottom line clear: reporting does not protect consumers. Transaction limits do.

Another myth is that states have settled on a single "best practice" in which new customers receive lower daily transaction limits while experienced users are granted higher limits. This claim is misleading and does not reflect what has actually occurred across the country. States have taken varied approaches: some have tiered limits, others have imposed flat limits for all users, and still others rely on different combinations of consumer protections. At least six states - California, Iowa, Louisiana, Maine, North Dakota, and South Dakota - have adopted a single-user framework, with Wisconsin implementing the same approach through regulation. This reflects increasing recognition that uniform rules are clearer, easier to enforce, and more effective at protecting consumers. At the same time, some states are questioning whether limits alone are sufficient, with Indiana recently enacting a full ban on crypto kiosks.

What states have learned - regardless of the structure they initially chose - is that "experience" does not reliably reduce fraud risk. Many victims are repeat users targeted over long periods of time, particularly in romance and investment scams. Tiered systems based on time or transaction counts have proven easy for scammers to defeat by coaching victims to wait out new-customer periods or reuse wallets to qualify for higher limits. Minnesota illustrates this clearly: its earlier law provided relatively modest protections, and lawmakers are now debating a full ban in response to continued fraud. The bottom line is that tiered systems create loopholes that criminals exploit, while uniform protections provide stronger, more durable safeguards.

Another falsehood is the claim that user identification is unnecessary, overly burdensome, or required only for large transactions. User verification is a basic, federally required safeguard – and cryptocurrency kiosk operators already collect and retain this information under existing law. These operators are regulated as Money Services Businesses (MSBs) under the Bank Secrecy Act (BSA) and must collect customer identifying information in multiple circumstances as part of federal anti-money laundering compliance.

Under federal law, MSBs must collect verified customer information for Travel Rule transactions of $3,000 or more and must file Currency Transaction Reports (CTRs) for cash transactions over $10,000 in a single day - both of which require customer identity verification. There is also no minimum dollar threshold for collecting customer information when an operator knows, suspects, or has reason to suspect fraud, structuring, or other suspicious activity - meaning low-dollar transactions are not exempt from scrutiny. User verification is essential at all transaction levels to prevent evasion and structuring. Without verification on smaller transactions, scammers can simply break large fraud losses into multiple low-dollar transactions, undermining both federal safeguards and state daily transaction limits. Verification is what makes daily transaction limits enforceable. Limits tied to an identified user - rather than a single machine or wallet - prevent repeat transactions across multiple kiosks in the same day. At least one major national kiosk operator says they already verify users for all transactions, demonstrating

that this safeguard is both feasible and already in place. The bottom line is clear: user verification is already required, already happening, and foundational to enforcing daily transaction limits.

On the issue of refunds and the claim that crypto kiosk operators should not be required to provide them, the facts tell a different story. Refund requirements are essential because cryptocurrency kiosk transactions are fast, high-risk, irreversible, and disproportionately used in scams - leaving victims with no meaningful recourse without state-level protections. Once funds are sent through a kiosk, victims almost never recover their money - even when fraud is clearly documented. Refunds are often the *only* way victims can be made whole. Moreover, federal and state investigations consistently show that crypto kiosks pose a higher fraud risk than traditional financial institutions and are heavily targeted in government impersonation, tech-support, and romance scams. While victims often lose thousands of dollars in minutes, kiosk operators profit directly through the fees collected on each transaction – even when the transaction is fraudulent. Requiring refunds creates accountability and real incentives for prevention by pushing operators to strengthen fraud detection, consumer warnings and transaction monitoring rather than relying on after-the-fact reporting. The bottom line is clear: refund requirements ensure that no one profits from fraud, provide victims with a meaningful path to recovery in an irreversible system, and create real incentives for kiosk operators to prevent scams - rather than treating fraud losses as a boost to their bottom line.

Lastly, we have heard the myth that federal law already regulates crypto kiosks sufficiently. In reality, federal rules are focused on financial system integrity - not consumer protection. Federal law does not require transaction limits, consumer warnings, receipts, refunds, or customer service standards. A 2025 U.S. Department of Treasury Financial Crimes Enforcement Notice – commonly referred to as a FinCEN notice - highlighted widespread non-compliance, high fees, and the outsized role crypto kiosks play in fraud and elder exploitation. State-level protections fill the gap where federal oversight does not reach. The bottom line is clear: in the absence of state action, consumers are left exposed.

Scams are not a series of isolated crimes - they are a global, industrialized threat that drains household wealth, fuels transnational criminal organizations, and undermines confidence in our financial and economic systems. The status quo empowers criminals, fails victims, and empowers criminals. Without decisive action, this crime will continue to erode retirement security, strain public safety nets, and drain billions from our economy each year.

Fighting fraud continues to be a top priority for AARP. As criminals find new ways to steal from their victims, we must respond with stronger safeguards and smarter consumer protections. AARP stands ready to work with both Committees and the full General Assembly to help turn the tide – because protecting Pennsylvanians, and all Americans, from fraud is not only achievable, it is essential to financial security, economic resilience, and the integrity of our Commonwealth and our nation.