COMMONWEALTH OF PENNSYLVANIA
OFFICE OF ATTORNEY GENERAL

DAVID W. SUNDAY, JR.
ATTORNEY GENERAL

Paul Edger, Pennsylvania Office of Attorney General Testimony
Joint Meeting of the Pennsylvania Senate Communications & Technology Committee
and Senate Banking and Insurance Committee
April 8, 2026

Good morning Chairs Pennycuick, Miller, Gebhard and Street, members of the committees. Thank you for the invitation to participate in today's joint hearing. My name is Paul Edger, and I am a Senior Deputy Attorney General in Charge with the Pennsylvania Office of Attorney General, assigned as the Attorney-in-Charge of the Harrisburg region of the Bureau of Consumer Protection. I send greetings and thanks on behalf of Attorney General Sunday for being asked to speak today regarding the use of cryptocurrency teller machines, also known as Crypto ATMs or virtual money kiosks ("kiosk"), and provide our perspective as law enforcement.

This is a matter of growing concern amongst law enforcement bodies across the United States, and the impact these kiosks are contributing toward scams in the Commonwealth is astounding. While law enforcement continues to crack down on the use of these kiosks being utilized for illegal purposes, more needs to be done to provide for stronger regulation on the operators installing these machines at local businesses across Pennsylvania.

I. Nationwide scam statistics

As this body is aware, scams continue to grow across the United States and here in the Commonwealth. In March of this year, the Federal Trade Commission ("FTC") testified before the United States House of Representatives Joint Economic Committee providing their annual review of scams and the impact on Americans.[1] This annual report has been used by law enforcement agencies to identify developing trends and assess priorities across state borders. In 2025, the FTC received over three (3) million complaints from American citizens alleging a loss in excess of $15.9 billion.[2] This number is an increase from prior years, as Americans lost $12.5 billion from scams in 2024 and $10.9 billion in 2023.[3] The largest reported scam scenario of 2025 was imposter scams.[4] These scams include individuals posing as legitimate businesses, such as Amazon or one's own bank, requesting a legitimate action such as confirming a purchase or authorizing a refund, when it is not in fact that business.[5] Imposter scams also include scammers

[1] https://www.ftc.gov/system/files/ftc_gov/pdf/ftc-testimony-jec-hearing-on-the-rising-scam-economy.pdf
[2] Id.
[3] https://www.ftc.gov/news-events/news/press-releases/2025/03/new-ftc-data-show-big-jump-reported-losses-fraud-125-billion-2024
[4] Id.
[5] These scams are also referred to in law enforcement as "phishing scams."

posing as a government agency or official, including the PA Turnpike Commission to pay an overdue toll, or a local county Sheriff threatening arrest for failure to appear for jury duty. More than one (1) million imposter scams were reported at the federal level, alleging losses of $3.5 billion.[6] However, the largest loss at the federal level reported by consumers in 2025 was investment scams, including the use of kiosks, with losses totaling $7.9 billion.[7]

II. Commonwealth scam statistics

In the Commonwealth, the Office of Attorney General, Bureau of Consumer Protection ("Bureau") has a team of dedicated Agents who focus solely on scam prevention, assisting consumers who have been defrauded and working with the banks and fellow law enforcement to reverse transactions. Additionally, our office's criminal section works with fellow law enforcement agencies at the local, federal, and international level, to attempt to trace identities of scammers; however, most scammers are located outside of the jurisdiction of the United States which restricts the ability to intercept and apprehend.

Since 2024, the Bureau has received 90 consumer complaints from Pennsylvania consumers who allege they were scammed and made a payment via cryptocurrency through a kiosk. Between January 1, 2024 and March 31, 2025 these losses totaled $12.3 million.[8] Additionally, 185 complaints were received during the same period alleging losses of $10.7 million where the currency was transmitted via cryptocurrency. These statistics reflect only those individuals who have filed a complaint with the Office of Attorney General. Many individuals take no additional steps after making a report with their local police department, as such, it is believed the actual number of victims and losses in Pennsylvania is significantly greater than current reported statistics.[9] Further, of the complaints received by the Bureau, more than 85% of the victims of these scams are elderly.[10]

Many Pennsylvania consumers are coerced into providing funds via a kiosk to what appear to be a trusted legitimate source, when in fact it is not. These criminals force the consumer to withdraw large sums of fiat money, in some instances up to $50,000 in cash[11], and then visit a convenience store or gas station which is housing a kiosk. Once at the kiosk, the victim is coerced into entering their own personal credentials to create an account with the kiosk operator, entering sensitive personally identifying information such as their telephone number and social security number.[12]

---

[6] https://www.ftc.gov/news-events/news/press-releases/2025/03/new-ftc-data-show-big-jump-reported-losses-fraud-125-billion-2024

[7] Id.

[8] These figures were compiled by the Bureau's scam team.

[9] Studies suggest shame and embarrassment as one of the main reason victims do not report the crime, and if the more individuals they tell the more embarrassed they are. *See* https://www.finrafoundation.org/sites/finrafoundation/files/Blame-and-Shame-in-the-Context-of-Financial-Fraud.pdf

[10] Pennsylvania's Unfair Trade Practice and Consumer Protection Law defines an "elderly" individual as sixty years of age or older. *See* 73 P.S. § 201-8(b).

[11] The Bureau has evidence of consumers transferring as much as $3 million as part of an ongoing scam.

[12] While kiosk operators have varying identification requirements based upon their own terms & conditions or relating to the amount of currency transmitted, the Bureau has discovered many do not comply with their

The victim is then pressured to insert this large sum of cash into the machine, all while remaining on the telephone with the criminal using manipulative emotions such as fear or affection to raise confidence in the legitimacy of the transaction. The consumer is provided with a digital wallet owned by the criminal, where the money will be converted into cryptocurrency and transferred to the criminal's digital wallet within seconds. By entering this digital wallet, the consumer is attesting to the kiosk operator that this wallet is their own. Due to the sophisticated nature of the digital wallet, the victim is unaware of its use or purpose and has no reason to doubt the legitimacy of the explanation offered by the scammer.[13]

III. Kiosk operators are aware of the fraud

Our review of these kiosk operators evidences many failing to follow their own Anti-Money Laundering[14] ("AML") and Know Your Customer[15] ("KYC") policies in collecting required information, such as a consumer's social security number or telephone phone number. Our office alleges that kiosk operators know scams are occurring at dangerously high numbers and provide minimal "warnings" for consumers utilizing the kiosks.[16] Further, our office alleges that because of the significant fees collected by the kiosk operator, they are willing to overlook questionable transactions or incomplete applications when authorizing the transfer. Without regulations to ensure compliance and stifle the ability of scammers to deceive consumers, we believe kiosk operators will continue to disregard their own policies, as well as those federally mandated, to permit the scams to occur while shifting the blame onto the consumer for ignoring basic warnings. Many kiosk operators are collecting a fee on the total amount of the transaction, as much as twenty-six (26%) percent.[17]

When a consumer approaches a kiosk, they are required to provide their credentials into the kiosk to log in and begin a transaction. Each operator's operating system is different, but many provide their terms & conditions and generic warnings before proceeding with a transaction. After providing their user data, the consumer is prompted to enter their digital wallet[18] as the destination where the funds will be sent. Scammers provide the consumer with a digital wallet. The consumer, in entering the digital wallet key[19] into the kiosk, is asserting they personally own the digital wallet and have access to it. Our office has seen many scared, intimidated, or anxious scam victims, who

---

requirements and permit users to create accounts with as little information as a fake name and a fake street address.

[13] In interviews conducted by Agents of the Bureau, many victims indicated they still do not know to this day what the wallet is, how it worked, or what it was used for. Instead, they were told by the criminal on the phone it was safe to use said wallet to complete the transaction.

[14] AML policies are required pursuant to the federal *Bank Secrecy Act of 1970*, 31 U.S.C. § 5311 *et seq.,* the *USA Patriot Act*, Pub. L. No. 107-56 (2001), and the *Anti-Money Laundering Act of 2020*, Pub. L. No. 116-283, 134 Stat. 3388 (2021).

[15] KYC policies are required pursuant to the *Bank Secrecy Act*, 31 U.S.C. at 5311-5314, 5316-5336, and *USA Patriot Act*, Pub. K. No. 107-56 (2001) at section 326.

[16] Many of the "warnings" are buried in long terms & conditions, and are in general terms not applicable to a specific situation.

[17] https://oag.dc.gov/release/attorney-general-schwalb-sues-crypto-atm-operator

[18] The digital wallet is a device or program utilized to access your cryptocurrency, randomly generated which serves as your username. https://www.fidelity.com/learning-center/trading-investing/crypto/crypto-wallet

[19] A digital wallet key are randomly generated numbers and letters, can vary between 26 to 63 characters. https://www.ic3.gov/CrimeInfo/Cryptocurrency

do not understand what a digital wallet is, be threatened or coerced by the scammer on the phone at the kiosk to accept that the digital wallet belongs to them. Kiosk operators point to this as their justification of innocence concerning the transaction, blaming the consumer for entering the digital wallet of the scammer.

Our office has concerns with the continued use of virtual currency kiosks, and their increased use in criminal activity. While their purported use is to permit the quick and easy conversion from fiat currency to cryptocurrency, these kiosks are overwhelmingly utilized to promote scams. Where scammers previously required their victims to purchase gift cards, scammers are adapting to growing technology and are now utilizing these kiosks. While the concept of cryptocurrency and the blockchain is to promote openness for all, the ability to trace the transfer of funds from the originating kiosk to numerous destinations before they are withdrawn is increasingly difficult for law enforcement.[20] Without preventing the scam at the outset at the kiosk, consumers will continue to be deceived without increased government oversight and prevention by kiosk operators.

IV. SB1015

Our office appreciates the General Assembly seeking to address the growing concern of virtual money kiosks and their use as a vehicle for scams and criminal activity. We have reviewed Senator Pennycuick's Senate Bill 1015 and are encouraged by the attempts of the legislature to curb the improper usage of kiosks. Through her work on this bill and on bills protecting our shared constituents from the dangers of AI and chatbots, Senator Pennycuick has been a true champion in ensuring that, as Attorney General Sunday says all the time, technological advancement and public safety are not mutually exclusive.

After reviewing the current draft of the legislation, we would like to use our time to suggest ways that the bill could be strengthened to provide even more protection to Pennsylvania consumers who are frequently defrauded through these kiosks. To be sure, Senate Bill 1015 as written would markedly improve the regulatory environment these kiosks operate in and would provide several critical warnings to prevent fraud from occurring. With the following recommendations we believe that Senate Bill 1015 would become a national model for regulation and fraud prevention.

a. Additional warnings

While the bill has specific requirements and warnings as required in sections four (4) and six (6) of the proposed bill, we would urge that each warning require an affirmative response from the individual attempting to utilize the machine.[21]

We also recommend that all warnings be obvious, occur in multiple steps, and appear in large unavoidable print that ensures the consumer sees it, specifically concerning the potential of being scammed, as indicated by section six (6). As mentioned previously, numerous individuals, mainly

[20] Many criminals have multiple "stops" or transfers from the kiosk to the final destination. Law enforcement have difficulty in tracing the final destination based upon the number of transfers, and therefore locating the criminal becomes increasingly difficult.

[21] Many consumers interviewed indicated that they saw the warning on the kiosk but did not believe it applied to them. We believe any additional warnings or affirmative actions for the consumer to accept will permit the consumer a moment to second-guess their action.

elderly victims, are coerced by the scammer on the telephone, either through threats or affection, telling them to ignore the warnings. Any additional steps that may alert the consumer to second guess the legitimacy of the transaction will better protect Pennsylvania consumers.

Warnings that are provided to consumers should be specifically targeted to the likelihood a scam is currently occurring. We would also request proposed language under section six (6) address the possibility of being coerced by a romance scam. Warnings that address being asked to provide funds to a "romantic interest" they have never met is likely a scam. Many vulnerable adults, especially elderly, will send funds to someone they have only spoken with on the phone, but have never met in person nor seen on video. We believe additional language which adapts to the current trends in scams would best serve consumers to question the legitimacy of the scam.[22]

b. User registration requirements

Greater requirements must be imposed on kiosk operators concerning what information is collected from new users to open an account, such as a user's full legal name, street address,[23] telephone number,[24] social security number, and a copy of an active state-issued identification. Kiosk operators should be required to utilize publicly available services such as Clear[25] to ensure the information entered is accurate and belongs to the user. In many instances, our office has located incomplete information collected by kiosk operators prior to the opening of a new user account, or users providing fake/incorrect information, and yet the operators open the user account regardless. By requiring operators to diligently review all information provided to ensure accuracy, our office trusts only those individuals utilizing the kiosks for legitimate purposes will apply and use the kiosks.

c. Regulations on kiosk hosting businesses

Most kiosks are placed in convenience stores, gas stations, or corner markets across the Commonwealth. As of April 1, 2026, there are approximately 1,423 kiosks in Pennsylvania, with over ninety-five (95%) percent located in those stores.[26] Our office would recommend regulations be imposed upon the store hosting the kiosk. In many situations, the kiosk operator is providing rent payments to a store for hosting the kiosk, usually in the form of a monthly stipend. However, the store owners and employees do not provide any customer service or engage with the kiosk or kiosk customers.[27] Requiring a hosting store place the kiosk in a well-lit, conspicuous location within their store that is clearly seen by store employees and/or store security would help cut down on scams. The bill should impose mandatory training on store owners and employees engaging with customers on how to spot a scam. Further, language which permits the store to refuse access

[22] As of December 31, 2025 the top scams in Pennsylvania include government imposter, phishing, tech support, romance, and cryptocurrency/investment.
[23] Not a post office (PO) box as many users have utilized.
[24] A primary phone number issued by a legitimate carrier (AT&T, Verizon, T-Mobile) and not a second VoIP phone number assigned through apps such as Google Voice or 2ndLine.
[25] https://legal.thomsonreuters.com/en/products/clear
[26] https://coinatmradar.com/state/39/bitcoin-atm-pennsylvania/
[27] Many witnesses interviewed indicated a store employee watched the consumer place significant sums of money into a kiosk, could see the consumer was visibly upset, yet did not engage or interact with the consumer to inquire into their well-being.

to a kiosk should the employee reasonably believe a scam is ongoing would be beneficial. In addition, our office would recommend that clear, conspicuous signage provided by the Office of Attorney General be placed near the kiosk to alert the consumer of the danger of scams.

Additionally, section fifteen (15) of the bill requires kiosk operators to report within forty-five (45) days the location of all kiosks in the Commonwealth. We support this registration requirement, and would encourage additional requirements to report the name, telephone number, and e-mail address of the Compliance Officer for the kiosk operator. The kiosk operator should also be required to include a fully executed contract entered between the kiosk operator and the store hosting the kiosk, at a minimum to include the pecuniary benefit derived from the kiosk to the store owner. The kiosk operator should also be required to provide to the Department any amended or supplemental agreements entered with the hosting store within thirty (30) days. These requirements will assist law enforcement who are investigating any illegal use of a kiosk to have an operator designee in which to interact and seek immediate assistance.

d. Regulations on banking operators

Greater regulations on financial institutions who interact with a consumer actively engaged in a scam, including banks and credit unions, should also be implemented in this bill. Preventing the scam before a financial loss to the consumer would deter bad actors from engaging with their victims, knowing they cannot access the funds to transact via the kiosk. Our office has interviewed many victims who obtained the initial funds to insert into the kiosk by withdrawing it from their personal bank via a teller in-person. Providing language in the bill that would require greater training for tellers to recognize a scam would be valuable.[28]

In addition, language that would permit a bank to temporarily freeze a withdrawal to an individual who shows signs of a scam should be implemented.[29] Providing the bank with the authority to place a reasonable hold on a cash withdraw over a specific amount where the consumer cannot provide proof of a legitimate purchase would halt the scam and increase the likelihood the scammer disengages.[30] We would further recommend that if the transaction is halted, that the bank immediately be required to notify law enforcement who will perform a "welfare" check on the consumer within twenty-four (24) hours, in order to speak with them before the scammer is able to reengage after the funds are released. We believe placing this onus on the bank will cut down on scams before consumers can proceed with the transaction.

e. Blacklist and graylist data publications

In addition to Clear searches, the kiosk operator must compare the information provided through self-maintained and publicly available blacklists, graylists, and government watchlists prior to authorizing the transfer of funds. In many cases, criminals will utilize one kiosk operator until they

[28] Many tellers interviewed by our office indicated they were confident the customer withdrawing the funds were engaged in a scam, but due to bank policy they could not stop it.

[29] Many scam victims actively engaged in a scam will not listen to a teller suggesting they hang up the phone or that they are being scammed. Language in the bill that would prohibit the individual from withdrawing the money would stop the scam from continuing and the scammer likely to discontinue the call.

[30] Many scam victims cannot show proof as to who they are sending the funds to, or get defensive. Placing this extra layer of security will permit the teller to act with reasonable judgment to deter a scam from continuing.

are caught, just to sign up with a competing kiosk operator. Because of the lack of oversight, and due to kiosk operators not sharing their blacklists amongst themselves, criminals are able to bounce between kiosk operators undetected. By comparing the information provided against publicly provided lists, as well as the mandatory government watchlists, kiosk operators can ensure that suspicious activity flagged from another kiosk operator does not occur at their own kiosk.

Kiosk operators, flagging suspicious digital wallets and/or users, must be required to publish and make this information available to other kiosk operators. By having a uniform blacklist and graylist database accessible by all kiosk operators engaging in business in the Commonwealth, this shared information can prevent criminals from bouncing between kiosk operators after they have been flagged for suspicious behavior.

f. Transaction authorizations

We recommend that a kiosk operator only authorizes a transaction after confirming the identity of the individual utilizing the kiosk. By utilizing the existing cameras already built into the kiosks, the operator can compare the user with the image from state issued ID provided during the account registration to confirm the identity of the user.[31] For an individual utilizing a kiosk for a legitimate purpose, this identity confirmation should be of no concern.

We also strongly encourage language that if an operator observes the consumer standing at the kiosk on their phone, that the transaction be denied. In ninety-five (95%) percent of consumer transactions reviewed by our office, the consumer engaged in a scam was on the telephone with their scammer. As mentioned previously, the scammer is generally threatening or coercing through affection the consumer to continue with the transaction, providing explanations as to why the warnings or alerts are misplaced or do not apply to them. By placing this onus on the operator, we believe numerous scams can be prevented.

Transactions should also be denied if the digital wallet and/or user account accessing the kiosk has been utilized recently in a separate location. Many criminals share the same digital wallet within and across state lines. We would recommend that a transaction be denied if a user account has been used within fifty (50) miles of the presently pending transaction location in the preceding twenty-four (24) hours, or in another state within the last three (3) days. Additionally, the same should apply for the use of a digital wallet. If a digital wallet was used at another location of any distance within two (2) hours of the pending transaction, it should be denied. These restrictions will cut down on criminals victimizing numerous consumers at the same time and hopefully minimize the ability to obtain new user registrations and new digital wallets based upon their frequent usage.

g. Money transmitter licenses

Our office supports the requirement that virtual currency kiosks be licensed by the Pennsylvania Department of Banking and Securities as a money transmitter as required under section 16 of the bill. Our office is aware of many operators who position themselves as a "middleman" and are not

[31] It is also believed that criminals will not risk exposing themselves utilizing the kiosks themselves and identifying themselves on camera.

required to be licensed. We believe the language proposed will ensure all kiosk operators abide by and obtain the requisite license. In addition to the proposed language, we would encourage language which subjects an operator to punishment should they fail to comply and obtain a license after the 60-day grace period following the bill's implementation, such as the inability to do business in the Commonwealth and seizure of those kiosks.

h. Violations of the Unfair Trade Practice and Consumer Protection Law

Finally, our office would propose language that provides that a violation of this proposed Act be a violation of the Unfair Trade Practice and Consumer Protection Law ("Consumer Protection Law").[32] Many other Pennsylvania statutes follow the same precedent,[33] and authorize the Attorney General to bring an action in the name of the Commonwealth to enjoin unfair and/or deceptive behavior and to ensure our Agents and Prosecutors have the proper legal tools to combat scammers via these kiosks. The Consumer Protection Law does provide the Attorney General with the authority to seek temporary and permanent injunctions, as well as seek civil penalties up to One Thousand Dollars ($1,000) per violation, or up to Three Thousand Dollars ($3,000) should the victim be age sixty (60) or older.

V. Conclusion

Our office believes that regulation from the General Assembly in accordance with SB1015 will prevent consumers from being deceived and falling victims of scams through virtual money kiosks. We believe with additional proposed language, the bill can assist law enforcement in reducing scams impacting many vulnerable Pennsylvania consumers.

On behalf of Attorney General Sunday, we appreciate the opportunity to address this joint session of the Senate Committees and support the ongoing protection of Pennsylvania consumers from scams and other bad actors.

Paul D. Edger
Senior Deputy Attorney General in Charge
Office of Attorney General
Bureau of Consumer Protection

[32] 73 P.S. §201-1 *et seq.*

[33] Including without limitation the *Manufactured Home Community Rights Act*, 68 P.S. § 398.1 *et seq.* and the *Automotive Industry Trade Practices*, 37 P.S. § 301.1 *et seq.*