Joint Testimony Submitted to the
Senate Communications and Technology Committee's
Hearing on Senate Bill 1015
April 8, 2026

Good morning, I am Frank Serina here today on behalf of the PA Bankers Association, the PA Association of Community Bankers and CrossState Credit Union Association. These three Associations collaborate on several issues including elder financial abuse prevention and response. I am the Chief Risk Officer from Members 1st Federal Credit Union and see fraud and abuse every day, week in and week out. We thank the sponsors of SB 1015 for introducing legislation to regulate virtual cryptocurrency kiosks.

Financial institutions are committed to meeting consumer demand for digital assets, including stablecoin and other cryptocurrencies, while mitigating the risks these emerging products and technologies pose to consumers and the broader financial system. We advocate for the application of the principle of "same risk, same activity, same regulation" to all entities that offer financial institution-like services.

We are very concerned about virtual currency kiosks because they are being used to defraud our customers and members - particularly seniors. Victims not only suffer financial harm but also endure emotional distress, facing the loss of their savings, homes, and dignity.[1] The impact extends to family caregivers and taxpayers who shoulder additional burdens to support financially devastated victims. As our nation undergoes a demographic shift, with more seniors than children projected within the next decade, the urgency to address elder financial exploitation grows.

The fraud schemes and illicit activities that some of our bank customers and credit union members are experiencing with crypto ATMs are alarming. We had one member initially request a $20,000 cashier's check payable to himself, claiming it was for a vehicle purchase to be signed over to a dealer. Staff identified the request as unusual and provided cautionary guidance. The member then returned the same day requesting $20,000 in cash instead, offering inconsistent explanations. Staff again intervened, reviewed scam prevention materials, and escalated concerns to Fraud Management. Due to limited cash availability, only $5,000 was withdrawn at

[1] The Thief Who Knows You: The Cost of Elder Exploitation Examined (aarp.org)

that time. When pressed, the member changed their story, claiming the funds were for purchasing a truck from a personal friend, but refused to provide details or allow verification.

The following day, a Fraud Investigator attempted to contact the member after discovering an additional $15,000 had been withdrawn from a different branch, bringing the total to $20,000. Despite further warnings at that branch, the member continued to insist the funds were for a legitimate vehicle purchase and denied any fraud involvement.

Later that same day, the member returned and disclosed they had been directed by scammers to fabricate the vehicle purchase story and convert the funds into cash for deposit into a Bitcoin ATM. A retail employee ultimately intervened before the transaction was completed, preventing any loss. The member admitted to following the scammers' instructions, and all $20,000 was successfully redeposited.

In another case, a member visited multiple branches and withdrew more than $45,000 in cash. The initial $37,000 withdrawal was attributed to the purchase of a 2020 BMW X5 from a long-time acquaintance who allegedly required cash payment. Recognizing potential red flags, branch staff and a Fraud Investigator conducted detailed scam prevention discussions. The member acknowledged the risks—including the inability to recover funds if scammed—but insisted the transaction was legitimate.

Later that same day, the member attempted additional withdrawals at other branches, offering inconsistent explanations such as household expenses, tuition, and holiday costs. Despite repeated questioning and continued scam awareness efforts, the member denied any fraudulent involvement. As concerns escalated, Fraud Management contacted both the member and her Power of Attorney and placed temporary restrictions on the account to mitigate further risk.

During a subsequent visit, the member disclosed that the incident began with a fraudulent "Microsoft" pop-up, which led to screen sharing and ongoing instructions from a scammer. She confirmed that $37,000 had already been deposited into a Bitcoin ATM. After reviewing prior warnings and identifying clear scam indicators, the member admitted she had misrepresented the purpose of the withdrawals under the scammer's direction. She reported that the remaining funds were still in her possession, and staff assisted in redepositing $12,500. The member's Power of Attorney was engaged for additional oversight, and the member received guidance on securing her devices, updating credentials, and filing a police report.

Together, these cases illustrate how scammer-directed coaching enables individuals to circumvent institutional controls by presenting consistent but false narratives. Despite multiple interventions, risk disclosures, and account restrictions, cryptocurrency kiosk transactions were still executed before the fraud was ultimately recognized.

The role of virtual currency kiosks in fraud and crime is now so pervasive that FinCEN, the Financial Crimes Enforcement Network, issued a notice last August urging financial institutions to significantly increase their vigilance in identifying and reporting suspicious activity involving virtual currency kiosks. The notice states that virtual currency kiosks are increasingly being used for fraud but also for other illegal activity, such as laundering money from illicit drug sales.

The FinCEN notice states that according to the Federal Bureau of Investigation's (FBI) Internet Crime Complaint Center (IC3), criminals engaged in fraud schemes often direct victims to use a Convertible Virtual Currency (CVC) kiosk to send payments under false pretenses. In 2024, the FBI's IC3 received more than 10,956 complaints reporting the use of CVC kiosks, with reported victim losses of approximately $246.7 million. This represents a 99 percent increase in the number of complaints and a 31 percent increase in reported victim losses from 2023. The Federal Trade Commission (FTC) likewise identified, based on an analysis of consumer reports, that fraud losses through CVC kiosks have skyrocketed. As we know, most cases of elder fraud go unreported due to victims' self-shame or fear of retribution from the criminals who threatened them.

Financial institutions comply with FinCEN guidance on reporting suspicious activity, but reporting has limited benefits. Thus, we urge the sponsors of the bill to include important consumer protections which are summarized below.

We also respectfully request your support for legislation providing financial institutions better tools to prevent and respond to elder financial abuse. There is room for improved collaboration between financial institutions and adult protective services. State legislatures are enacting laws to facilitate greater information sharing and allow for banks and credit unions to decline to engage in suspicious transactions before irreversible disbursements occur.

Our Associations support legislation such as SB 738 that:

- Establishes a clear legal framework for banks and credit unions to report suspected EFE to and cooperate with state authorities;
- Authorizes financial institutions to consult with an older adult's authorized contacts, guardians or other fiduciaries, and attorneys and financial advisors for assistance in addressing EFE;
- Enables financial institutions to hold, refuse or prevent suspicious transactions before irreversible or difficult to recover disbursements;
- Expands authorization for financial institutions to voluntarily provide records to area agencies on aging to investigate EFE and simplify procedures for area agencies to request additional records; and
- Authorizes AAAs to share information with FIs regarding investigations of EFE as necessary to protect older adults, such as whether to refuse, prevent or authorize transactions, or expand or release holds on transactions.

Such legislation would equip institutions with more proactive tools to protect our seniors.
On behalf of PA Bankers Association, the PA Association of Community Bankers, and CrossState Credit Union Association, I thank you for the opportunity to appear before you today and will answer any questions you may have.

Appended below: Summary of draft amendments to SB 1015

Summary of Financial Institutions' Suggested Draft SB 1015 Amendments

- Disclosure requirements are expanded to apply to all types of virtual currency business activity with PA residents rather than only transactions at virtual currency kiosks.
- The initial disclosure requirements regarding material risks and an account's general terms and conditions are required to be presented in a face-to-face, telephonic, or similar form of live interactive audio-visual communication.
- In addition to being provided in English, disclosures are also required to be given in any language used by a virtual currency business in advertising or to communicate with a customer.
- A scope provision is added that excludes from the act banks, savings associations, trust companies, activities governed by the SEC or under the PA Securities Act, foreign exchange transactions, escrow agreements of title companies and attorneys, the transfer of security interests, and persons who do not engage in virtual currency business activities for compensation.
- Exceptions to the bill's restrictions on access to information obtained by the PA Department of Banking and Securities (DoBS) in examinations and investigations are added that mirror the provisions of the PA Department of Banking and Securities Code that give the DoBS discretion to release information and allow for the disclosure of information in administrative adjudications.
- Prior to conducting any transaction with a customer, a virtual currency business is required to comply with know-your-customer requirements.
- Virtual currency businesses are required to give 30-days advance notice to customers of any changes in account terms and conditions.
- Fees charged for transactions are limited to the greater of $5 or 15% of the dollar value of the virtual currency included in the transaction.
- The material risk disclosures are expanded to include examples of typical types of fraud involved in virtual currency transactions and to include recommendations if fraud is suspect to contact adult protective services agencies in addition to law enforcement.
- The completion of transactions is required to be delayed for at least 15 minutes to give a customer an opportunity to review and correct any mistakes in a receipt issued for the transaction.
- In addition to blockchain analytics, a virtual currency business is required to adopt policies and procedures to prevent the transmission of virtual currency to digital wallets associated with fraudulent activities.

- A virtual currency business is required to adopt measures to deter fraud consistent with those imposed by federal FINCEN regulations.
- Virtual currency businesses are required to submit reports of suspected fraud and abuse involving older adults or other adults in need of protective services to area agencies on aging of local adult protective services agencies and are authorized to delay such transactions in a manner consistent with FINRA Rule 2165.
- Virtual currency kiosks are required to be in safe and well-lighted and well-traveled locations and to be assessable to persons with disabilities.
- A daily $1,000 limit is imposed on any transactions not authorized by direct communication between a customer and a virtual currency business, and for new customers, a $1,000 per-day, or aggregate $10,000 limit, is imposed on all transactions occurring within the first 30 days.
- Virtual currency businesses are required to (1) refund unauthorized transactions in the same manner as required by Regulation E; (2) refund fraudulently induced transactions if the virtual currency business fails to give the required disclosures required by the legislation, operates without a license, fails to comply with legislation's anti-fraud, financial exploitation, compliance, consumer protection, and transaction limits, or has actual knowledge that a transaction has been fraudulently induced; and (3) pay a $50 penalty or actual damages incurred for failure to provide a receipt as required by the legislation.
- Existing businesses, including kiosk operators, not currently permitted under the Money Transmitter Act, are required to submit a "complete" application within 60 days to continue operations.
- Severability provisions are added that ensure that If the money transmitted licensing requirements of the legislation are preempted by federal law or rules, or other provisions of the law are preempted by federal law, or otherwise held to be unenforceable, the remaining requirements of the legislation remain in effect.
- Surety bond requirements are increased and the DoBS is given the discretion to increase bonding amounts required to whatever amount is determined to be adequate to protect customers.
- If a virtual currency business takes custody of virtual currency on behalf of a customer, (1) the virtual currency is required to be held for the benefit of the customer, is not the property of the virtual currency business or subject to claims of creditors of the virtual currency business, and may not be subject to security without the consent of the customer; and (2) the virtual currency business is required to (i) maintain adequate amounts of each type of virtual held for its customers; (ii) follow the instructions of the customer regarding the transfer, exchange, redemption or disposition of the virtual currency; (iii) pass-through

to the customer all payments and distributions received from the issuer of the virtual currency, (iv) recover or compensate the customer for any virtual currency transferred without authorization; and (v) provide access to account statements at least monthly.

- The DoBS is authorized to collect assessments to be paid into a Virtual Currency Trust Fund to pay the expenses related to the examination and regulation of virtual currency businesses and is prohibited from using the Banking Trust Fund for the examination and regulation of virtual currency businesses.
- Require that anyone applying to be licensed is subject to the statute if they are a qualified provider or can be qualified.
- Reduce the ownership share from 20% to 5% for greater compliance.
- Violations of the legislation are defined as unfair and deceptive practices under the Unfair Trade Practices and Consumer Protection Law.