Crypto ATM Framework Keys: Registration, Transaction Information, Warnings, Active Support Hotlines, Recourse Policies, & Customer Verification

To mitigate and minimize the increasing use of crypto ATMs in cybercrimes and ensure that Crypto ATM businesses receive the oversight clarity and tools they require to be successful in neutralizing illicit activity it is important to develop a responsible and right sized oversight framework for the industry. A business-friendly framework that also protects seniors from cybercrime should contain the following components:

Essential Oversight Framework Components

- State Crypto ATM Kiosk Location & Operator Registration- Law enforcement and oversight agencies are frequently unaware of crypto ATM kiosk locations and their operators when they are attempting to investigate cybercrime incidents because kiosks are not registered at the state level, which can delay investigations. Due to how quickly cryptocurrency transactions settle it is vital that law enforcement/regulators can identify crypto ATM kiosks swiftly to obtain critical information to assist potential victims.

- Investigative Information & Crypto Wallet Addresses on ATM Receipts- To enable law enforcement and oversight agencies to investigate crypto ATM cybercrimes appropriately, it is necessary that they receive the information they require to trace potential illicit transactions quickly. Therefore, crypto ATM receipts should include transaction times, locations, dollar amounts, crypto hashes, and beneficiary crypto wallet addresses to assist customers and investigators in their fight against cybercrime.

- Enable Authorities to Post Cybercrime Warnings on Crypto ATMs- Sharing information about cybercrime schemes involving crypto ATMs can help make potential victims and/or staff at businesses hosting crypto ATM kiosks aware of popular cybercrimes to help protect victims. By allowing state and local authorities to post warnings the public will gain knowledge of cybercrime methodologies that can help protect the money of U.S. citizens and Idahoans.

- Operate Functional Law Enforcement/Regulator & Customer Support Hotlines – Customers, law enforcement officials, and oversight agencies regularly encounter either non-existent or non-functioning crypto ATM support lines, which frustrate both customers and law enforcement/oversight professionals investigating cybercrimes. Operators should have active well-functioning customer support and law enforcement lines during operating hours to assist with potential cybercrimes involving crypto ATMs.

- Develop Fair Recourse/Fee Return Policies – If it is found that a first-time crypto ATM cybercrime victim reports their fraudulent losses in a timely manner (e.g., 15 - 30 days) it makes sense for their fees to be refunded. However, crypto ATM operators should not be responsible for transaction costs when providing a refund (e.g., return ACH or wire fees).

- Implement Sound Identity Verification Practices & New Customer Protections – It is critical that customer verification operations (even for small transactions) require some type of government issued identification to prevent cybercrimes involving crypto ATMs. Currently, some crypto ATMs accept easily obtainable pieces of information such as phone numbers or social security numbers that make it easy for cybercriminals to pull off their schemes. Additionally, new crypto ATM customers can be cybercrime victims, so it is important to put some safeguards in place for the first 7- 14 days, such as transaction limits and verbal confirmations, to help protect them from becoming victims.

Potential Additional Oversight Framework Components

- Transaction Limits – Outside of new customer safeguards many states (e.g., Iowa, Louisiana, and Maine etc.) are placing dollar limits on crypto ATM transactions either on a daily basis or over a specified timeframe (e.g., 7 – 14 days) to minimize potential cybercrime losses.

- Resting Periods – The speed of crypto ATM transactions means that some friction in the settlement process could (e.g., anywhere between 1 – 24 hours) protect the funds of cybercrime victims before they are lost forever.