Surge in Cybercrimes Against Seniors Involving Crypto ATMs Necessitates the Development of an Oversight Framework

Senior Fraud & Financial Exploitation Prevention Working Group

Executive Summary

The digitization of society and growing acceptance of digital assets (e.g., Bitcoin and Ethereum) is leading to an exponential increase in cybercrimes involving cryptocurrency automated teller machines (ATMs), which makes the development of a crypto ATM oversight framework necessary to better protect Idaho and its senior community from illicit actors/cybercriminals. Known losses from cybercrimes involving cryptocurrency rose 66% nationally and over 76% in Idaho during 2024, while reported cryptocurrency ATM losses grew to $246.7 million in 2024 with seniors being three more times likely to become victims. The combination of Idaho's large senior population, the increasing usage of cryptocurrency/crypto ATMs, and growing cybercrime against Idaho's senior community makes the creation of a responsible oversight framework critical to protecting Idahoans from bad actors, while also enabling crypto ATM businesses to operate successfully.

Digital assets have the potential to create cheaper, quicker, and more inclusive/accessible financial services, but the absence of a right sized crypto ATM oversight framework that accounts for the pseudonymous/global nature, short settlement cycles, and accessibility of digital assets will be important for the industries legitimacy and protection of Idahoans.

An effective crypto ATM framework should start by establishing a state registration process for kiosk locations, documenting crypto wallet address information on transaction receipts, developing active and functional support hotlines, creating fair customer recourse/fee return policies, enabling cybercrime warnings to be placed on crypto ATMs, and ensuring sound customer verification practices and new customer protections are in place. This would provide crypto ATM businesses with a clear business friendly framework, while also protecting Idaho's senior population from potential financial losses and harm.

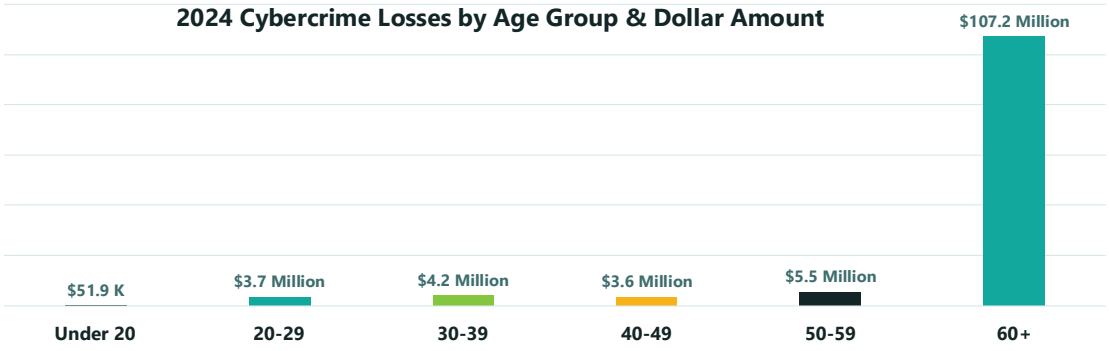
1 2 3

Cybercrimes Against Seniors Involving Crypto ATMs are Rising in the U.S. & Idaho

The absence of a well-defined crypto ATM oversight framework/legislation creates inconsistent standards, responsibilities, and authorities that make crypto ATMs an attractive tool for cybercriminals, which is leading to an exponential increase in cryptocurrency related cybercrimes against seniors throughout the U.S. and Idaho. Crypto ATMs enable users to convert cash into digital assets without the need for conducting business with traditional financial institutions. Since crypto ATMs mainly operate outside the traditional financial system and accompanying regulatory frameworks, bad actors are using this oversight gap to successfully carry out their cybercrime schemes and profit at the expense of U.S. and Idaho victims, especially seniors.

Cryptocurrency related crime in Idaho is rising at a higher rate than the national average and in many cases, cybercriminals are using crypto ATMs to steal money from Idahoans. Known cybercrime in Idaho involving cryptocurrency totaled over $35 million in 2024 up from $19 million in 2023.[4] [5] Additionally, known losses from cryptocurrency ATMs grew over 30% in 2024 and seniors continue to be the main targets of cybercriminals who are using crypto ATMs in their tech support, government imposter, and investment schemes.[6] The FBI's Internet Crime Complaint Center (IC3) highlights that victims 60 and over represent the number one age group for known losses with losses significantly higher than all other age groups combined. (see IC3 statistics chart below).[7]

SENIORS ARE THE #1 VICTIMS OF CRYPTO ATM CRIMES



Idaho requires a crypto ATM oversight framework that will provide crypto ATM stakeholders and businesses with the clarity they require to successfully operate, while concurrently closing the regulatory gaps that cybercriminals depend upon to steal the hard-earned money of seniors (and other citizens) throughout the U.S. and Idaho.

Cryptocurrency's Attributes & Increasing Acceptance Lead to Mounting Crypto ATM Usage by Cybercriminals

The benefits cryptocurrency provides in the form of transaction speed, one-way payments, decentralized control, cryptographic privacy, and global reach make it a useful tool for cybercriminals and is a key reason why they use crypto ATMs in their schemes. Cryptocurrency transactions can be settled in a matter of minutes or even seconds and once crypto assets are sent to a beneficiary's digital wallet there is no way to reverse the transaction since there is no centralized entity with authority/control over the transaction(s). Furthermore, cryptocurrency can be sent to anyone anywhere in the world at any time and it uses cryptography (mathematical algorithms that complete/verify transactions) that eliminates the need for actual

names to be used in transactions. When these unique cryptocurrency attributes and features are combined it is easy to see why cybercriminals are having victims send cryptocurrency to them via crypto ATMs.

The absence of a crypto ATM oversight framework often makes it beneficial for cybercriminals to have victims take cash out of their financial institutions and use crypto ATMs to facilitate illicit transactions rather than coaching them through the process of setting up accounts and opening digital wallets at entities with more oversight responsibilities/capabilities. Once physical cash is used at a crypto ATM and a victim sends cryptocurrency to an illicit actor's wallet address the transaction is complete and the cybercriminal(s) possesses full ownership/control of the funds.

The growth of the crypto industry is leading to an increase in crypto ATMs, which means that these machines need an oversight framework that will deter and prevent bad actors from exploiting victims both nationally and in Idaho. As cryptocurrency continues to become more mainstream its market cap is growing dramatically (totaling over $3 trillion in 2025) making it easier for cybercriminals to conceal their illicit activity, while concurrently making it more difficult for investigators to identify cybercrimes involving cryptocurrency/crypto ATMs.[8] As with any growing market, illicit actors/cybercriminals can hide in the noise of legitimate activity and services by incorporating the growing legitimacy of the crypto industry into their schemes (e.g., investment scams such as pig butcherings).[9]

Cybercrimes Against Seniors Involving Crypto ATMs are Likely to Rise in Idaho Due to Population Growth, Cybercriminal Targeting, & Weak Oversight

As cryptocurrency markets and Idaho's senior population continue to grow, cybercriminals will likely increasingly use crypto ATMs to conduct cybercrime until a clear well-defined crypto ATM oversight framework is implemented that helps better protect Idahoans in their golden years. According to recent studies, 22.7% of Idaho's population is aged 60 or over with research showing that Idaho ranks in the top three states for growth in seniors between 2010 - 2020.[10] [11] Since U.S. citizens aged 60 or over are the main victims of crypto ATM cybercrimes, it is imperative that a crypto ATM oversight framework is created that better protects Idaho's large senior community.[12]

The absence of a crypto ATM oversight framework in Idaho and the fact that seniors are a prime target for cybercriminals due to their increased reliance on online interactions (to avoid loneliness), large financial savings and asset ownership (e.g., houses), and good credit ratings means they are likely to be the main victims of cybercrimes involving crypto ATMs moving forward.[13] Currently, baby boomers and the silent generation have the highest net-worths per household and are estimated to have over $124 trillion in wealth ready to be transferred.[14] This wealth combined with crypto ATM oversight gaps will continue to incentivize cybercriminals to target seniors and direct them to use crypto ATMs in their illicit schemes.

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 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 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.

The bottom-line is that crypto ATM cybercrimes against seniors are proliferating throughout the U.S. and Idaho and will continue to grow without a fair and meaningful crypto ATM oversight framework in place. Until a crypto ATM oversight framework is created and implemented, Idaho's seniors will be less safe and continue to have their hard-earned money stolen at a rapid pace, which could cause them to become dependent on government services/support or even force them back to work (whether they are able to or not). Additionally, crypto ATM businesses should have a clear framework in place that accounts for both their business needs and those of their customers. This makes the creation and adoption of a crypto ATM oversight framework vitally important for protecting Idaho families and its senior community, while also enabling responsible business operators to succeed for the benefit of their customers.

SEE APPENDIX A FOR IDAHO CRYPTO ATM FINANCIAL CRIME EXAMPLES

Appendix A: Idaho Crypto ATM Financial Crime Examples

Bank Employee Imposter Scheme: $117,700 Crypto ATM Loss for Idaho Victim

Criminal actors posing as representatives of Chase Bank contacted a 72-year-old Star, ID victim and falsely told her that there were issues with her accounts. The suspects convinced the victim to withdraw $117,700 from her bank account and transfer the funds to the bad actor's accounts via a Cashier's Check and crypto ATMs to supposedly protect her funds. She later discovered she was a fraud victim and unable to recover her losses.

Fraudulent Retail Purchases Scheme: $77,500 Crypto ATM Loss for Idaho Victim

Two criminal actors posing as representatives from Amazon and Wells Fargo deceived a 67-year-old Meridian, ID victim into believing that someone was making fraudulent purchases on their Amazon account. The bad actors convinced the victim to take out $77,500 from his financial accounts and deposit them into crypto ATMs located in Boise, Meridian, and Nampa to supposedly protect the funds. Once the fraud was complete the victim was unable to recover his losses.

Family Emergency Scheme: $50,000 Crypto ATM Loss for Idaho Victim

A criminal actor convinced a 75-year-old victim that her adult child had been arrested for a serious felony crime in Meridian, ID. The suspect told the victim that she needed to take $50k out of her bank account and deposit the funds into multiple crypto ATMs in Ada County to pay her adult child's bond fees. Once the funds were deposited into the crypto ATMs the victim became aware that the money was stolen and could not be retrieved.

Tech Company Imposter Scheme: $25,000 Crypto ATM Loss for Idaho Victim

A 73-year-old victim from Star, ID reported that a criminal actor impersonating a Microsoft representative stole $25k from him using crypto ATMs. The bad actor told the victim to send $25k in Bitcoin to get a false charge reversed. The victim took money from his personal bank account and deposited it into a crypto ATM before learning that the money was stolen and could not be recovered.

Government Imposter Scheme: $11,000 Crypto ATM Loss for Idaho Victim

A criminal actor impersonating a law enforcement official contacted an elderly Idaho victim telling them that they missed jury duty and there was a warrant out for their arrest. The bad actor told the victim that they needed to settle the matter by depositing money into a crypto ATM. At the direction of the bad actor the victim took $11k out of their bank account and deposited it into a crypto ATM at a vape shop to supposedly settle the matter. The victim soon became aware that the money was stolen and could not be recovered.

End Notes

[1] https://www.ic3.gov/AnnualReport/Reports/2024_IC3Report.pdf.

[2] https://www.ic3.gov/annualreport/Reports/2024CryptocurrencyState/#?s=15.

[3] https://www.nbcnews.com/business/business-news/bitcoin-atm-scams-surge-disproportionately-duping-older-adults-rcna168976.

[4] https://www.ic3.gov/annualreport/Reports/2024CryptocurrencyState/#?s=15.

[5] https://www.ic3.gov/annualreport/Reports/2023CryptocurrencyState/#?s=15.

[6] https://www.ic3.gov/AnnualReport/Reports/2024_IC3Report.pdf.

[7] Ibid.

[8] https://www.reuters.com/technology/crypto-market-capitalisation-hits-record-32-trillion-coingecko-says-2024-11-14/#:~:text=The%20sum%20market%20value%20of,the%20Reuters%20Artificial%20Intelligencer%20newsletter.

[9] Pig butchering is a long-term financial scheme that combines elements of investment scams, friendship/romance scams, and cryptocurrency to steal all the money a person possesses or can access. For more information on pig butchering schemes please use this link.

[10] https://www.neilsberg.com/insights/idaho-population-by-age/.

[11] https://www.consumeraffairs.com/homeowners/elderly-population-by-state.html.

[12] https://www.ic3.gov/AnnualReport/Reports/2024_IC3Report.pdf.

[13] https://www.fbi.gov/how-we-can-help-you/scams-and-safety/common-frauds-and-scams/elder-fraud#:~:text=Seniors%20are%20often%20targeted%20because,make%20them%20attractive%20to%20scammers.

[14] https://finance.yahoo.com/news/124-trillion-great-wealth-transfer-133213515.html.