digitalmint

From the Desk of Marc Grens & Jonathan Solomon
Red Leaf Chicago, LLC., d/b/a DigitalMint
301 W Grand Ave, #383
Chicago, IL 60654
founders@digitalmint.io

February 2, 2026

RE: Comment for the State of Wisconsin Cryptocurrency Kiosk Legislation: from the Founders of the One of the Earliest and Largest Crypto ATM Operation in the United States

We write to you as the co-founders of DigitalMint, formerly one of the earliest and largest cash-to-cryptocurrency ATM operators in the United States. Founded in 2014, we built DigitalMint with the mission of providing financial services to the underbanked population, an onramp to digital payments for those who needed it most. We are writing today to offer our support for this legislation and to share the hard-won lessons from our decade of experience as former operators who voluntarily exited the industry in 2024 due to the systemic fraud and consumer harm we witnessed firsthand.

From our earliest days, we took a different approach than many of our competitors. Unlike many competitors who outsourced compliance and software, we developed our systems in-house to maintain strict control. As early as 2016, we were the first operator to require full government-issued identification for all account openings, regardless of transaction size. This rigorous approach gave us unprecedented visibility into who was using these machines and why.

What we discovered over the following years was deeply troubling and ultimately shaped our decision to exit the business entirely.

Our internal data, encompassing tens of thousands of records and interactions over several years with our customer support and fraud prevention teams revealed a striking correlation: nearly all customers who transacted $1,000 or more were victims of fraud. This was not an isolated phenomenon but a systemic problem inherent to the cryptocurrency kiosk model.

When we recognized the scope of the fraud problem, we attempted to lead the industry toward higher standards by establishing a non-profit industry think tank dedicated to improving fraud prevention across all cryptocurrency kiosk operators. However, when we approached executives at other major kiosk companies, the response was disheartening but clear: because there were no regulations forcing them to stop fraud, preventing scams would only decrease their revenues. Less scrupulous operators had no incentive to implement safeguards that might cause customers to abandon transactions. Consequently, bad actors were profiting immensely from the victimization of vulnerable citizens.

The economic reality made our position untenable. Because we implemented rigorous compliance procedures and refused to process transactions we believed were connected to fraud, our revenues per location were a fraction of those of all our competitors. This meant we could not compete for prime retail locations, as landlords naturally chose operators who could pay higher monthly fees. When we explained to retail partners that their higher rents were, in effect, subsidized by fraud victimization, we were greeted with little sympathy. The market rewarded those willing to look the other way.

By 2022, we faced an unavoidable conclusion: the cryptocurrency kiosk industry would not clean itself up, and fraud victimization would only worsen without external intervention. We made the difficult strategic decision to wind down our cryptocurrency kiosk operations entirely, a process we completed in 2024. Today, DigitalMint focuses exclusively on cyber incident response and ransomware settlement services, where our commitment to compliance is an asset rather than a competitive disadvantage.

We believe AB968 is a necessary corrective measure that the industry failed to implement on its own. Specifically, we support the following provisions and offer additional recommendations based on our operational experience:

1. **Money Transmitter License Requirement:** By extending money transmitter requirements to virtual currency kiosk operators, the bill closes a potential regulatory gap that has allowed inexperienced and non-compliant operators to proliferate. Requiring a money transmitter license ensures that kiosk operators are subject to meaningful oversight and accountability.

2. **The $500 Daily Transaction Limit:** Our data confirms fraud victimization was nearly universal among customers transacting at or above this threshold. However, nearly all customers above $1,000, whether observed by our fraud team or through pattern scenarios, were victims of fraud. This daily limit will serve as a critical safeguard to reduce the damage.

3. **Enhanced Identity Verification:** Requiring a photograph of the customer and a copy of their government-issued ID is essential. Scammers rely on anonymity; these requirements create a critical paper trail that deters fraud and aids law enforcement investigations.
    a. ***Recommended Enhancement: Identity Verification Standard***. The legislation should make clear that operators must verify customer identification *against reputable third-party databases* and maintain records of this verification. Simply collecting a copy of an identification document does not prevent the use of stolen or fraudulent IDs, which we encountered with disturbing frequency.

4. **Caps on Fees:** The fee cap of the greater of $5 or 3% prevents operators from exploiting vulnerable consumers with exorbitant charges; and, frankly, removes one of the economic incentives to target victims of fraud, who are often induced to pay higher fees as part of the scam.
    a. ***Recommended Enhancement: Fee Disclosure Requirement.*** The legislation should also require prominent disclosure of all fees at the point of transaction, including any other charges that may not be obvious to consumers. Our experience revealed that many victims were induced by other kiosk operators to pay fees they did not expect or understand.

5. **Mandatory Refunds for Fraud Victims**: The bill's refund provision for fraud victims who report within 30 days creates a powerful incentive for operators to take fraud seriously. When operators bear the financial cost of fraud, they have reason to implement the compliance procedures necessary to prevent it.
    a. ***Recommended Enhancement: Centralized Fraud Reporting***. The legislation should require operators to report suspected fraud transactions to a centralized database accessible to law enforcement and regulators. In the course of our operations, we developed significant intelligence about fraud patterns and scam methodologies, but there was no mechanism to share this information with other operators or with law enforcement systematically. A centralized reporting requirement would enable regulators and law enforcement to identify emerging fraud trends and take action before they become widespread.

Frequently Asked Questions from Regulators and Law Enforcement:

1. **What is the overall use-case for Crypto ATMs?**
    a. While originally intended to serve the underbanked as an on-ramp to digital payments, the reality we observed was that the use-case shifted increasingly and heavily toward fraud, especially at the $1,000 level and above. Scammers prefer cryptocurrency kiosks because they allow for the immediate, irreversible conversion of cash into limited traceability of assets or without the reversibility associated with bank transfers or credit card payments. Unfortunately, especially with transaction fees well over 10% and many other better options to purchase cryptocurrency or remit funds overseas, there is no longer any legitimate use-case for Crypto ATMs.

2. **Does having strong consumer warnings and questionnaires at the point of sale help protect against fraud?**
    a. Consumer warnings and questionnaires are necessary, but provide no help when it comes to stopping fraud. We implemented extensive warnings and required customers to acknowledge that

they were not sending money to a government agency, romantic prospects, or other common scam scenarios. While it may suggest that measures could prevent fraud, sophisticated scammers coach their victims on how to navigate these safeguards. The psychological manipulation employed by fraudsters is extremely powerful, and many victims simply ignored or dismissed warnings that should have been obvious red flags. Warnings are an important component of a comprehensive fraud prevention strategy, but they cannot be relied upon alone. Additionally, we recommend such warnings and disclosures clearly include the bill's concept of "fees or other charges" that would be charged to the customer. Overall, however, we do not expect to see a decrease in fraud as a result of these warning signs on Crypto ATMs.

3. **Does having blockchain forensics companies scanning wallets at the point of the sale help protect against fraud?**
    a. Blockchain forensics platforms are an essential component of any virtual currency business compliance program, serving as a valuable tool for investigating fraud and identifying patterns across transactions. However, they should not be viewed as a silver bullet for preventing fraud at the point of transaction. Fraudsters routinely utilize new wallets without prior transaction history, avoiding association with known blacklists or fraud labels. Blockchain analytics are most effective when used as part of post-transaction investigations and compliance monitoring programs, rather than as a standalone real-time fraud prevention tool. However, it is important to note that it may take a significant amount of time before a blockchain forensic company can attribute a specific fraud-related wallet in which the victim likely has lost most or all their savings prior to attribution and detection.

4. **Why is the Crypto ATM industry a much bigger concern for fraud victimization than the digital exchanges and brokers (ie. Coinbase, Gemini, Kraken, Cashapp, Venmo, etc)?**
    a. As licensed money transmitters, digital exchanges maintain robust Know Your Customer (KYC) processes, monitor for suspicious transactions, integrate directly with customers' bank accounts, have protocols to freeze transactions when fraud is detected, and maintain ongoing relationships with law enforcement.

    Cryptocurrency kiosks, however, have become uniquely attractive to fraudsters for several reasons. First, kiosks accept cash, an untraceable payment method that cannot be reversed like credit cards or bank transfers. Second, kiosks provide immediate access to cryptocurrency, allowing fraudsters to quickly move funds through multiple wallets before victims realize they have been defrauded. Third, the physical nature of kiosks creates a false sense of legitimacy that victims may not associate with purely online transactions. Fourth, and perhaps most critically, the cryptocurrency kiosk industry has historically operated with minimal regulatory oversight and compliance standards, creating an environment where fraud can flourish.

    The bill's requirement that kiosk operators become licensed as money transmitters is essential because the safeguards inherent to that licensing are largely absent from the cryptocurrency kiosk industry today.

    We appreciate the opportunity to provide testimony on this important legislation and urge the legislature to pass AB968. The cryptocurrency kiosk industry cannot be trusted to regulate itself, as our experience clearly demonstrates. This bill will protect Wisconsin consumers from the rampant fraud and victimization in this industry that we witnessed firsthand.

Sincerely,

Marc J. Grens
Jonathan C. Solomon
Co-Founders, DigitalMint