JOSH GREEN, M.D.
GOVERNOR

SYLVIA LUKE
LIEUTENANT GOVERNOR

SIERRA WHITESIDE
CHAIRPERSON

DAINTRY BARTOLDUS
EXECUTIVE ADMINISTRATOR

STATE OF HAWAIʻI
KA MOKUʻĀINA O HAWAIʻI
STATE COUNCIL ON DEVELOPMENTAL DISABILITIES
'A'UNIKE MOKU'ĀPUNI NO KA NĀ KĀWAI KULA
PRINCESS VICTORIA KAMĀMALU BUILDING
1010 RICHARDS STREET, Room 122
HONOLULU, HAWAIʻI 96813
TELEPHONE: (808) 586-8100 FAX: (808) 586-7543

April 1, 2026

The Honorable Representative David A. Tarnas, Chair
House Committee on Judiciary & Hawaiian Affairs
The Thirty-Third Legislature
State Capitol
State of Hawaiʻi
Honolulu, Hawaiʻi 96813

Dear Chair Tarnas and Committee Members:

SUBJECT: SB2387 SD1 HD1, Relating to Digital Financial Asset Transaction Kiosks

The Hawaiʻi State Council on Developmental Disabilities (Council) offers **SUPPORT** for SB2387 SD1 HD1, which establishes consumer protections, fraud prevention measures, and disclosure requirements for digital financial asset transaction kiosks.

The Council supports this measure as an important step toward strengthening consumer protections in an evolving financial landscape. Individuals with intellectual and developmental disabilities (I/DD), as well as many kupuna, may be disproportionately targeted by scams that rely on urgency, perceived authority, or coercion. Financial exploitation can have devastating and long-lasting impacts on independence, stability, and overall well-being.

This measure includes critical safeguards, including transaction limits to reduce significant financial loss, clear warnings to alert consumers to common scam tactics, live customer service access, and refund provisions for fraudulent transactions. These protections are especially important given the irreversible nature of many digital financial asset transactions.

The Council respectfully recommends an amendment:
To require that all disclosures, warnings, and customer interfaces be provided in **plain language and designed to meet a range of access and functional needs,** including cognitive accessibility. **We respectfully request the following amendment on page 2, line 6; after "activities of the digital financial asset transaction kiosk," insert: "provided that all disclosures required under this section shall be written in plain language and designed to be accessible to individuals with access and functional needs, including cognitive, sensory, and communication disabilities, consistent with Act 172 (2022), Relating to Plain Language."**

Applying this standard to digital financial asset transaction kiosks will help ensure that fraud warnings and financial information are understandable and actionable for all users.

SB2387 SD1 HD1 strikes an appropriate balance by allowing access to emerging financial technologies while establishing reasonable safeguards to prevent fraud and protect consumers across Hawai‘i.

Thank you for the opportunity to provide testimony, supporting SB2387 SD1 HD1.

Sincerely,

Daintry Bartoldus
Executive Administrator

JOSH GREEN, M.D.
GOVERNOR | KE KIA'ĀINA

SYLVIA LUKE
LIEUTENANT GOVERNOR | KA HOPE KIA'ĀINA

STATE OF HAWAII | KA MOKUʻĀINA ʻO HAWAIʻI
OFFICE OF THE DIRECTOR
DEPARTMENT OF COMMERCE AND CONSUMER AFFAIRS
KA ʻOIHANA PILI KĀLEPA
335 MERCHANT STREET, ROOM 310
P.O. BOX 541
HONOLULU, HAWAII 96809
Phone Number: 1-844-808-DCCA (3222)
Fax Number: (808) 586-2856
cca.hawaii.gov

NADINE Y. ANDO
DIRECTOR | KA LUNA HOʻOKELE

DEAN I. HAZAMA
DEPUTY DIRECTOR | KA HOPE LUNA HOʻOKELE

Testimony of the Department of Commerce and Consumer Affairs

Before the
House Committee on Judiciary & Hawaiian Affairs
Wednesday, April 1, 2026
2:00 p.m.
Via Videoconference
Conference Room 325

On the following measure:
S.B. 2387, S.D. 1, H.D. 1 RELATING TO DIGITAL FINANCIAL ASSET TRANSACTION KIOSKS.

Chair Tarnas and Members of the Committee:

My name is Emma Olsen, and I am an Enforcement Attorney at the Department of Commerce and Consumer Affairs' (Department) Office of Consumer Protection (OCP). The Department supports this bill.

The purpose of this bill is to mitigate fraud losses occurring through digital financial asset kiosks, or bitcoin kiosks, by prohibiting digital financial asset transaction kiosks from accepting United States currency by cash, credit card, or any other means, from a new customer in exchange for digital financial assets; and for existing customers, implementing daily and monthly transaction limits, requiring operators to use blockchain analytics to prevent fraud, requiring certain disclosures, providing printed receipts to consumers, providing full refunds under certain circumstances, requiring the operator to provide live customer service, and requiring a dedicated phone line to certain government agencies. The measure also requires wallet pinning and establishes a prospective ban,

effective January 1, 2030, on kiosk operators accepting funds in exchange for digital financial assets. In addition, the measure prohibits kiosk operators from allowing customers who have had an account for less than seven days to purchase cryptocurrency through the kiosk.

Due to the high rates of fraud associated with cryptocurrency kiosks, we believe that a ban is the most effective way to protect consumers. The prior Committee's amendment prohibiting operators from accepting United States currency by cash, credit card, or any other means, from a new customer, would effectively mitigate losses through fraud at kiosks by prohibiting operators from accepting deposits from new customers. (Page 2, lines 3-5).

The term "new customer" is appropriately defined at page 11, lines 8-10, to mean a person who has been a customer of an operator for less than seven days commencing from the establishment of an account with the operator. This definition builds in a delay period that will give a person who is the victim of fraud an opportunity to assess their desire to carry out a transaction over the course of a full week.

We do not support any amendment that would introduce a dollar threshold to the definition of a new customer. Any individual who is a new customer should have the benefit of the seven-day cooling-off period from the establishment of a new account to contemplate the benefits of purchasing cryptocurrency and assess the risks that they might be the victim of fraud or scam, no matter how big or small their intended purchase.

In 2024, Minnesota enacted a law that did not prevent new customers from depositing cash in exchange for cryptocurrency, but did impose daily transaction limits, clear disclosure, and full refund requirements for new customers. This session, Minnesota legislators and law enforcement are now advocating for a bill banning cryptocurrency kiosks altogether. Even after Minnesota enacted its 2024 law, fraudsters were able to circumvent the new customer protections, and 2025 was the worst year to date for crypto kiosk scams reported to Minnesota's Department of Commerce.[1]

---

[1] Cathy Wurzer, Gracie Stockton & Brian Bakst, *As Bill to Ban Cryptocurrency ATMs in Minnesota Gets Airing, Local Police Departments Back It*, MPR News (Feb. 26, 2026), Crytptocurrency ATM ban proposed in Minnesota | MPR News.

On March 9, 2026, Indiana Governor Mike Braun signed Public Law 143 (H.B. 1116), prohibiting the operation of virtual currency kiosks in Indiana and providing that a person violating the prohibition commits an act that is actionable under the law regarding deceptive consumer sales.[2]

Should cryptocurrency kiosks be permitted to continue accepting money from existing customers in Hawaii, as proposed in this bill, the loss mitigation steps contemplated in this bill are imperative in protecting consumers from the rampant fraud committed through these kiosks. These baseline protections are especially important, given that there is currently no State licensing regime for cryptocurrency.

We support mitigating harms to consumers from fraud occurring at digital financial asset kiosks. In particular, the seven-day hold period for new users, the $2,000 cap on daily transactions, the $10,000 cap on transactions in any thirty-day period, the provision requiring full refunds to remedy reported fraud, and the law enforcement cooperation requirement all have the potential to protect consumers from fraud losses. Should kiosk activity be allowed to continue in Hawai‘i, these provisions must be enacted to protect Hawai‘i consumers from fraud losses.

Fraudulent activity involving bitcoin kiosks has resulted in significant financial losses to consumers. At present, Hawai‘i has over two hundred bitcoin kiosks located in publicly accessible places like supermarkets, liquor stores, and gas stations. Credible reports nationwide and in Hawaii demonstrate scammers use digital financial asset kiosks to defraud consumers.[3] The scammer creates a sense of urgency or builds trust with the victim and then, often over the phone, directs the victim to deposit large amounts of cash into a bitcoin kiosk, which goes directly to the scammer’s digital wallet.

---

[2] House Bill 1116, Indiana General Assembly (available at IGA | House Bill 1116 - Virtual currency kiosks March 31, 2026).

[3] See, for example, **FinCEN Notice on the Use of Convertible Virtual Currency Kiosks for Scam Payments and Other Illicit Activity** (FIN-2025-NTC-1, Aug. 4, 2025) (see Attachment A) (“The U.S. Department of the Treasury’s Financial Crimes Enforcement Network (FinCEN) is issuing this Notice to financial institutions urging them to be vigilant in identifying and reporting suspicious activity involving convertible virtual currency (CVC) kiosks.”).

Attorney Generals in Iowa and Washington D.C. have sued kiosk operators and announced that scam transactions account for more than 90% of transactions at kiosks targeted by their investigations. In the Washington D.C. lawsuit, Attorney General Schwalb sued cryptocurrency kiosk operator Athena. When the lawsuit was filed, AG Schwalb announced that according to the Athena's own data, obtained during the course of investigation, 93% of all Athena BTM deposits were the direct result of scams, nearly half of all deposits were flagged to Athena as the product of fraud, and the median amount lost per scam transaction was $8,000, with one victim losing a total of $98,000.

Because of the startling revelations accompanying these and other enforcement actions, and credible reports of ongoing fraud compiled by the FBI, we have grave concerns that digital financial asset kiosks are misused for fraudulent activity more than they are used to conduct legitimate transactions.

The refund provision in this bill creates an important remedy that may encourage operators to innovate and implement new, more effective fraud deterrents. At present, many kiosk operators do not provide refunds, and when they do, they refund only the transaction fees, which comprise perhaps 20%-30% of the original transaction amount. Requiring full refunds, as this bill proposes, is a crucial first step. Operators who face the prospect of issuing full refunds will be highly motivated to take appropriate steps to reduce fraud losses occurring through their kiosks.

Should the Committee pass this bill, enforcement of this new section of the HRS will be the responsibility of the Department and the Department of the Attorney General. Enforcement will require resources and may require appropriations for such resources.

We respectfully request that the Committee pass this bill as is.

Thank you for the opportunity to testify in support of this bill.

Attachment A- Referenced in DCCA's Testimony on S.B. 2387, S.D. 1, H.D.1

FinCEN NOTICE

FIN-2025-NTC1 **August 4, 2025**

FinCEN Notice on the Use of Convertible Virtual Currency Kiosks for Scam Payments and Other Illicit Activity

Suspicious Activity Report (SAR) Filing Request

FinCEN requests that financial institutions reference this Notice in SAR field 2 (Filing Institution Note to FinCEN) and the narrative by including the key term "**FIN-2025-CVCKIOSK**".

The U.S. Department of the Treasury's Financial Crimes Enforcement Network (FinCEN) is issuing this Notice to financial institutions[1] urging them to be vigilant in identifying and reporting suspicious activity involving convertible virtual currency (CVC) kiosks. CVC kiosks—also called cryptocurrency (crypto) Automated Teller Machines (ATMs)—are ATM-like devices or electronic terminals that allow customers to exchange real (or fiat) currency for virtual currency and vice versa.[2]

While CVC kiosks can be a simple and convenient way for consumers to access CVC, scammers and other illicit actors can also exploit their simplicity and convenience. 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 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.[3] This represents a 99 percent increase in the number of complaints and a 31 percent increase in reported victim losses from 2023.[4] The Federal Trade Commission (FTC) likewise identified, based on an analysis of consumer reports, that fraud losses through CVC kiosks have skyrocketed.[5]

FinCEN, through analysis of Bank Secrecy Act (BSA) information, has observed that CVC kiosks have also been used to launder suspected drug proceeds. The Drug Enforcement Administration (DEA) reports that transnational criminal organizations (TCOs) such as Cartel Jalisco Nueva Generación are increasingly adopting CVC because it enables rapid international funds transfers.[6] In areas that face a significant drug-related threat and that have a significant

1. *See* 31 U.S.C. § 5312(a)(2); 31 CFR § 1010.100(t).
2. FinCEN previously discussed illicit finance risks related to CVC kiosks in a 2019 advisory. *See* FinCEN, FIN-2019-A003, "Advisory on Illicit Activity Involving Convertible Virtual Currency" (May 9, 2019), at p. 7. This Notice supplements the information provided in that 2019 advisory.
3. FBI, IC3, "Internet Crime Report 2024" ("2024 IC3 Report"), at p. 36.
4. *Id*.
5. *See* FTC, "Bitcoin ATMs: A payment portal for scammers" ("FTC Report") (Sept. 3, 2024).
6. *See* DEA, "2025 National Drug Threat Assessment" (May 2025), at pp. 10, 64.

number of CVC kiosks, TCOs may launder money through CVC kiosks as an alternative to bulk cash smuggling.[7]

This Notice describes illicit finance typologies associated with CVC kiosks, provides red flag indicators to assist with identifying and reporting related suspicious activity, and reminds financial institutions of their reporting requirements under the BSA. Illicit activity involving CVC kiosks is linked to fraud, certain types of cybercrime, and drug trafficking organization activity, which are three of FinCEN's Anti-Money Laundering and Countering the Financing of Terrorism (AML/CFT) National Priorities.[8]

The information contained in this Notice is derived from FinCEN's analysis of BSA data, open-source reporting, and information from law enforcement partners.

How CVC Kiosks Work

Whereas a traditional ATM enables customers to withdraw or deposit cash from a bank account, CVC kiosks enable customers to buy, and in some cases sell, CVC from a CVC wallet[9] or exchange.[10] CVC kiosks generate revenue for their operator through the collection of fees and are generally located in businesses with heavy foot traffic, long operating hours, and convenient access, such as convenience stores, gas stations, cafes, and supermarkets.[11]

Purchasing CVC at a CVC kiosk may resemble using an ATM, which may appeal to a customer who wishes to transact in CVC but lacks familiarity with blockchain technology. After providing the CVC kiosk with identification, which can range from a phone number to a scan of a government-issued ID, the customer enters the address of the CVC wallet that will receive the purchased CVC. The address could be the customer's own CVC wallet or that of a third party,[12] and is normally embedded in a quick response (QR) code, which is a square barcode that can be scanned and read with a smartphone or kiosk camera. Finally, the customer inserts cash or a debit or credit card into the machine to finalize the purchase of CVC.

7. For example, according to the DEA, large volumes of illicit proceeds are laundered throughout Illinois, with Chicago serving as the primary collection point for U.S. currency generated through illegal drug sales. With the presence of CVC kiosks in the area growing rapidly (with approximately 1,626 in Illinois and 1,167 in Chicago alone), virtual currency continues to be a popular and growing method used to launder illicit proceeds derived from drug sales. Law enforcement reporting indicates that individuals are traveling from other states to Chicago to use these kiosks. *See* DEA, "The Illegal Drug Threat to Illinois" (Sept. 2024), at pp. 2, 5.
8. FinCEN, "Anti-Money Laundering and Countering the Financing of Terrorism National Priorities" (June 30, 2021).
9. CVC wallets are interfaces housing the technical components required for storing and transferring CVC. There are different wallet types that vary according to the technology employed, where and how the value is stored, and who controls access to the value. *See* FinCEN, FIN-2019-G001, "Application of FinCEN's Regulations to Certain Business Models Involving Convertible Virtual Currencies" ("FinCEN 2019 CVC Guidance"), at pp. 15–17.
10. *See Id*. at p. 17. CVC kiosks most commonly support bitcoin transactions, but many also handle other CVCs such as litecoin, ether, tether, and U.S. dollar coin (USDC). Federal Reserve Bank of Kansas City, "Payments System Research Briefing: The Controversial Business of Cash-to-Crypto Bitcoin ATMs" ("Federal Reserve Report") (Aug. 30, 2023), at p. 1.
11. *See* FTC Report, *supra* note 5.
12. Some operators may require that users certify that the destination wallet belongs to the user and not a third party, which could discourage fraud. *See* New Jersey Commission of Investigation, "Bitcoin ATMs: Scams, Suspicious Transactions and Questionable Practices at Cryptocurrency Kiosks" (Feb. 2021), at p. 9.

CVC kiosks may connect directly to a separate CVC exchanger,[13] which performs the CVC transmission, or the kiosk may draw upon CVC held by its operator.[14] The operator must maintain sufficient CVC and cash balances to run the kiosk and may use accounts at CVC exchanges and depository institutions for this purpose.[15]

Non-compliant CVC Kiosk Operators

CVC kiosk operators generally facilitate money transmission[16] between a CVC exchanger and a customer's CVC wallet or operate as a CVC exchanger themselves and, as such, are considered money services businesses (MSBs) under the BSA.[17] CVC kiosk operators that meet their obligations under the BSA play a key role in combating fraud and other illicit activity.

In some states, CVC kiosk operators may also be subject to state law designed to, among other things, deter illicit activity and protect customers from fraud, including by imposing additional requirements on businesses subject to those state laws.[18] However, the rapid growth in the number of CVC kiosks in the United States[19] has coincided with substantial rates of non-compliance with AML/CFT rules by CVC kiosk operators. For example, a 2021 report by the State of New Jersey Commission of Investigation found that more than a third of the companies operating CVC

13. A CVC exchanger is a person or entity offering to exchange fiat currencies for virtual currencies or one virtual currency for another virtual currency. Depending on the specifics of their business model, CVC exchangers may be subject to obligations under the BSA. *See* FinCEN 2019 CVC Guidance, *supra* note 9, pp. 12–14; 31 CFR § 1010.100(ff)(8)(iii).
14. Under either formulation, CVC kiosk operators are subject to BSA obligations. *See* FinCEN 2019 CVC Guidance, *supra* note 9, at pp. 17-18.
15. *See* Federal Reserve Report, *supra* note 10.
16. Money transmission involves the "acceptance of currency, funds, or other value that substitutes for currency and the transmission of currency, funds, or other value that substitutes for currency to another location or person by any means." 31 CFR § 1010.100(ff)(5)(i)(A). Transmitting CVC (other value that substitutes for currency) may constitute money transmission. *See* FinCEN 2019 CVC Guidance, *supra* note 9, at pp. 6-7.
17. As an MSB, any non-exempt person engaged in money transmission must register with FinCEN within 180 days of starting to engage in money transmission. *See* 31 CFR § 1022.380. Money transmitters must also comply with the recordkeeping, reporting, and transaction monitoring obligations set forth in parts 1010 and 1022 of 31 CFR chapter X. Examples of such requirements include the filing of Currency Transaction Reports (31 CFR § 1022.310) and Suspicious Activity Reports (31 CFR § 1022.320), as well as general recordkeeping obligations (31 CFR § 1010.410).
18. For example, California's Digital Financial Assets Law, among other requirements, prohibits kiosk operators from accepting or dispensing more than $1,000 in a day from or to a customer via a kiosk. *See* Cal. Fin. Code § 3902; *see also* California Department of Financial Protection & Innovation, "Digital Financial Assets Law: Information for Kiosk Operators." CVC kiosk operators may also be subject to state laws and regulations that are not specific to CVC kiosk operators. For example, on February 26, 2025, the Iowa Attorney General announced lawsuits against two CVC kiosk operators for alleged failures that allowed Iowans to transfer millions of dollars to scammers through their kiosks in violation of the Iowa Consumer Fraud Act. *See* Iowa Office of the Attorney General, "Attorney General Bird Sues Crypto ATM Companies for Costing Iowans More than $20 Million" (Feb. 26, 2025).
19. The website Coin ATM Radar reports that the number of CVC kiosks in the United States increased from 4,128 on January 1, 2019, to 37,342 on January 1, 2025. *See* Coin ATM Radar, "Bitcoin ATM Installations Growth" (last accessed Feb. 27, 2025). The data on Coin ATM Radar are self-reported by operators and are not comprehensive, as some large operators and perhaps many small kiosk operators do not report to the website. *See* Federal Reserve Report, *supra* note 10.

kiosks in the state did not register with FinCEN as MSBs.[20] Some non-compliant kiosk operators have been prosecuted for operating an unlicensed money transmitting business and other related offenses.[21] CVC kiosks operated by non-compliant operators are especially vulnerable to abuse by scammers and other criminals. According to law enforcement, scammers have directed victims to specific CVC kiosks, in some cases across state lines, likely to avoid CVC kiosk operators with strong AML/CFT controls.

In some cases, a non-compliant operator may represent to other financial institutions that the CVC kiosk business is registered with FinCEN—implying that it also complies with other BSA requirements—while failing to implement an AML/CFT program or other BSA obligations, such as collecting, retaining, and verifying customer identification.[22] These non-compliant CVC kiosk businesses also often lack reasonably designed policies, procedures, and internal controls to respond to requests from law enforcement.[23]

In some instances, non-compliant CVC kiosk operators have provided financial institutions with false information to acquire accounts or engaged in money laundering. For example, kiosk operators have assisted in structuring transactions[24] or falsely represented the nature of their business to CVC exchanges and depository institutions at which they hold accounts. Some non-compliant operators may use a personal account or accounts in the names of fake businesses or other entities to make cash deposits and withdrawals.[25] If asked about the purpose of transactions, the operators may avoid answering or provide misleading answers to financial institutions.[26]

20. New Jersey Commission of Investigation, "Bitcoin ATMs: Scams, Suspicious Transactions and Questionable Practices at Cryptocurrency Kiosks" (Feb. 2021), at p. 9.
21. *See, e.g.*, U.S. Attorney's Office (USAO), Central District of California, Press Release, "Westwood Man Agrees to Plead Guilty to Federal Narcotics, Money Laundering Charges for Running Unlicensed Bitcoin Exchange and ATM" (Aug. 23, 2019); USAO, Eastern District of California, Press Release, "Bitcoin ATM Company Forfeited Over $1 Million for Conspiring to Violate the Bank Secrecy Act" (Sept. 12, 2023).
22. MSBs are required to register with FinCEN as part of their obligations under the BSA, but that registration with FinCEN and a company's appearance on the FinCEN MSB Registrant Search Page is not a recommendation, certification of legitimacy, or endorsement of the business by FinCEN or any other U.S. government agency. Further, while MSBs must register with and are regulated by FinCEN, FinCEN does not license MSBs to operate in the United States. Any claim that a registration with FinCEN is a recommendation, certification of legitimacy, or endorsement by FinCEN of the business, or equates registration as a license to operate in the United States, is false and may be part of a scam. *See* FinCEN, FIN-2024-Alert005, "FinCEN Alert on Fraud Schemes Abusing FinCEN's Name, Insignia, and Authorities for Financial Gain," (Dec. 18, 2024). The FinCEN MSB Registrant Search Page contains entities that have registered as MSBs pursuant to the BSA implementing regulations at 31 CFR § 1022.380. *See* FinCEN, MSB Registrant Search.
23. *See* 31 CFR § 1022.210(d)(1)(i)(D).
24. Structuring transactions is prohibited by federal law and includes the practice of breaking a transaction into smaller amounts to prevent a CTR from being filed or to evade reporting requirements. *See* 31 U.S.C. § 5324; 31 CFR § 1010.314.
25. *See, e.g.*, USAO, District of New Hampshire, Press Release, "Three Plead Guilty to Wire Fraud In Connection with Unlawful Virtual Currency Sales Business" (Apr. 18, 2022); *see also* FinCEN, FIN-2019-A003, "Advisory on Illicit Activity Involving Convertible Virtual Currency" (May 9, 2019), at p. 7.
26. *See, e.g.*, USAO, District of New Hampshire, Press Release, "Six Charged with Crimes Related to Virtual Currency Exchange Business" (Mar. 16, 2021).

Case Study:

Orange County Man Sentenced for Operating Illegal CVC Kiosk Network That Laundered Millions of Dollars of Bitcoin and Cash for Criminals' Benefit

On May 28, 2021, the U.S. Attorney's Office for the Central District of California announced that a court sentenced Kais Mohammad, a.k.a. "Superman29," to 24 months in federal prison for operating an illegal CVC MSB that exchanged up to $25 million—some of it on behalf of criminals—through in-person transactions and a network of CVC kiosks. Mohammad pleaded guilty in September 2020 to a three-count criminal information charging him with operating an unlicensed money transmitting business, money laundering, and failing to maintain an effective anti-money laundering program.

From December 2014 to November 2019, Mohammad owned and operated Herocoin. As part of his business, Mohammad offered Bitcoin-to-cash exchange services, charging commissions of up to 25 percent—significantly above the prevailing market rate.

During the time of Herocoin's operation, Mohammad, a former bank employee who trained others on compliance matters, intentionally failed to register his company with FinCEN. Mohammad was aware that he was required to—but chose not to—develop and maintain an effective anti-money laundering program, file currency transaction reports for exchanges of currency in excess of $10,000, conduct due diligence on customers, and file suspicious activity reports for transactions over $2,000 involving customers he knew, or had reason to suspect, were involved in criminal activity.

With respect to his CVC kiosk network, Mohammad's machines allowed customers to conduct financial transactions without requiring any identification and permitted customers to conduct multiple, consecutive transactions of up to $3,000 each without ever reporting suspicious activity to regulators or law enforcement.

After FinCEN contacted Mohammad in July 2018 about his need to register his company, Mohammad did so, but he continued to fail to comply fully with federal law concerning money laundering, conducting due diligence, and reporting suspicious customers.[27]

Use of CVC Kiosks to Facilitate Scam Payments

The speed and difficulty of reversing CVC transactions[28] makes CVC an attractive payment mechanism for scammers. Once a victim makes the transfer with a CVC kiosk, the recipient (*i.e.*, a

27. *See* U.S. Attorney's Office, Central District of California, Press Release, "Yorba Linda Man Sentenced to 2 Years in Prison for Operating Illegal ATM Network that Laundered Bitcoin and Cash for Criminals" (May 28, 2021).
28. Because most CVCs operate on permissionless blockchains (*i.e.* decentralized, digital ledgers anyone can use) to record transactions, there often is no centralized authority who can easily reverse a transaction in the event of fraud. *See* National Institute of Standards and Technology, "Blockchain Networks: Token Design and Management Overview" (Feb. 2021).

criminal actor associated with the scam) instantly owns the CVC, and often immediately transfers the funds into another CVC wallet or exchange account they control. This generally differs from traditional bank or wire transfers where a payment transaction can remain pending for one to two days before settlement. The nature of CVC transactions can also make law enforcement's recovery of the funds difficult. Scammers often seek to persuade victims to withdraw money from their traditional financial accounts, such as investment or retirement accounts, and use that money to send a payment via CVC kiosk.[29] CVC kiosks can have high transaction fees relative to other means of transferring funds for senders and recipients, ranging from 7–20 percent, but scammers are willing to accept these costs for the quick receipt of CVC from victims, according to BSA and open-source information.[30]

CVC Kiosks and Elder Fraud

Criminals targeting older individuals are particularly likely to direct victims to use CVC kiosks to send payments.[31] According to FTC data, people aged 60 and over were more than three times as likely as younger adults to report a loss using a CVC kiosk.[32] More than two of every three dollars reported lost to fraud using CVC kiosks was lost by an older adult.[33] In addition, according to law enforcement, CVC kiosks have increasingly facilitated elder fraud, especially among tech/customer supports scams, government impersonation, confidence/romance scams, emergency/person-in-need scams, and lottery/sweepstakes scams.[34]

Many scammers using CVC kiosks initiate contact with potential victims through unsolicited calls.[35] For example, a scammer may claim to be the victim's bank calling about an unauthorized charge or pose as a government agency demanding taxes or fees. The most common scam typology associated with CVC kiosks is tech and customer support scams, in which scammers impersonate well-known companies as tech and customer support representatives to falsely claim that a virus or other malware has compromised the victims' computers and direct victims to make payments by CVC

29. *See* FBI, IC3, "The FBI Warns of Fraudulent Schemes Leveraging Cryptocurrency ATMs and QR Codes to Facilitate Payment" (Nov. 4, 2021) ("FBI Crypto ATM PSA").
30. FinCEN, "Elder Financial Exploitation: Threat Pattern & Trend Information, June 2022 to June 2023" (Apr. 2024), at p. 4. *See also* Federal Reserve Report, *supra* note 10, at p. 3.
31. FBI, IC3, "2023 Elder Fraud Report" (2023), at p. 16.
32. *See* FTC Report, *supra* note 5.
33. In contrast, younger adults were more likely to report virtual currency fraud losses not involving CVC kiosks, primarily those due to fake virtual currency investment opportunities. *Ibid*.
34. FBI, IC3, "2023 Elder Fraud Report" (2023), at p. 16. *See also* FinCEN, FIN-2022-A002, "Advisory on Elder Financial Exploitation" (June 15, 2022); *see also* FBI, IC3, "FBI Warns of the Impersonation of Law Enforcement and Government Officials" (Mar. 7, 2022); FBI, IC3, "Tech/Customer Support and Government Impersonation"; FBI, IC3, "Technical and Customer Support Fraud" (Mar. 16, 2023).
35. According to FTC data, phone calls were the initial contact method in about 47 percent of reported fraud cases involving CVC kiosks, followed by online ads or pop-ups (16 percent), and emails (9 percent). *See* FTC Report, *supra* note 5. *See also* FinCEN, FIN-2023-Alert005, "FinCEN Alert on Prevalent Virtual Currency Investment Scam Commonly Known as 'Pig Butchering'" (Sept. 3, 2023).

kiosk to address the issue.[36] In such schemes, scammers may use online ads and emails to contact victims, which typically contain a phone number to call for assistance leading to the scammer.[37]

Regardless of the type of fraudulent scheme, the criminals typically provide detailed instructions to prospective victims, including how to (i) withdraw cash from their bank, (ii) locate a kiosk, and (iii) deposit and send funds using the CVC kiosk, normally using a QR code provided by the scammer to ensure the CVC is sent to the correct destination, *i.e.*, a CVC wallet the scammer controls. After providing the victim with the QR code, the scammer then directs the victim to a physical CVC kiosk to purchase and send the scammer CVC, often staying in constant online or phone communication with the victim and providing step-by-step instructions until the payment is completed.[38]

According to law enforcement sources, scammers may provide victims with instructions designed to circumvent reporting thresholds,[39] transaction limits, or other safeguards. For example, the scammer may direct the victim to separate cash deposits into multiple, lower-value transactions, which may constitute structuring. In some cases, the scammer may also direct the victim to split the payment across multiple different CVC kiosks, a tactic known as "smurfing."

Scammers also often attempt to extract repeated payments from the same victim. In some cases, the scammers may also ask the victim to make payments through a new mechanism, such as through wire transfers or by handing cash or gold to a courier.[40]

A scam operation may aggregate payments made by multiple victims into a single CVC wallet before continuing to launder the proceeds. Scammers will also often quickly swap scam proceeds into a stablecoin,[41] most frequently through cross-chain bridges that claim to operate as decentralized finance (DeFi) services.[42] Illicit actors use this technique, known as "chain-hopping," to make it more difficult for authorities to trace financial transactions or for service providers to detect if incoming funds are tied to illicit activity.[43]

36. Tech support scams represented 46 percent of crimes related to CVC kiosks that were reported to FBI IC3 in 2023. *See* FBI, IC3, "2023 Cryptocurrency Fraud Report" (2023) at p. 16; *see also* FinCEN, FIN-2022-A002, "Advisory on Elder Financial Exploitation" (June 15, 2022), at p. 7.
37. *See* FTC Report, *supra* note 5.
38. *See* FBI Crypto ATM PSA, *supra* note 29.
39. As MSBs, CVC kiosk operators are required to report suspicious activity involving any transaction or pattern of transactions that involves or aggregates funds or other assets of at least $2,000. 31 CFR § 1022.320(a)(2). Some transactions conducted through CVC kiosks may be subject to additional reporting requirements.
40. *See, e.g.*, U.S. Attorney's Office, District of Arizona, Press Release, "Participants in "Tech Support" Scheme Charged with Conspiracy to Launder Fraudulent Proceeds" (Dec. 30, 2024); *see also* U.S. Attorney's Office, Southern District of California, Press Release, "Man Charged in $1.49 Million Scam Involving Bitcoin ATM Deposits and Bulk Gold Purchases; Victim is Retiree who Lost Life Savings" (Apr. 18, 2024).
41. A stablecoin is a digital asset that aims to maintain a stable price (e.g., a 1:1 peg) compared to a reference asset, such as the U.S. dollar. Eva Su, "Stablecoins: Background and Policy Issues," Congressional Research Service (Nov. 10, 2021).
42. DeFi services are virtual asset protocols and services that purport to allow for some form of automated peer-to-peer (P2P) transactions, often using self-executing code known as "smart contracts" based on blockchain technology. Cross-chain bridges allow users to exchange virtual assets or information from one blockchain to another. *See* Treasury, "Illicit Finance Risk Assessment of Decentralized Finance" (Apr. 2023), at pp. 3, 10.
43. *Id.*, at p. 17. Despite these challenges, blockchain analytics can help financial institutions identify this particular type of suspicious activity because blockchain analysis often connects scam payments made through CVC kiosks at different times or by different victims. *See* FinCEN, FIN-2019-A003, "Advisory on Illicit Activity Involving Convertible Virtual Currency" (May 9, 2019).

Case Study:

Man Charged in $1.49 Million Scam Involving Bitcoin ATM Deposits and Bulk Gold Purchases; Victim Is Retiree Who Lost Life Savings

On April 18, 2024, the U.S. Attorney's Office for the Southern District of California announced that a California man made his first appearance in federal court to face charges that he participated in a multinational fraud conspiracy that targeted a 70-year-old retiree who was tricked into handing over $1.335 million.

The victim was using her computer when a pop-up window appeared, advising her to call for help because her computer had been hacked. When she made the call, she was transferred through a series of co-conspirators pretending to work in tech support who told her to download software on her computer. She was also told her personal identifying and bank account information were compromised and was subsequently referred to co-conspirators posing as employees from her financial institutions. The victim was then told she needed to "secure" her assets. At the direction of someone posing as a bank employee, she deposited approximately $55,700 into CVC kiosks located in North County San Diego.

The complaint further describes how once the scammers discovered the victim had substantial savings, they convinced her she could safeguard her funds by obtaining gold bars and sending them to the U.S. Treasury, which would create a locker under her name. In reality, the victim was scammed out of her life savings.[44]

Red Flag Indicators of Illicit Activity Involving CVC Kiosks

FinCEN has identified the following red flag indicators to help detect, prevent, and report potential suspicious activity related to illicit activity involving CVC kiosks. Because no single red flag is determinative of illicit or other suspicious activity, financial institutions should consider the surrounding facts and circumstances, such as a customer's historical financial activity, whether the transactions are in line with prevailing business practices, and whether the customer exhibits multiple red flags before determining if a behavior or transaction is suspicious or otherwise indicative of illicit activity.

Red Flags for Operators of CVC Kiosks Regarding Scam Payments

1. A customer sends multiple payments just below the suspicious activity reporting (SAR) threshold,[45] or other applicable threshold set by state law, from multiple kiosk locations.

44. U.S. Attorney's Office, Southern District of California, Press Release, "Man Charged in $1.49 Million Scam Involving Bitcoin ATM Deposits and Bulk Gold Purchases; Victim is Retiree who Lost Life Savings" (Apr. 18, 2024).
45. Money transmitters must report suspicious activity involving any transaction or pattern of transactions if it involves or aggregates funds or other assets of at least $2,000. *See* 31 CFR § 1022.320(a)(2).

2. A customer structures cash deposits just beneath the Currency Transaction Report (CTR) threshold,[46] or CVC kiosk daily limit, either by using multiple machines or multiple accounts (*i.e.*, smurfing).

3. A customer with limited or no transaction history makes a substantial deposit that is rapidly transferred through multiple addresses, commingled with multiple other deposits, or swapped into a different CVC.

4. Multiple customers use CVC kiosks in geographically disparate locations to make deposits to the same CVC address over a short period of time while certifying that they are the owners of the deposit address.

5. Multiple customer accounts or transactions are linked to the same phone number or CVC wallet address.

6. Blockchain analysis indicates that a customer's transaction is received by a CVC wallet that is identified as associated with fraud or other illicit activity.

7. Blockchain analysis indicates that a customer's transaction is received by a CVC wallet associated with a financial institution that has been identified as associated with TCOs perpetrating CVC investment scams.

Red Flags for Other Financial Institutions Regarding Use of CVC Kiosks for Scam Payments

8. A customer conducting an in-person banking transaction withdraws substantial amounts of cash from their bank account or retirement account and indicates that they have been directed by a person on the phone or internet to deposit the funds into a CVC kiosk.

9. An older customer with no history of CVC-related activity conducts a high-value transaction or series of transactions with a CVC kiosk operator.

10. A customer uses a debit card to make multiple payments below the CTR limit to a CVC kiosk operator.

Red Flags for Financial Institutions Identifying Potential Non-Compliant CVC Kiosk Owner-Operators

11. A customer operates a CVC kiosk business that is not registered with FinCEN as an MSB or does not maintain applicable state licenses.

12. A customer operates a CVC kiosk business that fails to collect required customer and transaction information.

13. A customer operates a CVC kiosk business that advertises the ability for customers to conduct transactions without identification, or with only a phone number or email address.

46. A report of each deposit, withdrawal, exchange of currency, or other payment or transfer, by, through, or to a financial institution that involves a transaction in currency of more than $10,000. Multiple transactions may be aggregated when determining whether the reporting threshold has been met. See 31 CFR §§ 1010.310-313, 1020.310-313, 1021.310-313, 1022.310-313, 1023.310-313, 1024.310-313, 1026.310-313.

14 A customer operates a CVC kiosk business that charges unusually high transaction fees relative to similarly situated operators, has opaque rates and fees, or has other business practices that diverge significantly from those of legitimate CVC kiosk operators.

15 A customer that operates a CVC kiosk business structures cash transactions below the SAR or CTR threshold.

Reminder of Relevant BSA Obligations and Tools for U.S. Financial Institutions

Suspicious Activity Reporting
Other Relevant BSA Reporting
USA PATRIOT ACT Section 314(b) Information Sharing Authority

Suspicious Activity Reporting

A financial institution is required to file a SAR if it knows, suspects, or has reason to suspect a transaction conducted or attempted by, at, or through the financial institution involves funds derived from illegal activity; is intended or conducted to disguise funds derived from illegal activity; is designed to evade regulations promulgated under the BSA; lacks a business or apparent lawful purpose; or involves the use of the financial institution to facilitate criminal activity.[47] All statutorily defined financial institutions may voluntarily report suspicious transactions under the existing suspicious activity reporting safe harbor.[48]

When a financial institution files a SAR, it is required to maintain a copy of the SAR and the original or business record equivalent of any supporting documentation for a period of five years from the date of filing the SAR.[49] Financial institutions must provide any requested SAR and all documentation supporting the filing of a SAR upon request by FinCEN or an appropriate law enforcement or supervisory agency.[50] When requested to provide supporting documentation, financial institutions should take special care to verify that a requestor of information is, in fact, a representative of FinCEN or an appropriate law enforcement or supervisory agency. A financial institution should incorporate procedures for such verification into its BSA compliance or AML program. These procedures may include, for example, independent employment verification with the requestor's field office or face-to-face review of the requestor's credentials.

47. *See* 31 CFR §§ 1020.320, 1021.320, 1022.320, 1023.320, 1024.320, 1025.320, 1026.320, 1029.320, 1030.320.
48. *See* 31 U.S.C. § 5318(g)(3). Financial institutions may report suspicious transactions regardless of amount involved and still take advantage of the safe harbor.
49. *See* 31 CFR §§ 1020.320(d), 1021.320(d), 1022.320(c), 1023.320(d), 1024.320(c), 1025.320(d), 1026.320(d), 1029.320(d), 1030.320(d).
50. *Id.; see* FinCEN, FIN-2007-G003, "Suspicious Activity Report Supporting Documentation" (June 13, 2007).

SAR Filing Instructions

SARs, and compliance with other BSA requirements, are crucial to identifying and stopping illicit activity related to CVC kiosks. FinCEN requests that financial institutions indicate a connection between the suspicious activity being reported and the activities highlighted in this Notice by including the key term "**FIN-2025-CVCKIOSK**" in SAR field 2 (Filing Institution Note to FinCEN), as well as in the narrative. Financial institutions may highlight additional advisory or notice keywords in the narrative, if applicable. Financial institutions also should select all other relevant suspicious activity fields, such as those in SAR Fields 36 (Money Laundering) and 38 (Other Suspicious Activities), if applicable.

Financial institutions should include all available information relating to the account(s) and location(s) involved in the reported activity, identifying information and descriptions of any legal entities or arrangements involved and associated beneficial owners, and any information about related persons or entities involved in the activity. Financial institutions also should provide all available information regarding other domestic and foreign financial institutions involved in the activity; where appropriate, financial institutions should consider filing a SAR jointly on shared suspicious activity.[51]

Other Relevant BSA Reporting Requirements

Financial institutions and other entities or persons also may have other relevant BSA reporting requirements to provide information in connection with the subject of this Notice. These include obligations related to the Currency Transaction Report (CTR),[52] Report of Cash Payments Over $10,000 Received in a Trade or Business (Form 8300),[53] Report of Foreign Bank and Financial Accounts (FBAR),[54] Report of International Transportation of Currency or Monetary Instruments (CMIR),[55] Registration of Money Services Business (RMSB),[56] and Designation of Exempt Person (DOEP).[57]

51. *See* 31 CFR §§ 1020.320(e)(1)(ii)(A)(2))(i), 1021.320(e)(1)(ii)(A)(2)), 1022.320(d)(1)(ii)(A)(2), 1023.320(e)(1)(ii)(A)(2)(i), 1024.320(d)(1)(ii)(A)(2), 1025.320(e)(1)(ii)(A)(2), 1026.320(e)(1)(ii)(A)(2)(i), 1029.320(d)(1)(ii)(A)(2), 1030.320(d)(1)(ii)(A)(2).
52. A report of each deposit, withdrawal, exchange of currency, or other payment or transfer, by, through, or to a financial institution that involves a transaction in currency of more than $10,000. Multiple transactions may be aggregated when determining whether the reporting threshold has been met. *See* 31 CFR §§ 1010.310-313, 1020.310-313, 1021.310-313, 1022.310-313, 1023.310-313, 1024.310-313, 1026.310-313.
53. A report filed by a trade or business that receives currency in excess of $10,000 in one transaction or two or more related transactions. The transactions are required to be reported on a joint FinCEN/Internal Revenue Service form when not otherwise required to be reported on a CTR. *See* 31 CFR §§ 1010.330, 1010.331. A Form 8300 also may be filed voluntarily for any suspicious transaction, even if the total amount does not exceed $10,000.
54. A report filed by a U.S. person that has a financial interest in, or signature or other authority over, foreign financial accounts with an aggregate value exceeding $10,000 at any time during the calendar year. *See* 31 CFR § 1010.350; FinCEN Form 114.
55. A form filed to report the transportation of more than $10,000 in currency or other monetary instruments into or out of the United States. *See* 31 CFR § 1010.340.
56. A form filed to register a money services business (MSB) with FinCEN, or to renew such a registration. *See* 31 CFR § 1022.380.
57. A report filed by banks to exempt certain customers from currency transaction reporting requirements. *See* 31 CFR § 1010.311.

Information Sharing

Information sharing among financial institutions is critical to identifying, reporting, and preventing identity theft and fraud schemes or other illicit financial activity. Financial institutions and associations of financial institutions sharing information under the safe harbor authorized by section 314(b) of the USA PATRIOT Act are reminded that they may share information with one another regarding individuals, entities, organizations, and countries suspected of possible terrorist financing or money laundering.[58] FinCEN strongly encourages such voluntary information sharing.

The Financial Crimes Enforcement Network's Advisory Program communicates priority money laundering, terrorist financing, and other illicit finance threats and vulnerabilities to the U.S. financial system. Financial institutions may use this information to support effective, risk-based, and reasonably designed anti-money laundering and countering the financing of terrorism (AML/CFT) programs and suspicious activity monitoring systems to help generate highly useful information for law enforcement and national security agencies.

For Further Information

FinCEN's website at www.fincen.gov contains information on how to register for FinCEN Updates. Questions or comments regarding the contents of this Notice should be addressed to the FinCEN Regulatory Support Section by submitting an inquiry at www.fincen.gov/contact.

The mission of the Financial Crimes Enforcement Network is to safeguard the financial system from illicit use, combat money laundering and its related crimes including terrorism, and promote national security through the strategic use of financial authorities and the collection, analysis, and dissemination of financial intelligence.

58. *See* FinCEN, "Section 314(b) Fact Sheet" (Dec. 2020).

RICHARD T. BISSEN, JR.
Mayor

ANDREW H. MARTIN
Prosecuting Attorney

SHELLY C. MIYASHIRO
First Deputy Prosecuting Attorney

LATE

DEPARTMENT OF THE PROSECUTING ATTORNEY
COUNTY OF MAUI
200 SOUTH HIGH STREET
WAILUKU, MAUI, HAWAI'I 96793
PHONE (808) 270-7777 • FAX (808) 270-7625

TESTIMONY ON
S.B. 2387 SD1 HD1
RELATING TO DIGITAL FINANCIAL ASSET TRANSACTION KIOSKS

April 1, 2026

The Honorable David A. Tarnas
Chair
The Honorable Mahina Poepoe
Vice Chair
and Members of the Committee on Judiciary & Hawaiian Affairs

Chair Tarnas, Vice Chair Poepoe, and Members of the Committee:

The Department of the Prosecuting Attorney, County of Maui respectfully submits the following comments **in support of S.B. 2387 SD1 HD1, Relating to Digital Financial Asset Transaction Kiosks**. This measure imposes various requirements for operators of digital financial asset transaction kiosks.

The Department of the Prosecuting Attorney, County of Maui supports this bill in part because of the increasing number of financial scams involving innocent citizens tricked into sending cash, gift cards or wire transfers to criminals via phone or internet contact. Digital financial asset transaction kiosks are another tool in a scammer's arsenal: They're the electronic equivalent of an ATM, with the added danger that digital assets purchased at one of these kiosks can be immediately transferred to a scammer's digital wallet and are nearly impossible to recover.

The HD1 version of this bill adds to the protections from prior versions by, *inter alia*, prohibiting the acceptance of US currency in any form by a new customer and, by 2030, any customer. These additional protections are a vital part of preventing fraudulent transactions because they restrict kiosk transactions to digital assets instead of currency, reducing the likelihood that consumers with no existing digital assets can be tricked or pressured into initiating fraudulent transactions at a kiosk.

For these reasons, the Department of the Prosecuting Attorney, County of Maui **supports S.B. 2387 SD1 HD1**. Please feel free to contact our office at (808) 270-7777 if you have any questions or inquiries. Thank you very much for the opportunity to provide testimony on this bill.

TESTIMONY SUBMITTED TO THE HOUSE JUDICIARY & HAWAIIAN AFFAIRS COMMITTEE

RE: SB 2387 SD1 HD1 Relating to Digital Financial Asset Transaction Kiosks

Aloha Chair Tarnas and members of the Committee,

My name is Louise Pais Meyers, Chief Compliance Officer for Hilt Ventures, the largest crypto kiosk operator in Hawaii.

Thank you for the opportunity to testify on SB 2387 SD1 HD1.

Hilt Ventures already implements — and in many cases exceeds — strong consumer protections, including clear fee disclosures, prominent scam warnings, detailed receipts, robust anti-fraud and AML programs, blockchain analytics, customer identification, transaction monitoring, refunds, and close coordination with law enforcement. We proactively detect and interrupt scams, often reaching out to customers before they realize they have been victimized.

However, several provisions in the current version of the bill are overly broad and depart from the balanced approach successfully adopted in the vast majority of other states.

We respectfully request two targeted amendments that would better protect consumers while reflecting proven, effective models:

1. Differentiated Refunds and Transaction Limits Fraud at crypto kiosks overwhelmingly targets first-time or new users. A uniform 90-day full refund requirement for all customers risks unintended abuse and does not align with actual risk patterns.

We urge the Committee to adopt a risk-based approach that has been endorsed by AARP in multiple states, including Arizona, Colorado, Nebraska, and others. Specifically:

- Define **"New User"** as a customer who has transacted with the operator for less than 7 days.
- Define **"Existing User"** as a customer who has transacted for 7 days or more.
- **Transaction Limits**: $2,000 per day for new users; $10,500 per day for existing users.
- **Refunds**: Full refund (including fees) for new users who report fraud to the operator and law enforcement within 30 days and upon verification; fee-only refund for existing users.

This tiered structure slows rapid scam transactions while preserving access for legitimate users and has proven effective elsewhere. Hilt's comments regarding the differentiation between new and existing customers were noted in SSCR3306 from the Senate Judiciary and Ways and Means Committees.

2. Remove the 2030 Kiosk Ban We strongly recommend deleting the House CPC amendment imposing a ban on crypto kiosks beginning in 2030. The Senate did not support a ban, and such a prohibition is not part of the effective, consumer-protection-focused laws enacted in other states.

Hilt Ventures is committed to working collaboratively with this Committee to refine SB 2387 SD1 HD1 into balanced, practical legislation that protects Hawaii's consumers — especially kūpuna — while maintaining responsible access to digital asset services.

We are happy to provide data on our fraud prevention results in Hawaii, share specific examples of thwarted scams, and answer any questions.

Thank you for your time and consideration.

Respectfully,

Louise Pais Meyers

1001 Bishop Street #625 | Honolulu, HI 96813
866-295-7282 | aarp.org/hi | hiaarp@aarp.org |
Twitter.com/aarpHawai'i | facebook.com/aarpHawai'i

The Thirty-Third State Legislature
House Committee on Judiciary and Hawaiian Affairs
Wednesday, April 1, 2026
Conference Room 325, 2:00 p.m.

TO: The Honorable David Tarnas, Chair
FROM: Keali'i S. López, State Director
RE: Strong Support for S.B. 2387, SD1, HD1 Relating to Digital Financial Asset Transaction Kiosks

Aloha Chair Tarnas, and Members of the Committee:
My name is Keali'i López, and I serve as State Director for AARP Hawai'i. AARP is a nonprofit, nonpartisan social impact organization dedicated to empowering people age 50 and older to choose how they live as they age. On behalf of our nearly 135,000 members statewide, we appreciate the opportunity to testify in strong support of S.B. 2387, S.D.1, H.D.2, with a minor comment for clarification.

Comment – Need for Technical Clarification
House Draft 2 includes important new consumer protections, including a prohibition on deposits by first-time customers, followed by a full ban on deposits for all users beginning in 2030. However, under Section 1, page 2, line 7, the use of the word "or" could be interpreted to suggest that the 2030 prohibition is optional rather than cumulative. If it reflects the Legislature's intent that both provisions apply, AARP Hawai'i respectfully requests that the word "or" be replaced with "and" to avoid ambiguity and ensure clear implementation.

Why S.B. 2387, S.D.1 Is Needed
AARP Hawai'i strongly supports this measure because it significantly strengthens consumer protections and reduces fraud risks associated with digital financial asset transaction kiosks, commonly referred to as cryptocurrency kiosks or crypto ATMs. These machines are increasingly used by criminals to exploit consumers, particularly older adults, leading to devastating and often irreversible financial losses.

Fraud involving cryptocurrency kiosks is rising sharply both nationally and in Hawai'i. According to the FBI's Internet Crime Complaint Center, Hawai'i reported 68 cryptocurrency kiosk–related complaints in 2024, with losses totaling more than $922,000. Nationally, more than 11,000

complaints resulted in losses exceeding $250 million—representing a 99 percent increase over the prior year.

Hawai‘i currently has at least 96 cryptocurrency kiosks located in common, everyday settings such as supermarkets, gas stations, convenience stores, bars, and restaurants. While these machines closely resemble traditional ATMs, they operate with far fewer consumer protection requirements. Unlike conventional banking transactions, cryptocurrency transfers are typically irreversible, making them especially attractive to scammers and leaving victims with little or no recourse once funds are transferred.

Older adults are disproportionately targeted in these schemes, and without strong statutory safeguards, criminals will continue to exploit regulatory gaps and siphon millions of dollars from unsuspecting residents.

Key Consumer Protections in S.B. 2387, S.D.1

S.B. 2387, S.D.1 establishes reasonable, commonsense safeguards that protect consumers while allowing legitimate businesses to continue operating. Specifically, the bill would:

- Establish a daily transaction limit of $2,000 and an aggregate cap of $10,000 over a 30-day period to prevent catastrophic financial losses;
- Require kiosk operators to refund fraudulent transactions;
- Mandate clear, upfront disclosure of all terms, fees, and exchange rates prior to completing a transaction;
- Require prominent and visible notices on kiosks informing consumers what to do if they suspect fraud;
- Ensure customers receive paper receipts containing relevant transaction details;
- Strengthen enforcement authority to investigate fraudulent activity;
- Require live customer service support during operating hours; and
- Provide a dedicated communication line for law enforcement.

House Draft 2 – Additional Protections

House Draft 2 further strengthens this measure by:

- Prohibiting deposits by first-time customers;
- Preventing multiple users from transacting through the same digital wallet; and
- Prohibiting deposits for all users beginning in 2030.

Together, these provisions provide consumers with meaningful tools to avoid fraud while equipping regulators and law enforcement with the authority necessary to deter, detect, and respond to criminal activity.

Conclusion

By adopting the safeguards contained in S.B. 2387, S.D.1, H.D.2, Hawai'i can take a critical step toward combating financial fraud and protecting the hard-earned savings of kūpuna and all consumers. This measure reflects a balanced approach that prioritizes consumer safety while keeping pace with emerging financial technologies.

AARP Hawai'i respectfully urges your support for S.B. 2387, S.D.1, H.D.2, with the suggested technical clarification.

Mahalo for the opportunity to testify in strong support of this important measure.

SB-2387-HD-1
Submitted on: 3/30/2026 10:11:03 PM
Testimony for JHA on 4/1/2026 2:00:00 PM

Submitted By	Organization	Testifier Position	Testify
GARY SIMON	Policy Advisory Board for Elder Affairs (PABEA)	Support	Written Testimony Only

Comments:

Dear Chair Tarnas, Vice Chair Poepoe, and Honorable Members of the House Committee on Judiciary and Hawaiian Affairs:

I am Gary Simon, a member of the Policy Advisory Board for Elder Affairs (PABEA), which is an appointed board tasked with advising the Executive Office on Aging (EOA). My testimony does not represent the views of EOA but of PABEA.

PABEA strongly supports SB 2387 SD 1 HD 1, which establishes limits on transactions through digital financial asset transaction kiosks. SB 2387 SD 1 HD 1 prohibits (1) the exchanging of United States currency from new customers for digital financial assets; (2) any two customers from transacting to the same digital financial asset wallet address; and (3) beginning January 1, 2030, the exchange of United States currency from customers for digital financial assets. SB 2387 SD 1 HD 1 also requires operators of digital financial asset transaction kiosks to use blockchain analytics and tracing software to prevent fraud; make certain disclosures; provide receipts to customers; provide full refunds under certain circumstances; and provide live customer service and a dedicated communications line for the Attorney General, Office of Consumer Protection, Department of Law Enforcement, and county police departments.

Cryptocurrency transactions come with many, real risks, including scams. Legislation is required to protect Hawaii's residents from these cryptocurrency scams.

We urge you to protect Hawaii's consumers and to recommend passage of SB 2387 SD 1 HD 1.

Mahalo for seriously considering the bill.

Gary Simon

Policy Advisory Board for Elder Affairs (PABEA)

Honolulu, Hawaii

TESTIMONY SUBMITTED TO THE HOUSE JUDICIARY & HAWAIIAN AFFAIRS COMMITTEE

RE: SB 2387 SD1 HD1 Relating to Digital Financial Asset Transaction Kiosks

Aloha Chair Tarnas and members of the Committee,

My name is Chip Meyers with Hilt Ventures.

Thank you for the opportunity to testify on SB 2387 SD1 HD1.

While we support reasonable efforts to combat fraud at cryptocurrency kiosks, SB 2387 SD1 HD1 is significantly overreaching and deviates sharply from the balanced approach adopted in nearly every other state.

Most states that have passed kiosk regulations — including Arizona, Arkansas, Colorado, Florida, Illinois, Oklahoma, Maryland, Rhode Island, and West Virginia — use a risk-based, tiered system. They allow new customers a limited daily amount (typically $2,000) and higher limits for existing customers (usually $10,000–$10,500). This approach effectively slows down scam transactions while still permitting legitimate use.

In contrast, SB 2387 SD1 HD1 is far more restrictive. It applies the same low $2,000 daily limit to all customers, adds a tight $10,000 monthly cap, and — most problematically — completely prohibits new customers from making any cash-to-crypto transaction.

This new customer prohibition is not only overly broad, but it creates a fundamental logical flaw: If a person cannot complete their first transaction because they are classified as a “new customer,” they can never become an “existing customer.” The bill sets up a tiered system that is impossible to use. This

drafting defect renders the customer distinction meaningless and severely restricts lawful access to digital assets.

We respectfully urge the Committee to remove the prohibition on new customers and amend the bill to adopt the more reasonable, risk-based tiered limits that have worked effectively in other states.

Thank you for your consideration.

State Bill Summary

State	Bill / Law	Definition of "New Customer"	New Customer Daily Limit	Existing Customer Daily Limit	Refunds	Effective / Status	Notes	AARP notes
Arizona	HB 2387	First 10 days after initial transaction	$2,000	$10,500	Full refund for new customers only. The victim must report the fraud to the operator and law enforcement / Attorney General's office within 30 days of the transaction and provide a law enforcement or government report confirming the customer was fraudulently induced. No full refund right for existing customers (fee refunds may apply in some cases).	Active	AARP Arizona strongly advocated for this bill as a top priority. Praised the full refund rule for new customers. Called it highly effective at protecting older adults. Since passage, AARP has highlighted real victim success stories as proof the law is working. Here is an article from AARP published March 1, 2026.	"Thanks to an Arizona law passed last May that aims to clamp down on cryptocurrency ATM fraud, Barr [a first time customer] was able to get all her money returned from the ATM operator. The law requires that ATM operators issue full refunds to [first time customers] who report to local law enforcement or the attorney general's office that they have been victims of fraud within 30 days of the transaction." https://www.aarp.org/states/arizona/arizona-fraud-law1/ In its newsletter, AARP Arizona refers to HB 2387 as one of their "most recent legislative wins" in anti-fraud work. https://www.aarp.org/states/arizona/aarp-arizona-advocacy-newsletter-blog-post/
Arkansas	Act 557 (2025)	Within 72 hours of first transaction	$2,000	$7,500	Full refund for new customers only. Operator must allow cancellation and provide a full refund for fraudulent transactions that occurred within 72 hours of the customer's first transaction. The customer must contact the operator and file a report with law enforcement/government agency within 14 days after the last transaction in that 72-hour window.	Active (Sept 2025)	AARP supported the bill for giving scam victims the ability to recoup losses through refund rights	
Colorado	SB 25-079	First 7 days after initial transaction	$2,000	$10,500	Full refund for new customers only (and limited to the customer's first transaction only). Operators must provide a full refund for a customer's first virtual currency transaction only if: (1) it was sent to a wallet or exchange outside the United States, (2) the customer contacts the operator and a government/law enforcement entity within 60 days, and (3) submits proof of fraud (e.g., police report or notarized declaration). The refund must be issued within 72 hours of notification.	Active (Jan 1, 2026)	AARP Colorado actively supported Senate Bill 25-079, the Colorado Vending of Digital Assets Act.	During legislative hearings, representatives from AARP and the AARP Fraud Watch Network, including Margaret Locke and Amy Nofziger, testified in support of the bill. In its public advocacy, AARP highlighted the importance of the bill's tiered daily transaction limits and the provision requiring a full refund of a customer's first virtual currency transaction if it is determined to be fraudulent and reported within 60 days with proof. AARP described these measures as practical safeguards that help protect older Coloradans from rapid, irreversible losses at crypto kiosks
Florida	HB 505 (2026)	Less than 7 days	$2,000	$10,000	Full refund for new customers only (and limited to customer's first virtual currency transaction). Customer must notify operator and law enforcement within 60 days and provide proof of alleged fraud (e.g., police report or notarized affidavit). Operator must refund customers within 72 hours after receiving the police report.	Passed (March 13, 2026); awaiting Governor	AARP Florida strongly supported HB 505. Emphasized that the full refund for the first transaction helps protect Floridians from losing life savings quickly. It emphasized the bill's tiered limits and the full refund for the first transaction as critical tools to protect older adults.	AARP Florida has framed the full refund for the first fraudulent transaction as one of the key victories for protecting seniors. https://floridapolitics.com/archives/786011-aarp-releases 2026-legislative-voting-record-spotlighting-its-priorities/
Illinois	Digital Asset Kiosk Act (SB 2319)	First 3 transactions **or** 7 days	$2,500	$10,500	Full refund to new customers only. Operators must issue full refunds for fraudulent transactions to new customers (during the new-customer period — first 3 transactions or 7 days). The new customer must submit a police report or government agency report within 60 days after the last transaction in the new-customer period. Existing customers may recover fees only under similar reporting conditions.	Active (Aug 2025)	AARP supported the Digital Asset Kiosk Act as providing "commonsense protections for older adults."	AARP Illinois has posted on social media "Now, thanks to the passage of the Digital Asset Kiosk Act (SB 2319), crypto machines are regulated with important safeguards." https://www.facebook.com/watch/?v=945626400906775 "This landmark legislation—the Digital Asset Kiosks Act—represents a major step forward in protecting Illinois consumers, especially older adults, from fraud and abuse..." https://www.aarp.org/states/illinois/aarp-illinois-
Maryland	SB 305 (Chapter 117, 2025)	Within 72 hours of first transaction	$2,000	$10,500	Fee refund only. No full principal refund is required by statute. Customer must submit a Notice of Fraud no later than 90 calendar days after the alleged fraudulent transaction.The operator has 30 calendar days from receipt of the Notice of Fraud to investigate the claim. Within 3 business days after completing the investigation, the operator must mail the user either grant the fee refund, or issue a letter denying the refund.	Active (Jan 2026)	AARP supported the bill overall as a step forward in oversight, but pushed for stronger full refunds for first-time victims.	In written testimony submitted to the House Economic Matters Committee on March 25, 2025, Tammy Bresnahan, Senior Director of Advocacy for AARP Maryland, stated that the bill represented "a crucial step toward protecting Marylanders — especially older adults — from this rising threat." AARP Maryland specifically highlighted the bill's provision requiring operators to refund transaction fees in cases of verified fraud as one of the important consumer protections included in the
Nebraska	LB 609	Within 14 days of first transaction	$2,000	$10,500	Full refund for new customers if reported to operator and law enforcement within 30 days; fees only for existing	Active (Sept 2025)	AARP actively advocated for LB 609 and praised the tiered approach and transparency requirements as strong consumer safeguards.	Following passage, AARP Nebraska was very positive and treated LB 609 as a major legislative win. They emphasized protection of older adults' savings, bipartisan support, and the combination of licensing, transaction limits, and refund rights for new customers.
Rhode Island	S 0016	Within 30 days of first transaction	$2,000	$5,000	Full refund for new customers if reported within 90 days; fees only for existing	Active (June 2025)	AARP Rhode Island actively and vocally supported the bill with direct testimony and public advocacy.	
West Virginia	HB 5353 (2026)	Customer for 10 days or less	$1,000	$10,000	Full refund for new customers only if reported within 30 days	Pending (March 25, 2026), awaiting Governor	AARP West Virginia strongly backed the overall bill and celebrated its passage.	
Federal	S. 710	Within 14 days of first transaction	$2,000	$10,000	Full refund for new customers if reported within 30 days; fees only for existing	Proposed		

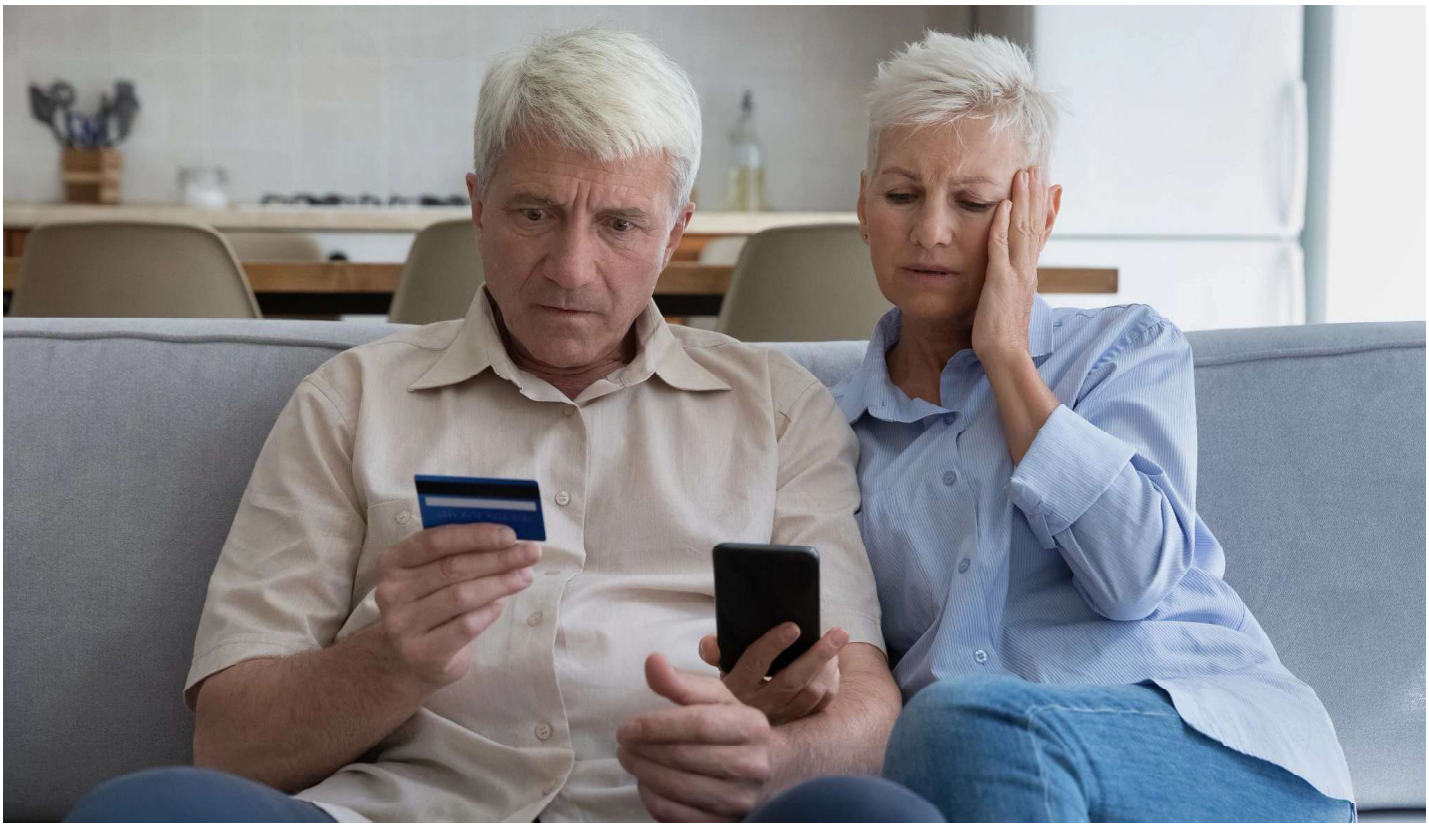
AARP Arizona

Arizona Law Aims to Stop Crypto ATM Scams

The new refund rule helps fraud victims

Julie Halpert, AARP

Published March 01, 2026



GETTY IMAGES

Gale Barr, a nurse practitioner living in Goodyear, got a voicemail on her 70th birthday this past October. The caller said he was a deputy sheriff and asked her to contact him about an important legal matter. Barr was curious. So, she returned the call.

She had two citations, he said, for failing to report for jury duty. A withdrawal of $9,260 from a bank account would take care of the legal issue, he said. All she had to do was deposit the cash into a Circle K convenience store cryptocurrency kiosk (also called a crypto ATM).

Barr was diagnosed with mild cognitive impairment after COVID, and she says that may have made her more vulnerable. "I was frightened," she says—and also worried about going to jail. "I thought it was real."

Barr deposited the cash. Then the "deputy sheriff" told her she had another citation. This one was for $12,000. She told the man she had only $3,000 in her account, and he said that would be enough. She headed to withdraw the money from a different bank branch, where a suspicious manager broke the news that she had been scammed.

The money had been set aside to help care for her son's mental and physical challenges. "I just cried," she says. "I worked for that money, for my son."

But thanks to an Arizona law passed last May that aims to clamp down on cryptocurrency ATM fraud, Barr was able to get all her money returned from the ATM operator. The law requires that ATM operators issue full refunds to those who report to local law enforcement or the attorney general's office that they have been victims of fraud within 30 days of the transaction.

AARP advocated for the law as part of its ongoing efforts — including prevention programs and anti-fraud resources — to teach older Americans how to stay safe.

With ATM crypto scams, the scammers use Bitcoin machines, typically found at convenience stores. They ask consumers to deposit cash withdrawn from their bank accounts into these machines, which then convert the cash to cryptocurrency. A QR code that the criminals provide allows the money to be deposited into the perpetrator's crypto account, and the scammer remains anonymous.

According to the FBI, the amount nationally lost to crypto ATM fraud was $246.7 million in 2024. Older Americans faced the largest losses to crypto ATM fraud. For those ages 50 to 59, the total loss was $5.5 million. For those over 60, it was $107.2 million. Beyond that, in a September 2024 report, the Federal Trade Commission indicated that in the first half of that year, people older than 60 were more than three times as likely as younger adults to report losing money to crypto ATM-related scams.

In 2024, the AARP Fraud Watch Network started a project to develop a broad message aimed at helping older adults and other consumers recognize and avoid scam attempts. The network came up with the "Pause. Reflect. Protect." program.

Education and knowledge are critical weapons against scams, says Laura Flannigan, AARP Arizona's advocacy analyst. AARP has 253 volunteers in Arizona who educate the public on fraud through events, presentations and other resources.

"We want the public to know that any request to pay for something through a crypto ATM deposit is extremely suspicious," she says.

- AARP Fraud Watch Network Learn more about AARP Fraud Watch Network resources.
- **AARP Fraud Watch Network Helpline** 877-908-3360

Julie Halpert covers aging and many other topics for publications including The Wall Street Journal *and* The New York Times.

Senate Engrossed House Bill

cryptocurrency kiosk; license; fraud prevention

State of Arizona
House of Representatives
Fifty-seventh Legislature
First Regular Session
2025

CHAPTER 171

HOUSE BILL 2387

AN ACT

AMENDING TITLE 6, CHAPTER 12, ARTICLE 1, ARIZONA REVISED STATUTES, BY ADDING SECTION 6-1236; RELATING TO MONEY TRANSMISSION.

(TEXT OF BILL BEGINS ON NEXT PAGE)

Be it enacted by the Legislature of the State of Arizona:

Section 1. Title 6, chapter 12, article 1, Arizona Revised Statutes, is amended by adding section 6-1236, to read:

6-1236. Cryptocurrency kiosk operator; disclosures; receipt; fraud prevention; refunds; enforcement; definitions

A. A CRYPTOCURRENCY KIOSK OPERATOR SHALL DISCLOSE IN A CLEAR, CONSPICUOUS AND EASILY READABLE AND UNDERSTANDABLE MANNER IN THE CHOSEN LANGUAGE OF THE CUSTOMER ALL RELEVANT TERMS AND CONDITIONS THAT ARE GENERALLY ASSOCIATED WITH THE PRODUCTS, SERVICES AND ACTIVITIES OF THE CRYPTOCURRENCY KIOSK OPERATOR AND VIRTUAL CURRENCY. THE CRYPTOCURRENCY KIOSK OPERATOR SHALL RECEIVE AN ACKNOWLEDGMENT OF RECEIPT OF ALL DISCLOSURES REQUIRED UNDER THIS SECTION FROM A CUSTOMER THROUGH CONFIRMATION OR CONSENT.

B. A CRYPTOCURRENCY KIOSK OPERATOR SHALL PROVIDE THE FOLLOWING DISCLOSURES SEPARATELY IN A FONT THAT CONTRASTS WITH THE BACKGROUND WHERE THE WRITTEN WARNING APPEARS AND THE CUSTOMER MUST ACCEPT THE TWO SEPARATE DISCLOSURES BEFORE EXECUTING A CRYPTOCURRENCY KIOSK TRANSACTION:

1. WARNING: CONSUMER FRAUD OFTEN STARTS WITH CONTACT FROM A STRANGER WHO IS INITIATING A DISHONEST SCHEME OR A CRIMINAL OR FRAUDULENT ACTIVITY THAT MAY APPEAR IN MANY FORMS, INCLUDING ANY OF THE FOLLOWING:

(a) CLAIMS OF A FROZEN BANK ACCOUNT OR CREDIT CARD.

(b) CLAIMS OF A FRAUDULENT BANK TRANSACTION.

(c) CLAIMS OF IDENTITY THEFT OR AN OFFER OF EMPLOYMENT IN EXCHANGE FOR PAYMENT.

(d) REQUESTS FOR A PAYMENT TO A GOVERNMENT AGENCY OR COMPANY.

(e) REQUESTS FOR DISASTER RELIEF DONATIONS OR LOANS.

(f) OFFERS TO PURCHASE LOTTERY TICKETS OR SWEEPSTAKES OR DRAWINGS FOR VEHICLES.

(g) PROMPTS TO CLICK ON DESKTOP POP-UPS THAT INCLUDE VIRUS WARNINGS OR COMMUNICATION FROM ALLEGED FAMILIAR MERCHANTS.

(h) COMMUNICATION FROM SOMEONE IMPERSONATING A REPRESENTATIVE OF YOUR BANK OR A LAW ENFORCEMENT OFFICER.

IF YOU BELIEVE YOU HAVE BEEN SCAMMED, STOP AND CALL YOUR LOCAL LAW ENFORCEMENT AND THE CRYPTOCURRENCY KIOSK OPERATOR.

2. WARNING: LOSSES DUE TO FRAUDULENT OR ACCIDENTAL TRANSACTIONS ARE NOT RECOVERABLE. TRANSACTIONS IN VIRTUAL CURRENCY ARE IRREVERSIBLE. PEOPLE MAY USE VIRTUAL CURRENCY TRANSACTIONS TO STEAL YOUR MONEY BY IMPERSONATING THE GOVERNMENT, ORGANIZATIONS OR PEOPLE YOU KNOW. IMPERSONATORS MAY THREATEN JAIL TIME, SAY YOUR IDENTITY HAS BEEN STOLEN, ALLEGE YOUR COMPUTER HAS BEEN HACKED, INSIST YOU WITHDRAW MONEY FROM YOUR BANK ACCOUNT TO PURCHASE VIRTUAL CURRENCY OR USE A NUMBER OF OTHER SCAMS. DO NOT DISCLOSE YOUR PRIVATE KEY THAT IS ASSOCIATED WITH YOUR VIRTUAL WALLET TO A THIRD PARTY.\ufffd IF YOU BELIEVE YOU ARE BEING SCAMMED, STOP AND CALL YOUR LOCAL LAW ENFORCEMENT AND THE CRYPTOCURRENCY KIOSK OPERATOR.

C. ON THE COMPLETION OF EACH CRYPTOCURRENCY KIOSK TRANSACTION, THE CRYPTOCURRENCY KIOSK OPERATOR SHALL PROVIDE THE INDIVIDUAL WHO MADE THE TRANSACTION AT THE CRYPTOCURRENCY KIOSK WITH A PHYSICAL OR DIGITAL RECEIPT IN THE LANGUAGE CHOSEN BY THE INDIVIDUAL THAT CONTAINS ALL OF THE FOLLOWING INFORMATION:

1. THE CRYPTOCURRENCY KIOSK OPERATOR'S NAME AND CONTACT INFORMATION, INCLUDING A TELEPHONE NUMBER TO ANSWER QUESTIONS AND

REGISTER COMPLAINTS.

2. THE STATE AND LOCAL LAW ENFORCEMENT OR GOVERNMENT AGENCY THAT RECEIVES COMPLAINTS OF FRAUD.

3. THE TYPE, VALUE, DATE AND PRECISE TIME OF A TRANSACTION, THE TRANSACTION HASH AND EACH APPLICABLE VIRTUAL CURRENCY ADDRESS.

4. THE NAME AND CONTACT INFORMATION OF THE SENDER.

5. THE NAME, CONTACT INFORMATION AND VIRTUAL WALLET NUMBER OF THE DESIGNATED RECIPIENT.

6. DAI FEES CHARGED. FOR THE PURPOSES OF THIS PARAGRAPH, "DAI" MEANS A DECENTRALIZED STABLECOIN TOKEN THAT IS DESIGNED TO MAINTAIN A VALUE OF THE UNITED STATES DOLLAR.

7. THE EXCHANGE RATE OF THE VIRTUAL CURRENCY TO THE UNITED STATES DOLLAR.

8. A STATEMENT OF THE CRYPTOCURRENCY KIOSK OPERATOR'S REFUND POLICY.

9. ANY ADDITIONAL INFORMATION THAT A GOVERNMENT AUTHORITY MAY REQUIRE.

D. A CRYPTOCURRENCY KIOSK OPERATOR SHALL USE BLOCKCHAIN ANALYTICS AND TRACING SOFTWARE TO HELP PREVENT FRAUD BY NOT SENDING PURCHASED VIRTUAL CURRENCY FROM A CRYPTOCURRENCY KIOSK OPERATOR TO A VIRTUAL WALLET KNOWN TO BE AFFILIATED WITH FRAUD AT THE TIME OF A TRANSACTION. A RELEVANT GOVERNMENT AUTHORITY MAY REQUEST EVIDENCE FROM ANY CRYPTOCURRENCY KIOSK OPERATOR OF CURRENT USE OF BLOCKCHAIN ANALYTICS.

E. ALL CRYPTOCURRENCY KIOSK OPERATORS SHALL TAKE REASONABLE STEPS TO DETECT AND PREVENT FRAUD, INCLUDING ESTABLISHING AND MAINTAINING A WRITTEN ANTI-FRAUD POLICY AND CONFORMING TO FEDERAL KNOW YOUR CONSUMER AND ANTI-MONEY LAUNDERING LAWS.

F. A CRYPTOCURRENCY KIOSK OPERATOR MAY NOT ACCEPT TRANSACTIONS OF MORE THAN $2,000 UNITED STATES DOLLARS IN CASH OR THE EQUIVALENT IN VIRTUAL CURRENCY IN ONE DAY FROM A NEW CUSTOMER IN THIS STATE THROUGH ONE OR MORE CRYPTOCURRENCY KIOSKS. FOR EXISTING CUSTOMERS, A CRYPTOCURRENCY KIOSK OPERATOR SHALL ENSURE THAT THE CRYPTOCURRENCY KIOSK DOES NOT, IN CONNECTION WITH CRYPTOCURRENCY SERVICES FOR A SINGLE PERSON IN THIS STATE USING ONE OR MORE CRYPTOCURRENCY KIOSKS, ACCEPT OR DISPENSE IN A SINGLE DAY MORE THAN $10,500.

G. ALL CRYPTOCURRENCY KIOSK OPERATORS PERFORMING BUSINESS IN THIS STATE SHALL PROVIDE LIVE CUSTOMER SERVICE AT A MINIMUM OF TWENTY-FOUR HOURS A DAY, SEVEN DAYS PER WEEK. THE CUSTOMER SERVICE TOLL-FREE NUMBER SHALL BE PROMINENTLY DISPLAYED ON THE CRYPTOCURRENCY KIOSK OR THE CRYPTOCURRENCY KIOSK SCREENS.

H. IF A NEW CUSTOMER AS DEFINED IN SUBSECTION L, PARAGRAPH 7 OF THIS SECTION HAS BEEN FRAUDULENTLY INDUCED TO ENGAGE IN A CRYPTOCURRENCY KIOSK TRANSACTION, THE CRYPTOCURRENCY KIOSK OPERATOR SHALL ISSUE A FULL REFUND FOR THE FRAUDULENTLY INDUCED CRYPTOCURRENCY KIOSK TRANSACTION, INCLUDING ANY FEES CHARGED IN ASSOCIATION WITH THE TRANSACTION, IF THE NEW CUSTOMER DOES ALL OF THE FOLLOWING:

1. CONTACTS THE CRYPTOCURRENCY KIOSK OPERATOR WITHIN THIRTY DAYS AFTER THE CRYPTOCURRENCY KIOSK TRANSACTION.

2. CONTACTS A LAW ENFORCEMENT AGENCY OR THE ATTORNEY GENERAL WITHIN THIRTY DAYS AFTER THE CRYPTOCURRENCY KIOSK TRANSACTION.

3. PROVIDES THE CRYPTOCURRENCY KIOSK OPERATOR WITH A REPORT FROM THE LAW ENFORCEMENT AGENCY OR ATTORNEY GENERAL'S OFFICE THAT DETERMINES THAT THE NEW CUSTOMER WAS FRAUDULENTLY INDUCED TO ENGAGE IN A CRYPTOCURRENCY KIOSK TRANSACTION.

I. A VICTIM OF FRAUD IS ELIGIBLE TO RECEIVE A REFUND EVEN IF A CRYPTOCURRENCY KIOSK OPERATOR PROVIDES THE REQUIRED DISCLOSURES PRESCRIBED IN SUBSECTIONS A AND B OF THIS SECTION AND THE RECEIPT PRESCRIBED IN SUBSECTION C OF THIS SECTION.

J. THE ATTORNEY GENERAL SHALL ENFORCE THIS SECTION. ANY ACT OR PRACTICE THAT VIOLATES THIS SECTION IS A VIOLATION OF SECTION 44-1522.

K. NOTWITHSTANDING ANY OTHER LAW, ALL INDIVIDUALS OR ENTITIES SUBJECT TO THIS SECTION SHALL BE CLASSIFIED AS A NEW CUSTOMER FOR THE PURPOSES OF COMPLIANCE ON THE EFFECTIVE DATE OF THIS SECTION. A NEW CUSTOMER AUTOMATICALLY CONVERTS TO AN EXISTING CUSTOMER TEN DAYS AFTER BECOMING A NEW CUSTOMER. AN EXISTING CUSTOMER IS SUBJECT TO THE TRANSACTION LIMITS PRESCRIBED IN THIS SECTION.

L. FOR THE PURPOSES OF THIS SECTION:

1. "BLOCKCHAIN ANALYTICS" MEANS THE ANALYSIS OF DATA FROM BLOCKCHAINS OR PUBLIC DISTRIBUTED LEDGERS, INCLUDING ASSOCIATED TRANSACTION INFORMATION.

2. "BLOCKCHAIN ANALYTICS AND TRACING SOFTWARE" MEANS A SOFTWARE SERVICE THAT USES BLOCKCHAIN ANALYTICS DATA TO PROVIDE RISK-SPECIFIC INFORMATION AND TRACING OF VIRTUAL CURRENCY WALLET ADDRESSES, AMONG OTHER VIRTUAL ITEMS.

3. "CRYPTOCURRENCY KIOSK":

(a) MEANS A PHYSICAL, ELECTRONIC TERMINAL THAT IS A MECHANICAL AGENT OF THE CRYPTOCURRENCY KIOSK OPERATOR AND THAT ENABLES A CRYPTOCURRENCY KIOSK OPERATOR TO FACILITATE THE PURCHASE, SALE OR EXCHANGE OF CRYPTOCURRENCY FOR MONEY, BANK CREDIT OR ANY OTHER VIRTUAL CURRENCY.

(b) INCLUDES A VIRTUAL CURRENCY EXCHANGE, WHICH PERFORMS THE ACTUAL VIRTUAL CURRENCY TRANSMISSION OR DRAWING ON THE VIRTUAL CURRENCY THAT IS IN THE POSSESSION OF THE ELECTRONIC TERMINAL OPERATOR.

4. "CRYPTOCURRENCY KIOSK OPERATOR" MEANS AN INDIVIDUAL OR ENTITY:

(a) THAT ENGAGES IN VIRTUAL CURRENCY BUSINESS ACTIVITY THROUGH A MONEY TRANSMISSION KIOSK IN THIS STATE.

(b) THAT OPERATES OR MANAGES A MONEY TRANSMISSION KIOSK WHERE VIRTUAL CURRENCY BUSINESS ACTIVITY IS OFFERED IN THIS STATE.

5. "CRYPTOCURRENCY KIOSK TRANSACTION" MEANS BOTH:

(a) A TRANSACTION CONDUCTED OR PERFORMED, IN WHOLE OR IN PART, BY ELECTRONIC MEANS THROUGH A CRYPTOCURRENCY KIOSK.

(b) A TRANSACTION MADE AT A CRYPTOCURRENCY KIOSK TO PURCHASE VIRTUAL CURRENCY WITH FIAT CURRENCY OR TO SELL VIRTUAL CURRENCY FOR FIAT CURRENCY.

6. "EXISTING CUSTOMER" MEANS A CONSUMER TRANSACTING AT A CRYPTOCURRENCY KIOSK IN THIS STATE WHO HAS BEEN A CUSTOMER WITH A CRYPTOCURRENCY KIOSK OPERATOR FOR AT LEAST TEN DAYS.

7. "NEW CUSTOMER" MEANS A CONSUMER TRANSACTING AT A CRYPTOCURRENCY KIOSK IN THIS STATE WHO HAS BEEN A CUSTOMER OF A CRYPTOCURRENCY KIOSK OPERATOR FOR LESS THAN TEN DAYS.

8. "TRANSACTION HASH" MEANS A UNIQUE IDENTIFIER MADE UP OF A STRING OF CHARACTERS THAT ACTS AS A RECORD OF AND PROVIDES PROOF THAT THE TRANSACTION WAS VERIFIED AND ADDED TO THE BLOCKCHAIN.

9. "VIRTUAL CURRENCY ADDRESS":

(a) MEANS A UNIQUE PUBLIC ALPHANUMERIC IDENTIFIER THAT IS ASSOCIATED WITH A VIRTUAL CURRENCY TYPE AND WALLET AND THAT IDENTIFIES THE LOCATION WHERE VIRTUAL CURRENCY TRANSACTION CAN BE SENT.

(b) IS REFERRED TO AS A PUBLIC KEY.

10. "VIRTUAL WALLET":

(a) MEANS A SOFTWARE APPLICATION OR OTHER MECHANISM THAT PROVIDES A MEANS TO HOLD, STORE OR TRANSFER VIRTUAL CURRENCY OR NONFUNGIBLE TOKENS.

(b) INCLUDES A PUBLIC KEY, PRIVATE KEY AND A PUBLIC RECEIVING ADDRESS. FOR THE PURPOSES OF THIS SUBDIVISION, A PRIVATE KEY MAY BE USED TO SIGN FOR A TRANSACTION WHEN SENDING CRYPTOCURRENCY FROM A VIRTUAL WALLET.

APPROVED BY THE GOVERNOR MAY 12, 2025.

FILED IN THE OFFICE OF THE SECRETARY OF STATE MAY 12, 2025.

SENATE BILL 25-079

BY SENATOR(S) Rich and Roberts, Hinrichsen, Kipp;
also REPRESENTATIVE(S) Taggart and Jackson, Bacon, Joseph, Lieder, Mabrey, Paschal, Ricks, Rutinel.

CONCERNING THE "COLORADO VENDING OF DIGITAL ASSETS ACT".

Be it enacted by the General Assembly of the State of Colorado:

SECTION 1. In Colorado Revised Statutes, **add** article 112 to title 11 as follows:

ARTICLE 112
Colorado Vending of Digital Assets

11-112-101. Short title. THE SHORT TITLE OF THIS ARTICLE 112 IS THE "COLORADO VENDING OF DIGITAL ASSETS ACT".

11-112-102. Definitions. AS USED IN THIS ARTICLE 112, UNLESS THE CONTEXT OTHERWISE REQUIRES:

(1) "BLOCKCHAIN TECHNOLOGY" HAS THE MEANING SET FORTH IN SECTION 24-36-121.5 (2)(a).

Capital letters or bold & italic numbers indicate new material added to existing law; dashes through words or numbers indicate deletions from existing law and such material is not part of the act.

(2) (a) "NEW CUSTOMER" MEANS A CUSTOMER TRANSACTING AT A VIRTUAL CURRENCY KIOSK IN COLORADO WHO HAS BEEN A CUSTOMER OF AN OWNER OR OPERATOR OF A VIRTUAL CURRENCY KIOSK FOR LESS THAN SEVEN DAYS.

(b) SEVEN DAYS AFTER A CUSTOMER FIRST TRANSACTS WITH AN OWNER OR OPERATOR OF A VIRTUAL CURRENCY KIOSK, THE CUSTOMER IS CONSIDERED AN EXISTING CUSTOMER AND IS NOT SUBJECT TO THE NEW CUSTOMER TRANSACTION LIMIT DESCRIBED IN SECTION 11-112-103 (6).

(3) "TRANSACTION HASH" MEANS A UNIQUE IDENTIFIER MADE UP OF A STRING OF CHARACTERS THAT ACTS AS A RECORD AND PROVIDES PROOF THAT A TRANSACTION WAS VERIFIED AND ADDED TO BLOCKCHAIN TECHNOLOGY.

(4) (a) "VIRTUAL CURRENCY" MEANS A TYPE OF DIGITAL UNIT THAT IS USED AS A MEDIUM OF EXCHANGE OR A FORM OF DIGITALLY STORED VALUE OR THAT IS INCORPORATED INTO PAYMENT SYSTEM TECHNOLOGY.

(b) "VIRTUAL CURRENCY" INCLUDES DIGITAL UNITS THAT:

(I) HAVE A CENTRALIZED REPOSITORY OR ADMINISTRATOR;

(II) ARE DECENTRALIZED AND HAVE NO CENTRALIZED REPOSITORY OR ADMINISTRATOR; OR

(III) MAY BE CREATED OR OBTAINED BY COMPUTING OR MANUFACTURING EFFORT.

(c) "VIRTUAL CURRENCY" DOES NOT INCLUDE DIGITAL UNITS THAT:

(I) ARE USED SOLELY WITHIN ONLINE GAMING PLATFORMS, WITH NO MARKET OR APPLICATION OUTSIDE THE GAMING PLATFORMS;

(II) ARE USED EXCLUSIVELY AS PART OF A CONSUMER AFFINITY OR REWARDS PROGRAM AND CAN BE APPLIED AS PAYMENT FOR PURCHASES WITH THE ISSUER OR OTHER DESIGNATED MERCHANTS BUT CANNOT BE CONVERTED INTO OR REDEEMED FOR FIAT CURRENCY; OR

(III) ARE USED AS PART OF A CONSUMER AFFINITY OR REWARDS PROGRAM OFFERED THROUGH AN INSTITUTION THAT IS INSURED BY THE FEDERAL DEPOSIT INSURANCE CORPORATION OR THE NATIONAL CREDIT UNION ADMINISTRATION.

(5) "VIRTUAL CURRENCY ADDRESS" MEANS AN ALPHANUMERIC IDENTIFIER REPRESENTING A DESTINATION FOR A VIRTUAL CURRENCY TRANSFER THAT IS ASSOCIATED WITH A VIRTUAL CURRENCY WALLET.

(6) "VIRTUAL CURRENCY KIOSK" MEANS AN ELECTRONIC TERMINAL ACTING AS A MECHANICAL AGENT OF THE OWNER OR OPERATOR TO ENABLE THE OWNER OR OPERATOR TO FACILITATE THE EXCHANGE OF VIRTUAL CURRENCY FOR OTHER VIRTUAL CURRENCY OR FIAT CURRENCY, INCLUDING BY:

(a) CONNECTING TO A SEPARATE VIRTUAL CURRENCY EXCHANGER THAT PERFORMS THE ACTUAL VIRTUAL CURRENCY TRANSMISSION; OR

(b) DRAWING UPON THE VIRTUAL CURRENCY IN THE POSSESSION OF THE OWNER OR OPERATOR OF THE ELECTRONIC TERMINAL.

(7) "VIRTUAL CURRENCY WALLET" MEANS A SOFTWARE APPLICATION OR OTHER MECHANISM PROVIDING A MEANS FOR HOLDING, STORING, AND TRANSFERRING VIRTUAL CURRENCY.

11-112-103. Virtual currency kiosks - disclosures - receipts - daily limit - cancellation and refund. (1) BEFORE ENTERING INTO A VIRTUAL CURRENCY TRANSACTION FOR, ON BEHALF OF, OR WITH A CUSTOMER, THE OWNER OR OPERATOR OF A VIRTUAL CURRENCY KIOSK SHALL DISCLOSE TO THE CUSTOMER IN CLEAR AND CONSPICUOUS WRITING IN THE ENGLISH LANGUAGE ALL MATERIAL RISKS ASSOCIATED WITH VIRTUAL CURRENCY. THE DISCLOSURES MUST BE DISPLAYED ON THE SCREEN OF THE VIRTUAL CURRENCY KIOSK WITH THE ABILITY FOR A CUSTOMER TO ACKNOWLEDGE RECEIPT OF THE DISCLOSURES. THE DISCLOSURES MUST INCLUDE AT LEAST THE FOLLOWING STATEMENT:

WARNING: THIS TECHNOLOGY CAN BE USED TO DEFRAUD YOU. IF YOU HAVE BEEN DIRECTED TO THIS MACHINE BY SOMEONE CLAIMING TO BE A GOVERNMENT AGENT, BILL COLLECTOR, LAW ENFORCEMENT OFFICER, OR

ANYONE YOU DO NOT KNOW PERSONALLY, STOP THIS TRANSACTION IMMEDIATELY AND CONTACT YOUR FINANCIAL ADVISOR AND LOCAL LAW ENFORCEMENT.

(2) WHEN OPENING AN ACCOUNT FOR A CUSTOMER, THE OWNER OR OPERATOR OF A VIRTUAL CURRENCY KIOSK SHALL DISCLOSE TO THE CUSTOMER IN CLEAR AND CONSPICUOUS WRITING IN THE ENGLISH LANGUAGE ALL RELEVANT TERMS AND CONDITIONS ASSOCIATED WITH THE PRODUCTS, SERVICES, AND ACTIVITIES OF THE OWNER OR OPERATOR AND VIRTUAL CURRENCY GENERALLY, INCLUDING THE FOLLOWING:

(a) THE CUSTOMER'S LIABILITY FOR UNAUTHORIZED VIRTUAL CURRENCY TRANSACTIONS;

(b) UNDER WHICH CIRCUMSTANCES THE OWNER OR OPERATOR WILL, ABSENT A COURT OR GOVERNMENT ORDER, DISCLOSE INFORMATION CONCERNING THE CUSTOMER'S ACCOUNT TO THIRD PARTIES;

(c) THE CUSTOMER'S RIGHT TO RECEIVE PERIODIC ACCOUNT STATEMENTS AND VALUATIONS FROM THE OWNER OR OPERATOR;

(d) THE CUSTOMER'S RIGHT TO RECEIVE A RECEIPT, A TRADE TICKET, OR OTHER EVIDENCE OF A VIRTUAL CURRENCY TRANSACTION; AND

(e) THE CUSTOMER'S RIGHT TO PRIOR NOTICE OF A CHANGE IN THE RULES OR POLICIES OF THE OWNER OR OPERATOR.

(3) PRIOR TO A TRANSACTION IN VIRTUAL CURRENCY FOR, ON BEHALF OF, OR WITH A CUSTOMER, THE OWNER OR OPERATOR OF A VIRTUAL CURRENCY KIOSK SHALL DISCLOSE TO THE CUSTOMER IN CLEAR AND CONSPICUOUS WRITING IN THE ENGLISH LANGUAGE THE TERMS AND CONDITIONS OF THE VIRTUAL CURRENCY TRANSACTION, INCLUDING THE FOLLOWING:

(a) THE AMOUNT OF THE TRANSACTION;

(b) THE FEES, EXPENSES, AND CHARGES BORNE BY THE CUSTOMER, INCLUDING APPLICABLE EXCHANGE RATES;

(c) THE TYPE AND NATURE OF THE TRANSACTION;

(d) A WARNING THAT, ONCE COMPLETED, THE TRANSACTION IS IRREVERSIBLE, IF APPLICABLE;

(e) THE DIFFERENCE IN THE VIRTUAL CURRENCY'S SALE PRICE VERSUS THE CURRENT MARKET PRICE; AND

(f) OTHER DISCLOSURES THAT ARE CUSTOMARILY GIVEN IN CONNECTION WITH A VIRTUAL CURRENCY TRANSACTION.

(4) THE OWNER OR OPERATOR OF A VIRTUAL CURRENCY KIOSK SHALL ENSURE THAT EACH CUSTOMER ACKNOWLEDGES RECEIPT OF ALL DISCLOSURES REQUIRED UNDER THIS SECTION.

(5) UPON THE COMPLETION OF A VIRTUAL CURRENCY TRANSACTION, THE OWNER OR OPERATOR OF A VIRTUAL CURRENCY KIOSK SHALL PROVIDE TO THE CUSTOMER AN ELECTRONIC RECEIPT CONTAINING THE FOLLOWING INFORMATION:

(a) THE NAME OF AND CONTACT INFORMATION FOR THE OWNER OR OPERATOR, INCLUDING A TELEPHONE NUMBER ESTABLISHED BY THE OWNER OR OPERATOR TO ANSWER QUESTIONS AND REGISTER COMPLAINTS;

(b) THE TYPE, VALUE, DATE, AND PRECISE TIME OF THE VIRTUAL CURRENCY TRANSACTION, THE TRANSACTION HASH, AND EACH VIRTUAL CURRENCY ADDRESS;

(c) THE FEE CHARGED;

(d) THE EXCHANGE RATE, IF APPLICABLE;

(e) A STATEMENT OF THE LIABILITY OF THE OWNER OR OPERATOR FOR NONDELIVERY OR DELAYED DELIVERY OF THE CURRENCY FOR WHICH THE CUSTOMER EXCHANGED VIRTUAL CURRENCY; AND

(f) A STATEMENT OF THE REFUND POLICY OF THE OWNER OR OPERATOR.

(6) (a) FOR A NEW CUSTOMER, THE MAXIMUM DAILY TRANSACTION LIMIT OF A VIRTUAL CURRENCY KIOSK IS TWO THOUSAND DOLLARS PER CUSTOMER.

(b) FOR AN EXISTING CUSTOMER, THE MAXIMUM DAILY TRANSACTION LIMIT OF A VIRTUAL CURRENCY KIOSK IS TEN THOUSAND FIVE HUNDRED DOLLARS PER CUSTOMER.

(7) (a) THE OWNER OR OPERATOR OF A VIRTUAL CURRENCY KIOSK SHALL, AT THE EXPENSE OF THE OWNER OR OPERATOR, ALLOW A CUSTOMER TO CANCEL AND RECEIVE A FULL REFUND FOR A VIRTUAL CURRENCY TRANSACTION IF:

(I) THE VIRTUAL CURRENCY TRANSACTION WAS THE CUSTOMER'S FIRST VIRTUAL CURRENCY TRANSACTION;

(II) THE VIRTUAL CURRENCY TRANSACTION WAS TO A VIRTUAL CURRENCY WALLET OR EXCHANGE LOCATED OUTSIDE OF THE UNITED STATES; AND

(III) WITHIN SIXTY DAYS AFTER THE VIRTUAL CURRENCY TRANSACTION, THE CUSTOMER CONTACTS THE OWNER OR OPERATOR OF THE VIRTUAL CURRENCY KIOSK AND A GOVERNMENT OR LAW ENFORCEMENT ENTITY REGARDING THE FRAUDULENT NATURE OF THE TRANSACTION AND SUBMITS PROOF OF THE FRAUD, SUCH AS A POLICE REPORT OR NOTARIZED DECLARATION DETAILING THE FRAUDULENT NATURE OF THE VIRTUAL CURRENCY TRANSACTION.

(b) IF THE CONDITIONS OF SUBSECTION (7)(a) OF THIS SECTION ARE MET, THE OWNER OR OPERATOR SHALL ISSUE A FULL REFUND WITHIN SEVENTY-TWO HOURS AFTER BEING NOTIFIED THAT THE VIRTUAL CURRENCY TRANSACTION WAS FRAUDULENT.

SECTION 2. Act subject to petition - effective date. This act takes effect January 1, 2026; except that, if a referendum petition is filed pursuant to section 1 (3) of article V of the state constitution against this act or an item, section, or part of this act within the ninety-day period after final adjournment of the general assembly, then the act, item, section, or part will not take effect unless approved by the people at the general election to be

held in November 2026 and, in such case, will take effect on the date of the official declaration of the vote thereon by the governor.

James Rashad Coleman, Sr.
PRESIDENT OF
THE SENATE

Julie McCluskie
SPEAKER OF THE HOUSE
OF REPRESENTATIVES

Esther van Mourik
SECRETARY OF
THE SENATE

Vanessa Reilly
CHIEF CLERK OF THE HOUSE
OF REPRESENTATIVES

APPROVED Monday June 2nd 2025 at 11:00 am
(Date and Time)

Jared S. Polis
GOVERNOR OF THE STATE OF COLORADO

Hawaii Bankers Association

DATE: March 31, 2026

TO: Representative David Tarnas, Chair
Committee on Judiciary & Hawaiian Affairs

FROM: Tiffany Yajima / Mihoko Ito

RE: **SB2387, SD1, HD1 – Relating to Digital Financial Asset Transaction Kiosks**
Hearing Date: Wednesday, April 1, 2026 at 2:00 p.m.
Conference Room: 325

Dear Chair Tarnas, Vice Chair Poepoe, and Members of the Committee:

We submit this testimony on behalf of the Hawaii Bankers Association (HBA). HBA represents seven Hawai`i banks and one bank from the continent with branches in Hawai`i.

HBA **supports** S.B. 2387, SD1, HD1, which among other things establishes safeguards on cryptocurrency kiosks by setting a daily transaction limit of $2,000 and a transaction limit of $10,000 in any thirty-day period to prevent large sums of money from being withdrawn or deposited via cryptocurrency kiosks.

The digital asset market includes a range of instruments – from speculative and highly price volatile cryptocurrencies (e.g., bitcoin and ether), to so-called stablecoins that are backed by a collection of assets (e.g., USDC and Tether), to digital representations of customer bank deposits on a blockchain. Each category of digital asset has unique risk characteristics depending on its issuer and use case.

As of December 2024, the total value of cryptocurrencies, including stablecoins, stands at around $3.7 trillion, besting its previous peak of $3 trillion in November 2021 and recovering from a recent low of about $1 trillion in the first half of 2022.

In 2022, the drop in cryptocurrency valuations coupled with risky, highly leveraged, and largely unregulated business models resulted in some digital asset companies becoming insolvent, wiping out some customers and leaving others frozen out of accounts they thought were protected.

Given there is no comprehensive regulatory framework that establishes guidelines for risk management and consumer protection in the digital asset market, HBA supports the intent of the bill because of the significant risks of fraud against consumers.

Scams and fraud have reached epidemic proportions. The Federal Trade Commission reports that fraud losses in the U.S. topped $23.7 billion last year, though some estimate that number could be as high as $158 billion. While these kiosks enable

Hawaii Bankers Association

people to make legitimate financial transactions every day, these kiosks are also increasingly being used in scams targeting older adults. In these scams, victims are convinced to use the kiosks to transfer cryptocurrencies to a wallet address controlled by the scammer.

HBA supports this measure as a way to protect consumers from fraud, exploitation, and coercive schemes in digital asset transactions.

Thank you for the opportunity to submit this testimony.

808-524-5161 P.O. Box 10065, Honolulu, Hawaii 96816 director@hawaiiba.org

TESTIMONY SUBMITED TO THE HAWAII HOUSE COMMITTEE ON JUDICIARY & HAWAIIAN AFFAIRS
Larry Lipka, General Counsel
April 1, 2026

Chairs Tarnas and honorable members of the House Consumer Protection and Commerce Committee, thank you for the opportunity to provide testimony today regarding legislation related to cryptocurrency kiosks.

CoinFlip does support proposed regulatory measures that would further consumer protection including but not limited to licensure, mandatory disclosures, compliance program requirements, and technology requirements. We appreciate the opportunity to offer additional consumer protection-focused recommendations that we know to be highly effective in preventing fraudulent transactions at virtual currency kiosks and look forward to continuing to work with the State of Hawaii to protect consumers.

Company Background

CoinFlip is a Chicago-based, global digital currency platform, focused on providing consumers with a simple and secure way to buy and sell virtual currency. Founded in 2015, CoinFlip is one of the world's largest operators of virtual currency kiosks, with more than 5,000 locations across the United States and in nine countries around the world, employing more than 200 people.

CoinFlip's kiosks make buying and selling major cryptocurrencies accessible and secure for consumers who wish to purchase their virtual currency using cash. CoinFlip has operated in the State of Hawaii since 2020. We applied for a money transmitter license in 2025 but were told by the department that none was required. Additionally, CoinFlip is a money service business ("MSB") registered with the Financial Crimes Enforcement Network. As an MSB, CoinFlip is subject to the Bank Secrecy Act ("BSA"), the United States PATRIOT Act, and their implementing rules and regulations.

CoinFlip embraces licensing regimes as an effective means to create baseline requirements for operations, as well as effective oversight. CoinFlip holds 41 money transmitter licenses with additional applications currently pending. CoinFlip has moved to obtain these licenses, even in states where there is no current licensing requirement, like Hawaii.

It is vital that smart, pro-consumer regulations are enacted to provide needed guardrails to the industry. However, it is important to remember that of all cryptocurrency scams that happened in the U.S. in 2024 (latest year data available), 3% happened at a kiosk, and 97% at another product. Additionally, the vast majority of the financial fraud still occurs at traditional financial institutions, gift cards, and payment apps like Venmo and PayPal.

SB 2387

CoinFlip supports SB 23887 but offers amendments to further protect consumers while allowing individuals to continue to purchase cryptocurrency in the manner of their choosing. The proposed transaction limits in the bill do not adequately consider federal reporting requirements. Under federal law, CoinFlip is required to file a Suspicious Activity Report ("SAR") for any suspected suspicious transactions of at least $2,000 and a Currency Transaction Report ("CTR") for transactions above $10,000. This information is placed in a repository for law enforcement to quickly and accurately conduct investigations.

Hawaii's proposed $2,000/day transaction limit and $10,000 monthly aggregate limit would encourage bad actors to split transactions across multiple operators ("stacking") in order to avoid state thresholds, undermining AML monitoring and making scams harder to detect. These limits would also reduce reporting: if transactions are forced below federal CTR thresholds, kiosk operators will not file CTRs, resulting in less information available to law enforcement.

Lastly, the refund provisions found in SB 2387 are unprecedented for money service businesses. No other financial service product has statutory requirements for authorized transactions like contained in this bill. Under Regulation E, a consumer is entitled to a refund only for an unauthorized transfer, not for transactions the consumer authorized or participated in (12 C.F.R. §§ 1005.2(m), 1005.11). Imposing this refund obligation solely on kiosk operators implies that no other participant in the scam ecosystem, such as phone carriers, social media platforms, email providers, or financial institutions, shares responsibility for the transaction, despite their role in enabling the fraud.

However, we do recognize that new customers are among the most vulnerable to scams, so we support refunds for new customers and refund of fees for any customer, as we do not want to profit off fraud. CoinFlip already voluntarily refunds fees to victims of scams.

Proposed Consumer Protection Policies

CoinFlip believes smart regulation is good for business. We believe that a regulatory framework is necessary to protect consumers and encourage innovation in the industry; however, transaction limits and refund provisions as currently proposed in SB 2387 do not take into consideration federal reporting requirements. Instead, we developed the following best practices that would further enhance consumer protections and support their inclusion in any legislation:

- **Require licensure with the state**. CoinFlip believes a money transmitter license should be required for all virtual currency kiosk operators, allowing for state oversight and periodic audits to determine the adequacy of compliance, finance, and cybersecurity programs.
- **Require robust compliance programs**. Kiosk operators should be required to directly employ a qualified, in-house, Chief Compliance Officer and compliance team, that does not have a large ownership interest in the company. At CoinFlip, we take compliance seriously: our Chief Compliance Officer is a former federal prosecutor, and our general counsel is a former Illinois Assistant Attorney General.

- **Require clear, highly visible warnings and fee disclosures**. We agree with the proposed legislation regarding the requirement of clear disclosures regarding all fees and terms of service. We also believe highly visible fraud warnings should be required to be displayed and acknowledged by the customer prior to the initiation and completion of any transaction.
- **Require blockchain analytics**. The use of blockchain analytics technology should be required to fight fraud by automatically blocking customer transactions to high-risk digital wallets.
- **Require live customer service**. Customer service is the first line of defense for consumer protection. We believe every virtual currency kiosk operator should be required to provide trained, live customer service at minimum during business hours.
- **ID Verification**. Require operators to follow federal law for money service businesses and take photo identification for transactions over $1,000 in a day. We use a third-party company to verify customer IDs are legitimate and match who is at the kiosk.
- **Daily Transaction Limits**. New customers are defined as those using machines in the first three days with a daily limit of $2,500. After the new customer period, existing customers have a limit of $10,500.
    - These limits track with Illinois, Maryland, Colorado, Nebraska, Oklahoma, Arizona. Missouri has no limits. Similar limits are currently proposed in Alabama, Florida, Georgia, Ohio, and New Hampshire.
- **Fee Cap**. Place a fee cap of 18% on kiosk transactions.
    - States that have instituted a fee cap have been between 15-18%.
- **First Transaction Hold.** Hold the first transaction of a new customer for 48 hours, during which time a customer can call and cancel the transaction with no questions asked.
- **Customer Refunds.** Require operators to refund fees of all transaction fees related to fraud.
- **Dedicated law enforcement contact.** Require operators to have a dedicated phone, email, and staff person assigned to receive law enforcement contacts.
- **Wallet Pinning.** Operators must link one wallet to one customer so that if it is attempted to be used by another customer, the transaction can be blocked.

CoinFlip shares your goals of consumer protection. Although blockchain technology and virtual currency kiosks are new, the fraud we see reported is all too familiar. Whether it's phone, email, text or an online pop-up, scammers repackage the same old tactics and utilize whatever methods they have at hand – Venmo, PayPal, Zelle, Gift Cards, MoneyGram or virtual currency kiosks – to dupe people out of their money.

The best defense for consumers is to be well-informed and well-alerted at the point of transaction. The best defense for companies is to have the right tools in place to help identify and fight fraud and help law enforcement catch the bad actors.

Sincerely,

/s/ Larry Lipka
Larry Lipka
General Counsel

House of Representatives
Notice of Hearing

Wednesday, April 1, 2026
2:00 p.m.

RELATING TO DIGITAL FINANCIAL ASSET TRANSACTION KIOSKS
S.B. 2387, SD1, HD1

House Committee on Judiciary and Hawaiian Affairs

Aloha Chair Tarnas, Vice Chair Poepoe and members of the Committee on Judiciary and Hawaiian Affairs.

My name is Carol Wakayama and I wish to express my STRONG SUPPORT for S.B. 2387, SD1, HD1.

During 2025, I heard comments about crypto-currency machines springing up in Hawaii. From what I understand, these machines are relatively new. There is, however, a potentially large risk to those with limited digital knowledge. Machines users could lose large amounts of monies and possibly their life/retirement savings - to criminal fraudsters.

Over the past decades, I have heard numerous stories of phone calls that are allegedly from law enforcement, attorneys or other individuals. These fraudsters appear to have one thing in common…. They prey on someone's "tendency for concern" by either pretending to be someone they are not or having a traumatic story that frightens the listener into handing over monies. These fraudsters are predators.

Passage of S.B. 2387, SD1, HD1 will help provide some protection and safeguards to the consumer. For example, posting of clearly worded signs that "warn users of potential financial risk"; how to contact law enforcement should the users suspect fraud; setting limits on transactions to a specific amount. By increasing protections for machine users, I hope that crypto-currency fraudsters will realize that Hawaii's residents are better protected/educated against fraud and may think twice before increasing the number of these machines in Hawaii. Thank you for your support of S.B. 2387, SD1, HD1.

Carol Wakayama
Punchbowl District

SB-2387-HD-1
Submitted on: 3/30/2026 5:53:22 PM
Testimony for JHA on 4/1/2026 2:00:00 PM

Submitted By	Organization	Testifier Position	Testify
William Caron	Individual	Support	Written Testimony Only

Comments:

Aloha Chair, Vice Chair, and members of the committee,

I am writing in **strong support** of SB2387, and I want to begin by acknowledging the significant improvements made by the previous committee. The amendments prohibiting cash purchases from new customers, restricting transactions between two customers to the same wallet address, and setting a January 1, 2030 deadline for a full prohibition on cash purchases represent significant and meaningful steps forward.

These changes reflect a genuine commitment to protecting Hawaiʻi's residents from the epidemic of fraud devastating our communities, particularly our kūpuna.

However, I respectfully urge this Committee to go further. While the amendments are a welcome and substantial improvement, they still leave critical gaps that scammers will exploit. The only truly effective solution remains a full and immediate ban on cash purchases at these kiosks.

The Amendments Are a Strong Step—But Not Yet Strong Enough

The previous committee's amendments deserve recognition. Prohibiting cash purchases from new customers immediately cuts off a significant vector of fraud, as scammers often target first-time users. Restricting wallet addresses prevents the complex laundering schemes that make recovery impossible. And setting a sunset date of 2030 establishes a clear endpoint for the industry to transition away from cash-to-crypto conversions.

These are thoughtful, targeted changes, and I commend the committee for their work.

However, the 2030 deadline is too far away. In the intervening years, countless more residents will fall victim to fraud. Scammers do not need new customers—they can still target existing users. And as long as cash purchases remain legal for anyone, the machines will continue to function as the primary vehicle for fraud.

The Vast Majority of Cash Deposit Transactions at These Kiosks Are Scams

Representative Scot Matayoshi, Chair of the House Consumer Protection Committee, has stated plainly: "These crypto kiosks, in my opinion, are mostly used for fraudulent transactions. The benefit to them doesn't outweigh the massive fraud going on with these ATMs."

When the primary purpose of a machine is to facilitate fraud, the only effective solution is to "make that number zero" for cash purchases at these kiosks. The Office of Consumer Protection itself has testified that a ban on cash purchases "is probably the best way to protect consumers from fraud."

The current amendments bring us closer to that goal, but they do not achieve it. They kick the can to 2030 while leaving the door open for scammers to continue exploiting the system.

A Full Ban on Cash Purchases Still Allows Legitimate Use

Importantly, a full and immediate ban on cash purchases would not prevent people from using these kiosks for legitimate purposes. Users could still:

- **Cash out their cryptocurrency** by converting digital assets into paper currency.
- **Convert from one cryptocurrency to another** without involving cash.

This approach targets the specific function that scammers exploit—the irreversible conversion of cash into crypto at the direction of a fraudster—while preserving access for those who already hold digital assets and wish to liquidate them.

The Harm Is Irreversible and Devastating

The financial damage victims face is lasting and severe. As AARP Hawai‘i State Director Keali‘i Lopez has testified: "When those tens of thousands of dollars are lost, they can't recoup it. When they lose their home, they can't recoup it."

In 2024 alone, Hawai‘i residents lost more than $922,000 in cryptocurrency ATM scams, and that number is likely underreported. Victims are often our kūpuna, who have spent their entire lives saving and cannot recover from such losses.

I commend the previous committee for the significant improvements made to SB2387. The amendments prohibiting new customer cash purchases, restricting wallet addresses, and setting a 2030 deadline are meaningful steps forward. But we cannot afford to wait four years while our kūpuna continue to lose their life savings.

I urge this Committee to accelerate the timeline and adopt a full, immediate ban on cash purchases at digital financial asset transaction kiosks—while preserving the ability to withdraw cash and exchange between cryptocurrencies. This is the approach endorsed by consumer protection experts and legislative leaders, and it is the approach that will finally protect our residents from irreversible financial ruin.

Mahalo for the opportunity to testify.

House Committee on Judiciary and Hawaiian Affairs
April 1 2026
Conference Room 325
2:00 p.m.

To: Chair Tarnas and members of the Committee

Position: STRONG SUPPORT – S.B. 2387 SD 1, HD 1
Relating to Digital Financial Assets Transactions Kiosk

Aloha Chair Tarnas and Members of the Committee,

My name is Beverly Gotelli and I am a Hawaiʻi consumer and community member writing in strong support of Senate Bill 2387 SD 1,HD1 which would establish critical safeguards for cryptocurrency transactions conducted through kiosks in Hawaiʻi.

I support innovation and responsible use of digital financial technology. However, as cryptocurrency kiosks have rapidly expanded across our islands, consumers—especially kupuna, and individuals with limited digital literacy—have been exposed to significant financial risk, fraud, and irreversible losses. Senate Bill 2387 SD 1, HD 1 is a reasonable, necessary, and consumer-focused response to these documented harms.

The additions to this bill will be additional safeguards for Kupuna.

I recently went to my local supermarket which has an ATM machine. I was curious as to what warning is written for the consumer. The one I saw had this written on it, “Avoid Fraud and Scams” Do not purchase cryptocurrency for someone you don’t know. Do not share your voucher code with anyone. If you’re already at the kiosk I don’t think you’re going to read this. Scammers are smart, we need to be proactive and protect our Kupuna.

Cryptocurrency is here to stay and we need to be proactive on how we can protect not only kupuna but everyone in the State.

Many consumers who use kiosks do not realize they are converting cash into crypto assets that cannot be disputed, refunded, or traced once sent. In Hawaiʻi, where many residents rely on cash, kiosks can create a false sense of security that mirrors traditional ATMs—but without the same protections.

I respectfully urge you to PASS Senate Bill 2387 SD 1. This measure reflects Hawaiʻi's values of pono, fairness, and protection of our people, while allowing innovation to move forward in a safe and responsible way.

Mahalo for your time, your consideration, and your commitment to protecting Hawaiʻi's consumers.

Respectfully submitted,
Beverly Gotelli

Testimony on Senate Bill No. 2387, SD1, HD1

RELATING TO Digital Financial Assets Transaction Kiosks

Wednesday, April 1, 2026 at 2:00 pm

Conference Room 325 & Videoconference

State Capitol

Aloha Chair Tarnas and Members of the Committee:

I am in strong support of Senate Bill no. 2387, SD1, HD1.

The number of cryptocurrency kiosks on all Hawaii islands has dramatically increased over the last two years. In 2024, 68 complaints were reported with losses of over $920,000 in Hawaii. The losses nationwide reached $250 million. These are very alarming numbers. Unfortunately, most of the victims of frauds involving cryptocurrency kiosks are kupunas. Many of them do not understand how transactions work with these machines. Without regulations limiting transaction amount and other protection measures, more kupunas will be victimized. The predators targeting kupunas are not going to stop their fraudulent acts.

I respectively ask you to support and pass this bill.

Mahalo for giving me this opportunity to testify!

Sai Peng Tomchak
Maui resident

April 1, 2026

Committee on Judiciary & Hawaiian Affairs
State Capitol
415 South Beretania Street
Honolulu, HI 96813

TESTIMONY IN SUPPORT OF SB2387 SD1

Chair David A. Tarnas, Vice Chair Mahina Poepoe, and Committee Members:

I write to express my strong support for SB2387 SD1 HD1 and ask the Committee to pass it.

SB2387 SD1 HD1 concerns cryptocurrency kiosks, also known as cryptocurrency ATMs. These kiosks enable people to purchase cryptocurrency, like Bitcoin and others, using cash. Cash is fed into the machine to complete the purchase of cryptocurrency. The user of the kiosk can then send the cryptocurrency to themselves or others.

This Bill would create a daily transaction limit for users of cryptocurrency kiosks in Hawai‘i. Why is this important? Because cryptocurrency kiosks are frequently used by scammers to take money from victims.

The story of the scam can take many forms—you owe the IRS; you need to pay off a bench warrant or fine;[1] your bank account is compromised, and you have to protect your money by changing it to crypto; etc.—but the end goal for the scammer is the same: get the victim to a kiosk with cash, and tell them how to send it. This video shows what that looks like as it's happening: https://youtu.be/lfHuSkQnBLk.

Besides a general under-resourcing of law enforcement to combat cyber and financial crimes, cryptocurrency-involved crimes pose additional challenges to investigate. Transactions involving cryptocurrency can move quickly and are very difficult to trace, leaving the final destination of funds unknown. Even if the destination can be determined, scammers are frequently overseas, in countries where US-based law enforcement has little influence.[2]

---

[1] *E.g.*, HNN Staff, Kauai Police Warn Public of Cryptocurrency Phone Scam, HawaiiNewsNow (Feb. 27, 2026), https://www.hawaiinewsnow.com/2026/02/27/kauai-police-alert-public-cryptocurrency-phone-scam/; Angela Cifone, Scammers Posing as Police Pressuring Kupuna to Send Thousands of Dollars, KITV (Jan. 31, 2026), https://www.kitv.com/news/crime/scammers-posing-as-police-pressuring-kupuna-to-send-thousands-of-dollars/article_10aac682-3335-4804-898d-64f868aa2c9c.html.

[2] For example, a large scam compound called KK Park was located in Myanmar. *See* Lewis Sanders IV et al., How Chinese Mafia Are Running a Scam Factory in Myanmar, DW (Jan. 30, 2024), https://www.dw.com/en/how-chinese-mafia-are-running-a-scam-factory-in-myanmar/a-68113480; Koh Ewe, How a Viral Post Saved a Chinese Actor

The speed at which transactions can occur and the challenges to tracing where funds end up are why reports by kiosk companies to the US Treasury Department's Financial Crimes Enforcement Network ("FinCEN") are not a sufficient safeguard. Such reports do not prevent a victim's money, once put into a cryptocurrency kiosk, from swiftly disappearing down a path of untraceable transactions to a country or region where law enforcement cannot follow.

If, instead of putting $20,000, $30,000, or $50,000 into a cryptocurrency kiosk during one visit, victims could only put in $2,000 total per day, that hard limit would severely restrict how lucrative Hawai‘i victims would be for scammers.

The transaction limit would not preclude anyone from buying or investing in cryptocurrency in other ways, and indeed, cryptocurrency kiosks with their high transaction fees are not used by legitimate cryptocurrency investors anyway. The limit would only affect illegitimate users of cryptocurrency.

I urge the Committees to pass SB2387 SD1 HD1 and to ask their colleagues to do the same.

Thank you for the opportunity to be heard on this important Bill.

Thomas J. Michener, Esq.

From Myanmar's Scam Centres, BBC (Jan. 9, 2024), https://www.bbc.com/news/articles/cd606l1407no; *see also* LastWeekTonight, *Pig Butchering Scams: Last Week Tonight with John Oliver (HBO)*, YouTube (Feb. 22, 2025), https://www.youtube.com/watch?v=pLPpl2ISKTg.

SB-2387-HD-1
Submitted on: 3/31/2026 8:22:51 AM
Testimony for JHA on 4/1/2026 2:00:00 PM

Submitted By	Organization	Testifier Position	Testify
Angela Serota	Individual	Support	Written Testimony Only

Comments:

Aloha Chair Tarnas and Members of the Committee,

My name is Angela Serota and I am in strong support of SB 2387 SD1 HD1 that would limit cryptocurrency transactions done through kiosks in Hawai'i.

Cryptocurrency is a relatively new and unregulated financial system. Most adults, especially Kupuna, do not understand this system. They do not realize that once cash is converted into crypto and fed into these kiosks, there is no ability to trace, dispute, or refund the transaction. As a result, these cryptocurrency kiosks are popular and dangerous vehicles to perpetuate fraud and scams.

Please pass Senate Bill 2837 to limit transactions in the cryptocurrency kiosks and to protect our hard working and vulnerable people.

Mahalo for your commitment to protecting the people of Hawai'i.

Angela Serota

Kilauea, HI

SB-2387-HD-1
Submitted on: 3/31/2026 8:53:33 AM
Testimony for JHA on 4/1/2026 2:00:00 PM

Submitted By	Organization	Testifier Position	Testify
John A. H. Tomoso	Individual	Support	Written Testimony Only

Comments:

03-31-26

RE: SB2387 SD1 HD1

Aloha mai/

I know Senate Bill 2387, SD1, HD1 Crypto-Currency ATM Transaction Protection Measure has been amended to include a ban for deposits from first time customers. I am in strong support of this Bill which is important for the protection of all, especially our beloved Kūpuna!

Mahalo a nui,

John A H Tomoso+, MSW (ret.), ACVCSW

51 Ku'ula St, Kahului, HI 96732-2906

john.a.h.tomoso@gmail.com

Testimony on Senate Bill 2387

RELATING TO Digital Financial Assets Transaction Kiosks

Aloha Chair Tarnas and Members of the Committee

My name is Merle Minami-Shima, and in STRONG SUPPORT of SB 2387, SD1 which would establish critical safeguards for cryptocurrency transactions conducted through kiosks in Hawai'i.

Our kupuna are vulnerable and trusting people which make them targets for the unscrupulous people who take advantage of them. They are easily tricked and manipulated to convert monies into crypto assets at kiosks without knowing that they cannot get refunds or dispute transactions if needed.

Crypto currency scams have caused some of our kupuna to lose large sums of money from their nest eggs when they can least afford to lose it.

Because of this, I strongly believe that it is our kuleana to protect our kupuna. To do this, we must PASS Senate Bill 2387. I respectfully urge your support in this matter.

Mahalo for your consideration of this issue.

Respectfully submitted,

Merle Minami-Shima

Wailuku, Maui, Hawaii

SB-2387-HD-1
Submitted on: 3/31/2026 9:56:08 AM
Testimony for JHA on 4/1/2026 2:00:00 PM

Submitted By	Organization	Testifier Position	Testify
David W Hudson	Individual	Support	Written Testimony Only

Comments:

Aloha Chair Tarnas and Members of the Committee:

My name is David Hudson and I strongly support SB 2387, SD1 which would establish critical safeguards for cryptocurrency transactions conducted through kiosks in Hawai'i. As a recently retired banker of over 40 years in Hawai'i I have seen the devastating impact of fraud and scams on our citizens particularly our most vulnerable kupuna. Cryptocurrencyt kiosks have rapidly expanded acrosss our islands, and consurmers - especially kupuna, have been exposed to significant financial risk, fraud and irreversible losses. Senate Bill 2387, SD1 is a reasonalbe, necessary, and consumer focused response to these documented harms.

Many consumers who use these kiosks do not realize that they are converting cash into crypto assets that cannot be disputed, refunded or traced once sent. In Hawai'i, where residents rely on cash, kiosks can create a false sense of security that mirrors traditional ATMs - but without the same regulatory protections.

I respectfuly urge you to PASS Senate Bill 2387. This measure reflects Hawai'i's values of fairness and protection of our people, while allowing innovation and technology to move forward in a safe and responsible manner.

Mahalo for your time, your consideration and your commitment to protecting Hawai'i's consumers.

David Hudson

Honolulu, Hawai'i

April 1, 2026

TO: Chair Tarnas and Committee Members

FROM: Carl Takamura

RE: SB 2387, SD 1

Mahalo for the opportunity to submit this testimony in strong support of **SB 2387, SD1** which establishes commonsense regulations for cryptocurrency kiosks in Hawaii.

Law enforcement and consumer protection agencies have documented a sharp rise in fraud schemes that direct victims to deposit cash into cryptocurrency kiosks. These scams often target seniors, many of whom are unfamiliar with digital assets and are more vulnerable to high pressure tactics. Once funds are transferred through a kiosk, they are virtually impossible to recover and perpetrators – often operating outside of Hawaii – face little accountability.

This bill will bring cryptocurrency kiosks in line with basic consumer protections already required of other financial institutions. Hawaii should not continue to allow an unregulated cash-to-crypto pipeline that criminals can exploit with ease. Our kupuna deserve better safeguards and family's better peace of mind.

I urge you to approve this important proposal.

Respectfully,

Carl Takamura

Carl Takamura
Hawaii Kai

SB-2387-HD-1
Submitted on: 3/31/2026 11:47:34 AM
Testimony for JHA on 4/1/2026 2:00:00 PM

Submitted By	Organization	Testifier Position	Testify
Esther Ueda	Individual	Support	Written Testimony Only

Comments:

Dear Chair Tarnas, Vice-Chair Poepoe and members of the Committee:

Please support SB2387 SD1HD1 relating to Digital Financial Asset Transaction Kiosks.

These kiosks have become more prevalent in our communties and are being used for fraudulent purposes, especially on unsuspecting seniors.

This proposed bill will provide safeguards for seniors and others against these fraudulent activites.

Please support this measure.

Esther Ueda, Pearl City

SB-2387-HD-1
Submitted on: 3/31/2026 12:17:35 PM
Testimony for JHA on 4/1/2026 2:00:00 PM

Submitted By	Organization	Testifier Position	Testify
Terri Yoshinaga	Individual	Oppose	Written Testimony Only

Comments:

I oppose this bill.

HOUSE COMMITTEE ON JUDICIARY & HAWAIIAN AFFAIRS

Rep. David A. Tarnas, Chair

Rep. Mahina Poepoe, Vice Chair

NOTICE OF HEARING

Wednesday, April 1, 2026, 2:00pm

Re: SB 2387 SD1 HD-1 RELATING TO DIGITAL FINANCIAL ASSET TRANSACTION KIOSKS.

Aloha Chair Tarnas and Vice Chair Poepoe. I am Linda Dorset and I am testifying in STRONG support of SB 2387 **which would establish critical safeguards for cryptocurrency transactions conducted through kiosks in Hawai'i and include a ban for deposits from first time customers, and a later ban for all users in 2030**

Cryptocurrency kiosks are rapidly expanding across our islands AND, many consumers who use kiosks do not realize they are converting cash into crypto assets that cannot be disputed, refunded, or traced once sent. Kupuna, especially, have been the victims of significant financial risk, fraud, and irreversible losses. These kiosks mirror traditional ATMs—but without the same protections.

The bill's daily and monthly caps coupled with required on-screen scam warnings, plainly and prominently displayed, can interrupt the emotional hijacking and meaningfully reduce the potential harm while still allowing lawful use of the technology

Senate Bill 2387 SD1HD-1 is a reasonable, necessary, and consumer-focused response to these documented harms.

I respectfully urge you to PASS Senate Bill 2387 SD1 HD-1. This measure reflects Hawai'i's values of fairness, and protection of our people, while allowing innovation and technology to move forward in a safe and responsible way.

Mahalo for your time, your consideration, and your commitment to protecting Hawai'i's consumers.

Linda Dorset
Maui Senior Citizen

SB-2387-HD-1
Submitted on: 3/31/2026 3:41:31 PM
Testimony for JHA on 4/1/2026 2:00:00 PM

Submitted By	Organization	Testifier Position	Testify
BLYTH KOZUKI	Individual	Support	Written Testimony Only

Comments:

Aloha Chair Tarnas and Members of the Committee:

My name is Blyth Kozuki, and I am a kupuna writing in strong support of Senate Bill 2387 SD1, HD1 which provides safeguards on cryptocurrency transactions conducted through kiosks in Hawai‘i.

I support innovation and the use of digital financial technology because it has proven to be convenient and efficient. But as someone who grew up before the advent of computers, it is difficult to keep pace with technology. So I am alarmed that cryptocurrency kiosks have rapidly expanded across our islands and I know that kupunas with limited digital literacy are easy targets to be scammed. These scams are especially tragic for kupunas because they often do not have the time nor the ability to rebuild their financial losses. In addition, it is easy to confuse a cryptocurrency kiosk for an ATM machine so kupunas may believe these kiosks are regulated in the same manner as banking ATMs.

My hope is that by establishing safeguards on cryptocurrency ATMs as written in Senate Bill 2387 SD1, HD1 this will discourage scammers from seeing our state as an easy target for our kupunas. I think it is urgent to PASS Senate Bill 2387 SD1, HD1 because the people who scam and their ability to scam keeps growing. Mahalo for your time, your consideration, and your commitment to protecting Hawai‘i’s consumers.

Respectfully submitted,

Blyth Kozuki - Honolulu, Hawai‘i