

JOSH GREEN, M.D.  
GOVERNOR



SIERRA WHITESIDE  
CHAIRPERSON

SYLVIA LUKE  
LIEUTENANT GOVERNOR

DAINTRY BARTOLDUS  
EXECUTIVE ADMINISTRATOR

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

March 18, 2026

The Honorable Representative Scot Z. Matayoshi, Chair  
House Committee on Consumer Protection & Commerce  
The Thirty-Third Legislature  
State Capitol  
State of Hawai'i  
Honolulu, Hawai'i 96813

Dear Chair Matayoshi and Committee Members:

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

The Hawai'i State Council on Developmental Disabilities (Council) offers **SUPPORT** for SB2387 SD1, 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.

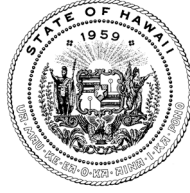
SB2387 SD1 strikes an appropriate balance by allowing access to emerging financial technologies while establishing reasonable safeguards to prevent fraud and protect consumers across Hawai'i.

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

Sincerely,

A handwritten signature in blue ink that reads "Daintry Bartoldus". The signature is written in a cursive, flowing style.

Daintry Bartoldus  
Executive Administrator



STATE OF HAWAII | KA MOKU'ĀINA 'O HAWAI'I  
OFFICE OF THE DIRECTOR  
DEPARTMENT OF COMMERCE AND CONSUMER AFFAIRS  
KA 'OIHANA 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

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

SYLVIA LUKE  
LIEUTENANT GOVERNOR | KA HOPE KIA'ĀINA

NADINE Y. ANDO  
DIRECTOR | KA LUNA HO'OKELE

DEAN I. HAZAMA  
DEPUTY DIRECTOR | KA HOPE LUNA HO'OKELE

## Testimony of the Department of Commerce and Consumer Affairs

Before the  
House Committee on Consumer Protection & Commerce  
Wednesday, March 18, 2026  
2:00 p.m.  
Via Videoconference  
Conference Room 329

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

Chair Matayoshi 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 the intent of this measure and offers the following comments.

The purpose of this bill is to curb fraud occurring through digital financial asset kiosks, or bitcoin kiosks, by 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.

We strongly support H.B. 1642, which would enact a ban on purchasing digital financial assets from digital financial asset kiosks. We support the intent of this bill, however, and find that this bill provides meaningful consumer protections. We support

mitigating harms to consumers from fraud occurring at digital financial asset kiosks. In particular, 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.<sup>1</sup> 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.

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.

---

<sup>1</sup> 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.").

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 additional resources, including appropriations and personnel. We respectfully request that an unspecified general fund appropriation be added to the bill for the Department as we assess the resources needed to effectuate this bill.

Thank you for the opportunity to testify on this bill.



# 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<sup>1</sup> 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.<sup>2</sup>

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.<sup>3</sup> This represents a 99 percent increase in the number of complaints and a 31 percent increase in reported victim losses from 2023.<sup>4</sup> The Federal Trade Commission (FTC) likewise identified, based on an analysis of consumer reports, that fraud losses through CVC kiosks have skyrocketed.<sup>5</sup>

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.<sup>6</sup> 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.<sup>7</sup>

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.<sup>8</sup>

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<sup>9</sup> or exchange.<sup>10</sup> 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.<sup>11</sup>

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,<sup>12</sup> 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,<sup>13</sup> which performs the CVC transmission, or the kiosk may draw upon CVC held by its operator.<sup>14</sup> 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.<sup>15</sup>

### Non-compliant CVC Kiosk Operators

CVC kiosk operators generally facilitate money transmission<sup>16</sup> 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.<sup>17</sup> 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.<sup>18</sup> However, the rapid growth in the number of CVC kiosks in the United States<sup>19</sup> 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.<sup>20</sup> Some non-compliant kiosk operators have been prosecuted for operating an unlicensed money transmitting business and other related offenses.<sup>21</sup> 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.<sup>22</sup> These non-compliant CVC kiosk businesses also often lack reasonably designed policies, procedures, and internal controls to respond to requests from law enforcement.<sup>23</sup>

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<sup>24</sup> 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.<sup>25</sup> If asked about the purpose of transactions, the operators may avoid answering or provide misleading answers to financial institutions.<sup>26</sup>

- 
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.<sup>27</sup>

## Use of CVC Kiosks to Facilitate Scam Payments

The speed and difficulty of reversing CVC transactions<sup>28</sup> 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.<sup>29</sup> 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.<sup>30</sup>

## CVC Kiosks and Elder Fraud

Criminals targeting older individuals are particularly likely to direct victims to use CVC kiosks to send payments.<sup>31</sup> 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.<sup>32</sup> More than two of every three dollars reported lost to fraud using CVC kiosks was lost by an older adult.<sup>33</sup> 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.<sup>34</sup>

Many scammers using CVC kiosks initiate contact with potential victims through unsolicited calls.<sup>35</sup> 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.<sup>36</sup> 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.<sup>37</sup>

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.<sup>38</sup>

According to law enforcement sources, scammers may provide victims with instructions designed to circumvent reporting thresholds,<sup>39</sup> 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.<sup>40</sup>

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,<sup>41</sup> most frequently through cross-chain bridges that claim to operate as decentralized finance (DeFi) services.<sup>42</sup> 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.<sup>43</sup>

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.<sup>44</sup>

## 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*




 A customer sends multiple payments just below the suspicious activity reporting (SAR) threshold,<sup>45</sup> 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,<sup>46</sup> 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.<sup>47</sup> All statutorily defined financial institutions may voluntarily report suspicious transactions under the existing suspicious activity reporting safe harbor.<sup>48</sup>

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.<sup>49</sup> 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.<sup>50</sup> 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.<sup>51</sup>

## 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),<sup>52</sup> Report of Cash Payments Over \$10,000 Received in a Trade or Business (Form 8300),<sup>53</sup> Report of Foreign Bank and Financial Accounts (FBAR),<sup>54</sup> Report of International Transportation of Currency or Monetary Instruments (CMIR),<sup>55</sup> Registration of Money Services Business (RMSB),<sup>56</sup> and Designation of Exempt Person (DOEP).<sup>57</sup>

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.<sup>58</sup> 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](http://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](http://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).

**DEPARTMENT OF THE PROSECUTING ATTORNEY  
KA 'OIHANA O KA LOIO HO'OPI'I  
CITY AND COUNTY OF HONOLULU**

ALII PLACE  
1060 RICHARDS STREET • HONOLULU, HAWAII 96813  
PHONE: (808) 768-7400 • FAX: (808) 768-7515 • WEBSITE: www.honoluluprosecutor.org

STEVEN S. ALM  
PROSECUTING ATTORNEY  
LOIO HO'OPI'I



THOMAS J. BRADY  
FIRST DEPUTY PROSECUTING ATTORNEY  
HOPE MUA LOIO HO'OPI'I

**THE HONORABLE SCOT Z. MATAYOSHI, CHAIR  
HOUSE COMMITTEE ON CONSUMER PROTECTION & COMMERCE  
Thirty-Third State Legislature  
Regular Session of 2026  
State of Hawai'i**

March 18, 2026

**RE: S.B. 2387, S.D.1; RELATING TO DIGITAL FINANCIAL ASSET TRANSACTION KIOSKS.**

Chair Matayoshi, Vice-Chair Grandinetti, and members of the House Committee on Consumer Protection & Commerce, the Department of the Prosecuting Attorney of the City and County of Honolulu (“Department”) submits the following testimony in **support** of S.B. 2387, S.D.1.

S.B. 2387, S.D.1 establishes reasonable daily and monthly transaction limits, mandatory fraud warnings, and clear disclosures regarding fees, exchange rates, and risks. These measures are critical. Many victims—particularly elderly or vulnerable individuals—lose life-altering sums of money in a single day or over a short period. The bill’s discrete and aggregate limit on transactions meaningfully reduce potential harm while still allowing lawful use of the technology.

Required on-screen scam warnings, written in plain language and displayed prominently, mirror fact patterns we see repeatedly in criminal cases. Posing as government agents, law enforcement, or bill collectors, con artists may frighten victims into parting with their money. Conversely, some swindlers impersonate helpful computer technicians or acquaintances of a family member. Timely warnings can interrupt the emotional hijacking critical to many of these schemes.

S.B. 2387, S.D.1 requires kiosk operators to use blockchain analytics and tracing software. This provision is particularly important. While digital assets are often described as anonymous, modern investigative tools can identify fraud patterns and trace transactions when operators enable commonsense recordkeeping software. Not only can this assist in combating fraud, but it is also essential for defeating money laundering schemes.

The refund provision deserves special mention. In many fraud cases, even when a suspect is identified, restitution is unlikely or delayed. Requiring operators to issue refunds when fraud is promptly reported provides immediate relief to victims and reduces the long-term emotional and financial harm caused by these crimes.

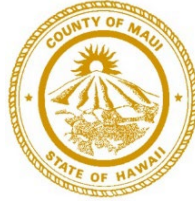
For all of the foregoing reasons, the Department of the Prosecuting Attorney of the City and County of Honolulu **supports** the passage of **S.B. 2387, S.D.1.**

Thank you for the opportunity to testify.

**RICHARD T. BISSEN, JR.**  
Mayor

**ANDREW H. MARTIN**  
Prosecuting Attorney

**SHELLY C. MIYASHIRO**  
First Deputy Prosecuting Attorney



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

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

March 17, 2026

The Honorable Scot Z. Matayoshi  
Chair  
The Honorable Tina Nakada Grandinetti  
Vice Chair  
and Members of the Committee on Consumer Protection and Commerce

Chair Matayoshi, Vice Chair Grandinetti, 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, 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.

This bill would protect our community by, *inter alia*, creating daily and monthly transaction limits on kiosk transfers by a single person, as well as requiring multiple warnings and disclosures to consumers about digital assets in general and their potential for use in scams. It would also require each kiosk operator to implement a refund process for fraudulent transactions and provide point of contact information for regulating government entities. These protections are a vital part of ensuring that digital asset transactions at these kiosks are safe, secure and legitimate.

For these reasons, the Department of the Prosecuting Attorney, County of Maui **supports S.B. 2387 SD1**. 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.



1001 Bishop Street #625 | Honolulu, HI 96813  
866-295-7282 | [aarp.org/hi](http://aarp.org/hi) | [hiaarp@aarp.org](mailto:hiaarp@aarp.org) |  
[Twitter.com/aarpHawaii](https://twitter.com/aarpHawaii) | [facebook.com/aarpHawaii](https://facebook.com/aarpHawaii)

**The Thirty-Third State Legislature  
House Committee on Consumer Protection and Commerce  
Wednesday, March 18, 2026  
Conference Room 329, 2:00 p.m.**

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

Aloha Chair Matayoshi, 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 135,000 Hawai'i members, thank you for the opportunity to testify in **strong support** of S.B. 2387, S.D.1.

AARP Hawai'i strongly supports this measure because it **strengthens consumer protections and reduces fraud risks associated with digital financial asset transaction kiosks**, commonly known as cryptocurrency kiosks or crypto ATMs. These machines are increasingly being used by criminals to exploit consumers, particularly older adults, resulting in devastating and often irreversible financial losses.

**Why S.B. 2387 SD1 Is Needed**

Frauds involving cryptocurrency kiosks are rising sharply across the nation and here at home. According to the FBI's Internet Crime Complaint Center, Hawai'i recorded sixty-eight cryptocurrency kiosk-related complaints in 2024, with losses totaling more than \$922,000. Nationally, losses exceeded \$250 million from more than 11,000 complaints, a 99 percent increase from the previous year.

Hawai'i currently has at least ninety-six cryptocurrency kiosks located in everyday settings such as supermarkets, gas stations, convenience stores, bars, and restaurants. While these machines closely resemble traditional ATMs, they are subject to far fewer consumer protection requirements. Unlike conventional financial transactions, cryptocurrency transactions are



typically **irreversible**, making them especially attractive to scammers and leaving victims with little or no recourse. Older adults are disproportionately targeted in these schemes. Without strong statutory safeguards, criminals will continue to exploit regulatory gaps, siphoning millions of dollars from unsuspecting residents.

### **Key Consumer Protections in S.B. 2387 SD1**

S.B. 2387 SD1 establishes reasonable, commonsense safeguards that protect consumers while allowing legitimate businesses to operate. The bill would:

- Set a **daily transaction limit of \$2,000**, with an aggregate cap of **\$10,000 over a thirty-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 before a transaction occurs.
- Require **prominent, visible notices** on kiosks explaining what consumers should do if they suspect fraud.
- Ensure customers receive **paper receipts** with relevant transaction details.
- Strengthen **enforcement authority** to investigate fraudulent activity.
- Require **live customer service support during operating hours**.
- Provide a **dedicated communication line for law enforcement**.

These protections give consumers meaningful tools to avoid fraud and provide regulators and law enforcement with the authority they need to deter and investigate criminal activity.

### **A Balanced Approach**

AARP Hawai'i is **not opposed to cryptocurrency**, nor are we opposed to cryptocurrency kiosks. Innovation can and should continue, but not at the expense of consumer safety. S.B. 2387 SD1 strikes the right balance by allowing digital financial services to operate while ensuring appropriate guardrails are in place to protect the public.

### **Conclusion**

By adopting the safeguards contained in S.B. 2387, S.D.1, Hawai'i can take a critical step toward combating financial fraud and **protecting the hard-earned savings of kūpuna and all consumers**.

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

**SB-2387-SD-1**

Submitted on: 3/16/2026 2:30:01 PM

Testimony for CPC on 3/18/2026 2:00:00 PM

<b>Submitted By</b>	<b>Organization</b>	<b>Testifier Position</b>	<b>Testify</b>
GARY SIMON	Hawai'i Family Caregiver Coalition	Support	Written Testimony Only

Comments:

Dear Chair Matayoshi, Vice Chair Grandinetti, Honorable Members of the House Committee on Consumer Protection and Commerce:

I am Gary Simon, a member of the board of the Hawai'i Family Caregiver Coalition, whose mission is to improve the quality of life of those who give and receive care by increasing community awareness of caregiver issues through continuing advocacy, education, and training. I am offering testimony on behalf of the Hawai'i Family Caregiver Coalition.

The Hawai'i Family Caregiver Coalition strongly supports SB 2387 SD 1, which establishes limits on transactions through digital financial asset transaction kiosks. SB 2387 SD 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.

Mahalo for seriously considering the bill.

Gary Simon

Hawai'i Family Caregiver Coalition



## TESTIMONY SUBMITTED TO THE HOUSE COMMITTEE ON CONSUMER PROTECTION & COMMERCE

### Re: SB 2387 SD1 Relating to Digital Financial Asset Transaction Kiosks

Aloha Representative Matayoshi, Vice Chair Grandinetti, and Members of the Committee:

My name is Louise Pais Meyers. My husband and I own Hilt Ventures, a locally operated cryptocurrency kiosk provider in Hawaii. We have proudly served residents of Hawaii since 2021 and operate 24 kiosks located in conveniently trusted retail partners across Oahu, Maui, Kauai, and the Big Island.

Thank you for the opportunity to share testimony on SB 2387 SD1.

Hilt already implements many of the provisions included in SB 2387 SD1 such as blockchain analytics requirements, disclosures, receipt requirements, availability of customer service representatives, and coordination with law enforcement. These measures are a step in the right direction to build trust in this emerging technology.

However, as proposed, we have concerns applying daily transaction limit and refund provisions that do not differentiate between **new customers** and **existing customers**. In our experience, **customers who are the victims of fraud are new, first-time customers, not existing customers**. An existing customer who has used our services many times without incident has a far **different risk profile** than a customer that has never used our kiosk before.

Hilt would support this bill if the **transaction limits provisions differentiated between new and existing customers**, a distinction that has been recognized by other states. This would include the following:

- \$2,000 or the equivalent in digital financial assets per day for a new customer; and
- \$10,500 or the equivalent in digital financial assets per day for an existing customer.

Furthermore, Hilt would support this bill if the **refund provisions similarly differentiated between new and existing customers**. This would include the following:

- If a new customer has been fraudulently induced to engage in a digital financial asset transaction and contacts the kiosk operator and a law enforcement agency or government agency to inform the operator and agency of the fraudulent nature of the transaction within thirty days after the transaction, then, upon request of the customer, the operator shall issue a full refund for the fraudulently induced digital financial asset transaction, including fees charged in association with the transaction.

- If an existing customer has been fraudulently induced to engage in a digital financial asset transaction and contacts the kiosk operator and a law enforcement agency or government agency to inform the operator and agency of the fraudulent nature of the transaction within thirty days after the transaction, then, upon request of the customer, the operator shall issue a full refund for the fees charged in association with the transaction.

- "New Customer" means a customer who has been a customer of an operator of a digital financial asset transaction kiosk for less than seven days.
- "Existing Customer" means a customer who has transacted with the operator of a digital financial asset transaction kiosk for seven or more days.

Finally, Hilt suggests the addition of a simple annual registration (including a reasonable registration fee to cover administrative costs) and certification requirement (a simple online certification form attesting to compliance) with the Office of Consumer Protection (OCP) for operators who wish to continue operating in Hawaii, with suspension or revocation of registration for operators with high scam reports or patterns of facilitating fraud.

Federal agencies like FinCEN and the FTC, along with other state regulators and law enforcement, consistently emphasize that non-compliant operators create significantly higher vulnerabilities for scams. Scammers often direct victims to specific kiosks, likely to avoid operators with strong controls. (FIN-2025-NTC1 Notice, August 4, 2025). "... differences in fraud prevention measures taken by various operators" (e.g., no KYC, no monitoring) exacerbate consumer fraud by providing fewer barriers.

SB 2387 SD1, if amended as suggested above, would be beneficial for legitimate, compliant operators like Hilt — it levels the playing field, enhances credibility, reduces unfair competition from non-compliant operators, and supports long-term business sustainability without resorting to outright bans.

The guardrails would also create significant friction for criminals and scammers, making their schemes "too much hassle."

Thank you for the opportunity to share comments regarding this bill.



# holomua

COLLABORATIVE

---

## OUR MISSION

To support and advance public policies that make Hawai'i affordable for all working families.

## OUR VISION

Collaborative, sustainable, and evidence-based public policies that create a diverse and sustainable Hawai'i economy, an abundance of quality job opportunities, and a future where all working families living in Hawai'i can thrive.

---

## BOARD MEMBERS

Jason Fujimoto  
Meli James, *Board Chair*  
Micah Kāne  
Brandon Kurisu  
Brad Nicolai  
Mike Pietsch  
Sunshine Topping

## ADVISORY COMMITTEE

Josh Feldman  
Brittany Heyd  
Alicia Moy  
Ed Schultz

Josh Wisch  
*President & Executive Director*

---

827 Fort Street Mall, 2<sup>nd</sup> Floor  
Honolulu, Hawaii 96813

+1 (808) 542-4089  
info@holomuacollaborative.org

HolomuaCollaborative.org

---

Page 1 of 1

**Committee:** House Committee on Consumer Protection and Commerce  
**Bill Number:** SB2387 SD1, Relating to Digital Financial Asset Transaction Kiosks  
**Hearing Date and Time:** March 18, 2026, at 2:00pm (Room 329)  
**Re:** Testimony of Holomua Collaborative in support

Aloha Chair Matayoshi, Vice Chair Grandinetti, and Members of the Committees:

We write in support of SB2387 SD1, Relating to Digital Financial Asset Transaction Kiosks. This bill strengthens consumer protections and reduces the risk of fraud at cryptocurrency kiosks.

Our organization is committed to finding ways to keep all local working families in Hawai'i by ensuring they can afford to stay. This measure is crucial to protecting our community from escalating financial scams that significantly affect individuals' finances and, consequently, their ability to live in the state.

Financial scams, especially those involving digital assets such as cryptocurrency, have been on the rise in Hawai'i and nationwide. In 2024, Hawai'i recorded 68 cryptocurrency fraud complaints, resulting in total losses of \$922,022, according to the Federal Bureau of Investigation's Internet Crime Complaint Center (IC3). These staggering losses not only cause severe financial hardship for individuals but also contribute to broader economic instability, driving up the cost of living as victims struggle to recover.

One key factor enabling these scams is the irreversible, anonymous nature of cryptocurrency transactions, which makes it difficult for victims to recover lost funds. To mitigate these risks, this proposed legislation—modeled after a similar law recently enacted in California—would limit daily cryptocurrency transactions to \$2,000 and monthly transactions to \$10,000 for transactions made through a digital financial-asset transaction kiosk.<sup>1</sup> By capping daily and monthly transaction limits, this measure aims to prevent significant financial losses, particularly for vulnerable groups such as older adults who are frequently targeted by fraudsters.

We appreciate the opportunity to testify in support of SB2387 SD1.

Sincerely,

Matthew Prellberg  
Policy and Communications Director

---

<sup>1</sup> Cal. Fin. Code § 3901.



**SanHi**

GOVERNMENT STRATEGIES

A LIMITED LIABILITY LAW PARTNERSHIP

DATE: March 17, 2026

TO: Representative Scot Matayoshi  
Chair, Committee on Consumer Protection & Commerce

FROM: Tiffany Yajima / Mihoko Ito

RE: **S.B. 2387, SD1 – Relating to Digital Financial Asset Transaction Kiosks  
Hearing Date: Wednesday, March 18, 2026 at 2:00 p.m.  
Conference Room: 329**

---

Dear Chair Matayoshi, Vice Chair Grandinetti, 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 to set 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 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 to impose a more modest daily transaction limit to prevent large sums of money from being withdrawn or deposited thereby reducing consumer exposure to fraud, abuse, or coercion.

Thank you for the opportunity to submit this testimony.



**TESTIMONY SUBMITTED TO THE HAWAII HOUSE COMMITTEE ON CONSUMER  
PROTECTION & COMMERCE**

**Larry Lipka, General Counsel**

**March 18, 2026**

Chairs Matayoshi 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 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 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 approximately 40 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



Testimony to the House Committee on Consumer Protection & Commerce  
Wednesday, March 18, 2026, 2:00 PM  
Conference Room 329

**LATE**

To: The Honorable Scot Matayoshi, Chair  
The Honorable Tina Grandinetti, Vice-Chair  
Members of the Committee

My name is Stefanie Sakamoto, and I am testifying on behalf of the Hawaii Credit Union League (HCUL), the local trade association for 45 Hawaii credit unions, representing over 879,000 credit union members across the state.

HCUL offers the following testimony in support of SB 2387. This bill establishes limits on transactions through digital financial asset transaction kiosks and requires operators of digital financial asset transaction kiosks to use blockchain analytics and tracing software to prevent fraud

Credit unions prioritize the financial well-being and security of our members. As member-owned financial cooperatives, we are committed to ensuring consumer protection in financial transactions for our members. This bill aligns with these values by providing safeguards that protect from potential financial harm while maintaining access to emerging financial technologies.

Implementing a transaction cap aligns with best practices in financial regulation. Many other financial services, including cash withdrawals from traditional ATMs, are subject to daily limits to prevent large-scale fraud and ensure compliance with anti-money laundering regulations. By extending similar safeguards to digital asset transactions, Hawaii can maintain a balanced approach to financial innovation and consumer protection.

Thank you for the opportunity to provide comments on this important issue.

**SB-2387-SD-1**

Submitted on: 3/16/2026 2:23:45 PM

Testimony for CPC on 3/18/2026 2:00:00 PM

<b>Submitted By</b>	<b>Organization</b>	<b>Testifier Position</b>	<b>Testify</b>
Jerry Orten	Individual	Support	Written Testimony Only

Comments:

Aloha committee members!

I write in support of this bill.

Protect residents and particularly kapuna by passing this bill.

Stop thieves from stealing and defrauding from those who are vulnerable to the sophisticated schemes of criminals!!

Mahalo!!

Jerry Orten

Lihue

**SB-2387-SD-1**

Submitted on: 3/16/2026 2:53:39 PM

Testimony for CPC on 3/18/2026 2:00:00 PM

Submitted By	Organization	Testifier Position	Testify
Nadine NEWLIGHT	Individual	Support	Written Testimony Only

Comments:

Testimony on House Bill No. 1642

RELATING TO Consumer Protection

Wednesday, March 18, 2026 at 9:30 am

Conference Room 229 & Videoconference

State Capitol

415 South Beretania Street

Aloha Chair Keohokalole and Members of the Committee:

My name is Nadine Newlight, and I am in **STRONG SUPPORT of HB 1642 HD1 which bans deposits for cryptocurrency transactions conducted through kiosks in Hawai‘i.**

**Cryptocurrency kiosks have rapidly expanded across our islands, consumers—especially kupuna, have been exposed to significant financial risk, fraud, and irreversible losses.**

**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 Hawai‘i, 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 House Bill 1642 HD1.**

**Mahalo for your time, your consideration, and your commitment to protecting Hawai‘i’s consumers.**

Nadine NEWLIGHT

2040 Kauhikoa Road

Ha`iku. HI 96708

Committee of Consumer Protection and Commerce

March 18, 2026

2:00 p.m.

To: Chair Matayoshi and Member of the Committee

Position: STRONG SUPPORT – S.B. 2387 SD 1

Relating to Digital Financial Assets Transactions Kiosk

Aloha Chair Matayoshi and Members of the Committee,

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

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 is a reasonable, necessary, and consumer-focused response to these documented harms.

I have not been affected by this, but have attended community meetings where stories have been shared. It is scaring to know that there are those in the community who are preying on Kupuna. Kupuna when hearing an injury of a loved one, or being arrested, they become very compassionate and forget about reality. They lose all sense of what is right and wrong.

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 Hawai'i, 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 Hawai'i'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 Hawai'i's consumers.

Respectfully submitted,  
Beverly Gotelli

March 18, 2026

TO: Chair Matayoshi and Committee Members  
FROM: Carl Takamura  
RE: SB 2387

Mahalo for the opportunity to submit this testimony in strong support of **SB 2387** 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-SD-1**

Submitted on: 3/16/2026 7:14:16 PM

Testimony for CPC on 3/18/2026 2:00:00 PM

<b>Submitted By</b>	<b>Organization</b>	<b>Testifier Position</b>	<b>Testify</b>
Ann H Paulino	Individual	Support	Written Testimony Only

Comments:

Aloha. My name is Ann Paulino, a resident of Hilo, Hawaii and a kupuna. Ever since I retired in 2017, I receive multiple robocalls for one scam or another on a daily basis. Fortunately I have learned to block calls and have calls screened. This AFTER I was scammed from my computer by a company claiming to help me fix my computer. I was so angry and upset that I was a target of a scam.

I am a caretaker for my aunt because she has been scammed many times to the tune of \$60,000. I now handle her finances so she will not be a constant target. I am aware that there are cryptocurrency kiosks around Hilo that are used by scammers as well. These kiosks have no safeguards which is the norm for ATMS. Users are unaware that their transactions will not be recorded and that their money is being converted to crypto assets. There is not a limit to the amount of money involved in the transaction so kupuna have lost thousands.

I humbly request that you support and pass SB2387 SD1 to protect us from further scams.

**SB-2387-SD-1**

Submitted on: 3/16/2026 7:31:13 PM

Testimony for CPC on 3/18/2026 2:00:00 PM

Submitted By	Organization	Testifier Position	Testify
Rick Tabor	Individual	Support	Written Testimony Only

Comments:

Thank you, Chair Matayoshi and Members of the Committee for hearing Senate Bill No. 2387, SD1

RELATING TO Digital Financial Assets Transaction Kiosks.

My name is Rick Tabor.

I strongly support of SB2387, SD1

establishing critical safeguards for cryptocurrency transactions conducted at kiosks in Hawai‘i.

I was shocked hearing cryptocurrency kiosks are in so many places on our islands with no safeguards. This issue is something our Kūpuna should not have to worry about. My biggest concern is the potential exposure of financial risk, extortion, trickery and fraud with irreversible losses. Senate Bill 2387, SD1 is a reasonable, necessary, consumer-focused safe-guard measure that helps set reasonable parameters that can help prevent the numerous documented cryptocurrency kiosk crimes Hawaii residents are currently experiencing.

Kūpina who use kiosks doubtfully realize they are converting cash into crypto assets that cannot be disputed, refunded, or traced once sent.

In Hawai‘i, where many residents rely on cash, kiosks can create a false sense of security that mirrors traditional ATMs— without the same protections.

I respectfully 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 way.

Mahalo for your time, your consideration, and your commitment to protecting Hawai‘i’s residents.

Rick Tabor

Honolulu, Hawaii



**SB-2387-SD-1**

Submitted on: 3/16/2026 8:31:56 PM

Testimony for CPC on 3/18/2026 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 **support** of SB2387, but I respectfully urge this Committee to strengthen the bill by amending it to include a **total ban on cash purchases of cryptocurrency at these kiosks**. While the current bill's guardrails—such as blockchain analytics, live customer service, and refund requirements—are well-intentioned, the evidence demonstrates that they are largely unenforceable and insufficient to stop the epidemic of fraud devastating Hawai‘i's residents, particularly our kūpuna.

**The Current Approach Is Inadequate—These Guardrails Are Unenforceable in Practice**

The current version of SB2387 relies on measures like blockchain analytics and tracing software to prevent fraud. However, law enforcement officials have repeatedly testified that these tools cannot stop the scam once a victim has been coerced. Scammers operate from outside U.S. jurisdiction, use sophisticated social engineering, and keep victims on the phone throughout the transaction, guiding them step-by-step to bypass any warnings or alerts.

As Honolulu police have stated, the majority of fraudsters are outside the country, making prosecution "extremely problematic." By the time a scam is discovered, the money has been converted to cryptocurrency and instantly split into multiple wallets, making recovery nearly impossible. No amount of analytics software can reverse that reality.

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

The fundamental problem is that the primary use case for these machines—converting cash to crypto—has become a vehicle for fraud. While industry representatives claim that only a small percentage of crypto scams occur at kiosks, that argument misses the point. 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, it is clear we should ban that function entirely. As Representative Matayoshi has argued, 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."

### **A Ban on Cash Deposits Still Allows Legitimate Use of the Technology**

Importantly, a 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 Hawaii 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.

The current bill represents a good-faith effort to address a serious problem, but half-measures will not stop the fraud. Scammers are sophisticated, relentless, and operating from outside our reach. The only way to truly protect Hawai‘i residents is to remove the tool they exploit. I urge this Committee to amend SB2387 to prohibit cash purchases at digital financial asset transaction kiosks entirely, 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 save our residents from irreversible financial ruin.

Mahalo for the opportunity to testify.

**Testimony on Senate Bill No. 2387, SD1**  
**RELATING TO Digital Financial Assets Transaction Kiosks**  
**Wednesday, March 18, 2026 at 2:00 pm**  
**Conference Room 329 & Videoconference**  
**State Capitol**

Aloha Chair Matayoshi and Members of the Committee:

I am in support of Senate Bill no. 2387.

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 respectfully ask you to support and pass this bill.

Mahalo for giving me this opportunity to testify!

Sai Peng Tomchak  
Maui resident

**SB-2387-SD-1**

Submitted on: 3/17/2026 2:40:57 AM

Testimony for CPC on 3/18/2026 2:00:00 PM

<b>Submitted By</b>	<b>Organization</b>	<b>Testifier Position</b>	<b>Testify</b>
BLYTH KOZUKI	Individual	Support	Written Testimony Only

Comments:

**Aloha Chair Matayoshi, and Members of the Committees,**

**My name is Blyth Kozuki, and I am a kupuna writing in strong support of Senate Bill 2387 SD1, which establishes critical safeguards for 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 putting safeguards in place as written in Senate Bill 2387 SD1 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 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**

March 18, 2026

Committee on Consumer Protection & Commerce  
State Capitol  
415 South Beretania Street  
Honolulu, HI 96813

### **TESTIMONY IN SUPPORT OF SB2387 SD1**

Chair Scot Z. Matayoshi, Vice Chair Tina Nakada Grandinetti, and Committee Members:

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

SB2387 SD1 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;<sup>1</sup> 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.<sup>2</sup>

---

<sup>1</sup> *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](https://www.kitv.com/news/crime/scammers-posing-as-police-pressuring-kupuna-to-send-thousands-of-dollars/article_10aac682-3335-4804-898d-64f868aa2c9c.html).

<sup>2</sup> 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 From Myanmar's Scam Centres, BBC (Jan. 9, 2024),

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 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.

---

<https://www.bbc.com/news/articles/cd60611407no>; see also LastWeekTonight, *Pig Butchering Scams: Last Week Tonight with John Oliver (HBO)*, YouTube (Feb. 22, 2025), <https://www.youtube.com/watch?v=pLPpl2ISKTg>.

House of Representatives  
Notice of Hearing

Wednesday, March 18, 2026  
2:00 p.m.

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

House Committee on Consumer Protection & Commerce

Aloha Chair Matayoshi, Vice Chair Grandinetti and members of the Committee on Consumer Protection & Commerce.

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

During 2025, I heard comments about crypto-currency machines springing up in Hawaii. These machines are relatively new. There is a huge risk - especially to those with limited digital knowledge - that machine users could lose huge amounts of monies and potentially their life/retirement savings - to criminal fraudsters.

Over the past several decades, I have heard numerous stories of phone calls that are allegedly from law enforcement, attorneys or other individuals. However, these fraudsters/callers seem 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 will help provide some protection and safeguards to the consumer. For example, clearly worded signs that "warn users of potential financial risk"; how to contact law enforcement should the users suspect fraud; setting a limit on daily 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.

Carol Wakayama  
Punchbowl District

**SB-2387-SD-1**

Submitted on: 3/17/2026 9:45:30 AM

Testimony for CPC on 3/18/2026 2:00:00 PM

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

Comments:

Aloha

I am in strong support of SB2387 SD1, as  
"Consumer Protection" and "Fraudulent Financial Practices" are always of concern to Kūpuna!!!

Mahalo

John A H tomoso+, MSW.ACSW

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

john,a,h,tomosogmail.com

Testimony on Senate Bill No. 2387, SD1  
RELATING TO DIGITAL FINANCIAL ASSETS TRANSACTIONS KIOSKS  
Wednesday, March 18, 2026, at 2:pm  
Conference Room 329 & Videoconference  
State Capitol  
415 South Beretania Street

Aloha Chair Matayoshi and Members of the Committee:

My name is Christina Enoka, and I am in STRONG SUPPORT of SB 2387, SD1 which would set up critical safeguards for cryptocurrency transactions conducted through kiosks in Hawaii.

Cryptocurrency fraud is on the rise, and the kiosks offer a simple opportunity to launder funds or defraud unsuspecting victims. Safeguards must be in place to eliminate and/or reduce significant financial risk to the consumer, especially our kupuna. These safeguards can inform consumers of how crypto assets cannot be refunded or disputed after the transaction. The financial impact can be substantial to the consumer.

Mahalo for the opportunity to testify!

Christina Enoka  
Mililani, Oahu  
Ncsmn150@gmail.com