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

SYLVIA LUKE
LIEUTENANT GOVERNOR | KA HOPE KIA'ĀINA

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

NADINE Y. ANDO
DIRECTOR | KA LUNA HOʻOKELE

DEAN I. HAZAMA
DEPUTY DIRECTOR | KA HOPE LUNA HOʻOKELE

Testimony of the Department of Commerce and Consumer Affairs

Before the
Senate Committee on Judiciary
Senate Committee on Ways and Means
Wednesday, March 4, 2026
10:35 a.m.
Via Videoconference
Conference Room 211

WRITTEN TESTIMONY ONLY

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

Chairs Rhoads, Dela Cruz, and Members of the Committees:

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.[1] 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

[1] 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) ("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.").

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

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

Enforcement of this new section of the HRS by the Department and the Department of the Attorney General 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.

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

FinCEN NOTICE

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

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

Suspicious Activity Report (SAR) Filing Request

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

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

While CVC kiosks can be a simple and convenient way for consumers to access CVC, scammers and other illicit actors can also exploit their simplicity and convenience. According to the Federal Bureau of Investigation's (FBI) Internet Crime Complaint Center (IC3), criminals engaged in fraud schemes often direct victims to use a CVC kiosk to send payments under false pretenses. In 2024, the FBI's IC3 received more than 10,956 complaints reporting the use of CVC kiosks, with reported victim losses of approximately $246.7 million.[3] This represents a 99 percent increase in the number of complaints and a 31 percent increase in reported victim losses from 2023.[4] The Federal Trade Commission (FTC) likewise identified, based on an analysis of consumer reports, that fraud losses through CVC kiosks have skyrocketed.[5]

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

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

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

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

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

How CVC Kiosks Work

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

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

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

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

Non-compliant CVC Kiosk Operators

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

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

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

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

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

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

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

Case Study:

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

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

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

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

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

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

Use of CVC Kiosks to Facilitate Scam Payments

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

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

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

CVC Kiosks and Elder Fraud

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

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

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

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

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

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

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

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

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

Case Study:

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

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

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

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

Red Flag Indicators of Illicit Activity Involving CVC Kiosks

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

Red Flags for Operators of CVC Kiosks Regarding Scam Payments

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Suspicious Activity Reporting

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

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

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

SAR Filing Instructions

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

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

Other Relevant BSA Reporting Requirements

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

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

Information Sharing

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

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

For Further Information

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

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

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

JOSH GREEN, M.D.
GOVERNOR OF HAWAIʻI
KE KIAʻĀINA O KA MOKUʻĀINA ʻO HAWAIʻI

KENNETH FINK, MD, MGA, MPH
DIRECTOR OF HEALTH
KA LUNA HOʻOKELE

STATE OF HAWAIʻI
DEPARTMENT OF HEALTH
KA ʻOIHANA OLAKINO
EXECUTIVE OFFICE ON AGING
NO. 1 CAPITOL DISTRICT
250 SOUTH HOTEL STREET, SUITE 406
HONOLULU, HAWAIʻI 96813-2831

CAROLINE CADIRAO
DIRECTOR
Executive Office on Aging

Telephone
(808) 586-0100

Fax
(808) 586-0185

Testimony in SUPPORT of SB2387 SD1
RELATING TO DIGITAL FINANCIAL ASSET TRANSACTION KIOSKS

COMMITTEE ON WAYS AND MEANS
Senator Donovan M. Dela Cruz, Chair
Senator Sharon Y. Moriwaki, Vice Chair

COMMITTEE ON JUDICIARY
Senator Karl Rhoads, Chair
Senator Mike Gabbard, Vice Chair

Testimony of Caroline Cadirao
Director, Executive Office on Aging
Attached Agency to the Department of Health

Hearing: Wednesday, March 4, 2026, 10:35A.M. Conference Room: 211

EOA Position: The DOH, Executive Office on Aging (EOA) strongly supports SB2387 SD1.

Purpose: This measure proposes consumer protection safeguards for cryptocurrency transactions conducted through kiosks and ATMs to reduce the risk of fraudulent activities.

The prevalence of cryptocurrency and kiosk-related scams in Hawaiʻi is a growing concern. In 2024, the FBI reported nearly 11,000 complaints involving crypto kiosks nationwide, resulting in losses totaling approximately $247 million. These figures are likely to be underreported, meaning the actual impact could be significantly higher.

Recommendation: EOA strongly supports this measure as an important step toward protecting the financial security and well-being of our kūpuna.

Thank you for the opportunity to provide testimony.

DEPARTMENT OF THE PROSECUTING ATTORNEY
KA ʻOIHANA O KA LOIO HOʻOPIʻI
CITY AND COUNTY OF HONOLULU

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

STEVEN S. ALM
PROSECUTING ATTORNEY
LOIO HOʻOPIʻI

THOMAS J. BRADY
FIRST DEPUTY PROSECUTING ATTORNEY
HOPE MUA LOIO HOʻOPIʻI

THE HONORABLE DONOVAN M. DELA CRUZ, CHAIR
SENATE COMMITTEE ON WAYS AND MEANS

THE HONORABLE KARL RHOADS, CHAIR
SENATE COMMITTEE ON JUDICIARY

Thirty-Third State Legislature
Regular Session of 2026
State of Hawai`i

March 3, 2026

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

Chairs Dela Cruz and Rhoads, Vice-Chairs Gabbard and Moriwaki, and members of the Senate Joint Committees on Ways and Means and on Judiciary, 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 establishes reasonable 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 daily and monthly caps meaningfully reduce the 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 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.

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, HAWAI'I 96793
PHONE (808) 270-7777 • FAX (808) 270-7625

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

March 3, 2026

The Honorable Donovan M. Dela Cruz
Chair
The Honorable Sharon Y. Moriwaki
Vice Chair
and Members of the Committee on Ways and Means

The Honorable Karl Rhoads
Chair
The Honorable Mike Gabbard
Vice Chair
and Members of the Committee on Judiciary

Chairs Dela Cruz and Rhoads, Vice Chairs Moriwaki and Gabbard, and Members of the Committees:

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.

DEPARTMENT OF THE PROSECUTING ATTORNEY
KA ʻOIHANA O KA LOIO HOʻOPIʻI
CITY AND COUNTY OF HONOLULU

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

STEVEN S. ALM
PROSECUTING ATTORNEY
LOIO HOʻOPIʻI

THOMAS J. BRADY
FIRST DEPUTY PROSECUTING ATTORNEY
HOPE MUA LOIO HOʻOPIʻI

THE HONORABLE DONOVAN M. DELA CRUZ, CHAIR
SENATE COMMITTEE ON WAYS AND MEANS
AND
THE HONORABLE KARL RHOADS, CHAIR
SENATE COMMITTEE ON JUDICIARY
Thirty-Third State Legislature
Regular Session of 2026
State of Hawai`i

March 03, 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 and 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 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 daily and monthly caps meaningfully reduce the 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 on this matter.

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

The Thirty-Third State Legislature
Senate Committee on Judiciary
Senate Committee on Ways and Means
March 4, 2026
Conference Room 211, 10:35 a.m.

TO: The Honorable Karl Rhoads, Chair
The Honorable Donovan M. Dela Cruz, Chair
FROM: Kealiʻi S. López, State Director
RE: Strong Support for S.B. 2387, SD1 Relating to Digital Financial Asset Transaction Kiosks

Aloha Chair Rhoads, Chair Dele Cruz, and Members of the Committees:

My name is Kealiʻi López, and I serve as State Director for AARP Hawaiʻi. 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 Hawaiʻi members, thank you for the opportunity to testify **in strong support** of S.B. 2387, S.D.1.

AARP Hawaiʻi 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, Hawaiʻi 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.

Hawaiʻi 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.

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.

827 Fort Street Mall, 2nd Floor
Honolulu, Hawaii 96813

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

HolomuaCollaborative.org

Committee: **Senate Committee on Judiciary**
Senate Committee on Ways and Means
Bill Number: **SB2387 SD1, Relating to Digital Financial Asset Transaction Kiosks**
Hearing Date and Time: **March 4, 2026, at 10:35am (Room 211)**
Re: **Testimony of Holomua Collaborative in support**

Aloha Chair Rhoads, Chair Dela Cruz, Vice Chair Gabbard, Vice Chair Moriwaki, 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.[1] 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

[1] Cal. Fin. Code § 3901.

SB-2387-SD-1
Submitted on: 3/2/2026 9:32:55 PM
Testimony for JDC on 3/4/2026 10:35:00 AM

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

Comments:

Dear Chair Dela Cruz, Vice Chair Moriwaki, Honorable Members of the Senate Committee on Ways and Means, Chair Rhoads, Vice Chair Gabbard, and Honorable Members of the Senate Committee on Judiciary:

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

PABEA strongly supports SB 2387 SD 1, 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

PABEA Board Member

SB-2387-SD-1
Submitted on: 3/2/2026 4:17:13 PM
Testimony for JDC on 3/4/2026 10:35:00 AM

Submitted By	Organization	Testifier Position	Testify
Rick Tabor	Testifying for PABEA	Support	Written Testimony Only

Comments:

Thank you for hearing SB2387, SD1 which would establish critical safeguards for cryptocurrency transactions conducted through kiosks in Hawai‘i.

I am Rick Tabor, from Honolulu, HI, I humbly serve in a few nomprofit leadership roles. Today I testify on behalf of PABEA as their Legislative Committee Chair. In my positions, I testify that The Policy Advisory Board for Elder Affairs and Kūpuna Caucus both stand in strong support of SB2387, SD1 which would establish critical safeguards for cryptocurrency transactions conducted through kiosks in Hawai‘i.

Note; my PABEA testimony is submitted seperate of EOA.

For the record, I’m a retired mental health clinician, past in-home care operation manager, veteran field medical Navy hospital corpsman.

As a member of several Kūpuna nonprofits, I thank you for your support and all you do for Hawaii. I appreciated it.

As you know, fraud issues, involving Cryptocurrency kiosks, have rapidly expanded in Hawaii. Our kūpuna, are vulnerable, all alone, lonely, eager to help out. As such, they are frequent scam targets! Easily taken advantage of, being exposed to significant financial risk schemes, fraudulant transactions, resulting in irreversible losses.

Senate Bill 2387 SD1 would be a reasonable safe-gaurd start. It is a strongly recommended, best practice, consumer-focused safety response for our Island’s cryptocurrency issues.

People who use cryptocurrency kiosks typically do not realize they are converting cash into crypto assets that, once sent, cannot be traced, disputed, or refunded.

In Hawai‘i, where many residents rely on quick access to their cash. Cryptocurrency kiosks can create a false sense of easy access. And a false perception of security that mirrors traditional ATMs. Most people are unaware of cryptocurrency kiosk’s lack of protection. Friends have shared their stories. For each of them, the cryptocurrency kiosk scam was a costly, embarrassing, rude awakening, with no recourse.

I join many in my respectful ask; please pass Senate Bill 2387. In the spirit of Aloha, let's promote Hawai‘i’s values of fairness, and protect our people, especially those who once protected us, our Kūpuna. Progress need not be ‘The Wild Wild West.’ Innovation in a safe and responsible way is wise and proactive. Enough of these reckless, rush with no safety plans. Stop, Think, and do right, with ressonable safegaurds before launching.

Thank you for your time, your thoughtful consideration. Your commitment to protecting Hawai‘i’s people is always appreciate.

Mahalo Nui Loa,

-Rick Tabor

TESTIMONY SUBMITTED TO THE SENATE COMMITTEE ON JUDICIARY AND COMMITTEE ON WAYS & MEANS

Louise Pais, Chief Compliance Officer

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

Aloha Chair Rhoads, Vice Chair Gabbard, and Members of the Committee on Judiciary

Aloha Chair Dela Cruz, Vice Chair Moriwaki, and Members of the Committee on Ways & Means

I am Louise Pais, Chief Compliance Officer for Hilt Ventures, LLC ("Hilt"). Hilt is a small crypto kiosk operator on a national level but is the largest operator in the state of Hawaii. Hilt has been operating here since April of 2021 and takes compliance and consumer protection very seriously. Thank you for the opportunity to share testimony on SB 2387 SD1.

Hilt supports and 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.

However, as proposed, we have concerns applying a daily transaction limit of $2,000 and a monthly transaction limit of $10,000 to all customers, with no differentiation between new customers and established customers. In our experience, customers who are the victims of fraud are new, first-time customers, not established 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.

We would support a different approach regarding transaction limits, with a focus on new customers similar to 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.

In addition, Hilt has concerns regarding some of the language to be included on a customer receipt as well as the form of that receipt.

We would support language that allows for a paper “or” electronic receipt and that allows for the phone number established to answer questions and register complaints that is not necessarily a toll-free number.

Hilt also has concerns regarding the refund language as proposed in the current bill. The current bill requires a full refund (not just fees) to all customers, new and existing, if a customer reports the fraud within 90 days of the transaction.

We would support a different approach, once again with the focus on differentiating 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.

Hilt proposes adding the definition of new customer and existing customer to the bill:

- "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.

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

Hawaii Credit Union League
Your Partner For Success
Unite for Good
1654 South King Street
Honolulu, Hawaii 96826-2097
Telephone: (808) 941.0556
Fax: (808) 945.0019
Web site: www.hcul.org
Email: info@hcul.org

Testimony to the Senate Committees on Judiciary and Ways & Means
Wednesday, March 4, 2026
Conference Room 229

To: The Honorable Karl Rhoads, Chair
The Honorable Mike Gabbard, Chair
The Honorable Donovan Dela Cruz, Vice-Chair
The Honorable Sharon Moriwaki, Vice-Chair
Members of the Committees

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.

SanHi
GOVERNMENT STRATEGIES
A LIMITED LIABILITY LAW PARTNERSHIP

DATE: March 3, 2026

TO: Senator Donovan DelaCruz
Chair, Committee on Ways and Means

Senator Karl Rhoads
Chair, Committee on Judiciary

FROM: Tiffany Yajima / Mihoko Ito

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

Hearing Date: Wednesday, March 4, 2026 at 10:35 a.m.
Conference Room: 211

Dear Chair Dela Cruz, Chair Rhoads, and Members of the Joint Committees:

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 submits this testimony in **support** of SB2387, 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.

First Hawaiian Center
999 Bishop Street, Suite 1400
Honolulu, HI 96813
T 808-539-0400
F 808-533-4945

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.

March 4, 2026

TO: Chairs Rhoads and Dela Cruz 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: 3/2/2026 1:51:35 PM
Testimony for JDC on 3/4/2026 10:35:00 AM

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

Comments:

Aloha Chair Dela Cruz, Chair Rhoads 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

COMMITTEE ON WAYS AND MEANS
Senator Donovan M. Dela Cruz, Chair
Senator Sharon Y. Moriwaki, Vice Chair

COMMITTEE ON JUDICIARY
Senator Karl Rhoads, Chair
Senator Mike Gabbard, Vice Chair

NOTICE OF DECISION MAKING
Wednesday, March 4, 2026, 10:35am

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

Aloha Chairs Dela Cruz and Rhoads, and Vice Chairs Moriwaki and Gabbard. I am Linda Dorset and I am testifying in STRONG support of SB 2387 **which would establish critical safeguards for cryptocurrency transactions conducted through kiosks in Hawai'i and set a limit of $2,000 or a limit of $10,000 in any thirty-day period.**

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

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

Senate Bill 2387 SD1 is a reasonable, necessary, and consumer-focused response to these documented harms.

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

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

Linda Dorset
Maui Senior Citizen

SB-2387-SD-1
Submitted on: 3/2/2026 6:21:47 PM
Testimony for JDC on 3/4/2026 10:35:00 AM

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

Comments:

Aloha Chair Rhoads, Chair Dela Cruz and Members of the Committee:

My name is Angela Serota and I am writing to STRONGLY SUPPORT SB 2387 that would ensure crucial limits and safeguards for cryptocurrency transactions done through kiosks in Hawai'i.

These cryptocurrency kiosks are found throughout the islands and are known to be used to scam consumers, especially kupuna. Many consumers do not know that their cash is converted into crypto assets that cannot be refunded or traced once sent. These kiosks look similar to traditional ATMs but do not provide the same protections.

Please PASS SB 2387 to help protect Hawai'i consumers from falling prey to this relatively new and often confusing currency system.

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

Angela Serota

Kilauea, HI

SB-2387-SD-1
Submitted on: 3/2/2026 7:33:40 PM
Testimony for JDC on 3/4/2026 10:35:00 AM

Submitted By	Organization	Testifier Position	Testify
Warren Wong	Individual	Support	Written Testimony Only

Comments:

This bill doesn't eliminate cryptocurrency aTM's. it just provides guiderails. Theres a crypto ATM at the Safeway near my home. it doesn't need a lot of traffic, just one big wrong move.

March 4, 2026

Committee on Ways and Means
Committee on Judiciary
State Capitol
415 South Beretania Street
Honolulu, HI 96813

TESTIMONY IN SUPPORT OF SB2387 SD1

Chairs Donovan M. Dela Cruz and Karl Rhoads, Vice Chairs Sharon Y. Moriwaki and Mike Gabbard, 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;[1] your bank account is compromised, and you have to protect your money by changing it to crypto; etc.—but the end goal for the scammer is the same: get the victim to a kiosk with cash, and tell them how to send it. This video shows what that looks like as it's happening: https://youtu.be/lfHuSkQnBLk.

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

---

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

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

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.

---

factory-in-myanmar/a-68113480; Koh Ewe, How a Viral Post Saved a Chinese Actor From Myanmar's Scam Centres, BBC (Jan. 9, 2024), https://www.bbc.com/news/articles/cd606l1407no; *see also* LastWeekTonight, *Pig Butchering Scams: Last Week Tonight with John Oliver (HBO)*, YouTube (Feb. 22, 2025), https://www.youtube.com/watch?v=pLPpl2ISKTg.

SB-2387-SD-1
Submitted on: 3/2/2026 11:00:00 PM
Testimony for JDC on 3/4/2026 10:35:00 AM

Submitted By	Organization	Testifier Position	Testify
Barbara J. Service	Individual	Support	Written Testimony Only

Comments:

Aloha Chairs Dela Cruz and Rhoads and committee members:

Please pass SB 2387, dealing with cryptocurrency. This measure will put safeguards on transactions at crytocurrency kiosks. Kupuna and others have been taken advantage of by the lure of easy money. Digital financial asset transaction kiosk operators will be required to provide receipts, provide full refunds under some circumstances, provide live customer service, etc.

As with children, Kupuna are most precious and also vulnerable.

Please protect Kupuna and others from potentially losing everything through possible unscrupulous practices.

Mahalo for allowing me to testify.

Barbara J, Service. MSW

Child Welfare Supervisor (ret.)

Passionate Kupuna advocate

LATE

SB-2387-SD-1
Submitted on: 3/3/2026 12:08:40 PM
Testimony for JDC on 3/4/2026 10:35:00 AM

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

Comments:

Aloha Chair Rhoads, Chair Dela Cruz and Members of the Committees:

My name is Nadine NEWLIGHT, and I am in **STRONG SUPPORT of SB 2387, SD1, which would establish critical safeguards 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. Senate Bill 2387, SD1 is a reasonable, necessary, and consumer-focused response to these documented harms.

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. This measure reflects Hawai‘i’s values of fairness, and protection of our people, while allowing innovation and technology to move forward in a safe and responsible way.

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

Nadine NEWLIGHT

Ha`iku, HI

SB-2387-SD-1
Submitted on: 3/3/2026 9:25:49 AM
Testimony for JDC on 3/4/2026 10:35:00 AM

Submitted By	Organization	Testifier Position	Testify
Marilyn Seely	Individual	Support	Written Testimony Only

Comments:

COMMITTEE ON WAYS AND MEANS
Senator Donovan M. Dela Cruz, Chair
Senator Sharon Y. Moriwaki, Vice Chair

COMMITTEE ON JUDICIARY
Senator Karl Rhoads, Chair
Senator Mike Gabbard, Vice Chair

Committee on the Judiciary

Chair Rhoads

Vice Chair Gabbared

Committee on Ways and Means

Chair Dela Cruz,

Vice Chair Moriwaki

RE SB 2387 relating to the digital ifnancial asset transations kiosks

I am strongly in favor of this bill. Having experienced family members being taken in by financial criminals I understand the vulnerability of older adults regarding their income and asset protection. It is far to easy to rob these folks and criminals know well how to exploit them. We must increase our protection not make it easier for them to rob folks of their life savings. and ruin the remaining years of their lives. You can make a difference in combating this world wide scheme by passing this bill and be a part of taking care of vulnerable people. Thank you.

Marilyn Seely

Testimony on Senate Bill No. 2387, SD1
RELATING TO DIGITAL FINANCIAL ASSETS TRANSACTIONS KIOSKS
Wednesday, March 4, 2026, at 10:35 am
Conference Room 211 & Videoconference
State Capitol
415 South Beretania Street

Aloha Chair Rhoads, Chair Dela Cruz 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.

Mahalo for the opportunity to testify!

Christina Enoka
Mililani, Oahu
Ncsmn150@gmail.com

LATE

Testimony on Senate Bill No. 2387, SD1

RELATING TO Digital Financial Assets Transaction Kiosks

Wednesday, March 4, 2026 at 10:35 am

Conference Room 211 & Videoconference

State Capitol

Aloha Chair Rhoads, Chair Dela Cruz and Members of the Committees:

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 respectively ask you to support and pass this bill.

Mahalo for giving me this opportunity to testify!

Sai Peng Tomchak
Maui resident