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

SYLVIA LUKE
LIEUTENANT GOVERNOR | KA HOPE KIA'ĀINA

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

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
Senate Committee on Commerce and Consumer Protection
Wednesday, March 18, 2026
9:30 a.m.
Via Videoconference
Room 229

On the following measure:
H.B. 1642, H.D. 1, RELATING TO CONSUMER PROTECTION

Chair Keohokalole 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 offers testimony in strong support of this bill.

The purpose of this bill is to prohibit the operation of digital financial asset transaction kiosks, also sometimes called cryptocurrency ATMs, that accept U.S. currency in exchange for digital financial assets.

Fraudulent activity involving digital financial asset kiosks has resulted in significant financial losses to consumers. At present, Hawai'i has over two hundred digital financial asset 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 digital financial asset kiosk, and the digital financial asset ultimately ends up in a third-party 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. Until operators can effectively demonstrate that legitimate use of digital financial asset kiosks demonstrably outweighs fraudulent uses, allowing purchases of digital financial assets from kiosks is contrary to the consumer public's interests. We understand that certain operators believe they have tools to counteract fraud at their kiosks. One operator has engaged our office and been willing to share metrics that support their conclusions. However, the vast majority of kiosk operators have as yet been unwilling to demonstrate their approach to fraud prevention to our office's satisfaction; indeed, they have yet to engage with our office meaningfully in any manner. We do not know what their level of commitment is to counteracting fraud at their kiosks. Until adoption of fraud counteraction measures is widespread across the operator ecosystem, and operators have demonstrated their commitment to

[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.").

counteracting fraud, digital financial asset kiosks will remain a conduit for fraudulent activities, and we will support a ban on purchases of digital financial assets from kiosks as a matter of good public policy.

Digital financial assets can be purchased through bank-funded and exchange-funded transactions. For consumers who are interested in purchasing digital financial assets, our research suggests that exchange-funded or bank-funded transfers at present are a more common method of funding digital financial asset purchases than cash.[2] Given this evidence, this measure's prohibition on cash purchases would not appreciably limit access to digital financial assets for the majority of consumers interested in purchasing it. Consumers who presently use cash to purchase digital financial assets would presumably use bank- or exchange-funded purchases to make their purchases if this measure were enacted.

Because of the ongoing misuse of kiosks for fraudulent activity, and the apparent failure by certain operators to implement reforms to control fraud, a ban on digital financial asset kiosk purchases using cash is appropriate for consumer protection.

We respectfully request that the bill be voted out of committee.

Thank you for the opportunity to testify on this bill.

---

[2] Industry sources such as The Block estimate the daily average volume of cryptocurrency trading at` $155 billion. Evidence of the amount of purchases of cryptocurrency in the United States is harder to come by. Information from CoinFlip asserts that CoinFlip has the second-largest fleet of Bitcoin ATMs by company, with around 5,500 Bitcoin ATMs worldwide and growing. Bitcoin ATM Industry Insights: Trends and Statistics. CoinFlip claims to have processed nearly $4 billion in transactions since its inception in 2015. Bitcoin ATM Industry Insights: Trends and Statistics. This transaction volume while large would represent a small fraction of overall trading in cryptocurrency.

We would welcome more direct evidence about the methods of funding of cryptocurrency purchases and the prevalence of cash-funded purchases.

Attachment A- Referenced in DCCA's Testimony on H.B. 1642, H.D. 1

FinCEN NOTICE

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

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

Suspicious Activity Report (SAR) Filing Request

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

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

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

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

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

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

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

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

How CVC Kiosks Work

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

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

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

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

Non-compliant CVC Kiosk Operators

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

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

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

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

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

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

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

Case Study:

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

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

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

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

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

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

Use of CVC Kiosks to Facilitate Scam Payments

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

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

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

CVC Kiosks and Elder Fraud

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

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

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

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

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

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

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

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

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

Case Study:

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

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

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

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

Red Flag Indicators of Illicit Activity Involving CVC Kiosks

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

Red Flags for Operators of CVC Kiosks Regarding Scam Payments

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Suspicious Activity Reporting

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

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

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

SAR Filing Instructions

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

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

Other Relevant BSA Reporting Requirements

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

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

Information Sharing

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

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

For Further Information

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

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

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

TESTIMONY OF
THE DEPARTMENT OF THE ATTORNEY GENERAL
KA ʻOIHANA O KA LOIO KUHINA
THIRTY-THIRD LEGISLATURE, 2026

ON THE FOLLOWING MEASURE:
H.B. NO. 1642, H.D. 1, RELATING TO CONSUMER PROTECTION.

BEFORE THE:
SENATE COMMITTEE ON COMMERCE AND CONSUMER PROTECTION

DATE: Wednesday, March 18, 2026 **TIME:** 9:30 a.m.

LOCATION: State Capitol, Room 229

TESTIFIER(S): Anne E. Lopez, Attorney General, or
James C. Paige or Christopher J.I. Leong
Deputy Attorneys General

Chair Keohokalole and Members of the Committee:

The Department of the Attorney General supports this bill.

This bill would ban, effective October 1, 2026, the ownership, operation, or management in the State of a digital financial asset transaction kiosk that accepts United States currency from a customer in exchange for a digital financial asset. Fraudsters have used these kiosks to scam vulnerable consumers out of thousands of dollars. The victims of these scams are often seniors who have little recourse and face poor prospects of recovery once they have been tricked into depositing their cash into these kiosks. This bill will protect consumers by banning a particular type of kiosk that has been associated with significant levels of fraud.

Thank you for considering our comments.

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 Commerce and Consumer Protection
Wednesday, March 18, 2026
Conference Room 229, 9:30 a.m.

TO: The Honorable Jarrett Keohokalole, Chair
FROM: Kealiʻi S. López, State Director
RE: Strong Support for H.B. 1642, HD1 Relating to Consumer Protection

Aloha Chair Keohokalole and Members of the Committee:

My name is Kealiʻi López, and I serve as State Director for AARP Hawaiʻi. AARP is a nonprofit, nonpartisan organization dedicated to empowering people age fifty and older to choose how they live as they age. We advocate on behalf of the issues that matter most to older adults and their families. On behalf of AARP's more than **135,000 Hawaiʻi members**, I write in **strong support of H.B. 1642, H.D.1.**

Fraud prevention is one of AARP's highest priorities, and the threat posed by cryptocurrency-related frauds is growing rapidly. As criminals evolve their tactics, state policy must keep pace. Cryptocurrency kiosks also known as crypto ATMs or bitcoin ATMs have quickly become a **preferred tool for scammers** to extract money from victims. These machines are widely available in everyday locations such as supermarkets, gas stations, convenience stores, and pharmacies, and they closely resemble traditional bank ATMs, making them particularly deceptive and dangerous for consumers.

The scope of the harm is staggering. In just the **first eleven months of 2025**, the FBI reported that more than **12,000 consumers lost $333 million** through cryptocurrency kiosk fraud. These figures reflect only reported losses; the true impact is far greater, as many victims, especially older adults, are reluctant or embarrassed to report fraud. Data from the FBI and the Federal Trade Commission consistently show that **kupuna are disproportionately targeted and harmed** by these schemes.

H.B. 1642, H.D.1 takes decisive action by prohibiting cryptocurrency kiosks that accept U.S. currency in exchange for digital financial assets. This prohibition directly disrupts one of the most effective mechanisms scammers use to collect stolen funds quickly and irreversibly. By cutting

off this avenue, the Legislature can meaningfully reduce fraud and protect Hawai‘i consumers from devastating monetary loss.

While AARP Hawai‘i supports this bill, we note that **S.B. 2387, S.D.1** establishes daily transaction limits, mandates refunds, requires clear and consistent warning signage, ensures access to live customer service, and provides paper receipts with transaction details useful to law enforcement. **Versions of this comprehensive framework have already passed in eighteen other states and have demonstrated success in reducing fraud.** As **H.B. 1642, H.D.1** moves forward, we respectfully ask that legislators ensure this measure will be supported by the Governor and enacted into law.

AARP supports both measures, and we strongly urge the Legislature, once these bills reach Conference, to **come to agreement on a single bill that will become law this session**. Hawai‘i residents cannot afford inaction or delay. Every month without meaningful safeguards results in **millions of additional dollars lost** to scams that exploit regulatory gaps and consumer confusion. Failure to enact legislation this year would leave consumers exposed to ongoing and preventable harm. That is not an acceptable outcome particularly when effective policy solutions are clearly before you.

Mahalo for the opportunity to submit testimony in strong support of **H.B. 1642, H.D.1**, and for your continued commitment to protecting Hawai‘i’s consumers.

TESTIMONY SUBMITTED TO THE SENATE COMMITTEE ON COMMERCE AND CONSUMER PROTECTION

RE: HB 1642 HD1 Relating to Consumer Protection

Aloha Senator Keohokalole, Vice Chair Fukunaga, and Members of the Senate Commerce and Consumer Protection 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 Hawaiian customers since 2021 and have 24 kiosks located in conveniently trusted retail partners across Oahu, Maui, Kauai, and the Big Island.

We respectfully oppose HB 1642 HD1 in its current form and strongly urge you to replace the language of HB 1642 HD1 with the language found in SB 2387 SD1 (common sense guardrails, including the edits suggested by Hilt and noted in Standing Committee Report 3036 regarding differentiating between first time and existing customers for transaction limits and refund provisions).

Alternatively, if the Committee cannot consider replacing the current language with such guardrails (with suggested edits), then we urge you to amend HB 1642 HD1 to carve out a narrow exception for "good operators" – those that have never declared bankruptcy, have never been fined by another state's Attorney General's office or FinCEN, and have never received a cease-and-desist order from another state regulator as a result of deceptive practices or non-compliance with the law.

<u>AMEND HB 1642 HD1 by replacing an outright ban with more common-sense safeguards.</u>

We share the deep concern for protecting kūpuna and all 'ohana from devastating scams. However, a blanket ban is neither effective nor fair. Fraudsters adapt quickly: banning crypto kiosks won't stop scams; victims will simply be directed to other irreversible methods that remain fully legal and unrestricted.

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. We have called out portions

of the bill that we believe should differentiate between new and existing customers - the provisions relating to transaction limits and refunds. 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

With respect to transaction limits:

$2,000 (or equivalent in digital financial assets) per day for new customers; and

$10,500 (or equivalent) per day for existing customers.

With respect to the refund provision:

- 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 the following definitions of new customer and existing customer:

- "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.

<u>ALTERNATIVELY, AMEND HB 1642 HD1 to allow a narrow exemption for operators with no problematic compliance histories</u>.

As an alternative to the above, Hilt urges you to provide a narrow exemption for legitimate operators in Hawaii while applying a ban on rogue operators that fall into the following categories:

- any operator who has previously filed bankruptcy while operating crypto kiosks in another state

- any operator who has been fined by another state or federal government for non-compliance with the law
- any operator who has received a cease-and-desist order from another state regulator as a result of deceptive practices

The above would eliminate all rogue operators who are behind 99% of all scams in this space.

This targeted approach would allow compliant operators like Hilt Ventures to continue serving Hawaii's communities, while excluding bad actors and maintaining strong consumer protections.

Such exemptions are not novel in Hawaii's legislative history; Hawaii has a long tradition of incorporating carve-outs in bans to balance broad restrictions with practical, equitable considerations. This precedent demonstrates that thoughtful exemptions can achieve policy goals without overreach, ensuring legislation serves our ʻohana, and specifically, our kūpuna effectively.

Please oppose any outright ban and replace the language in HB 1642 HD1 with the language found in SB 2387 SD1 (common sense guardrails, including the edits suggested by Hilt and noted in Standing Committee Report 3036 regarding differentiating between first time and existing customers for transaction limits and refund provisions).

Alternatively, if the Committee cannot consider such guardrails (with suggested edits), then please amend HB 1642 HD1 to carve out a narrow exception for good operators.

Our ʻohana—and especially our kūpuna—deserve real, effective solutions to combat scams, not arbitrary restrictions that leave other major scam avenues wide open.

Thank you for the opportunity to testify regarding this bill. We welcome an opportunity to meet to discuss further and answer any questions.

Respectfully,

Louise

TESTIMONY SUBMITED TO THE HAWAII SENATE COMMITTEE ON COMMERCE AND CONSUMER PROTECTION
Larry Lipka, General Counsel
March 17, 2026

CoinFlip supports strong, commonsense consumer protections for cryptocurrency kiosks. While we oppose the ban in the proposed legislation, we support regulatory measures that meaningfully enhance consumer safety including licensure, clear and strong consumer disclosures, compliance program requirements, and appropriate technology standards.

For the past few years, CoinFlip has actively engaged with legislators and regulatory agencies in Hawaii to advocate for a clear and effective regulatory framework for cryptocurrency kiosks

We appreciate the opportunity to offer additional consumer protection-focused recommendations that we know to be effective in preventing fraudulent transactions at virtual currency kiosks. CoinFlip looks forward to continuing to work with the State of Hawaii and this Committee to strengthen protections for consumers while preserving access to lawful, regulated financial services.

HB 1642

CoinFlip respectfully opposes HB 1642, which would ban cryptocurrency kiosks in Hawaii. Cryptocurrency kiosks provide a safe and regulated way for residents to access cryptocurrency using cash, which remains how many people, including unbanked consumers, manage their finances day to day. Kiosks serve an important role in expanding financial access and consumer choice.

Even with the growth of online banking and mobile payments, not every consumer is comfortable using online exchanges. With the prevalence of data breaches and online hacking, many people are hesitant to link their bank accounts to online platforms. Others simply prefer a physical, in-person option, much like why people still visit bank branches. Cryptocurrency kiosks serve as a bridge between the cash economy and the digital economy.

Kiosks can also provide meaningful consumer protections. For individuals who find online exchanges confusing or intimidating, kiosks offer a step-by-step, guided transaction flow with multiple, prominent scam warnings before a transaction is completed. Many kiosk operators, like CoinFlip, also offers 24/7 live customer service with staff who are trained twice a year in anti-money laundering and scam identification.

Rather than eliminating this option for Hawaii consumers, CoinFlip supports state licensure and targeted regulatory safeguards that protect consumers, enhance transparency, and remove bad actors from the market without restricting access for law-abiding residents. SB 2387 accomplishes this goal, and because it has already passed the Senate, we urge the committee to continue supporting it as the more balanced alternative to a ban.

HB-1642-HD-1
Submitted on: 3/16/2026 2:01:45 PM
Testimony for CPN on 3/18/2026 9:30:00 AM

Submitted By	Organization	Testifier Position	Testify
GARY SIMON	Testifying for Hawai?i Family Caregiver Coalition	Support	Written Testimony Only

Comments:

Dear Chair Keohokalole, Vice Chair Fukunaga, and Honorable Members of the Senate Committee on Commerce and Consumer Protection,

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 HB 1642 HD 1, which, beginning October 1, 2026, prohibits the ownership, operation, or management of a digital financial asset transaction kiosk that accepts United States currency from a customer in exchange for a digital financial asset.

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 HB 1642 HD 1.

Mahalo for seriously considering the bill.

Gary Simon

Hawai‘i Family Caregiver Coalition

HB-1642-HD-1
Submitted on: 3/15/2026 9:14:14 AM
Testimony for CPN on 3/18/2026 9:30:00 AM

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

Comments:

Aloha Chair, Vice Chair, and Members of the Committee,

I am writing in **strong support** of HB1642, a targeted and necessary measure to protect Hawai‘i's consumers—particularly our kūpuna—from a growing epidemic of cryptocurrency kiosk scams.

Why Is This Important?

Cryptocurrency kiosks, often placed in convenience stores, gas stations, and other easily accessible locations, may look like a harmless new technology. But the evidence from across the country paints a starkly different picture: these machines have become a primary tool for scammers to steal life savings from vulnerable individuals, especially older adults.

The findings from the initial committee report are deeply alarming and must guide our action. Investigations by the attorneys general for the District of Columbia and Iowa determined that **more than 93% of transactions at the kiosks they investigated were scam transactions**. These machines are not legitimate financial tools in any practical sense; they are, in overwhelming majority, instruments of fraud.

How the Scams Work

The pattern is now familiar and devastating. A scammer contacts a victim—often an older adult—posing as a government agent, a tech support representative, a family member in distress, or a romantic interest. They create a story of urgency and fear: your bank account is compromised, you owe back taxes, your grandchild is in jail and needs bail. The victim is instructed to withdraw cash, go to a cryptocurrency kiosk, and deposit that cash into a digital wallet address provided by the scammer.

Once the cash is converted to cryptocurrency and sent, it is gone. Irretrievably. There is no "undo" button, no fraud department to call, no chargeback to file. The money vanishes into the anonymous world of digital assets, and the victim is left with nothing.

Why a Ban Is Necessary

Some have argued for warning labels or disclosure requirements. But when 93% of transactions are fraudulent, warnings are not enough. Scammers are sophisticated; they coach victims on what to say, how to avoid detection, and how to dismiss any concerns raised by store employees or family members. A warning sign on a machine will not stop a scammer who has already spent hours building trust and manufacturing fear.

HB1642 takes the only truly effective approach: it **prohibits the ownership, operation, or management of a digital financial asset transaction kiosk that accepts United States currency from a customer in exchange for a digital financial asset**. In plain language, it stops the cash-in function that scammers rely on.

Importantly, as the committee report notes, this measure is carefully limited. It **does not** affect the ability to exchange one digital financial asset for another. It **does not** prohibit selling digital financial assets for United States currency through these kiosks. Consumers who already hold cryptocurrency and wish to cash out can still do so. The bill simply closes the entry point that scammers exploit to turn cash into untraceable crypto.

Consumers Have Other Options

The committee report correctly observes that consumers have other means of participating in the digital financial asset market. For those who wish to invest in cryptocurrency legitimately, online exchanges, brokerage platforms, and other regulated channels remain available. These alternatives come with consumer protections, fraud monitoring, and the ability to reverse or report suspicious transactions. Kiosks offer none of that.

A Matter of Protection

This bill is about protecting our kūpuna, our neighbors, and our communities from a predatory technology that has proven, time and again, to be a vehicle for devastating financial fraud. It is about recognizing that when more than nine out of 10 transactions are scams, the machine is not a legitimate business tool—it is a weapon aimed at the most vulnerable among us.

I urge this committee to pass HB1642 and shut down this pipeline of fraud before another family loses their savings.

Mahalo for the opportunity to testify.

HB-1642-HD-1
Submitted on: 3/15/2026 3:03:51 PM
Testimony for CPN on 3/18/2026 9:30:00 AM

Submitted By	Organization	Testifier Position	Testify
Ken Y	Individual	Oppose	Written Testimony Only

Comments:

I own a Texaco gas station where Hilt has had a crypto kiosk for many years. As a local business owner, I oppose a ban on crypto kiosks in Hawaii.....totally unnecessary.

Ken Y.

Honolulu, HI

HB-1642-HD-1
Submitted on: 3/15/2026 3:10:54 PM
Testimony for CPN on 3/18/2026 9:30:00 AM

Submitted By	Organization	Testifier Position	Testify
Rorrie O	Individual	Oppose	Written Testimony Only

Comments:

I own a mom and pop mini mart and have had Hilt kiosks in my location since 2023. I oppose a ban on crypto kiosks in Hawaii.

Rorrie O

Honolulu, HI

HB-1642-HD-1
Submitted on: 3/16/2026 9:03:26 AM
Testimony for CPN on 3/18/2026 9:30:00 AM

Submitted By	Organization	Testifier Position	Testify
Jerry Orten	Individual	Support	Written Testimony Only

Comments:

Aloha Honorable Chairman Matayoshi and distinguished members of the Senate Committee on Commerce and Consumer Protection-

i write to request your support of this bill.
This bill, when passed, will protect residents and kupuna from fraud facilitated via crypto ATMs.

Our people must be protected from those who would defraud them of their life savings, or significant funds.

Mahalo!

Jerry Orten

Lihue

HB-1642-HD-1
Submitted on: 3/16/2026 2:15:30 PM
Testimony for CPN on 3/18/2026 9:30:00 AM

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.**

As 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

HB-1642-HD-1
Submitted on: 3/17/2026 2:55:55 AM
Testimony for CPN on 3/18/2026 9:30:00 AM

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

Comments:

Aloha Chair Keohokalole and Members of the Committee:

My name is Blyth Kozuki, and I am a kupuna writing in strong support of House Bill 1642 HD1, which bans 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 banning cryptocurrency ATMs as written in House Bill 1642 HD1 will discourage scammers from seeing our state as an easy target for our kupunas. I think it is urgent to PASS House Bill 1642 HD1 because the people who scam and their ability to scam keeps growing. Mahalo for your time, your consideration, and your commitment to protecting Hawai‘i’s consumers.

Respectfully submitted,

Blyth Kozuki

Honolulu, Hawai‘i

March 18, 2026

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

TESTIMONY IN SUPPORT OF HB1642 HD 1

Chair Jarrett Keohokalole, Vice Chair Carol Fukunaga, and Committee Members:

I write to express my strong support for HB1642 HD 1 and ask the Committee to pass it.

HB1642 HD 1 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 ban cryptocurrency kiosks in Hawai‘i, which would provide immense assistance to protecting our citizens from scams.

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

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

---

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

[2] For example, a large scam compound called KK Park was located in Myanmar. *See* Lewis Sanders IV et al., How Chinese Mafia Are Running a Scam Factory in Myanmar, DW (Jan. 30, 2024), https://www.dw.com/en/how-chinese-mafia-are-running-a-scam-factory-in-myanmar/a-68113480; Koh Ewe, How a Viral Post Saved a Chinese Actor From Myanmar's Scam Centres, BBC (Jan. 9, 2024), https://www.bbc.com/news/articles/cd606l1407no; *see also* LastWeekTonight, *Pig*

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.

Banning cryptocurrency kiosks would eliminate them as an avenue for scammers to steal from Hawai'i citizens. In a time of increasingly sophisticated crimes using social engineering and artificial intelligence, let's make it harder to steal from folks in Hawai'i.

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

I urge the Committee to pass HB1642 HD 1 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.

Butchering Scams: Last Week Tonight with John Oliver (HBO), YouTube (Feb. 22, 2025), https://www.youtube.com/watch?v=pLPpl2ISKTg.

THE SENATE
KA ʻ AHA KENEKOA

NOTICE OF HEARING
March 18, 2026
9:30 a.m.

RELATING TO CONSUMER PROTECTION
H.B. 1642, HD1

Committee on Commerce & Consumer Protection

Aloha Chair Keohokalole, Vice Chair Fukunaga and Members of the Senate Committee on Commerce & Consumer Protection.

My name is Carol Wakayama and I wish to express my STRONG SUPPORT for H.B. 1642, HD1.

During 2025, I heard comments about cryptocurrency machines springing up in Hawaii. These machines are a relatively new concept. 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 H.B. 1642, HD1 will help provide some protection and safeguards to the consumer, particularly because it bans all cash/credit card **deposits** into the crypto-currency ATM. 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 H.B. 1642, HD1.

Carol Wakayama
Punchbowl District

LATE

SENATE COMMITTEE ON COMMERCE AND CONSUMER PROTECTION
Senator Jarrett Keohokalole, Chair
Senator Carol Fukunaga, Vice Chair

NOTICE OF HEARING
Tuesday, March 18, 2026, 9:30pm

Re: HB 1642, HD1 RELATING TO CONSUMER PROTECTION.

Aloha Chair Keohokalole and Vice Chairs Fukunaga, I am Linda Dorset and I am testifying in support of HB1642 HD1 which would establish critical safeguards for cryptocurrency transactions conducted through kiosks in Hawai‘i.

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.

House Bill 1642 HD1 is a reasonable, necessary, and consumer-focused response to these documented harms.

I respectfully urge you to PASS House Bill 1642, (although I prefer Senate Bill 2387). Both measures reflect 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. I don’t want to let perfect get in the way of good.

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

Linda Dorset
Maui Senior Citizen