

VERMONT DEPARTMENT OF FINANCIAL REGULATION

Report On Virtual Currency Kiosks Pursuant to 8 V.S.A. § 2577(g)

Effectiveness of Existing Protections and Recommendations for Additional Safeguards

January 15, 2025

To: House Committee on Commerce and Economic Development and
Senate Committee on Finance

From: Sandy Bigglestone, Acting Commissioner of Financial Regulation

8 V.S.A. § 2577(g) directs the Commissioner of Financial Regulation (the "Commissioner") to report to the House Committee on Commerce and Economic Development and to the Senate Committee on Finance on:

- a. Whether the requirements of 8 V.S.A. § 2577 ("Section 2577") applicable to virtual currency kiosks, coupled with relevant federal requirements, are sufficient to protect customers in Vermont from fraudulent activity;
- b. Recommendations for additional statutory or regulatory safeguards that the Commissioner deems necessary or appropriate; and
- c. Recommendations for enhanced oversight and monitoring of virtual currency kiosks for the purpose of minimizing their use for illicit activities as described in the U.S. Government Accountability Office report on virtual currencies, GAO-22-105462, dated December 2021.

The withdrawal of a large kiosk operator from Vermont, coupled with Section 2577's moratorium on new virtual currency kiosks until July 1, 2025, has reduced the number of cash-accepting virtual currency kiosks in Vermont by over 94%. There are currently only three virtual currency kiosks operating in Vermont. The unavailability of virtual currency kiosks has effectively protected customers in Vermont from fraudulent activity involving such kiosks since Section 2577 went into effect on July 1, 2024.

After the expiration of the moratorium, the Department of Financial Regulation (the "Department") expects the number of virtual currency kiosks to return to pre-moratorium levels. The Department anticipates that instances of fraud involving virtual currency kiosks will increase in tandem with the proliferation of new installations, but that Section 2577's \$1,000 daily transaction limit will substantially reduce the aggregate losses from scams that use such kiosks as a method of payment. The Department does not expect the \$1,000 daily transaction limit to completely prevent larger losses. The \$1,000 daily transaction limit will not be effective at reducing fraud losses under \$1,000.

The State of Connecticut recently passed legislation that imposes additional fraud protections for virtual currency kiosks, in addition to revising its pre-existing daily transaction limits.¹ The Commissioner recommends adopting variations of several of these additional safeguards in Vermont, including full refunds for new customers that file fraud reports, refunds of all fees for existing customers that file fraud reports, new minimum identity verification requirements, additional disclosure requirements for paper receipts, and requirements for mandatory phone screening of new customers over 60 and customers that engage in larger transaction volumes.

In preparation for this Report, the Department solicited and reviewed comments from the public and stakeholders. The Department received 13 submissions, including comments from Vermont Attorney General Charity Clark, AARP Vermont, two Vermont banks, the Vermont Bankers Association, four virtual currency kiosk operators, and three individuals. Although the Commissioner did not adopt all of the recommendations in the comment letters, it considered the points raised and recommends that the legislature consider these comments letters independently. Especially noteworthy are the views of Vermont Attorney General Charity Clark, who concludes that existing protections are insufficient and recommends extending the moratorium. Certain of the comment submissions are discussed within this report and all are included in full in Appendix A.

I. Background on Virtual Currency Kiosks and Fraudulent Activities.

Virtual currency kiosks are unstaffed machines that accept funds from consumers to buy and send virtual currency. They are also a popular payment method for scammers, who frequently employ virtual currency kiosks in connection with government impersonation, business impersonation, tech support, and other scams.² Criminals are known to give detailed instructions to their victims, including how to withdraw cash from their bank, locate a kiosk, and then use the kiosk to deposit the cash to buy and send virtual currency to the criminals in irreversible transfers.³

Federal Trade Commission (FTC) Consumer Sentinel Network data shows that reported fraud losses at virtual currency kiosks increased nearly tenfold from 2020 to 2023.⁴ When victims used virtual currency kiosks, their reported losses were especially high. In the first six months of 2024, the median loss reported by U.S. victims was \$10,000.⁵ People sixty years old and over were more than three times as likely as younger adults to report fraud losses involving virtual currency kiosks.⁶

¹ An Act Concerning Virtual Currency and Money Transmission, Conn. Pub. Act No. 24-146 (June 6, 2024), *available at* Appendix A.

² Emma Fletcher, *Bitcoin ATMs: A payment portal for scammers*, FED. TRADE COMM'N DATA SPOTLIGHT (Sept. 3, 2024),: <https://www.ftc.gov/news-events/data-visualizations/data-spotlight/2024/09/bitcoin-atms-payment-portal-scammers#edn4>

³ Federal Bureau of Investigation Cryptocurrency Fraud Report 2023: (2024), https://www.ic3.gov/Media/PDF/AnnualReport/2023_IC3CryptocurrencyReport.pdf

⁴Fletcher, *Bitcoin ATMs: A payment portal for scammers*, FED. TRADE COMM'N DATA SPOTLIGHT.

⁵ *Id.*

⁶ *Id.*

Vermont Attorney General Charity Clark reports that over the last three years the AGO's Consumer Assistance Program ("CAP") has received at least 45 reports of cryptocurrency frauds or scams, representing more than \$3 million in losses.⁷ Although not all reports specify the means of transfer, at least 14 reports (roughly one-third) indicated that virtual currency kiosks were used to perpetrate the scam. This likely reflects a small fraction of the actual harm, as Vermonters report complaints to many government agencies besides CAP,⁸ and the vast majority of fraud losses are never reported at all.⁹

II. Sufficiency of Existing Requirements in Section 2577 to Protect Customers in Vermont from Fraudulent Activity.

A Vermont money transmitter license has always been required to sell and transmit virtual currency using a virtual currency kiosk.¹⁰ Each kiosk location was required to be separately registered with and approved by the Department prior to operating.

To protect Vermont consumers from fraudulent activities involving virtual currency kiosks, the Vermont Legislature passed Act 110, which imposed several new requirements on virtual currency kiosk operators in 8 V.S.A. § 2577 ("Section 2577"), which became effective on July 1, 2024. The primary protective mechanisms in Section 2577 are:

- (a) the moratorium in 8 V.S.A. § 2577(f), which prohibits the operation of virtual currency kiosks in Vermont prior to July 1, 2025, but does not apply to virtual currency kiosks that were operational in Vermont on or before June 30, 2024 (the "Moratorium");
- (b) a \$1,000 daily transaction limit for cash purchases of virtual currency at money transmission kiosks (the "Transaction Cap"); and
- (c) a cap on fees for all virtual currency transactions at money transmission kiosks equal to the greater of \$5 or 3% of the transaction value (the "Fee Cap").

At the beginning of June 2024, there were five money transmitters engaging in virtual currency transactions using kiosks in the state of Vermont. Thirty-six cash-accepting kiosks were duly licensed and approved by the Department. Approximately twenty additional cash-accepting kiosks in Vermont were not registered with or approved by the Department.

⁷ Letter from Charity R. Clark, Attorney Gen., State of Vt., to Kevin Gaffney, Comm'r of Fin. Regul., Vt. Dept. of Fin. Regul. (Oct. 15, 2024), *available at* [Appendix C-1](#).

⁸ Complaints may be reported to local police, State's Attorneys, the Office of the Attorney General, the Federal Trade Commission, the Consumer Financial Protection Bureau, the U.S. Attorney's Office, the FBI, our Congressional delegation, and others. *See* Comment Letter from Charity Clark, Vermont Attorney General.

⁹ Fletcher, "Bitcoin ATMs: A payment portal for scammers," *Federal Trade Commission Data Spotlight*.

¹⁰ In 2015, the Department initiated Administrative Charges against PYC, Inc. and BLU-BIN, Inc. for the unlicensed operation of a virtual currency kiosk. *See In re PYC, Inc. and BLU-BIN, Inc.*, Docket No. 15-004-B; *see also* Taylor Dobbs, "State Regulators Force Vermont's Only Bitcoin ATM Offline," *Vermont Public* (February 17, 2015), *available at* <https://www.vermontpublic.org/vpr-news/2015-02-17/state-regulators-force-vermonts-only-bitcoin-atm-offline>

After the passage of Act 110 into law on May 20, 2024, the Department directed operators of unregistered kiosks to cease operations until such kiosks were duly registered and approved. None of these operators completed the registration and approval process prior to July 1, 2024.

Separately, in June of 2024, the largest virtual currency kiosk operator, which had thirty-three registered and approved kiosks in Vermont, voluntarily surrendered its money transmitter license.

This left only three registered and approved virtual currency kiosks operating in Vermont when the Moratorium went into effect on July 1, 2024.

A. Effectiveness of the Moratorium.

The unavailability of virtual currency kiosks in Vermont due to the Moratorium has effectively protected consumers from fraudulent transactions involving virtual currency kiosks.

The Moratorium in 8 V.S.A. § 2577(f) prohibits the operation of virtual currency kiosks¹¹ in Vermont prior to July 1, 2025, but does not apply to virtual currency kiosks that were operational in Vermont on or before June 30, 2024. The Department of Financial Regulation interpreted the grandfather clause in the Moratorium as only applying to *legally* operational kiosks, where the operator was duly licensed as a Vermont money transmitter and the kiosk was duly registered and approved by the Department. Only three virtual currency kiosks in the state met these requirements on July 1, 2024.

On July 1, 2024, the Department ceased accepting, considering or approving virtual currency kiosk registration applications, including any pending applications for unregistered kiosks that may have operated in violation of Vermont law prior to July 1, 2024. Applicants who wished to avoid denial of their application were directed to withdraw any pending, unapproved applications. To ensure that the Department’s registration and approval process will incorporate any subsequently enacted legal requirements, the Department does not intend to accept new kiosk registration applications until the weeks prior to the expiration of the Moratorium.

¹¹ The term “virtual currency kiosk” is not defined. But based on the definition of “virtual currency kiosk operator” in 8 V.S.A. § 2503(31), the Department interprets the term “virtual currency kiosk” to mean “a money transmission kiosk located in this State through which virtual-currency business activity is offered.” The Department applied the Moratorium to all such money transmission kiosks, including those that do not accept cash and only allow transactions by ATM cards. This resulted in Moon, Inc. *dba* LibertyX, a company that accepts ATM card payments for virtual currency purchase through certain traditional ATMs, ceasing to offer such services at several traditional ATMs in Vermont during the Moratorium. In its comment letter, Moon, Inc. *dba* LibertyX advocates for an exemption for devices that utilize debit card readers solely for payment processing without accepting cash, whether standalone or integrated into an ATM, vending machine, or any other hardware, used exclusively for processing card payments. *See* Letter from Simon Spektor, Chief Counsel & Compliance Officer, Moon, Inc. *dba* LibertyX, to Kelley Reed, Regulatory and Consumer Affairs Dir., Banking Div., Vt. Dept. of Fin. Regul. (Sept. 19, 2024), *available at* [Appendix C-13](#). Because it will not reduce fraud risk, the exemption requested by Moon, Inc. *dba* LibertyX is outside the scope of the Commissioner’s recommendations in this report.

The large reduction in virtual currency kiosks operating in Vermont immediately prior to the Moratorium, combined with the inability of licensees to register new kiosks during the Moratorium, has resulted in a corresponding drop in virtual currency kiosk transactions. According to quarterly call report data filed with the Department, the number of transactions reported by all licensed virtual currency kiosk operators in Vermont dropped by over 96% from the Second Quarter of 2024¹² to the Third Quarter of 2024.¹³ The general unavailability of virtual currency kiosks due to the Moratorium has been singularly effective in reducing the amount of fraudulent activity involving virtual currency kiosks.

As the scheduled expiration of the Moratorium approaches on July 1, 2025, the Department anticipates a significant influx of applications for new kiosks. The Department received several kiosk registration applications in the week immediately prior to the Moratorium going into effect. And the Department has received multiple inquiries from licensees seeking to register additional kiosk locations during the Moratorium, including in each of the thirty-three locations where registered kiosks ceased operating prior to the Moratorium.

The Vermont Attorney General's Office supports a moratorium on virtual currency kiosks until federal and state government and regulatory agencies with appropriate oversight powers can guarantee Vermont consumers will be protected from, or have adequate access to remedies relating to, criminal activity connected to virtual currency kiosks located in Vermont.¹⁴ But for purposes of evaluating the sufficiency of the existing protections in Section 2577, this Report assumes that the Moratorium will not be extended.

B. Effectiveness of the Daily Transaction Limit.

The Commissioner believes that the \$1,000 daily transaction limit for cash transactions at virtual currency kiosks will be partially effective at protecting consumers, by making it substantially more difficult and time consuming to send large amounts of funds to scammers using virtual currency kiosks. The daily transaction limit will not be effective at protecting consumers from fraud losses of \$1,000 dollars or less, which are the most reported scams.

1. The Commissioner Believes the Daily Transaction Limit Will be Effective at Reducing Large Losses.

The unavailability of virtual currency kiosks in Vermont due to the Moratorium has resulted in a lack of Vermont-specific data to evaluate the effectiveness of the remaining protective provisions of Section 2577. But based on the Department's research and discussions with regulators in other states that have enacted similar limits, the Commissioner believes the \$1,000 daily transaction

¹² The three-month period ending on June 30, 2024, the quarter immediately prior to the effective date of the Moratorium.

¹³ The three-month period ending on September 30, 2024, the quarter beginning on the effective date of the Moratorium.

¹⁴ Letter from Charity R. Clark, Attorney Gen., State of Vt., to Kevin Gaffney, Comm'r of Fin. Regul., Vt. Dept. of Fin. Regul. (Oct. 15, 2024), available at [Appendix C-1](#).

limit for cash purchases will reduce the amount of large fraud losses involving kiosks, by making it more difficult and time consuming to send large amounts of funds to criminals.

A common tactic of scammers is to induce an overwhelming sense of false urgency and panic, that overrides a victim's critical thinking and judgement. The scammer will convince the victim that bad things will happen imminently if the victim doesn't act. For example, a scammer might convince a victim that a hacker will empty their bank account at any moment, unless the victim withdraws and unwittingly transfers their funds to the scammer first. In the scammer's telling, there is no time for second opinions or investigation. If the victim hesitates, the scammer promises that bad things will happen. There are countless variations of this fact pattern. The longer it takes a victim to transfer their funds to the scammers, the more likely it is that the haze of false urgency and deception will lift.

International criminals favor virtual currency kiosks due to the speed and ease with which victims can convert large amounts of cash into virtual currency and instantly transfer it out of the country. This is because in-person transactions initiated using cash or ATM cards at virtual currency kiosks typically settle instantly and aren't subject to the same clearance and settlement times as online credit card purchases or electronic funds transfers from a bank to an online virtual currency seller or exchange. Before the imposition of the daily transaction limits, a victim could deposit \$10,000 or more into a virtual currency kiosk and transfer the funds to scammers in a matter of minutes. With the \$1,000 daily transaction limit in place, a victim would have to repeatedly return to the same machine over the course of 10 days to transfer the same amount.

In addition to Vermont, several other states have adopted daily transaction limits that went into effect in 2024. These daily limits are so new, that data and analysis regarding their effectiveness and impact on fraud losses isn't generally available. But preliminary analysis and anecdotal reports from law enforcement and regulators in other states suggest that similar daily transaction limits have meaningfully reduced fraud losses involving virtual currency kiosks.

Anthony Moore, a detective for the Fraud and Cybercrimes Bureau at the Los Angeles County Sheriff's Department (LASD) filed a Declaration¹⁵ in connection with a 2024 lawsuit brought by The Alliance for the Fair Access to Cryptocurrency Terminals against the State of California, challenging the statute imposing a similar \$1,000 daily transaction limit.¹⁶ Detective Moore used blockchain analytics software to analyze transfers from kiosks to digital wallet addresses with known associations with fraud and human trafficking and detailed the results in his Declaration to the Court, concluding that multiple virtual currency kiosk operators in California had seen a substantial reduction in the dollar amounts of transactions attributed to scams, fraud and human trafficking since the \$1,000 daily transaction limit under California law took effect:

¹⁵ Decl. of Anthony Moore in Supp. of D.'s Opp'n to Mot. for Prelim. Inj., All. for the Fair Access to Cryptocurrency Terminals v. St. of Cal., No. 23STCP04679 (Cal. Super. Ct., Cnty. of L.A.)(April 22, 2024), *available at* [Appendix B](#).

¹⁶ The Superior Court for the District of Los Angeles dismissed the lawsuit on August 30, 2024. The Alliance for the Fair Access to Cryptocurrency Terminals has appealed the dismissal .

14. As part of my primary duties at LASD, I regularly use Chainalysis in my investigation of cryptocurrency crimes, including crypto kiosk crimes. I have reviewed the data provided by Chainalysis since the daily transaction limit set forth in SB 401 took effect on January 1, 2024. I have determined that there is a reduction in crypto kiosk scams and fraud since the daily transaction limit became effective. I have also determined that there has been a reduction in the use of crypto kiosks for escort services which are known to involve human trafficking.

...

16. I have reviewed the data for 2023 and year-to-date 2024 transactions for RockItCoin, LLC (RockItCoin) – a member of Alliance for the Fair Access to Cryptocurrency Terminals who is the plaintiff in this action. RockItCoin has crypto kiosk locations throughout the nation including Puerto Rico. It also has a significant presence in California with crypto kiosks located throughout the state. In reviewing the data, I determined that the dollar amounts of RockItCoin transactions attributed to scams, fraud, and human trafficking has significantly decreased in the first quarter of 2024 compared to the first quarter of 2023.

17. The dollar amounts of RockItCoin transactions attributed to fraud from January through March of 2023 totaled \$102,043.10. This is a conservative number because it only accounts for transactions that Chainalysis analysts have definitively determined was attributed to fraud. The dollar amounts of RockItCoin transactions attributed to fraud from January through March of 2024 totaled \$1,133.86, a significant decrease compared to the first quarter of 2023.

18. The dollar amounts of RockItCoin transactions attributed to scams from January through March of 2023 totaled \$257,237.38. This is also a conservative number because it only accounts for transactions that Chainalysis analysts have definitively determined was attributed to scams. The dollar amounts of RockItCoin transactions attributed to scams from January through March of 2024 totaled \$2,298.16, a significant decrease compared to the first quarter of 2023.

19. Crypto kiosks have frequently been used to facilitate human trafficking. The dollar amounts of RockItCoin transactions attributed to human trafficking from January through March of 2023 totaled \$20,982.26. This is also a conservative number because it only accounts for transactions that Chainalysis analysts have definitively determined was attributed to human trafficking. The dollar amounts of RockItCoin transactions attributed to human trafficking from January through March of 2024 totaled \$117.59, a significant decrease compared to the first quarter of 2023.

20. The Chainalysis data I have reviewed shows that RockItCoin is not the only crypto kiosk company that has seen a substantial reduction in the dollar amounts of transactions attributed to scams, fraud and human trafficking since the daily transaction limit under SB 401 took effect. It is just one example demonstrating that the daily transaction cap is serving its intended purpose of reducing crypto kiosk crime.

2. Large Fraud Losses Remain Possible.

Although the Commissioner believes that the \$1,000 daily transaction limit will be effective at reducing the amount of large losses from fraudulent transactions involving virtual currency kiosks in Vermont, it will not be completely effective. Many of the largest and most devastating frauds stretch over long periods of time and involve multiple transfers of funds. Scammers may direct victims to visit multiple kiosks operated by different operators over many days. Scammers may also direct victims to out-of-state kiosks that have no transaction limits or employ payment methods other than virtual currency kiosks.

The Department has also heard anecdotal reports from regulators in other states of illicit actors using multiple accounts under different names to circumvent daily transaction limits.

3. The Daily Transaction Limit Will Not Protect Against Fraud Losses Under \$1,000.

The most reported frauds involve losses under \$1,000. The Federal Trade Commission reports that the median reported loss in its Consumer Sentinel database of nationwide 2023 fraud reports was \$500 for all payment methods (i.e., not limited to virtual currency kiosks).¹⁷ Of the 2023 fraud reports that included loss amounts, over 60% involved losses under \$1,000 and less than 15% involved losses over \$10,000.¹⁸ For Vermont, the median reported fraud loss in 2023 was \$400 for all payment methods.¹⁹ The \$1,000 daily transaction limit will do nothing to prevent fraud losses under \$1,000. These fraud losses may be especially hard on vulnerable and lower-income Vermonters.²⁰

4. The Daily Transaction Limit Does Not Protect Against Fraud Losses from Non-Cash Transactions.

The \$1,000 Daily Transaction Limit does not apply to non-cash transactions or to transactions other than virtual currency transactions. The Department is not aware of complaints regarding fraudulent transactions in Vermont involving non-cash payments at virtual currency kiosks.²¹ That could change in the future if virtual currency kiosk operators pivot to other transaction offerings and payment structures in response to the Daily Transaction Limit and Fee Cap.

¹⁷ Fed. Trade Commission, *Consumer Sentinel Data Book 2023* (February 2024), *available at* https://www.ftc.gov/system/files/ftc_gov/pdf/CSN-Annual-Data-Book-2023.pdf

¹⁸ *Id.*

¹⁹ *Id.*

²⁰ Matt Schulz, *49% of Americans Can't Afford a \$1,000 Emergency, With Many Relying on Credit Cards for Unexpected Expenses* (December 11, 2023), *available at* <https://www.lendingtree.com/debt-consolidation/emergency-savings-survey/> (According to a 2023 Lending Tree poll, 49% of Americans can't cover a \$1,000 emergency out of cash or savings. 70% of Americans making less than \$35,000 a year can't cover a \$1,000 emergency.).

²¹ Moon, Inc., *dba LibertyX* argues in its comment letter that virtual currency transactions where payment is made via ATM debit card readers are subject to additional safeguards that do not apply to cash transactions. The Department has not verified or evaluated the veracity of these arguments. *See* Letter from Simon Spektor, Chief Counsel & Compliance Officer, Moon, Inc. *dba LibertyX*, to Kelley Reed, Regulatory and Consumer Affairs Dir., Banking Div., Vt. Dept. of Fin. Regul. (Sept. 19, 2024), *available at* [Appendix C-10](#).

5. Interplay Between Daily Transaction Limits and Federal Reporting Requirements.

Three virtual currency kiosk companies, GPD Holdings LLC *dba* Coinflip, Byte Federal, Inc., and Bitcoin Depot (collectively, the “Commenting Kiosk Companies”), each submitted comment letters that argued (among other things) that the \$1,000 daily transaction limit hinders their ability to fulfill their compliance obligations, particularly in filing FinCEN reports, including Currency Transaction Reports (CTRs) and Suspicious Activity Reports (SARs). The Commenting Kiosk Companies each note that they are required to file a SAR for any suspected suspicious transactions above \$2,000 and a CTR for transactions above \$10,000. These reports are important tools for law enforcement to detect illicit activity. The Commenting Kiosk Companies argue that the \$1,000 daily transaction limit will encourage customers to stack transactions across multiple kiosk companies, which will make it more difficult for each of them to detect suspicious activity and reduce the number of transactions that meet the federal reporting thresholds for SARs and CTRs. The Commenting Kiosk Companies argue that the daily transaction limit therefore undermines the effectiveness of these federal reporting requirements.

No similar concerns have ever been expressed to the Department or the Commissioner by law enforcement or regulatory agencies. The Department is not aware of any state, local, or federal law enforcement or regulatory agencies that share the Commenting Kiosk Companies’ concerns about this issue.

The Department believes that the reduction in high-dollar fraud losses suffered by consumers and the disruption of illicit activity caused by the Daily Transaction Limit more than offsets the purported harm resulting from any reduction in reporting of large transactions or suspicious activities that may occur.

C. Effectiveness of the Fee Cap.

Section 2577(b) provides that the aggregate fees and charges, directly or indirectly, charged to a customer related to a single transaction or series of related transactions involving virtual currency effected through a money transmission kiosk in Vermont, including any mark-ups over the prevailing market value, shall not exceed the greater of \$5.00 or three percent (3%) of the transaction value.

The Fee Cap was primarily intended to protect consumers from excessive fees. The Fee Cap was also expected to slow the proliferation of virtual currency kiosks in Vermont, which may indirectly protect Vermont customers from fraudulent activity. Each of the Commenting Kiosk Companies claim that the Fee Cap does not provide for sufficient revenue to cover the costs of operating a virtual currency kiosk in Vermont and would discourage Companies from adopting more robust and expensive anti-fraud procedures. Nevertheless, the Department has been contacted by many companies seeking to register Kiosks since the passage of Act and believes that the impact on the proliferation of virtual currency kiosks in Vermont will be substantially less than initially anticipated.

In their comment letters, each of the Commenting Kiosk Companies assert that the fees allowed under the Fee Cap are insufficient to cover the costs of operating their virtual currency kiosks. Such costs include, among other things, the costs of acquiring, installing and maintaining the

physical kiosk machines, and the costs of securely collecting physical cash from kiosks, and the costs of compliance and anti-fraud measures. The Commenting Kiosk Companies claim that the combined effect of the Daily Transaction Limits and the Fee Cap is that they cannot profitably operate virtual currency kiosks in Vermont under the existing law.

The Commenting Kiosk Companies also argue that these impacts create incentives for less employment of more robust practices to prevent fraud and protect consumers. Examples of such practices may include, without limitation:

- Integrating blockchain analytics software to prevent transfers to known fraudulent and illicit digital wallet addresses;
- Providing live customer support and assistance from personnel trained to spot fraud and assist victims;
- Employing enhanced customer screening procedures, which may include calling high risk consumers to screen out potential scam victims;
- Refunding fees incurred in fraudulent transactions; and
- Performing active and continuous fraud monitoring.

An impact of the Fee Cap may be that the most conscientious kiosk operators can't afford to operate in the state, and the operators that remain will be those with the lowest costs. And the operators with the lowest cost may be less likely to employ costly non-mandatory fraud prevention practices.

The Commissioner believes kiosk operators will ultimately do what is in their economic best interests, and that Vermont law should not incentivize cost minimization at the expense of fraud prevention. But the economic imperative for kiosk operators to minimize costs will be fundamentally misaligned with the fraud prevention interests of consumers and regulators, as long as:

- (a) the costs of fraud losses are born exclusively by consumers, and not kiosk operators;
- (b) kiosk operators profit from fees earned on fraudulent transactions; and
- (c) spending on effective fraud prevention measures only increases kiosk operators' costs and reduces their profits.

To address this misalignment of interests, the Commissioner's Recommendations for Additional Statutory and Regulatory Safeguards in Section III, below, include adopting mandatory refund requirements for fraudulently induced transactions. These refund requirements shift all or a portion of the costs of fraud losses to the kiosk operator, such that it will be in the kiosk operator's economic interests to prevent fraud losses.

The Commissioner also recommends mandating certain additional practices and procedures to raise the minimum standards that all licensees must satisfy, including adopting mandatory customer identification protocols, additional disclosure and receipt requirements, and enhanced customer screening and support for customers over 60 years of age and customers that engage in more than \$5,000 of transactions during any consecutive 10-day period.

Because the additional requirements recommended by the Commissioner will require kiosk operators to incur additional costs, the Commissioner recommends that the Legislature consider raising the amount of the Fee Cap. Raising the Fee Cap could potentially result in more virtual currency kiosks operating in Vermont.

III. Recommendations for Additional Statutory or Regulatory Safeguards.

Section 2577(g) requires that this report include recommendations for additional statutory or regulatory safeguards that the Commissioner deems necessary or appropriate to protect against fraudulent transactions and recommendations for enhanced oversight and monitoring of virtual currency kiosks for the purpose of minimizing their use for illicit activities as described in the U.S. Government Accountability Office report on virtual currencies, GAO-22-105462, dated December 2021. There is substantial overlap in the Commissioner’s recommendations aimed at fraud protection and the recommendations intended to enhance oversight and monitoring of virtual currency kiosks for the purpose of minimizing their use for illicit activities. The discussion of these recommendations is combined in this Section III.

The Commissioner recommends enhancing consumer protections by requiring full and partial refund requirements for fraudulent transactions. The Commissioner also recommends adopting mandatory customer identification protocols, additional disclosure and receipt requirements, and enhanced customer screening and support for customers over 60 years of age and customers that engage in more than \$5,000 of transactions during any consecutive 10-day period.

Except where otherwise noted, the majority of the Commissioner’s recommendations are based, in-part, on additional safeguards and requirements adopted by the State of Connecticut on June 6, 2024, pursuant to Public Act No. 24-146 (“CT Act 24-146”).²²

Refund Requirements:

The Commissioner recommends adding the following mandatory refund requirements for fraudulent transactions to Section 2577:

- Full Refunds for New Customers: Require full refunds for fraudulent transactions within the first seven days from and after a Vermont customer's first kiosk transaction.²³ This offers immediate protection to new users who are most vulnerable to scams and fraud.

²² An Act Concerning Virtual Currency and Money Transmission, CONN. PUB. ACT NO. 24-146 (June 6, 2024), *available at Appendix A.*

²³ CT Act 24-146 amends Conn. Gen. Stat. § 36a-613(h) to require full refunds for “any fraudulent virtual currency transactions that occurred not later than seventy-two hours after the new customer registered as a customer of such owner or operator....” AARP Vermont recommended extending the full refund period for transactions by new customers during their first 30 days. See Letter from Greg Marchildon, State Dir., AARP Vt., to Kelley Reed, Regulatory and Consumer Affairs Dir., Banking Div., Vt. Dept. of Fin. Regul. (Oct. 14, 2024), *available at Appendix C-3.* This report recommends extending the period of refundable transactions to seven days after a customer’s first transactions at a virtual currency kiosk. The recommendation does not tie the refund period to the date of registration, because the Department has heard anecdotal reports of criminals providing victims with pre-existing account credentials to use for kiosk transactions.

- Fee Refunds for Existing Customers: For fraudulent transactions that occur after the first 7 days after a customer's initial kiosk transaction, require the refund of all fees associated with the fraudulent transactions.²⁴ This provides partial recovery for victims and incentivizes kiosk operators to screen out fraud.
- Reporting and Request Timeline: In order to receive a refund, a customer must report the fraud to a law enforcement or regulatory agency and request a refund within 6 months after the last fraudulent transaction.²⁵ The reporting requirement will deter false claims, encourages prompt reporting and ensure timely redressal.
- Scope of Fraudulent Transactions: The refund requirements will apply to both authorized and unauthorized fraudulent transaction, as scammers frequently trick victims into authorizing transactions.

Additional Protections:

Based on CT Act 24-146, the Department recommends the following:

1. Customer Identification: Collect detailed customer information, including government-issued ID,²⁶ name, date of birth, address, telephone number and e-mail address before accepting payment from a customer in connection with any transactions at a virtual currency kiosk.
2. Customer Support: Provide live telephone support during kiosk operation hours.²⁷ Accessible support can assist consumers in real-time, potentially preventing fraudulent transactions.
- : 3. Mandatory Live Screening of Older Customers: Require operators to identify and speak with new customers over age sixty by telephone before their first transaction to discuss potential fraud.²⁸ During such communication, which shall be recorded and retained by such operator, the

²⁴ Refunding fees for existing customers is not included in CT Act 24-146, but was recommended by AARP Vermont. *See* Letter from Greg Marchildon, State Dir., AARP Vt., to Kelley Reed, Regulatory and Consumer Affairs Dir., Banking Div., Vt. Dept. of Fin. Regul. (Oct. 14, 2024), *available at* [Appendix C-3](#). At least two virtual kiosk operators claim to already refund fees of fraud victims.

²⁵ CT Act 24-146 amends Conn. Gen. Stat. § 36a-613(h) to condition the full refund requirement on victims filing a report with a government or law enforcement agency memorializing the fraudulent nature of the transaction and contacting the owner or operator of the kiosk with 30 days. Because scams may continue for longer periods of time, this report recommends giving victims 6 months after the last fraudulent transaction to report.

²⁶ CT Act 24-146 amends Conn. Gen. Stat. § 36a-613(1)(i) to require obtaining a copy of a government-issued identification card that identifies each customer.

²⁷ CT Act 24-146 amends Conn. Gen. Stat. § 36a-613(1)(i)(6) to require kiosk operators to offer, during the hours of operation of the virtual currency kiosks, live customer support by telephone from a telephone number prominently displayed at or on such virtual currency kiosks.

²⁸ CT Act 24-146 amends Conn. Gen. Stat. § 36a-613(1)(i)(7) to require operators to identify and speak by telephone with any new customer over sixty years of age prior to such new customer completing such new customer's first virtual currency transaction with such operator. During such communication, which shall be recorded and retained by such owner or operator, the owner or operator shall (A) reconfirm any

operator shall (A) positively identify such customer, (B) reconfirm any attestations made by such new customer at a virtual currency kiosk owned or operated by such operator, (C) discuss the transaction and (D) discuss types of fraudulent schemes relating to virtual currency. This demographic is often targeted by scammers, and direct communication can serve as a preventive measure.

4. Mandatory Live Screening of Customers that Engage in More Than \$5,000 of Transactions During any Consecutive 10-day Period. Require operators to identify and speak with customers by telephone if such customers are attempting to conduct more than \$5,000 of virtual currency transactions during any consecutive 10-day period.²⁹ During such communication, which shall be recorded and retained by such operator, the operator shall (A) positively identify such customer, (B) review such customer's stated purpose of the transaction, and (C) discuss types of fraudulent schemes relating to virtual currency.

Receipt and Transfer Record Requirements:

- Receipts: Require paper receipts that include public wallet addresses, the full name of the account owner,³⁰ unique transaction identifiers, and a mandatory statement of the fraud victim refund policy.³¹ This information will help consumers and law enforcement in the event of fraudulent transactions.
- Records: In addition to mandatory paper receipts, require licensees to email customers details of virtual currency transfers, including wallet addresses and transaction identifiers. This provides consumers with a digital record for reference.

Recommendation on Fee Cap Reconsideration:

If the Legislature chooses to adopt the Commissioner's recommendations above, the Commissioner recommends that the Legislature reconsider the current fee cap imposed on virtual currency kiosk transactions. Multiple kiosk operators have represented to the Department that the current fee caps result in the revenue from Vermont Kiosks transactions being insufficient to cover the existing operational costs associated with the virtual currency kiosk business model.

attestations made by such new customer at a virtual currency kiosk owned or operated by such operator, (B) discuss the transaction, and (C) discuss types of fraudulent schemes relating to virtual currency. Such operator's approval of the transaction shall be dependent upon such operator's assessment of such communication.

²⁹ CT Act 24-146 amends Conn. Gen. Stat. § 36a-613(1)(i)(8) to require operators to identify and speak by telephone with any new customer attempting to perform a virtual currency transaction that exceeds an amount that has been predesignated by such owner or operator as a large transaction amount before such transaction may be completed. This report recommends a similar requirement for any customer engaging in larger transactions.

³⁰ Scammers are known to direct victims to use pre-existing accounts set up by the scammers. We have heard anecdotal reports of victims first realizing they were scammed when they saw someone else's name on their receipt.

³¹ CT Act 24-146 amends Conn. Gen. Stat. § 36a-613(e) to impose substantially similar receipt requirements.

Adopting the recommended additional requirements will add additional compliance costs, which the existing Fee Cap may not support. Other jurisdictions have imposed a fee cap of 15%.

INDEX OF APPENDICES

Appendix A – Connecticut Act Concerning Virtual Currency and Money Transmission

An Act Concerning Virtual Currency and Money Transmission, CONN. PUB. ACT NO. 24-146 (June 6, 2024) Appendix A

Appendix B – Declaration of Detective Anthony Moore

Decl. of Anthony Moore in Supp. of D.’s Opp’n to Mot. for Prelim. Inj., *All. for the Fair Access to Cryptocurrency Terminals v. St. of Cal.*, No. 23STCP04679 (Cal. Super. Ct., L.A. Cnty.)(April 22, 2024)..... Appendix B

Appendix C - Comment Letters

Law Enforcement Comments

Letter from Charity R. Clark, Attorney Gen., State of Vt., to Kevin Gaffney, Comm'r of Fin. Regul., Vt. Dept. of Fin. Regul. (Oct. 15, 2024)..... Appendix C-1

Nonprofit Comments

E-mail from Christopher D’Elia, President, Vt. Bankers Ass'n, to Kelley Reed, Regulatory and Consumer Affairs Dir., Banking Div., Vt. Dept. of Fin. Regul. (Sept. 26, 2024, at 11:04 ET). Appendix C-2

Letter from Greg Marchildon, State Dir., AARP Vt., to Kelley Reed, Regulatory and Consumer Affairs Dir., Banking Div., Vt. Dept. of Fin. Regul. (Oct. 14, 2024)..... Appendix C-3

Bank Comments

E-mail from Christine Martin, BSA Officer, Northfield Savings Bank, to Kelley Reed, Regulatory and Consumer Affairs Dir., Banking Div., Vt. Dept. of Fin. Regul. (Sept. 18, 2024, at 13:47 ET). Appendix C-4

E-mail from Robert F. O’Neill, Security Officer, Northfield Savings Bank, to Kelley Reed, Regulatory and Consumer Affairs Dir., Banking Div., Vt. Dept. of Fin. Regul. (Sept. 20, 2024, at 15:23 ET) Appendix C-5

E-mail from Kim Scott, AVP Fraud Detection Officer, Mascoma Bank, to Kelley Reed, Regulatory and Consumer Affairs Dir., Banking Div., Vt. Dept. of Fin. Regul. (Oct. 9, 2024, at 16:06 ET). Appendix C-6

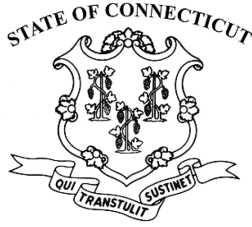
Individual Comments

E-mail from Greg Nixon, to Kelley Reed, Regulatory and Consumer Affairs Dir., Banking Div., Vt. Dept. of Fin. Regul. (Sept. 18, 2024, at 7:39 ET). Appendix C-7

E-mail from Martin P. Wagner, to Kelley Reed, Regulatory and Consumer Affairs Dir., Banking Div., Vt. Dept. of Fin. Regul. (Sept. 18, 2024, at 9:01 ET).	Appendix C-8
E-mail from Tom Cooper, to Kelley Reed, Regulatory and Consumer Affairs Dir., Banking Div., Vt. Dept. of Fin. Regul. (Sept. 19, 2024, at 18:17 ET).	Appendix C-9
Virtual Currency Kiosk Operators	
Letter from Simon Spektor, Chief Counsel & Compliance Officer, Moon, Inc. dba LibertyX, to Kelley Reed, Regulatory and Consumer Affairs Dir., Banking Div., Vt. Dept. of Fin. Regul. (Sept. 19, 2024).	Appendix C-10
Letter from Mark Paolillo, CFO and CCO, Byte Federal, Inc., to Kelley Reed, Regulatory and Consumer Affairs Dir., Banking Div., Vt. Dept. of Fin. Regul. (Sept. 24, 2024).	Appendix C-11
Letter from Mark J. Smalley, Chief Compliance Officer, Bitcoin Depot, to Vt. Dept. of Fin. Regul. (Oct. 11, 2024).	Appendix C-12
CoinFlip’s Written Comments on 8 V.S.A. § 2577(g) (Oct. 15, 2024).....	Appendix C-13

APPENDIX A

An Act Concerning Virtual Currency and Money Transmission, CONN. PUB. ACT
No. 24-146 (June 6, 2024)



Substitute House Bill No. 5211

Public Act No. 24-146

AN ACT CONCERNING VIRTUAL CURRENCY AND MONEY TRANSMISSION.

Be it enacted by the Senate and House of Representatives in General Assembly convened:

Section 1. Section 36a-596 of the 2024 supplement to the general statutes is repealed and the following is substituted in lieu thereof (*Effective October 1, 2024*):

As used in sections 36a-595 to [36a-613] 36a-614, inclusive, as amended by this act, unless the context otherwise requires:

(1) "Advertise" or "advertising" has the same meaning as provided in section 36a-485.

(2) "Authorized delegate" means a person designated by a person licensed pursuant to sections 36a-595 to 36a-612, inclusive, to provide money transmission services on behalf of such licensed person.

(3) "Control" means (A) the power to vote, directly or indirectly, at least twenty-five per cent of the outstanding voting shares or voting interests of a licensee or person in control of a licensee, [;] (B) the power to elect or appoint a majority of key individuals or executive officers, managers, directors, trustees or other persons exercising managerial authority of a person in control of a licensee, [;] or (C) the power to

Substitute House Bill No. 5211

exercise, directly or indirectly, a controlling influence over the management or policies of a licensee or person in control of a licensee. For purposes of this subdivision, [:] (i) [A] a person is presumed to exercise a controlling influence when the person holds the power to vote, directly or indirectly, at least ten per cent of the outstanding voting shares or voting interests of a licensee or person in control of a licensee, (ii) a person presumed to exercise a controlling influence can rebut such presumption if the person is a passive investor, and (iii) to determine the percentage of control, a person's interest shall be aggregated with the interest of any other immediate family member, including the person's spouse, parent, child, sibling, mother-in-law, father-in-law, son-in-law, daughter-in-law, brother-in-law, sister-in-law and any other person who shares the person's home.

(4) "Control person" means any individual in control of a licensee or applicant, any individual who seeks to acquire control of a licensee or a key individual.

(5) "Electronic payment instrument" (A) means a card or other tangible object (i) for the transmission of money or monetary value or payment of money, (ii) which contains a microprocessor chip, magnetic stripe [,] or other means for the storage of information, (iii) that is prefunded, and (iv) for which the value is decremented upon each use, [but] and (B) does not include a card or other tangible object that is redeemable by the issuer in the issuer's goods or services.

(6) "Existing customer" means a consumer who (A) is engaging in a transaction at a virtual currency kiosk in the state, (B) has performed not fewer than three virtual currency transactions with the owner or operator of such virtual currency kiosk, and (C) has been registered as a customer of such owner or operator for more than seventy-two hours.

[(6)] (7) "Holder" means a person, other than a purchaser, who is either in possession of a payment instrument and is the named payee

Substitute House Bill No. 5211

thereon or in possession of a payment instrument issued or endorsed to such person or bearer or in blank. "Holder" does not include any person who is in possession of a lost, stolen or forged payment instrument.

[(7)] (8) "Key individual" means any individual ultimately responsible for establishing or directing policies and procedures of the licensee, including, but not limited to, an executive officer, manager, director or trustee.

[(8)] (9) "Licensee" means any person licensed or required to be licensed pursuant to sections 36a-595 to 36a-612, inclusive.

[(9)] (10) "Main office" has the same meaning as provided in section 36a-485.

[(10)] (11) "Monetary value" means a medium of exchange, whether or not redeemable in money.

[(11)] (12) "Money transmission" means engaging in the business of issuing or selling payment instruments or stored value, receiving money or monetary value for current or future transmission or the business of transmitting money or monetary value within the United States or to locations outside the United States by any and all means including, but not limited to, payment instrument, wire, facsimile, electronic transfer or virtual currency kiosk.

(13) "New customer" means a consumer who (A) is engaging in a transaction at a virtual currency kiosk in the state, (B) has performed fewer than three virtual currency transactions with the owner or operator of such virtual currency kiosk, and (C) has been registered as a customer of such owner or operator for less than seventy-two hours.

[(12)] (14) "Outstanding" means (A) in the case of a payment instrument or stored value, that [:] (i) [It] such instrument or value is sold or issued in the United States, [:] (ii) a report of [it] such instrument

Substitute House Bill No. 5211

or value has been received by a licensee from its authorized delegates, [;] and (iii) [it] such instrument or value has not yet been paid by the issuer, and (B) for all other money transmissions, the value reported to the licensee for which the licensee or any authorized delegate has received money or its equivalent value from the customer for transmission, but has not yet completed the money transmission by delivering the money or monetary value to the person designated by the customer.

[(13)] (15) "Passive investor" means a person that [:] (A) [Does] does not have the power to elect a majority of key individuals or executive officers, managers, directors, trustees or other persons exercising managerial authority of a person in control of a licensee, [;] (B) is not employed by and does not have any managerial duties of the licensee or person in control of a licensee, [;] (C) does not have the power to exercise, directly or indirectly, a controlling influence over the management or policies of a licensee or person in control of a licensee, [;] and (D) attests to subparagraphs (A), (B) and (C) of this subdivision in the form and manner prescribed by the commissioner.

[(14)] (16) "Payment instrument" means a check, draft, money order, travelers check or electronic payment instrument that evidences either an obligation for the transmission of money or monetary value or payment of money, or the purchase or the deposit of funds for the purchase of such check, draft, money order, travelers check or electronic payment instrument.

[(15)] (17) "Permissible investment" means [:] (A) [Cash] (i) cash in United States currency, [;] including, but not limited to, demand deposits, savings deposits and funds in demand deposit and savings deposit accounts held for the benefit of a licensee's customers in an insured depository institution, and (ii) cash equivalents, including, but not limited to, (I) automated clearing house items in transit to a licensee or payee, (II) international wires in transit to a payee, (III) cash in transit

Substitute House Bill No. 5211

via armored car, (IV) cash in smart safes, (V) cash in locations owned by licensees, (VI) transmission receivables that are funded by debit cards or credit cards and owed by any bank, and (VII) money market mutual funds rated "AAA" or the equivalent by S & P Global, Incorporated, in the "S & P Global Ratings" or by any other rating service recognized by the commissioner, (B) time deposits, as defined in section 36a-2, or other debt instruments of a bank, [;] (C) bills of exchange or bankers acceptances which are eligible for purchase by member banks of the Federal Reserve System, [;] (D) commercial paper of prime quality, [;] (E) interest-bearing bills, notes, bonds, debentures or other obligations issued or guaranteed by [;] (i) [The] the United States or any of its agencies or instrumentalities, or (ii) any state, or any agency, instrumentality, political subdivision, school district or legally constituted authority of any state if such investment is of prime quality, [;] (F) interest-bearing bills or notes, or bonds, debentures or preferred stocks, traded on any national securities exchange or on a national over-the-counter market, if such debt or equity investments are of prime quality, [;] (G) receivables due from authorized delegates consisting of the proceeds of the sale of payment instruments which are not past due or doubtful of collection, [;] (H) gold, [;] and (I) any other investments approved by the commissioner. Notwithstanding the provisions of this subdivision, if the commissioner at any time finds that an investment of a licensee is unsatisfactory for investment purposes, the investment shall not qualify as a permissible investment.

[(16)] (18) "Prime quality" of an investment means that it is within the top four rating categories in any rating service recognized by the commissioner unless the commissioner determines for any licensee that only those investments in the top three rating categories qualify as prime quality.

[(17)] (19) "Purchaser" means a person who buys or has bought a payment instrument or who has given money or monetary value for

Substitute House Bill No. 5211

current or future transmission.

(20) "Receipt" means a paper record, electronic record or other written confirmation of a money transmission transaction.

[(18)] (21) "Stored value" means monetary value that is evidenced by an electronic record. For the purposes of this subdivision, "electronic record" means information that is stored in an electronic medium and is retrievable in perceivable form.

[(19)] (22) "Travelers check" means a payment instrument for the payment of money that contains a provision for a specimen signature of the purchaser to be completed at the time of a purchase of the instrument and a provision for a countersignature of the purchaser to be completed at the time of negotiation.

[(20)] (23) "Unique identifier" has the same meaning as provided in section 36a-485.

[(21)] (24) "Virtual currency" means any type of digital unit that is used as a medium of exchange or a form of digitally stored value or that is incorporated into payment system technology. Virtual currency shall be construed to include digital units of exchange that (A) have a centralized repository or administrator, [;] (B) are decentralized and have no centralized repository or administrator, [;] or (C) may be created or obtained by computing or manufacturing effort. Virtual currency shall not be construed to include digital units that are used (i) solely within online gaming platforms with no market or application outside such gaming platforms, or (ii) exclusively as part of a consumer affinity or rewards program, and can be applied solely as payment for purchases with the issuer or other designated merchants, but cannot be converted into or redeemed for fiat currency.

[(22)] (25) "Virtual currency address" means an alphanumeric identifier representing a destination for a virtual currency transfer that

Substitute House Bill No. 5211

is associated with a virtual currency wallet.

[(23)] (26) "Virtual currency kiosk" means an electronic terminal acting as a mechanical agent of the owner or operator to enable the owner or operator to facilitate the exchange of virtual currency for fiat currency or other virtual currency, including, but not limited to, by (A) connecting directly to a separate virtual currency exchanger that performs the actual virtual currency transmission, or (B) drawing upon the virtual currency in the possession of the owner or operator of the electronic terminal.

[(24)] (27) "Virtual currency wallet" means a software application or other mechanism providing a means for holding, storing and transferring virtual currency.

Sec. 2. Subsection (a) of section 36a-597 of the general statutes is repealed and the following is substituted in lieu thereof (*Effective October 1, 2024*):

(a) No person shall engage in the business of money transmission in this state, or advertise or solicit such services, without a main office license issued by the commissioner as provided in sections 36a-595 to 36a-612, inclusive, except as an authorized delegate of a person that has been issued a license by the commissioner and in accordance with section 36a-607. Any activity subject to licensure pursuant to sections 36a-595 to 36a-612, inclusive, shall be conducted from an office located in a state, as defined in section 36a-2. On and after October 1, 2024, any person who owns, operates, solicits, markets, advertises or facilitates virtual currency kiosks in this state shall be deemed to be engaged in the business of money transmission in this state and shall be subject to licensure pursuant to sections 36a-595 to 36a-612, inclusive. A person engaged in the business of money transmission is acting in this state under this section if such person: (1) Has a place of business located in this state, (2) receives money or monetary value in this state or from a

Substitute House Bill No. 5211

person located in this state, (3) transmits money or monetary value from a location in this state or to a person located in this state, (4) issues stored value or payment instruments that are sold in this state, [or] (5) sells stored value or payment instruments in this state, or (6) owns, operates, solicits, markets, advertises or facilitates virtual currency kiosks physically located in this state.

Sec. 3. Section 36a-599 of the general statutes is repealed and the following is substituted in lieu thereof (*Effective October 1, 2024*):

(a) Each applicant for a money transmission license shall pay to the system any required fees or charges and a license fee of one thousand eight hundred seventy-five dollars. Each such license shall expire at the close of business on December thirty-first of the year in which the license was approved, unless such license is renewed, except that any such license approved on or after November first shall expire at the close of business on December thirty-first of the year following the year in which it is approved. An application for renewal of a license shall be filed between November first and December thirty-first of the year in which the license expires. Each applicant for renewal of a money transmission license shall pay to the system any required fees or charges and a renewal fee of one thousand one hundred twenty-five dollars.

(b) Not later than fifteen days after the date a licensee ceases to engage in the business of money transmission in this state for any reason, including a business decision to terminate operations in this state, license revocation, bankruptcy or voluntary dissolution, such licensee shall request surrender of the license in accordance with subsection (c) of section 36a-51 for each location where such licensee has ceased to engage in such business. The licensee shall also identify, in writing, to the commissioner the location where the records of the licensee will be stored and the name, address and telephone number of an individual authorized to provide access to the records. The surrender of a license does not reduce or eliminate the licensee's civil or criminal

Substitute House Bill No. 5211

liability arising from acts or omissions occurring prior to the surrender of the license, including any administrative actions undertaken by the commissioner to revoke or suspend a license, assess a civil penalty, order restitution or exercise any other authority provided to the commissioner.

(c) Each license shall remain in force and effect until the license has been surrendered, revoked or suspended or has expired in accordance with the provisions of sections 36a-595 to 36a-612, inclusive. No abatement of the license fee shall be made if the applicant is denied or withdrawn prior to issuance of the license or if the license is surrendered, revoked or suspended prior to the expiration of the period for which it was issued. All fees required by this section shall be nonrefundable.

(d) Each licensee shall maintain a detailed plan and accounting as to how the licensee shall engage in winding down operations, and shall provide such plan and accounting to the commissioner upon request. Such plan and accounting shall contain:

(1) A record showing that the licensee's minimum net worth and reserves are sufficient to prevent losses to consumers and purchasers and to repay any outstanding obligations or accounts payable;

(2) Procedures to ensure that, after winding down operations, the licensee shall not retain any consumer funds, purchaser funds or other client funds;

(3) A plan demonstrating that consumers shall have access to consumer funds in the licensee's custody;

(4) Detailed instructions informing consumers how they may withdraw consumer funds upon request; and

(5) Any other records and information requested by the

Substitute House Bill No. 5211

commissioner regarding winding down operations.

(e) No licensee shall terminate such licensee's business unless the following conditions are met:

(1) The licensee provides written notice to the commissioner of the proposed termination at least thirty days prior to the effective date of such proposed termination;

(2) The licensee notifies, in writing, all consumers, purchasers and users of the licensee of the proposed termination, and the date of such proposed termination, at least thirty days prior to the date of such proposed termination;

(3) The licensee provides all consumers, purchasers and users of the licensee with detailed final accountings of the accounts of such consumers, purchasers and users;

(4) The licensee remits all money held in the custody of the licensee on behalf of consumers, purchasers and users to such consumers, purchasers and users; and

(5) The licensee files a request to surrender such licensee's license and the commissioner accepts such request.

Sec. 4. Section 36a-613 of the 2024 supplement to the general statutes is repealed and the following is substituted in lieu thereof (*Effective October 1, 2024*):

(a) The owner or operator of a virtual currency kiosk shall, in establishing a relationship with a customer and prior to entering into an initial virtual currency transaction for, on behalf of or with the customer, disclose in clear, conspicuous and legible writing in the English language all material risks associated with virtual currency generally, including, but not limited to, the following:

Substitute House Bill No. 5211

(1) A disclosure, which shall be acknowledged by the customer, provided separately from the disclosures provided pursuant to subdivisions (2) to (9), inclusive, of this subsection and written prominently and in bold type, stating the following: "WARNING: LOSSES DUE TO FRAUDULENT OR ACCIDENTAL TRANSACTIONS MAY NOT BE RECOVERABLE AND TRANSACTIONS IN VIRTUAL CURRENCY ARE IRREVERSIBLE.";

(2) Virtual currency is not backed or insured by the government and accounts and value balances are not subject to Federal Deposit Insurance Corporation, National Credit Union Administration or Securities Investor Protection Corporation protections;

(3) Some virtual currency transactions shall be deemed to be made when recorded on a public ledger, which may not be the date or time when the customer initiates the virtual currency transaction;

(4) The value of virtual currency may be derived from the continued willingness of market participants to exchange fiat currency for virtual currency, which may result in the permanent and total loss of the value of a particular virtual currency, if the market for that virtual currency disappears;

[(5) There is no assurance that a person who accepts a virtual currency as payment today will continue to do so in the future;]

[(6)] (5) The volatility and unpredictability of the price of virtual currency relative to fiat currency may result in a significant loss over a short period of time;

[(7) The nature of virtual currency may lead to an increased risk of fraud or cyber attack;

(8) The nature of virtual currency means that any technological difficulties experienced by the owner or operator may prevent access to

Substitute House Bill No. 5211

or use of a customer's virtual currency; and]

[(9)] (6) Any bond maintained by the owner or operator for the benefit of the customers of such owner or operator may not be sufficient to cover all losses incurred by such customers; and

(7) Virtual currency transactions are irreversible and are used by persons seeking to defraud customers, including, but not limited to, a person impersonating a customer's loved one, threatening jail time, stating that a customer's identity has been stolen, insisting that a customer withdraw money from the customer's bank account and purchase cryptocurrency or alleging a customer's personal computer has been hacked.

(b) The owner or operator of a virtual currency kiosk shall, when opening an account for a new customer and prior to entering into an initial virtual currency transaction for, on behalf of or with such customer, disclose in clear, conspicuous and legible writing in the English language, using not less than twenty-four point sans-serif-type font, all relevant terms and conditions associated with the products, services and activities of the owner or operator and virtual currency generally, including, but not limited to, the following:

(1) The customer's liability for unauthorized virtual currency transactions;

(2) The customer's right to stop payment of a preauthorized virtual currency transfer and the procedure used to initiate a stop-payment order;

(3) Under what circumstances the owner or operator will, absent a court or government order, disclose information concerning the customer's account to third parties;

[(4) The customer's right to receive periodic account statements and

Substitute House Bill No. 5211

valuations from the owner or operator;]

(4) The requirement that the owner or operator communicate to the customer what customer information may be disclosed to third parties;

(5) The customer's right to receive a physical, printed receipt [, trade ticket or other evidence of] for a virtual currency transaction at the time of the transaction; and

(6) [The] Upon any change in the rules or policies of the owner or operator, the customer's right to [prior notice of a change in the] consent to such changed rules or policies [of the owner or operator] prior to performing any transaction after such change.

(c) The owner or operator of a virtual currency kiosk shall, prior to each transaction in virtual currency for, on behalf of or with a customer, disclose to such customer in clear, conspicuous and legible writing in the English language, using not less than twenty-four point sans-serif-type font, the terms and conditions of the virtual currency transaction, including, but not limited to, the following:

(1) The amount of the transaction;

(2) Any fees, expenses and charges borne by the customer, including, but not limited to, applicable exchange rates;

(3) The type and nature of the virtual currency transaction;

(4) A warning that, once executed, the virtual currency transaction may not be undone, if applicable;

(5) A daily virtual currency transaction limit in accordance with subsection (g) of this section; and

(6) The difference in the sale price of the virtual currency versus the current market price.

Substitute House Bill No. 5211

(d) The owner or operator of a virtual currency kiosk shall ensure that each customer acknowledges receipt of all disclosures required under this section.

(e) (1) The owner or operator of a virtual currency kiosk shall, upon the completion of any virtual currency transaction, provide to the customer a receipt containing the following information:

[(1)] (A) The name of, and contact information for, the owner or operator, including, but not limited to, the owner or operator's business address and a customer service telephone number established by the owner or operator to answer questions and register complaints;

(B) The name of the customer;

[(2)] (C) The type, value, date and precise time of such virtual currency transaction, and each virtual currency address;

(D) The amount of such virtual currency transaction expressed in United States currency;

(E) The full unique transaction hash or identification number;

(F) The public virtual currency address of the customer;

(G) The unique identifier;

[(3) The] (H) Any fee charged, including, but not limited to, any fee charged directly or indirectly by the owner or operator or a third party involved in such virtual currency transaction;

[(4)] (I) The exchange rate, if applicable;

(J) Any tax collected by the owner or operator for such virtual currency transaction;

[(5)] (K) A statement of the liability of the owner or operator for

Substitute House Bill No. 5211

nondelivery or delayed delivery;

[(6)] (L) A statement of the refund policy of the owner or operator;
[and]

(M) The name and telephone number of the Department of Banking and a statement disclosing that the owner or operator's customers may contact the department with questions or complaints about the owner or operator's virtual currency kiosk services; and

[(7)] (N) Any additional information the Banking Commissioner may require.

(2) The receipt required under subdivision (1) of this subsection:

(A) Shall be provided in (i) a retainable form, (ii) the English language, and (iii) the language principally used by the owner or operator of the virtual currency kiosk to advertise, solicit or negotiate, either orally or in writing; and

(B) May be provided electronically if the customer requests or agrees to receive an electronic receipt.

(f) The [Banking Commissioner may establish a schedule of maximum fees that] total amount of any fee and commission charged by an owner or operator of a virtual currency kiosk [may charge for specific services] for a virtual currency transaction shall not exceed fifteen per cent of the amount of the virtual currency transaction.

(g) There [is] are established [a] the following maximum daily virtual currency kiosk transaction [limit of two] limits:

(1) Two thousand [five hundred] dollars for each new customer of a virtual currency kiosk; and

(2) Five thousand dollars for each existing customer of a virtual

Substitute House Bill No. 5211

currency kiosk.

(h) The owner or operator of a virtual currency kiosk shall [, at such owner's or operator's cost and within seventy-two hours after a virtual currency transaction, allow the] allow a new customer, upon the request of the new customer, to cancel and receive a full refund for [the] any fraudulent virtual currency [transaction if such virtual currency transaction: (1) Is the customer's first virtual currency transaction with such owner or operator; and (2) is to a virtual currency wallet or exchange located outside of the United States.] transactions that occurred not later than seventy-two hours after the new customer registered as a customer of such owner or operator if, not later than thirty days after the last virtual currency transaction that occurred during such seventy-two hour period, the new customer:

(1) Contacts such owner or operator and a government or law enforcement agency to inform such owner or operator and government or law enforcement agency of the fraudulent nature of such virtual currency transaction; and

(2) Files a report with a government or law enforcement agency memorializing the fraudulent nature of such virtual currency transaction.

(i) Each owner or operator of a virtual currency kiosk shall:

(1) Obtain a copy of a government-issued identification card that identifies each customer of such owner or operator;

(2) Maintain restrictions that prevent more than one customer of such owner or operator from using the same virtual currency wallet;

(3) Be able to prevent designated virtual currency wallets from being used at any virtual currency kiosk owned or operated by such owner or operator;

Substitute House Bill No. 5211

(4) Use an established third party that specializes in performing blockchain analyses to preemptively perform such analyses to identify and prevent high risk or sanctioned virtual currency wallets from being used by customers at virtual currency kiosks owned or operated by such owner or operator;

(5) Define, in such owner or operator's policies and procedures, a risk-based method of monitoring customers of such owner or operator on a post-transaction basis;

(6) Offer, during the hours of operation of the virtual currency kiosks owned or operated by such owner or operator, live customer support by telephone from a telephone number prominently displayed at or on such virtual currency kiosks;

(7) Identify and speak by telephone with any new customer over sixty years of age prior to such new customer completing such new customer's first virtual currency transaction with such owner or operator. During such communication, which shall be recorded and retained by such owner or operator, the owner or operator shall (A) reconfirm any attestations made by such new customer at a virtual currency kiosk owned or operated by such owner or operator, (B) discuss the transaction, and (C) discuss types of fraudulent schemes relating to virtual currency. Such owner or operator's approval of the transaction shall be dependent upon such owner or operator's assessment of such communication;

(8) Identify and speak by telephone with any new customer attempting to perform a virtual currency transaction that exceeds an amount that has been predesignated by such owner or operator as a large transaction amount before such transaction may be completed. During such communication, which shall be recorded and retained by such owner or operator, the owner or operator shall (A) positively identify such new customer, (B) review such new customer's stated

Substitute House Bill No. 5211

purpose of the transaction, and (C) discuss types of fraudulent schemes relating to virtual currency. Such owner or operator's approval of the transaction shall be dependent upon such owner or operator's assessment of such communication;

(9) Designate and employ a chief compliance officer who shall:

(A) Be qualified to coordinate and monitor a compliance program to ensure compliance with this section and all other applicable federal and state laws, rules and regulations;

(B) Be employed on a full-time basis by such owner or operator; and

(C) Not own more than twenty per cent of the virtual currency kiosk owner or operator that employs such officer; and

(10) Use full-time employees to fulfill such owner or operator's compliance responsibilities under federal and state laws, rules and regulations.

Sec. 5. Subsection (b) of section 36a-614 of the 2024 supplement to the general statutes is repealed and the following is substituted in lieu thereof (*Effective October 1, 2024*):

(b) The commissioner may, in accordance with the provisions of chapter 54, adopt, amend and rescind regulations, forms and orders governing the business use of digital assets, including, but not limited to, virtual currencies, [and] stablecoins and nonfungible tokens, by entities that, and individuals who, are subject to regulation by the commissioner, which regulations, forms and orders shall ensure consumer protection. As used in this subsection, "nonfungible tokens" shall not include tokens issued or sold primarily for consumptive, personal or household purposes.

Approved June 6, 2024

APPENDIX B

Decl. of Anthony Moore in Supp. of D.'s Opp'n to Mot. for Prelim. Inj., *All. for the Fair Access to Cryptocurrency Terminals v. St. of Cal.*, No. 23STCP04679 (Cal. Super. Ct., L.A. Cnty.)(April 22, 2024)

1 ROB BONTA
Attorney General of California
2 BRIAN D. WESLEY
Supervising Deputy Attorney General
3 ANNA BARSEGYAN
Deputy Attorney General
4 State Bar No. 271878
300 South Spring Street, Suite 1702
5 Los Angeles, CA 90013-1230
Telephone: (213) 269-6091
6 Fax: (916) 731-2144
E-mail: Anna.Barsegyan@doj.ca.gov
7 *Attorneys for Defendants State of
California and Department of Financial
8 Protection and Innovation*

*Exempt from fees pursuant to
Government Code section 6103*

9 SUPERIOR COURT OF THE STATE OF CALIFORNIA

10 COUNTY OF LOS ANGELES

<p>13 ALLIANCE FOR THE FAIR ACCESS TO 14 CRYPTOCURRENCY TERMINALS, a 15 California unincorporated association, 16 Plaintiff, 17 v. 18 THE STATE OF CALIFORNIA, et al., 19 Defendants.</p>	<p>Case No. 23STCP04679 DECLARATION OF ANTHONY MOORE IN SUPPORT OF DEFENDANTS' OPPOSITION TO MOTION FOR PRELIMINARY INJUNCTION Date: April 22, 2024 Time: 8:30 a.m. Dept: 32 Judge: The Honorable Daniel S. Murphy Trial Date: n/a Action Filed: December 29, 2023</p>
--	---

1 I, Anthony Moore, declare as follows:

2 1. I am over the age of 18 years and a United States citizen. I have personal knowledge
3 of the following facts, and if called as witness, I could and would testify competently thereto.

4 2. I have been a law enforcement officer at the Los Angeles County Sheriff's
5 Department (LASD) for approximately 26 years. I am currently a detective for the Fraud and
6 Cybercrimes Bureau. My current responsibilities include investigating financial crimes with a
7 cyber nexus. I am also assigned as a task force officer to the White Collar Squad at the Federal
8 Bureau of Investigation (FBI) Criminal Investigation Division.

9 3. Prior to my current assignment, I was assigned to numerous positions at LASD,
10 including the Cyber Intel Unit, Sexual Assault and Felony Enforcement Team, Los Angeles
11 Regional Human Trafficking Task Force, and Internet Crimes Against Children Unit.

12 4. I also assisted LASD in creating the Electronic Communications Triage (eComm)
13 Unit, the first new unit for the agency in over 50 years. The mission of the eComm unit is to listen
14 to, to train on the use of, and to conduct research about electronic and web-based
15 communications. The eComm unit also shares information with the public that will help keep the
16 communities throughout Los Angeles County safe through the use of the LASD's web sites and
17 social media platforms.

18 5. In 2017, I was part of Operation Cryptonite, and worked with federal law
19 enforcement partners to investigate and successfully prosecute the first major crypto kiosk
20 takedown (Herocoin) that seized 16 crypto kiosks.

21 6. I also hold Advanced Instructor Certifications through the California Peace Officers
22 Standards and Training (POST), and am a nationally certified law enforcement instructor with the
23 International Association of Directors for Law Enforcement Standards and Training. This
24 certification allows me to conduct law-enforcement-training in all 50 states.

25 7. I have created numerous courses of instruction to educate fellow department and
26 national law enforcement personnel on expansive tools and techniques to perform their duties
27 effectively.

28

1 8. In 2011, I assisted in creating and implementing social media and crisis
2 communication training for hundreds of law enforcement agencies worldwide.

3 9. I have instructed over 1,000 hours for LASD's Advanced Training Unit (AOT), and
4 have created cyber-related content for several AOT courses, including: (i) Background
5 Investigators course; (ii) Operation Safe Streets (Gang Unit) course; (iii) Sexual Assault
6 Investigator course; (iv) Basic and Intermediate Detective course; and (v) LASD Supervisor
7 School.

8 10. Since 2014, I have also been an instructor for the California Department of Justice,
9 Advanced Training Center. I have taught courses on Basic Computer Data Acquisition and
10 Forensics, Dark Web, and Cryptocurrency Investigations. I have also taught a course on Policing
11 Cryptocurrency, the first of its kind in the United States that focused on investigative techniques
12 for law enforcement.

13 11. I have investigated over 100 cases of cybercrimes at the Fraud and Cybercrime
14 Bureau. Approximately ninety percent of these investigations have been related to cryptocurrency
15 crimes, including crypto kiosk crimes. Based on my experience and training, crypto kiosks pose
16 more risk to consumers than other crypto exchanges because it facilitates the crime by making it
17 easier to convert a victims' funds to crypto assets.

18 12. I have knowledge of the provisions of Senate Bill (SB) 401, including the \$1,000
19 daily transaction limit placed on crypto kiosk operators.

20 13. One of the investigation software services that LASD subscribes to, Chainalysis,
21 assists law enforcement in investigating criminal activity related to cryptocurrency. Chainalysis is
22 a blockchain data platform that provides data, software, services and research to government
23 agencies, exchanges, financial institutions and insurance and cybersecurity companies.
24 Chainalysis assists LASD in tracing cryptocurrency funds as they are transferred across multiple
25 tokens and chains. A review of the services that Chainalysis provides can be found at
26 <https://www.chainalysis.com/>.

27 14. As part of my primary duties at LASD, I regularly use Chainalysis in my
28 investigation of cryptocurrency crimes, including crypto kiosk crimes. I have reviewed the data

1 provided by Chainalysis since the daily transaction limit set forth in SB 401 took effect on
2 January 1, 2024. I have determined that there is a reduction in crypto kiosk scams and fraud since
3 the daily transaction limit became effective. I have also determined that there has been a
4 reduction in the use of crypto kiosks for escort services which are known to involve human
5 trafficking.

6 15. Based on my review of open-sourced information and data obtained from
7 <https://coinatmradar.com/>, California has the most crypto kiosk locations in the world.

8 16. I have reviewed the data for 2023 and year-to-date 2024 transactions for RockItCoin,
9 LLC (RockItCoin) – a member of Alliance for the Fair Access to Cryptocurrency Terminals who
10 is the plaintiff in this action. RockItCoin has crypto kiosk locations throughout the nation
11 including Puerto Rico. It also has a significant presence in California with crypto kiosks located
12 throughout the state. In reviewing the data, I determined that the dollar amounts of RockItCoin
13 transactions attributed to scams, fraud, and human trafficking has significantly decreased in the
14 first quarter of 2024 compared to the first quarter of 2023.

15 17. The dollar amounts of RockItCoin transactions attributed to fraud from January
16 through March of 2023 totaled \$102,043.10. This is a conservative number because it only
17 accounts for transactions that Chainalysis analysts have definitively determined was attributed to
18 fraud. The dollar amounts of RockItCoin transactions attributed to fraud from January through
19 March of 2024 totaled \$1,133.86, a significant decrease compared to the first quarter of 2023.

20 18. The dollar amounts of RockItCoin transactions attributed to scams from January
21 through March of 2023 totaled \$257,237.38. This is also a conservative number because it only
22 accounts for transactions that Chainalysis analysts have definitively determined was attributed to
23 scams. The dollar amounts of RockItCoin transactions attributed to scams from January through
24 March of 2024 totaled \$2,298.16, a significant decrease compared to the first quarter of 2023.

25 19. Crypto kiosks have frequently been used to facilitate human trafficking. The dollar
26 amounts of RockItCoin transactions attributed to human trafficking from January through March
27 of 2023 totaled \$20,982.26. This is also a conservative number because it only accounts for
28 transactions that Chainalysis analysts have definitively determined was attributed to human

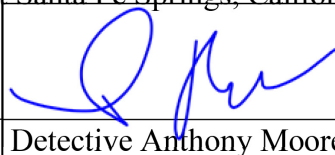
1 trafficking. The dollar amounts of RockItCoin transactions attributed to human trafficking from
2 January through March of 2024 totaled \$117.59, a significant decrease compared to the first
3 quarter of 2023.

4 20. The Chainalysis data I have reviewed shows that RockItCoin is not the only crypto
5 kiosk company that has seen a substantial reduction in the dollar amounts of transactions
6 attributed to scams, fraud and human trafficking since the daily transaction limit under SB 401
7 took effect. It is just one example demonstrating that the daily transaction cap is serving its
8 intended purpose of reducing crypto kiosk crime.

9 21. The daily transaction cap is not overly restrictive, and protects consumers from
10 experiencing significant financial loss from scams, fraud, and other illegal activity. The crypto
11 kiosk transaction data I have reviewed also shows that the average daily transaction amount for
12 crypto kiosk users is approximately \$150, well below the \$1,000 daily transaction limit set forth
13 in SB 401.

14 I declare under penalty of perjury under the laws of the State of California that the
15 foregoing is true and correct.

16 Executed on April 08, 2024 at Santa Fe Springs, California.

17 
18
19

Detective Anthony Moore

20
21 LA2024800124
22
23
24
25
26
27
28

DECLARATION OF SERVICE BY E-MAIL

Case Name: **Alliance for the Fair Access to Cryptocurrency Terminals v. State of California**

Case No.: **23STCP04679**

I declare:

I am employed in the Office of the Attorney General, which is the office of a member of the California State Bar, at which member's direction this service is made. I am 18 years of age or older and not a party to this matter. I am familiar with the business practice at the Office of the Attorney General located at 300 South Spring Street, Suite 1702, Los Angeles, CA 90013, for collection and processing of correspondence.

On April 9, 2024, I served the attached **DECLARATION OF ANTHONY MOORE IN SUPPORT OF DEFENDANTS' OPPOSITION TO MOTION FOR PRELIMINARY INJUNCTION** by transmitting a true copy via electronic mail, addressed as follows:

John W. Howard, Esq.
JW HOWARD ATTORNEYS LTD
600 West Broadway, Suite 1400
San Diego, CA 92101
E-mail Address:
johnh@jwhowardattorneys.com

Scott J. Street, Esq.
JW HOWARD ATTORNEYS LTD
201 South Lake Avenue, Suite 303
Pasadena, CA 91101
E-mail Address:
sstreet@jwhowardattorneys.com

*Attorneys for Plaintiff,
Alliance for the Fair
Access to Cryptocurrency Terminals*

I declare under penalty of perjury under the laws of the State of California and the United States of America the foregoing is true and correct and that this declaration was executed on April 9, 2024 at Los Angeles, California.

Anthony Conklin
Declarant

Anthony Conklin
Signature

APPENDIX C-1

Letter from Charity R. Clark, Attorney Gen., State of Vt., to Kevin Gaffney,
Comm'r of Fin. Regul., Vt. Dept. of Fin. Regul. (Oct. 15, 2024).



STATE OF VERMONT
OFFICE OF THE ATTORNEY GENERAL
109 STATE STREET
MONTPELIER, VT
05609-1001

October 15, 2024

Commissioner Kevin Gaffney
Department of Financial Regulation
State of Vermont
89 Main Street
Montpelier, VT 05620-3101

Re: Comment and recommendations concerning enhanced oversight of virtual currency kiosks (pursuant to 8 V.S.A. § 2577(g))

Dear Commissioner Gaffney:

Thank you for the opportunity to provide comments and recommendations concerning the challenges that virtual currency kiosks (or crypto-kiosks) present here in Vermont. As you know, the Department of Financial Regulation (DFR) has been charged by the House Committee on Commerce and Economic Development and the Senate Committee on Finance to determine “whether the requirements of 8 V.S.A. § 2577(g) regarding virtual currency kiosks, coupled with relevant federal requirements, are sufficient to protect customers in Vermont from fraudulent activity.” Further, DFR is to make recommendations for statutory or regulatory safeguards “if deemed necessary and appropriate.”

When it comes to fraudulent activity, my office’s Consumer Assistance Program (CAP) are undoubtedly experts. CAP responds to 8,000-12,000 calls for help from Vermont consumers each year. About half of those calls specifically relate to scams or criminal attempts to separate Vermonters from their hard-earned money. Victims of scams often do not know the true identity of these criminal actors or their physical whereabouts. With scams, law enforcement faces significant challenges identifying perpetrators, tracing transactions, or recovering money lost.

The rise of cryptocurrency—an unregulated virtual currency without backing or sufficient oversight from federal authorities—has made the task of protecting Vermonters from scammers even more challenging. I won’t sugarcoat this: Expanding and simplifying access to cryptocurrency through crypto-kiosks without sufficient controls creates an outsized risk to Vermonters.

The Vermont Legislature has requested whether Vermont law provides sufficient protections for users of virtual currency kiosks. The answer is no.

Last year, my office testified in support of a two-year moratorium on all crypto-kiosk activity in Vermont. Since then, we have learned more about crypto-kiosks. There are 36 crypto-kiosks located in Vermont, which operate like traditional ATMs but give access to cash and cryptocurrency. The Federal Bureau of Investigation (FBI) annual report for 2023 indicates that more than 69 Vermonters complained of more than \$5 million in losses in conjunction with cryptocurrency.¹ This is an extremely conservative estimate. Vermonters report complaints to many different agencies (local police, State’s Attorneys, the Office of the Attorney General, the Federal Trade Commission, the Consumer Financial Protection Bureau, the U.S. Attorney’s Office, the FBI, our Congressional delegation, and others). CAP reports that over the last three years we have received at least 45 reports of cryptocurrency frauds or scams representing more than \$3 million in losses (see table below). Not all reports specifically single out the means of transfer, but we know *at least* 14 reports (roughly one-third) indicated that crypto-kiosks were used to perpetrate the scam. This number, which we believe reflects underreporting, is concerning.

	2022	2023	2024 (to date)	Totals
# of reports without financial loss	9	16	12	37
# of reports with financial loss	11 (0 crypto-kiosks)	23 (9 crypto-kiosks)	11 (5 crypto-kiosks)	45 (14 crypto-kiosks)
TOTALS	20 Total Reports	39 Total Reports	23 Total Reports	82 Total Reports
Total \$ lost	\$134,745	\$2,655,079	\$430,219	\$3,220,043

We aren’t the only office with concerns. The FBI reports: “Criminals are known to direct individuals to use a cryptocurrency kiosk to send funds, which enables a more anonymous transaction than depositing the cash at a financial institution.”² The FBI goes on to note the increased use of crypto-kiosks to perpetrate fraud, particularly given the ease with which scammers can coerce individuals to access such kiosks:

Typically, criminals give detailed instructions to individuals, to include how to withdraw cash from their bank, how to locate a kiosk, and how to deposit and send funds using the kiosk. In most instances, the cryptocurrency kiosk transactions are facilitated using QR codes, square barcodes with information that can be scanned and read with a smartphone or kiosk camera. An individual can scan the QR code of an intended recipient at a cryptocurrency kiosk, making it easier to send cryptocurrency to the correct destination.

This pattern describes events already happening in Vermont. For example, my office received notice from Vermonters who received a form scam letter threatening them with extortion. The letter falsely states the recipient unwittingly gave access to the criminal, that their activity is being monitored, and that embarrassing or unlawful activity, photos, or video will be sent to all of the individual’s contacts unless the scammer’s demands are met. The scam notices included a

¹ 2023 IC3 Cryptocurrency State Reports (Vermont) (available at: <https://www.ic3.gov/Media/PDF/AnnualReport/2023CryptocurrencyState/StateReport.aspx?s=51>).

² Federal Bureau of Investigation Cryptocurrency Fraud Report 2023; available at: https://www.ic3.gov/Media/PDF/AnnualReport/2023_IC3CryptocurrencyReport.pdf

QR code in the letter, just as described in the FBI's warning about facilitating cryptocurrency transfers via crypto-kiosks.

Furthermore, crypto-kiosks side-step other established means of protecting Vermonters from scams. For example, many businesses, such as banks and credit unions, now train their staffs to spot scams and try to prevent them. Gift card producers and retailers now routinely limit how many cards may be purchased at one time; banks and wire transmitters ask customers if they know the identity of the entity to whom they are sending the money. These partners routinely engage in scam prevention practices to help their customers. We regularly instruct retailers and financial institutions to have their customers call my office if they have questions before they make a money transfer. Crucially, contrary to most other forms of money transfer available through retail operators in Vermont, ***there is no oversight, monitoring, or support staff at crypto-kiosks*** to offer similar assistance to the unwary consumer. We routinely counsel individuals to ask:

- Is this transfer for you? Or, for someone else?
- Do you control the account or wallet where the money is going?
- How much are you transferring?
- Who asked you to transfer this money? Do you know them personally? Or, was the request unsolicited or part of an online ad or social media contact?
- If you must transfer funds, can you do so by some other means that may be more secure (such as through a bank or credit card)?

In contrast to the opportunity for a conversation with a bank teller or wire transmitter, the static, multi-screen disclosures and consumer warnings present on these crypto-kiosks are insufficient to protect consumers and are unlikely to be improved upon for multiple reasons, including:

- The disclosures are lengthy and, like many click-through warnings, most consumers are unlikely to read through them all;
- Victims of frauds and scams are operating emotionally, not rationally. It is unlikely that someone feeling time pressure because they are scared that they will be exposed, thinking they are transferring money to a loved one, or afraid they will be arrested will pause to reflect on a touch screen, rather than affirmatively responding to questions;
- The general ease of use and familiarity with standard ATM's breeds a false sense of security with crypto-kiosks. It is simple enough to put money in and get a receipt. The victim may discover only later that the money was not sent where they thought, or they were not dealing with a legitimate party. Because the kiosks are unregulated and not backed or insured, there is nothing to protect the consumer after the fact.

Importantly, while the risks of crypto-kiosks are clear and present, the rewards are limited. Legitimate investors wishing to speculate in cryptocurrency may do so online, via their smartphones, by establishing accounts with exchanges, or otherwise exercising their rights as consumers in a "buyer beware" marketplace. Dumping cash into a kiosk and transferring it to virtual wallets that may or may not be known to the user is ***not*** a safe, reliable, or prudent way to manage investments. It is, however, an efficient means for a criminal to coerce, threaten, or trick unsuspecting Vermonters into transmitting vast sums of money that may be untraceable and that are unlikely ever to be recovered.

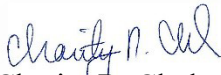
In summary, without proper regulatory protection and controls—security controls, insurance, or backing from financial institutions or the federal government—to guard against consumer losses,

crypto-kiosks are a losing proposition for Vermont consumers. ***I firmly believe that the risks of fraudulent use far outweigh any reward or convenience.*** The best way to protect Vermont consumers from criminal activity associated with cryptocurrency is to build in consumer protections into the market, not to make it easier for victims to fall prey, which is what crypto-kiosks do. My office supports a moratorium on these products until federal and state government and regulatory agencies with appropriate oversight powers can guarantee Vermont consumers will be protected from, or have adequate access to remedies relating to, criminal activity connected to crypto-kiosks located in Vermont.

In the meantime, Vermonters should continue to contact my office to report scams and frauds of any type, including cryptocurrency scams, at 800-649-2424, or ago.cap@vermont.gov. We will continue to do everything we can to prevent Vermonters from falling prey to scammers, and work with our federal partners and financial institutions to try to recover stolen funds whenever possible.

Thank you for your request for comment, for your consideration, and for all you do to protect Vermont consumers from scams, frauds, and unfair or deceptive practices.

Sincerely yours,


Charity R. Clark
Vermont Attorney General

cc: Kelley Reed, Director
Regulatory and Consumer Affairs
Vermont Department of Financial Regulation

APPENDIX C-2

E-mail from Christopher D'Elia, President, Vt. Bankers Ass'n, to Kelley Reed, Regulatory and Consumer Affairs Dir., Banking Div., Vt. Dept. of Fin. Regul.
(Sept. 26, 2024, at 11:04 ET).

From: vtbanker@sover.net
To: [Reed, Kelley](#)
Subject: RE: Request for Comment - 8 VSA 2577(g) - VC Kiosks Comments
Date: Thursday, September 26, 2024 11:04:28 AM

EXTERNAL SENDER: Do not open attachments or click on links unless you recognize and trust the sender.

Kelley,

Thank you for the opportunity to comment on VC Kiosks. During the 2024 legislative session, I had the opportunity to listen to the testimony offered in both the House Commerce Committee and Senate Finance Committee. Based on the discussion, I only have two concerns.

1. Similar to ATM machines, VC kiosks should be required to comply with state and federal regulations on siting, signage, disclosures, contact information of the owner, etc. This is critical, in the event something were to go wrong, the consumer needs to know who to turn to. The consumer also needs to know, the extent of any fees being charged by the VC company.
2. Our concern is not with the reputable VC companies, but rather how their machines and the technology are being used by criminals. For example: Bank customer receives an email (looks like it is from their bank) stating their account has a problem with it. In order to correct the problem, take out a large sum of money, go to a crypto currency machine and deposit the funds. The funds will be routed back to their bank account and the problem corrected. Bottom line, there is no problem with the account and the funds are lost to the criminal. Regardless of the scam, kiosks are being used as a vehicle for transmitting the funds. We would hope DFR looks at what role the VC companies should play in educating consumers about such scams.

Thank you again for the opportunity to comment.

Chris

Christopher D'Elia, President
Vermont Bankers Association
P.O. Box 587
Montpelier, Vermont 05601
802-793-1123

APPENDIX C-3

Letter from Greg Marchildon, State Dir., AARP Vt., to Kelley Reed, Regulatory and Consumer Affairs Dir., Banking Div., Vt. Dept. of Fin. Regul. (Oct. 14, 2024).



To: Kelley Reed, Department of Financial Regulation
From: Greg Marchildon, State Director, AARP Vermont
Re: 8 V.S.A. § 2577(g) - VC Kiosks Comments
Date: October 14, 2024

Dear Ms. Reed,

Please accept the following comments from AARP Vermont regarding 8 V.S.A. § 2577(g) and Virtual Currency Kiosks.

AARP is a nonpartisan, social mission organization with 38 million members nationwide and nearly 110,000 members in Vermont. We advocate on issues that impact older adults and appreciate the opportunity to provide recommendations for additional statutory or regulatory safeguards to 8 V.S.A. § 2577(g).

Overall, we appreciated and supported the legislative efforts to bring consumer protections to virtual currency transactions, especially at virtual currency kiosks. Robust consumer protections help safeguard older Vermonters financial well-being by ensuring transparency, fairness, and accountability.

We believe strong protections against fraud are needed as cryptocurrency used as a payment for scams is a fast-growing problem. The law can be made stronger by considering the usage of cryptocurrency kiosks in fraud.

The impact of fraud on victims and their families is wide reaching and can be financially and emotionally devastating, especially for older adults. The FBI's annual Elder Fraud Report revealed that in 2023, individuals over the age of 60 reported losses exceeding \$3.4 billion, marking an almost 11% increase from 2022.

Additionally, there was a 14% rise in complaints filed with the Internet Crime Complaint Center (IC3) by elderly victims and the FTC's Consumer Sentinel Network reported 47,537 scams using cryptocurrency as payment resulting in theft of \$1.409 million in 2023, second by payment losses only to bank transfers/payments.

Below are several recommendations to strengthen the law as well as provisions that should be retained.

Section 2577 (a) Daily transaction limits: We support the enactment of the \$1000 daily transaction limit for all customers as it protects victims from large losses and limits the use of kiosks for criminal activity.

Recommendation: Keep the \$1000 daily transaction limit in place.



Section 2577 (d) Licensing requirement: We support the licensing of kiosk operators and would like to ensure that this requirement includes registering kiosk locations. This helps law enforcement track fraudulent activity.

Recommendation: Ensure that the locations of all kiosks are recorded and updated as part of the licensing requirement.

Section 2577 (b) fees: We support that fees should be reasonable and defined. In addition, we would like to see a refund provision added in cases of fraud. An example of a refund can be found in the recently passed legislation in Minnesota. Below, please find language we would like to see added:

- a. **Refunds for new customers.** A virtual currency kiosk operator must issue a refund to a new customer for the full amount of all transactions made within a thirty (30) day new customer time period upon the request of the customer. In order to receive a refund under this section, a new customer must have been fraudulently induced to engage in the virtual currency transactions and contacts the virtual currency kiosk operator and a government or law enforcement to inform them of the fraudulent nature of the transaction agency within ninety (90) days of the last transaction to occur during the thirty (30) day new customer time period.
- b. **Refunds for existing customers.** A virtual currency kiosk operator must issue a refund to an existing customer for the full amount of all transaction fees upon the request of an existing customer. In order to receive a refund under this section, a customer must have been fraudulently induced to engage in the virtual currency transactions and contacts the virtual currency kiosk operator and a government or law enforcement agency to inform them of the fraudulent nature of the transaction within ninety (90) days of the transaction.

Recommendation: Transactions based on fraudulent activity should be refunded to the victim.

Section 2507 Receipts: Receipts are an important part of investigations by law enforcement. We would like to have paper receipts required at virtual currency kiosks. In addition, all receipts should have information of who to contact when fraud is suspected as well as all other transaction information.

Recommendation: Require paper receipts and law enforcement contact information on all receipts.

Section 2507 Disclosures: Disclosures are an important part of consumer and fraud protection. We support the statute's inclusion of disclosures would suggest the addition of a fraud warning.

Recommendation: Warnings regarding fraud should be required at virtual currency kiosks.

Sincerely,

Greg Marchildon
State Director, AARP Vermont

APPENDIX C-4

E-mail from Christine Martin, BSA Officer, Northfield Savings Bank, to Kelley Reed, Regulatory and Consumer Affairs Dir., Banking Div., Vt. Dept. of Fin. Regul. (Sept. 18, 2024, at 13:47 ET).

From: Christine Martin <Christine.Martin@NSBVT.COM>

Sent: Wednesday, September 18, 2024 1:47 PM

To: Reed, Kelley <Kelley.Reed@vermont.gov>

Subject: VSA 2577(g) - VC Kiosks Comments

EXTERNAL SENDER: Do not open attachments or click on links unless you recognize and trust the sender.

Hi Kelley,

Thanks for sharing the information.

From a banking perspective, we appreciate the recent restrictions placed on kiosks offering virtual currency transactions. I've seen NO customers that have had a need to use a virtual currency kiosk – EXCEPT in conjunction with a scam. We've had multiple customers that have either used a local kiosk or attempted to find one, at the instruction of a scammer. Because of Vermont's low number of available kiosks, it's helped slow the flow of funds to the scammers.

When a customer wants to legitimately invest in crypto, there are multiple ways for them to do so, none of which involve the kiosks.

I would like to see Vermont continue to strictly regulate virtual currency kiosks.

Thank you!



Christine Martin, BSA Officer

1021 Paine Turnpike N | Berlin, VT 05602

P.O. Box 7180 | Barre, VT 05641-7180

802-661-5231 (o) | 802-917-4325 (c)

APPENDIX C-5

E-mail from Robert F. O'Neill, Security Officer, Northfield Savings Bank, to Kelley Reed, Regulatory and Consumer Affairs Dir., Banking Div., Vt. Dept. of Fin. Regul. (Sept. 20, 2024, at 15:23 ET).

From: [Robert O'Neill](#)
To: [Reed, Kelley](#)
Subject: Re: 8 V.S.A. § 2577(g) - VC Kiosks Comments
Date: Friday, September 20, 2024 3:24:21 PM
Attachments: [image001.png](#)

EXTERNAL SENDER: Do not open attachments or click on links unless you recognize and trust the sender.

The state should:

- limit the Kiosks in the state; use strong signage.
- allow a "Hold" on deposits for new cryptocurrency purchases for 24 or 48 hours to prevent/protect victims of scams; works to protect victims of scams.
- not allow "Blender Wallets" to be used for new cryptocurrency purchases; easier to track if scammed.
- mandate contacts for cryptocurrency companies for financial institutions and LEO's, with pre-known steps for records requests and methods to seize/hold funds involved.



Robert F. O'Neill, CFE
Security Officer
1021 Paine Turnpike N | Berlin, VT 05602
P.O. Box 7180 | Barre, VT 05641-7180
[802-871-4486 \(o\)](tel:802-871-4486) | [802-917-6491 \(c\)](tel:802-917-6491)
nsbvt.com

APPENDIX C-6

E-mail from Kim Scott, AVP Fraud Detection Officer, Mascoma Bank, to Kelley Reed, Regulatory and Consumer Affairs Dir., Banking Div., Vt. Dept. of Fin. Regul. (Oct. 9, 2024, at 16:06 ET).

From: [Kim Scott](#)
To: [Reed, Kelley](#)
Subject: 8 V.S.A. § 2577(g) - VC Kiosks Comments
Date: Wednesday, October 9, 2024 4:06:15 PM
Attachments: [image001.png](#)

You don't often get email from kim.scott@mascomabank.com. [Learn why this is important](#)

EXTERNAL SENDER: Do not open attachments or click on links unless you recognize and trust the sender.

Cryptocurrencies are fast money transfers that typically will not collapse at a single point of failure. Crypto ATMs are attractive to criminals. The increasing number and accessibility of these ATMs makes it easier to facilitate illicit transactions. Regulations are lacking and inconsistent in many states. Multiple ATM owners in the same geographical area do not communicate with each other, which allows laundering to occur, whereas the same customer conducting those transactions in a financial institution would be subject to review within BSA departments and proper Currency Transaction Reports or Suspicious Activity Reports filed.

Cryptocurrency payments are typically not reversible. In most cases that we've seen, the customer/victim was sent a QR code with specific instructions of which terminal to go to, bring cash, scan the code and deposit the money. Simple and quick. We have been unsuccessful in obtaining who or where this money was sent to and have been encouraging victims to report the fraud to www.ftc.gov where they can look for similarities within the victims.

Kim Scott | AVP Fraud Detection Officer | **Mascoma Bank**
137-139 Broad Street | Claremont, NH 03743
Phone: (603) 443-8665 | Kim.Scott@MascomaBank.com



Confidentiality Notice: The information contained in this e-mail and any attachments is privileged and confidential and may contain information that is protected by law. It is intended only for the use of the addressee(s) indicated above. Use or disclosure of information e-mailed in error is respectfully prohibited. If you have received this e-mail in error, please contact the sender and immediately delete the original message.

APPENDIX C-7

E-mail from Greg Nixon, to Kelley Reed, Regulatory and Consumer Affairs Dir.,
Banking Div., Vt. Dept. of Fin. Regul. (Sept. 18, 2024, at 7:39 ET).

From: [Greg Nixon](#)
To: [Reed, Kelley](#)
Subject: "8 V.S.A. § 2577(g) - VC Kiosks Comments" in the email or letter.
Date: Wednesday, September 18, 2024 7:39:56 AM

You don't often get email from grgnxn@gmail.com. [Learn why this is important](#)

EXTERNAL SENDER: Do not open attachments or click on links unless you recognize and trust the sender.

Crypto currencies are energy wasting, zero use case Ponzi's that have no business existing. If the SEC and politicians were not being bribed by fraudsters, they would be banned. Please do not allow crypto kiosks.

Greg Nixon

APPENDIX C-8

E-mail from Martin P. Wagner, to Kelley Reed, Regulatory and Consumer Affairs
Dir., Banking Div., Vt. Dept. of Fin. Regul. (Sept. 18, 2024, at 9:01 ET).

From: [Martin Wagner](#)
To: [Reed, Kelley](#)
Subject: 8 V.S.A. § 2577(g) - VC Kiosks Comments
Date: Wednesday, September 18, 2024 9:01:06 AM

You don't often get email from martinpwagner@protonmail.com. [Learn why this is important](#)

EXTERNAL SENDER: Do not open attachments or click on links unless you recognize and trust the sender.

I do not believe the state needs to do anything in regards to oversight of virtual currency and kiosks. The state has shown time and time again their inability to administer even the simplest of public services and oversight. This would simply be another oversight of individuals that simply don't have the capacity or even the understanding of crypto in charge. It would essentially be giving fictitious power to people that don't understand crypto at even an elementary level. This, by in of itself is extremely dangerous to Vermonters. The department of financial regulation is also not a law creating body, they're an enforcing agency. This would be attempting to give power to an agency that is simply not equipped nor has any legal standing.

The harsh reality is that the US physical dollar will inevitably be going away. What is the time frame? No one is sure, but I can assure you that creating dollar bills is expensive in of itself. Once the federal reserve realizes the massive savings they will achieve by going to the digital dollar, I'm sure both the house and senate will come together propose regulation. This is why the 10th amendment is important. Simply put, there is no one within government in the state of Vermont that could provide competent decision making on something they know nothing about. Crypto is not a 5 minute video to understand it.

Martin P. Wagner

Sent with [Proton Mail](#) secure email.

APPENDIX C-9

E-mail from Tom Cooper, to Kelley Reed, Regulatory and Consumer Affairs Dir.,
Banking Div., Vt. Dept. of Fin. Regul. (Sept. 19, 2024, at 18:17 ET).

From: [Tom Cooper](#)
To: [Reed, Kelley](#)
Subject: 8 V.S.A. § 2577(g) - VC Kiosks Comments
Date: Thursday, September 19, 2024 6:17:37 PM

[You don't often get email from wleat@yahoo.com. Learn why this is important at <https://aka.ms/LearnAboutSenderIdentification>]

EXTERNAL SENDER: Do not open attachments or click on links unless you recognize and trust the sender.

I am a retired mathematician. For years I have puzzled over the claims of value for "Virtual Currencies", and my evaluation is that all they represent is an unverified claim of being "unstealable", when in fact there are at least theoretical methods which make this claim false. It takes a lot of electrical power to execute the algorithms used to "make" these currencies, electrical power that could be used for better purposes, or not used at all which removes environmental concerns. With large scale AI on the horizon we are going to need a lot more electrical power for many things in any case.

If we are going to have kiosks selling virtual currencies we should also have kiosks dispensing psychic readings predicting the future, part ownership in large bridges, deeds to square-inch tracts of land on the deepest part of the Pacific ocean floor, certificates protecting the bearer from various diseases, and so forth. The wild predictions of wealth involved with virtual currencies remind me of the Beany Baby craze. At least someone does in fact win the Powerball game from time to time.

If there are kiosks to sell such tokens then there should be cash machines to redeem them. Buyers should be able to compare the buy-back price to the selling price before they make a purchase. It's only fair. However, my belief is that no kiosks are better for Vermont than any at all.

Tom Cooper
143 Spruce St.
Burlington, VT 05401

(802)598-0107 cell phone

PS - Maybe cash machines already work with tokens. The ATM at my bank does not.

APPENDIX C-10

Letter from Simon Spektor, Chief Counsel & Compliance Officer, Moon, Inc. dba LibertyX, to Kelley Reed, Regulatory and Consumer Affairs Dir., Banking Div., Vt. Dept. of Fin. Regul. (Sept. 19, 2024).

Moon Inc.

864 Spring St. NW
Atlanta, GA 30308
+1 (800) 511-8940



September 19, 2024

TO: kelley.reed@vermont.gov

Kelley M. Reed, CPM

Regulatory and Consumer Affairs Director
89 Main Street
Montpelier, VT 05620-3101
Fax: 802-828-1477
Phone: 802-828-0526

Subject: Virtual Currency Kiosk Regulations - Request for POS Card Payments Exemption

Dear Ms. Reed,

The rise of cash accepting virtual currency kiosks, commonly known as Bitcoin Teller Machines (BTMs), has provided a way for individuals to exchange cash for virtual currencies. These kiosks, which enable the direct conversion of physical currency into virtual currencies, have gained popularity as virtual currency has become more accepted and of interest across society growing from ~6,000 to ~38,000 devices between 2020 and 2024¹. However, the rapid expansion of BTMs has exposed significant vulnerabilities, particularly in terms of third-party fraud. Criminals have increasingly exploited BTMs, often targeting elderly Americans.² Given these concerns, we support the establishment of a regulatory framework to mitigate the risks associated with BTMs. This letter, however, aims to clarify an important qualification regarding any proposed Virtual Currency Kiosk regulations. Specifically, we advocate for an exemption for POS card payments (authorized debit card purchases) completed at traditional ATMs, a distinct funds flow utilized by companies like Moon Inc. dba LibertyX (hereinafter “LibertyX”), supported by sponsor banks, and codified by EFT networks such as Visa.

Operational Model:

LibertyX operates as a non-custodial bitcoin exchange, enabling US users to purchase bitcoin after successfully passing through a rigorous customer identification and sanctions screening process. All LibertyX transactions are initiated online through the LibertyX mobile app, where users select “Buy” and specify the amount of bitcoin they wish to purchase. Users are presented with all associated fees and, upon confirming the intent to purchase, receive fulfillment instructions.

¹ Bitcoin ATM Installation Growth (coinatmradar.com)

² <https://www.nbcnews.com/business/business-news/bitcoin-atm-scams-surge-disproportionately-duping-older-adults-rcna168976>

Moon Inc.

864 Spring St. NW
Atlanta, GA 30308
+1 (800) 511-8940



Distinctively, LibertyX does not allow customers to complete payment online. Instead of entering card details online, LibertyX requires customers to physically go to a location of their choosing and use their chip enabled debit card with PIN entry at a LibertyX enabled traditional ATM. Currently, LibertyX PIN debit POS payments exclusively occur at third-party debit card readers integrated into traditional ATMs.³ Leveraging the ATM debit card reader for point-of-sale (POS) payment processing is akin to entering debit card details online, with the added security of requiring a physical card entry and a PIN. These card payments are regular POS card network transactions, fully compliant with card network rules which have been specifically proscribed by networks such as Visa to allow financial institutions to decide whether to approve transactions that consumers attempt⁴. LibertyX does not support credit card fulfillment of virtual currency purchases. Only PIN debit cards that have supported EFT networks such as Visa and NYCE where issuers of the cards approve the properly routed transaction elements are supported.

Distinction from BTMs:

LibertyX's unique funds and customer journey flow often leads to mischaracterization as a BTM company. However, LibertyX does not own or operate BTMs or any hardware. It contracts with third parties solely to "rent" the debit card reader built into the ATM, allowing LibertyX customers to complete payment for their online purchases using debit cards that follow proscribed EFT network rules and only when approved by issuing financial institutions. Requiring an in person visit and coupling that with debit card PIN use serves as a crucial anti-money laundering and fraud control measure (i.e., two-factor payment authentication). Unlike BTMs, LibertyX does not permit simply inputting debit card details on a phone and does not accept cash at ATMs. This critical distinction enables LibertyX to implement additional anti-fraud controls specific to the physical debit card fulfillment method. A consumer cannot walk up to a LibertyX enabled traditional ATM and both initiate and complete a transaction interacting with the ATM itself.

Additionally, one of the concerns commonly raised by regulators regarding BTMs is the high transaction fees they impose. These fees can be prohibitively expensive, deterring legitimate customers from using BTMs for their virtual currency transactions. This deterrence likely leads to a disproportionate amount of BTM transactions being for illicit purposes, as legitimate users seek more cost-effective alternatives.

LibertyX, however, avoids the operational costs associated with BTMs, as it does not manufacture or maintain kiosks, nor does it handle cash logistics. As such, LibertyX does not need to impose the high fees typically charged by BTM companies. The affordability and transparency of our fee structure make our platform more appealing to everyday users looking for a cost-effective way to purchase virtual currency. As a result, LibertyX attracts a vast majority of legitimate customers, with fraud being an

³ In the future LibertyX may contract with third party debit card terminal providers to leverage stand-alone debit card readers or debit card readers built into vending machines or other similar hardware. Debit POS payment transactions are processed identically regardless of the debit card reader hardware used.

⁴ See VBN attachment.

Moon Inc.

864 Spring St. NW
Atlanta, GA 30308
+1 (800) 511-8940



almost insignificant concern relative to our transaction volume. This further distances LibertyX from the regulatory concerns typically associated with BTMs, where high fees are seen as a barrier to legitimate use and a potential indicator of illicit activity.

Exclusion of POS card fulfillment made at traditional ATMs:

LibertyX requests that any proposed legislation explicitly exempts the use of traditional ATMs for POS payments from the definitions of “virtual currency kiosks” and/or “virtual currency kiosk operators. These transactions are fundamentally different from those involving BTMs, which are designed solely to accept and dispense cash in exchange for virtual currency. LibertyX’s use of ATMs for debit card fulfillment aligns with traditional POS transactions as all are proscribed by networks such as Visa and should not be incrementally subjected to the same regulatory framework as BTMs who have no network or sponsor bank guidance that ATMs already do.

ATM initiated, PIN debit POS card payments are subject to stringent card network and sponsor bank requirements designed to protect consumers, issuers, merchants, and the integrity of the overall payment system. One critical requirement is that merchants must keep their chargeback rates below the thresholds set by the National Automated Clearing House Association (NACHA). Chargebacks occur when a cardholder disputes a transaction, often due to fraud or dissatisfaction with the purchase.

To remain compliant, merchants must implement robust fraud prevention measures to ensure that chargebacks remain below the NACHA minimum threshold, typically set at 1% of total transactions. If a merchant exceeds this threshold, they face significant penalties, including increased fees, stricter monitoring, and ultimately, exclusion from participating in card networks.

In contrast, BTMs do not process card payments and therefore do not fall under the same regulatory scrutiny. BTMs accept cash, which lacks the built-in fraud prevention mechanisms inherent in card network transactions. Cash transactions are more challenging to trace and monitor, making BTMs more susceptible to fraudulent activities. Consumers have no claims protection in a systematic manner with BTMs and are subject to terms of service with a given operator. LibertyX PIN debit POS transactions follow network operating rules which delineate clear responsibilities between issuers (banks) and acquirers (ATMs).

Additionally, merchants like LibertyX can partner with payment processors to access the name and card number used for payment. This information can be leveraged to better identify that the individual completing the POS debit payment at an ATM is the same as the one who initiated the transaction, further combating scams such as “pig butchering” that the legislature aims to prevent. This level of verification is not possible with cash transactions at BTMs, highlighting another critical difference that justifies the exclusion of ATM POS card payments from BTM regulations.

Moon Inc.
864 Spring St. NW
Atlanta, GA 30308
+1 (800) 511-8940



Proposed Language for the Bill:

To ensure clarity and prevent misclassification, we propose the following language be added to the bill:

Exclusion Clause:

“Virtual currency kiosk” does not include devices that:

- Utilize debit card readers solely for payment processing without accepting cash.

Definitions:

“debit card readers” refers to devices, whether standalone or integrated into an ATM, vending machine, or any other hardware, used exclusively for processing card payments.

From our experience, the above express language is necessary as we continue to encounter confusion among state regulators despite regulations defining “virtual currency kiosk” as a “*cash*” accepting device.

Additional Specific Exemption Request:

We have also observed misclassifications of third-party ATM owners/operators as “authorized delegates.” Third-party debit card reader owners should not be designated as authorized delegates. These providers are not involved in the transaction or funds flow; they merely supply the hardware used to process debit card payments. It is more accurate to describe them as “debit card terminal hardware providers.” The use of debit card readers for POS processing is common in various industries. For example, money transmitters like Western Union use debit card readers to process payments, but the providers of these readers are not considered authorized delegates of the retailers. Similarly, LibertyX’s use of debit card readers should not result in the classification of these hardware providers as authorized delegates. Thus, in the event that our request for a complete exemption is denied, we respectfully request an exemption from any requirements to register ATM locations and/or ATM owner/operators as authorized delegates.

Conclusion

LibertyX’s unique operational model and compliance measures clearly differentiate it from traditional virtual currency kiosk operators. Including the proposed exclusion clause in the bill will prevent any

Moon Inc.

864 Spring St. NW
Atlanta, GA 30308
+1 (800) 511-8940



potential misclassification and ensure that LibertyX, or any other similarly situated businesses, are not inadvertently regulated under this legislation.

We appreciate your consideration of our request and do support the creation of a regulatory framework. We would also welcome the opportunity to meet on this topic to answer any questions you have about LibertyX, explain how we differ from BTM companies, and highlight the extent to which we prioritize fraud prevention. Please let us know if a follow-up conversation is possible.

Sincerely,

Simon Spektor, Esq. CAMS
Chief Counsel & Compliance Officer, LibertyX

APPENDIX C-11

Letter from Mark Paolillo, CFO and CCO, Byte Federal, Inc., to Kelley Reed,
Regulatory and Consumer Affairs Dir., Banking Div., Vt. Dept. of Fin. Regul.
(Sept. 24, 2024).

Byte Federal, Inc.
2389 E. Venice Ave, #504
Venice, FL, 34292



Subject: 8 V.S.A. § 2577(g) - VC Kiosks Comments

September 24, 2024

Dear Vermont Department of Financial Regulation,

We appreciate the opportunity to provide feedback on the proposed regulations under 8 V.S.A. § 2577(g). Although we do not currently operate in Vermont due to the regulatory environment, we believe it is critical to participate in this discussion. The virtual currency industry requires thoughtful regulation to promote consumer protection and sustainable industry growth. However, the proposed limits on fees and daily transactions for Bitcoin kiosk operators raise serious concerns that we believe deserve close consideration.

Recently, we had the opportunity to speak at the Money Transmitter Regulators Association (MTRA) Annual Conference in Philadelphia. It was a great experience discussing virtual currency kiosks and the evolving technology behind them.

The conversation centered around how we, as an industry, can collaborate with regulators to strengthen consumer protection and implement effective safeguards against fraud and illicit activity. We hope the insights shared will help support informed decision-making and contribute to shaping sound policies that benefit both the industry and consumers alike.

We want to be a resource and partner in this process. If we can assist further—by providing an educational overview of virtual currency technology and our compliance measures, or by offering industry insights—please don't hesitate to reach out.

We are here to support you in any way we can as we work together to ensure the safe and responsible growth of our industry.

Introduction

While we strongly support regulations aimed at combating fraud and illicit activity, such regulations must address these issues in a targeted and effective manner. Unfortunately, the arbitrary limits proposed on fees and daily transactions fail to consider the operational realities of Bitcoin kiosks, which operate under stringent federal and state regulations. These restrictions risk stifling innovation and complicating compliance without effectively deterring criminal activity.

In the following sections, we outline why these proposed limits will not achieve their intended goals and, instead, undermine the industry's ability to support law enforcement efforts while maintaining sustainable operations. We urge Vermont regulators to reconsider these proposals and collaborate with industry participants to craft regulations that truly address illicit activity without imposing undue burdens on legitimate businesses.

Caps on Fees

The proposed fee cap of 15% or \$5 per transaction poses significant challenges for Bitcoin kiosk operators. These limits do not address scams or illicit activity and instead threaten to undermine the viability of our business model. While modeled after California's regulations, the economic impact on industry participants has not been fully considered.

Bitcoin kiosk operators face substantial operational costs that other financial services do not, including compliance with both federal and state regulations, higher banking fees, third-party cash transport services, machine maintenance, customer support, and ongoing software development. These expenses are essential to running a compliant, secure business, and they exceed the margins that a 15% cap would allow. Limiting fees without regard to these realities will only force many operators out of business.

Moreover, comparable industries like peer-to-peer payment systems and traditional money transmitters face no such fee limits despite being susceptible to the same types of scams. If fee

caps were a proven solution to combating fraud, they would have been applied across these sectors. The reality is that these caps do not stop fraud—they only make it harder for compliant businesses to operate sustainably.

By capping fees, Vermont would limit consumers' access to secure and regulated financial services while driving them to unregulated alternatives. Rather than arbitrary fee limits, the focus should be on policies that target fraudulent activity directly, such as enhanced compliance, better consumer education, and fostering industry collaboration.

One must assume that the motive for such laws is simply to eliminate the industry and not eliminate the scam.

Daily Transaction Limits

Setting a daily transaction limit, such as the \$1,000 cap seen in California, does little to deter scams or illicit activity. In fact, it hinders Bitcoin kiosk operators' ability to fulfill their compliance obligations, particularly in filing FinCEN reports, including Currency Transaction Reports (CTRs) and Suspicious Activity Reports (SARs).

The FinCEN thresholds for reporting are \$2,000, \$3,000, and \$10,000, and these thresholds are critical for tracking and prosecuting bad actors. With a \$1,000 daily limit, it becomes impossible for operators to identify patterns of structuring, where customers break up transactions to avoid detection. This restricts our ability to monitor suspicious activities and report it to law enforcement.

Additionally, customers circumventing these limits by using multiple operators prevents us from gaining a comprehensive view of their activity, further complicating compliance efforts. These limits obstruct the very transparency that is essential for combatting fraud and illicit finance.

Our compliance department, staffed by experienced professionals, is dedicated to reviewing transactions and reporting suspicious activities. However, the proposed limits would significantly

diminish the amount of useful data we could provide to law enforcement. This makes it harder, not easier, to identify and stop bad actors.

We urge Vermont to reconsider these arbitrary limits, as they undermine the effectiveness of the very safeguards we have put in place to combat illicit activity.

Proven Methods for Combating Illicit Activity

At our Bitcoin kiosks, we have implemented a robust suite of anti-fraud measures that are notably absent from Vermont's proposed regulations. Our focus on risk mitigation goes beyond arbitrary limits and addresses the specific ways in which scams and fraudulent activity occur.

Key components of our fraud prevention strategy include:

- A comprehensive **Know Your Customer (KYC) policy** that applies to every transaction, regardless of size. Customers must provide full identification details, including government-issued photo ID, a selfie, source and use of funds, and their cryptocurrency wallet address. Wallet addresses are automatically screened against the Chainabuse.com database to preempt potential illicit activity.
- **Automated scam deterrent messages** sent to all customers, as well as non-bypassable screens that educate them on common scams.
- **Additional support for vulnerable populations**, particularly customers aged 60 or older, who must complete a call with our support team before transacting. Our staff is trained to identify signs of potential fraud during these conversations.

These measures, combined with our comprehensive compliance protocols, allow us to detect and prevent fraudulent activity effectively. The proposed regulations in Vermont do not account for these important practices, which are far more effective than arbitrary fee and transaction limits in combating fraud.

Conclusion

We believe that regulation is crucial for the growth and integrity of the virtual currency industry. However, regulations must be designed with a clear understanding of how illicit activity occurs and the practical realities of operating a regulated business. The fee caps and daily transaction limits proposed in Vermont's regulations will only stifle innovation and hinder the ability of legitimate operators to comply with the law.

One must assume that the motive for such laws is simply to eliminate the industry and not eliminate the scam. The fraud will continue whether virtual currency kiosks exist or not.

We stand ready to collaborate with regulators to develop meaningful, targeted policies that enhance consumer protection, promote industry growth, and effectively combat fraud. If we can provide further insights or assistance in refining these regulations, we would be happy to do so.

Thank you for considering our comments.

Sincerely,

Mark Paolillo, CPA, CGMA

Byte Federal, Inc.

CFO, CCO

2389 E. Venice Ave, #504

Venice, FL, 34292

Mark@ByteFederal.com

941-716-4307

APPENDIX C-12

Letter from Mark J. Smalley, Chief Compliance Officer, Bitcoin Depot, to Vt.
Dept. of Fin. Regul. (Oct. 11, 2024).



Department of Financial Regulation
Comment Intake - 8 V.S.A. § 2577(g) - VC Kiosks
Attention: DFR Director Kelley Reed
89 Main Street, Montpelier, VT 05620-3101

BITCOIN DEPOT
2870 Peachtree Rd. NW, #327
Atlanta, GA 30305
www.bitcoindepot.com
PH: (678) 961-0059
FAX: (470) 430-3609

October 11, 2024

Re: 8 V.S.A. § 2577(g) - VC Kiosks Comments

Thank you for the opportunity to provide this comment letter on House Bill 659 as the legislature and Department Commissioner continue to assess virtual currency kiosk business activity and regulations in Vermont. As we shared during the crafting of the bill, we have concerns about the effectiveness of the bill to allow legitimate operators and customers to do business in the state. Before addressing our specific concerns and suggested considerations, we offer background on our Company.

Bitcoin Depot's Primary Business Model

The Company's primary business model is to buy and sell Bitcoin. Bitcoin Depot operates company-owned Automated Teller Machines (BTMs or kiosks) throughout the United States, Puerto Rico, Australia and Canada that are installed at various locations, such as convenience stores and gas stations. Nearly all of the kiosks only have the ability to sell Bitcoin to customers, while a limited number of the kiosks offer customers the ability to sell Bitcoin to the Company. Our customers value our product for its convenience, speed, physical presence and ability to directly own their cryptocurrency as opposed to an exchange; shielding them from the risks of a total loss of their assets in the event of an exchange's financial collapse such as the one we saw in the case of FTX.

Bitcoin Depot's History and Commitment to Compliance

The Company was established in 2016 and has grown to its current state by investing in people, technology, and processes that support a culture of compliance. The Company became a public entity on June 30, 2023, and trades on the NASDAQ under the ticker symbol BTM. As a public company, the Company is fully accountable to and regulated by the Securities & Exchange Commission (SEC). Additionally, the Company is a registered Money Services Business (MSB) with the Financial Crimes Enforcement Network (FinCEN) and maintains state money transmitter licenses throughout the country.^{1,2} The Company is and has always been committed to compliance and working cooperatively with state and federal agencies of all types for the betterment of the Company, industry, and financial system.

Bitcoin Depot's Monitoring Process and Consumer Safeguarding

The Company has implemented various safeguards for consumers and the financial system. It employs the most state-of-the-art and sophisticated transaction monitoring and case management software to detect

¹ Currently, the company has nineteen state money transmitter or virtual currency licenses, and other pending license applications are in process. For states where the Company does not maintain a license, it periodically confirms with the state to confirm that no license is required to operate in such state.

² With the IRS being the primary regulatory body overseeing MSBs.



BITCOIN DEPOT

and prevent financial crimes.³ Additionally, the Company utilizes third-party blockchain analytics services to identify higher-risk and criminal wallets. More specifically:

- The Company has implemented a number of customer-facing safeguards to warn about scam-related activity, such as hard copy warnings physically present on the kiosk, on screen notices, several of which require the customer to make affirmative attestations before moving past the screen, and short text messages. (Copies of these warning messages are attached as **Appendix A** to this letter).
- The Company has invested considerable resources to deploy third-party blockchain analytic software and other technology-based solutions for sanction monitoring, Office of Foreign Assets Control (OFAC) and Politically Exposed Person (PEP) screening. These technologies allow us to flag and report suspicious activity at our kiosks in instances related to terrorist financing, child exploitation or human trafficking - regardless of transaction size.
- Customers designate a digital wallet of their choice that must be in the customer's control pursuant to the Company's Terms & Conditions. The Company does not host customer wallets, nor does it assume custody of customer funds.
- As a requirement prior to completing a transaction, the customer must agree to the Company's publicly available [Terms & Conditions](#) which mandate that the customer is required to send the Bitcoin only to their own wallet.
- The Company links the customer's wallet address to his/her user account in an effort to block Bitcoin from being sent to third parties.
- The Company only sells Bitcoin and does not sell or provide services for any other cryptocurrency.

Bitcoin Depot's Mature Compliance Program

The Company's Chief Compliance Officer directly reports to the Company's Chief Executive Officer (CEO). Bitcoin Depot's compliance program is fully documented in policies and procedures and is reviewed annually by an independent third-party auditor. The Company's Compliance program includes the following:

- Bank Secrecy Act (BSA)/Anti-Money Laundering (AML)/Office of Foreign Assets Control (OFAC) Compliance.
 - The Chief Compliance Officer, Mark Smalley, has over 25 years of applicable legal and compliance experience.
 - Two dedicated AML compliance teams - one focused on customer diligence and one focused on transaction monitoring and investigations.
 - Dedicated analysts for Know Your Customer (KYC), OFAC, sanctions, and Politically Exposed Person (PEP) alerts.
 - The BSA / AML / OFAC Compliance team is comprised of approximately 15 individuals exclusively dedicated to financial crime and sanctions compliance.
 - Dedicated resources to suspicious activity reporting, currency transaction reporting, and funds travel rule compliance.
 - Enterprise Risk Management (assessments, self-testing, and training regarding compliance for the areas above in addition to third-party risk management and business resiliency).

³ According to Chainalysis, the leading provider of blockchain analytics and data on the cryptocurrency economy, in 2022 there was \$20.6 billion in fraud across the entire cryptocurrency economy. Kiosks, such as BTMs, represented less than 1% of that total.



BITCOIN DEPOT

- **Licensing & Registration**
 - Registered with FinCEN as an MSB (federal).
 - Registered with the Secretary of State in every state, the District of Columbia and Puerto Rico.
 - For state money transmitter licenses (MTL), the Company is either licensed in the state or periodically confirms with the state that its no-action position remains unchanged. Currently, the company has nineteen state money transmitter or virtual currency licenses, with a dedicated team to licensing and registration.
 - Other pending MTL Applications are in process.
- **Privacy and Consumer Compliance**
 - Dedicated compliance resources to ensure compliance with all applicable consumer protection laws, including complaints, funds availability, abandoned property, and refunds.
 - Dedicated resources to compliance with all applicable federal and state privacy laws, including contract provisions, data accessibility, and opt-in / opt-out provisions.

Key Legislative Components Should be Reconsidered

1. Transaction Limits and the Unintended Consequences

Placing an arbitrary deposit and withdrawal limit on a customer may decrease customer protection and the ability to detect malicious actors. As customers increase their purchases, cryptocurrency kiosk companies require additional forms of identification and authentication. Imposing arbitrary limits on a transaction amount undermines the additional authentication and verification steps and instead encourages bad actors to spread transactions across multiple companies in smaller amounts, potentially obscuring their activities and identities. Additionally, daily limits such as that passed in Vermont, skirt federal reporting requirements - Currency Exchange Record (CER) at \$1,000, Monetary Instrument Log (MIL) at \$3,000, Funds Travel Rule (FTR) at \$3,000, and Currency Transaction Report (CTR) at \$10,000 - which translates routine reporting obligations into obfuscation.

Pertinent suspicious activity reporting is also likely to be negatively impacted. Federal regulations have strict guidelines for filing a suspicious activity report (SAR) of any suspicious transaction over \$2,000. SARs, along with other transaction reporting, are indispensable tools of law enforcement (e.g., law enforcement has access to and can review and analyze these critical forms of intelligence to support its investigations, and quickly request supporting documentation regarding transactions, digital wallet addresses, correspondence, and KYC identification).⁴

Lower daily limits likely will lead to transactions being spread across multiple companies and eliminate certain reporting that is essential information to law enforcement. This is imperative at a time when human and drug trafficking are on the rise, with the Government Accountability Office (GAO) finding a fivefold increase from 2017 to 2020 for SARs filed that involved virtual currency and drug trafficking, and that sensitive data on virtual currency use for human and drug trafficking “may not be consistently captured.” (See U.S. Government Accountability Office report on virtual currencies, GAO-22-105462, dated December 2021.) While Bitcoin Depot understands the issues brought on by fraud by some bad actors and empathizes with the victims, Vermont’s approach, although good intentioned, may end up having little effect on protecting consumers and a reverse effect on other public concerns and illicit activities as described in GAO-22-105462.

⁴ See 31 CFR § 1022.320.



BITCOIN DEPOT

2. “Fee Caps” Will Remove Compliant Operators From Vermont

Operating a cryptocurrency kiosk has unique costs, including purchasing, installing, and maintaining the kiosk equipment. There are also recurring costs, including rent to small businesses hosting a kiosk, insurance, legal fees, bank fees, blockchain access fees, cash management, armored vehicles, monitoring and surveillance, BSA / AML compliance, OFAC compliance, cybersecurity, fraud detection, and customer support. Vermont should desire to have the most reputable BTM operators in the state (which have higher costs of compliance) for consumer protection. Other states allow for market-driven transaction exchange rates and fees, which allows for competition and larger more reputable operators to do business in their states. Unfortunately, Vermont has not only broadly defined what constitutes a “fee” by including exchange rates (a practice inconsistent with how it treats foreign currency exchange) but has imposed unrealistic caps that will drive reputable operators from the state.

BTM companies must maintain an inventory of cryptocurrency offerings that could fluctuate as much as 10-30% on any given day. While cryptocurrency exchanges may charge a lower fee or have a lower exchange rate, they do not offer customers the same convenience and ease of using a kiosk at their local convenience store to make a voluntary purchase of cryptocurrency with cash. In fact, exchanges do not offer customers who want to buy cryptocurrency with cash any option — which also means exchanges have lower operational costs and can charge lower fees than crypto kiosk companies. This is because exchanges do not have hardware, cash management fees, maintenance and repair costs, wireless internet, insurance on hardware, rental payments to stores, or other operational expenses.

Since the law’s implementation, we have found that compliant operators have been pushed out of the state by overly burdensome regulatory practices and arbitrary transaction limitations put in place by the law. Similarly, Bitcoin Depot has ceased operations altogether in Vermont. The exit of compliant operators is thus leaving only smaller operators who may lack similar resources to combat fraud and effectively aid in addressing broader money laundering issues. Vermont should reconsider its approach to how it defines a fee and the related requirements placed on kiosk operators.

3. Regulatory Efficiency and Supporting Innovation

The Department should consider actions that create more efficiency for industry players and regulators alike, and reduce unnecessary regulatory burdens for larger multistate entities that are subject to multiple layers of regulation, especially those that are publicly traded on the NYSE or NASDAQ. For example, Vermont should consider, consistent with § 2500 (Purpose) in HB 659, working more closely with other states to provide for streamlined licensing, examination coordination, information sharing, and license reciprocity, especially for entities that maintain the NY Bitlicense or have Money Transmitter licenses or similarly equivalent virtual currency licenses in a number of other states. These concepts support a healthy financial system, allowing companies to innovate to provide better products and services to consumers and allow regulators to focus limited resources on the true bad actors.

Respectfully, it is difficult to see how HB 659 has provided a real solution while unnecessary regulatory burdens continue to increase. For example, Vermont has adopted an outlier approach in its licensing requirements. Vermont requires operators to secure multiple licenses in the Nationwide Multistate Licensing System & Registry (NMLS) system for the same company, including a standard Money Transmitter license and a license for a trade name (DBA). Now, Vermont is requiring NMLS licensure for each individual kiosk. In other words, Vermont is requiring multiple licenses and NMLS entries for one company, whereas most states that require a money transmission license only require one entry in NMLS.

While Bitcoin Depot commends states’ efforts, such as Vermont, in passing the Modernization Model Act, which purpose is stated in 8 V.S.A. § 2500 to “eliminate unnecessary regulatory burden and more effectively use regulator resources” and “support[] innovative and competitive business practices,” the effectiveness of such effort will be commensurate with each state’s implementation and practices. States’ inability to support uniformity, efficiency and consistency for multistate companies will continue to increase the calls for and potential for federal preemption in this space, leaving the states at that point with a limited to no role



BITCOIN DEPOT

in supervision.⁵ In addition, driving out competition from the state through onerous regulation is likely to have the opposite effect of bolstering consumer protection by giving consumers less options when choosing to use alternative banking methods, such as BTMs.

Conclusion

Bitcoin Depot is proud of the company that we have established and the services we provide to consumers in the United States, Canada, and Vermont. Vermont should be, likewise, excited to have companies like Bitcoin Depot doing business within the state. Bitcoin Depot has established itself as a key player in an emerging market that has balanced economic growth with Compliance and Consumer Protection. Our Company wants Vermont to regulate this space to encourage the good actors to flourish while weeding out the bad actors.

Bitcoin Depot respectfully requests the opportunity to have additional conversations with the Legislature to allow for a better understanding of a complex and non-traditional technology that is elective yet appealing to many Vermont citizens looking to diversify their assets and financial tools. We look forward to additional conversations, and please do not hesitate to contact me with any questions.

DocuSigned by:

Mark Smalley

3018EDC30FFF4F9...

Sincerely,

/S/ Mark J. Smalley

Mark J. Smalley,
Chief Compliance Officer

⁵ See Remarks by Under Secretary for Domestic Finance Nellie Liang “Modernizing the Regulatory Framework for Domestic Payments” at the Chicago Payments Symposium, hosted by the Federal Reserve Bank of Chicago, October 9, 2024 (<https://home.treasury.gov/news/press-releases/jy2639>).




Appendix A





BITCOIN DEPOT

 **BITCOIN DEPOT**

Enter SMS Code

Please enter the 6-Digit verification code sent to your mobile

Haven't received your verification code yet?

[Call me instead](#)

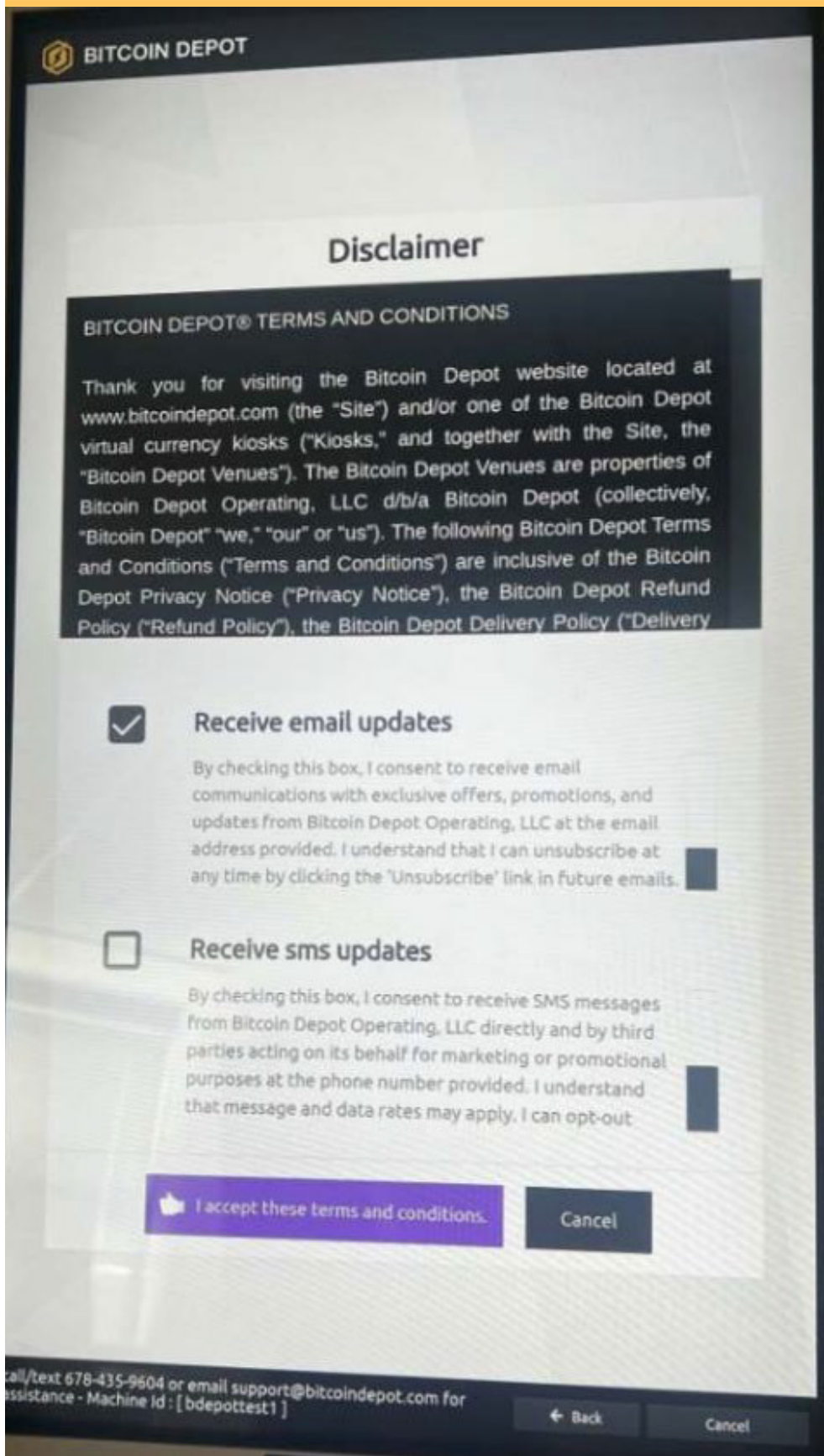
1	2	3
4	5	6
7	8	9
+	0	⌫

[Proceed](#)

Use a Secret PIN instead of SMS text going forward?

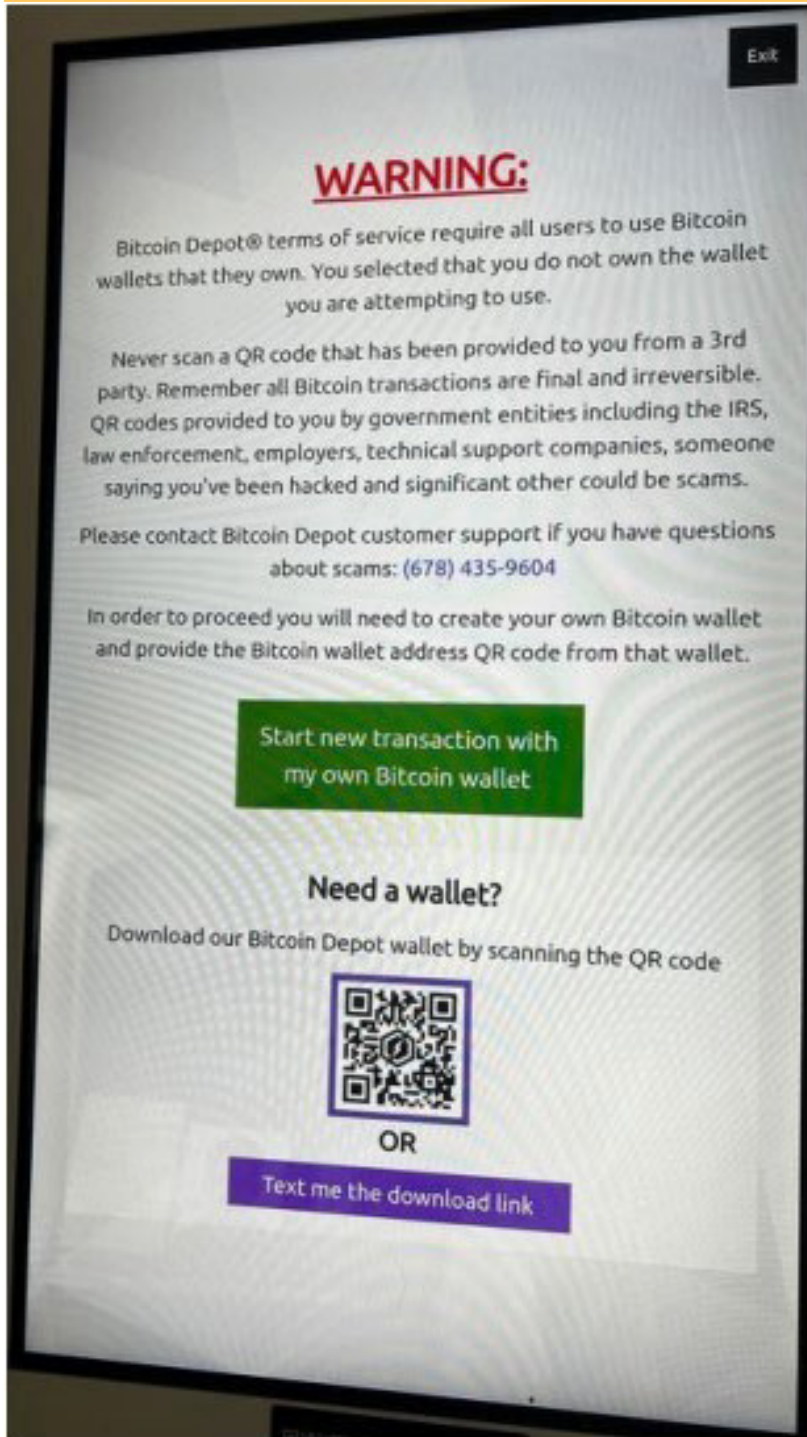
If someone else sent you to this machine and provided you with a QR Code or wallet ID to send funds to, it is most likely a scam.

call/text 678-435-9604 or email support@bitcoindpot.com for assistance - Machine Id : [nathan9] [Cancel](#)





BITCOIN DEPOT



 **BITCOIN DEPOT**

Scan your digital wallet

Make sure that your entire QR Code is visible on the screen below



Wallet Already in Use

This wallet is already associated with another customer account. Please continue with a different wallet address or call or text Customer Support at (678) 435-9604 if you believe it's yours.

[Continue transaction with a new wallet address that belongs to you](#)

If you need a wallet, see the instructions below if you'd like to download our Bitcoin Depot mobile app.

Need a wallet?

Download our Bitcoin Depot wallet by scanning the QR code



OR

[Text me the download link](#)

call/text 678-435-9604 or email support@bitcoindotcom for assistance - Machine Id : [nathan2]

[← Back](#) [Cancel](#)



BITCOIN DEPOT



BITCOIN DEPOT

[Locations](#)

[Buy Crypto](#) ▾

[Learn](#) ▾

[Partner With Us](#) ▾

[Company](#) ▾

ATTENTION: SENDING TO A WALLET THAT YOU DO NOT CONTROL IS AN EXPRESS VIOLATION OF OUR TERMS AND WILL RESULT IN YOU BEING BANNED FROM OUR PLATFORM.



BITCOIN DEPOT

ARE YOU BEING SCAMMED?

ARE YOU BEING SCAMMED? Do not buy bitcoin for IRS
payments, utility bills, or if someone says you have been
hacked or are being investigated. These are scams!

WARNING: LOSSES DUE TO FRAUDULENT OR
ACCIDENTAL TRANSACTIONS MAY NOT BE
RECOVERABLE AND TRANSACTIONS IN VIRTUAL
CURRENCY ARE IRREVERSIBLE

Exit

Continue



BITCOIN DEPOT

New Customer SMS Scam Warning

10:36 PM

Warning! Don't use Depot's ATMs for payments to any govt entities, law enforcement, employers, tech support companies, anyone saying you've been hacked, or significant others, as it's likely a scam. Don't use a QR code provided by a 3rd party. Need help? Call 678-435-9604.

APPENDIX C-13

CoinFlip's Written Comments on 8 V.S.A. § 2577(g) (Oct. 15, 2024).



CoinFlip's Written Comments on 8 V.S.A. § 2577(g)

Pursuant to the Vermont Department of Financial Protection's September 17, 2024 request for comment on 8 V.S.A. § 2577(g) regarding virtual currency kiosks, CoinFlip respectfully requests the State of Vermont reconsider specific portions of 8 V.S.A. § 2577(g) and the negative effects it has on responsible virtual currency kiosk operators. Responsible virtual currency kiosk operators employ robust consumer protections that protect consumers while still allowing operation in the State of Vermont. Despite statements by the legislature that they did not want to drive virtual currency kiosk operators out of business in Vermont, this statute has unfortunately done just that. Although responsible virtual currency kiosk operators want to continue operations, they are unable to due to these restrictions. CoinFlip appreciates the opportunity to offer additional consumer protection-focused recommendations that it knows to be highly effective through experience.

Company Background

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

CoinFlip's kiosks make buying and selling major virtual currency accessible and secure for consumers who wish to purchase their virtual currency using cash. CoinFlip operates three virtual currency kiosks in the State of Vermont and holds a Money-Transmitter-License granted by the State's Department of Financial Regulation on September 24, 2021. Under Vermont law, CoinFlip must apply for, and Vermont must approve, each location prior to operating a virtual currency kiosk.

Since 2015, CoinFlip has been a money service business registered with the Financial Crimes Enforcement Network ("FinCEN") and subject to the Bank Secrecy Act ("BSA"), the United States PATRIOT Act, and their implementing rules and regulations. As a money service business, CoinFlip maintains enhanced due diligence policies and procedures. CoinFlip embraces licensing regimes as effective means to create baseline requirements for operations, as well as effective oversight. CoinFlip currently has approximately 26 money transmitter licenses or virtual currency licenses associated with its kiosk business across the country and numerous additional applications currently pending with additional states. CoinFlip has moved to obtain these licenses, even in states where the current regulatory regime may not specifically cover virtual currency kiosk operators. CoinFlip undergoes periodic audits in each of its licensed jurisdictions with reviews of its compliance, finance, and cybersecurity programs.

CoinFlip's compliance and consumer protection efforts are overseen by its Chief Legal & Compliance Officer, General Counsel, BSA Officer and Global Head of AML, and a dedicated

Consumer Protection Officer. This group, led by a former senior federal prosecutor, collectively has decades of consumer protection, compliance and AML experience addressing sophisticated and novel financial scams, including those targeting the elderly. CoinFlip's Know Your Customer ("KYC") and AML policies and procedures, internal controls, and training programs reflect this expertise and are reviewed and updated on a regular basis to account not only for changes in regulations, but also changes in CoinFlip's business model, emerging industry trends, and best practices gleaned from participation in industry associations. CoinFlip is an enterprise member of the Association of Certified Anti-Money Laundering Specialists (ACAMS), the largest international membership organization for anti-financial crime professionals. Our in-house compliance department is certified through ACAMS, which is the gold standard for anti-money laundering certification and is recognized by governments and regulators worldwide. ACAMS certification is an important tool for any money service business to combat, prevent, and investigate fraud.

CoinFlip's compliance team utilizes state-of-the-art blockchain analytics and compliance tools to help prevent, detect and report fraud. These tools screen and block sanctioned wallets and wallets linked to criminal activity. They also help our team detect and report potential suspicious activity through the filing of Suspicious Activity Reports. In addition to blocking transactions, CoinFlip permanently blacklists digital wallet addresses to prevent those high-risk digital wallets from ever being used at a CoinFlip kiosk again.

8 V.S.A. § 2577(g) – Virtual Currency Kiosks

Unfortunately, 8 V.S.A. § 2577(g) relies on policy recommendations that create a false sense of consumer protection, and result in a de facto ban for virtual currency kiosks in Vermont. CoinFlip still has three virtual currency kiosks in Vermont that are currently operating at a loss. Under information and belief, CoinFlip believes most other operators, if not all, have pulled out of Vermont due to the financial circumstances imposed by 8 V.S.A. § 2577(g). CoinFlip continues operations in Vermont in hopes of additional conversations over these regulations and to ensure its commitment to

The imposed transaction limits do not adequately consider federal reporting requirements. Under federal law, CoinFlip is required to file a Suspicious Activity Report ("SAR") for any suspected suspicious transactions above \$2,000 and a Currency Transaction Report ("CTR") for transactions above \$10,000. This information is placed in a repository for law enforcement to quickly and accurately conduct investigations. Vermont's \$1,000 transaction limit encourages stacking transactions across multiple kiosk operators, and limits companies' Anti-Money Laundering efforts. Further, the limit will result in less information available to law enforcement as kiosk operators will no longer file any SAR or CTR.

The addition of transaction fee caps does not prevent customer fraud and in combination with transaction limits, inadvertently creates incentives for less transparency and less use of expensive compliance tools which keep consumers safe. Unlike online exchanges, kiosk operators have additional operational costs such as device hardware and maintenance, rent payments to local small business hosts, armored car service costs, customer service, holding stores of virtual currency, and

blockchain analytics. In fact, due to the transaction fee caps, there are circumstances where online exchanges are now *more expensive* than transactions at virtual currency kiosks, including situations where an individual is purchasing virtual currency online via credit or debit card. Other states that have considered legislation for virtual currency kiosks have realized these unique expenses and increased the fee caps accordingly. The proposed Vermont fee limits do not take into consideration these unique operational costs and are a de facto ban of kiosks in Vermont.

Proposed Consumer Protection Policies

CoinFlip believes smart regulation is good for business. CoinFlip believes that a regulatory framework is necessary to protect consumers and encourage innovation in the industry. As a result, the Company developed the following best practices that would further enhance consumer protections:

- **Require licensure with the state.** CoinFlip agrees that a money transmitter license should be required for all digital currency kiosk operators, allowing for state oversight and periodic audits to determine the adequacy of compliance, finance, and cybersecurity programs.
- **Require robust compliance programs.** Virtual currency kiosk operators should be required to directly employ a qualified, in-house, Chief Compliance Officer and compliance team, that does not have a large ownership interest in the company.
- **Require clear, highly visible warnings and fee disclosures.** CoinFlips agrees with the requirement of clear disclosures regarding all fees and terms of service. CoinFlip also believes highly visible fraud warnings should be required to be displayed and acknowledged by the customer prior to the initiation and completion of any transaction.
- **Require blockchain analytics.** The use of blockchain analytics technology should be required to prevent fraud by automatically blocking customer transactions to high-risk digital wallets.
- **Require live customer service.** Customer service is the first line of defense for consumer protection. CoinFlip believes every virtual currency kiosk operator should be required to provide trained, live customer service for a minimum during business hours. CoinFlip's customer service is trained at least biannually related to compliance requirements and financial crime typologies with an emphasis on fraud and fraud prevention.

Conclusion

CoinFlip believes that a regulatory framework is necessary to protect consumers and encourage innovation; however, 8 V.S.A. § 2577(g) has proven to be an unworkable solution for virtual currency kiosk operators and a de facto ban. CoinFlip shares the goal of consumer protection, but 8 V.S.A. § 2577(g) does not implement the policies to achieve it. Although blockchain technology and virtual currency kiosks are new, the fraud we see reported is all too familiar. Whether it's phone, email, text or an online pop-up, scammers repackage the same old tactics and utilize

whatever methods they have at hand – Venmo, PayPal, Zelle, Gift Cards, MoneyGram or Bitcoin ATMs – to dupe people out of their money.

CoinFlip looks forward to working with the Vermont legislature and this committee to improve 8 V.S.A. § 2577(g) to achieve the right balance to protect Vermonters and ensure continued access for lawful virtual currency transactions.