



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