COINFLIP

03/12/2024

House Commerce Finance and Policy Committee
Minnesota House of Representatives
100 Rev. Dr. Martin Luther King Jr. Blvd.
Saint Paul, MN 55155

Re: ***Opposition to H.F. No. 4717 as written***

Chair Stephenson, Vice-Chair Kotyza-Witthuhn, and honorable members of the Commerce Finance and Policy Committee. Thank you for the opportunity to express our concerns on H.F. 4717. CoinFlip opposes H.F. 4717 as currently written but welcomes the opportunity to work with the Minnesota legislature on improving the bill to enhance consumer protection.

CoinFlip Company Background

Incorporated in December 2015 and headquartered in downtown Chicago, CoinFlip operates over 4,500 Bitcoin Automatic Teller Machines ("BATMs") across 49 states, the District of Columbia, Puerto Rico, Canada, Australia, Panama, Brazil, Italy, and South Africa. These kiosks allow customers to purchase Bitcoin and other select virtual currency with physical fiat currency. The Company sells its own stores of virtual currency directly to customers, charging a markup as well as a blockchain fee. CoinFlip does not custody customer funds or virtual currency.

Culture of Compliance

CoinFlip is a money service business ("MSB") registered with the Financial Crimes Enforcement Network ("FinCEN"). As an MSB, CoinFlip is subject to the Bank Secrecy Act ("BSA"), the United States PATRIOT Act, and their implementing rules and regulations. CoinFlip is required to develop and maintain Know Your Customer ("KYC") and anti-money laundering ("AML") policies and procedures that align with its risk profile. CoinFlip's BSA/AML policies, dedicated resources, internal controls, and training program are designed to ensure compliance with all applicable BSA regulations and are reviewed and updated on a regular basis to account for both changes in regulations and changes in CoinFlip's business model. As an MSB, CoinFlip also maintains enhanced due diligence policies, including policies and procedures aimed at identifying and protecting senior citizens.

CoinFlip embraces licensing regimes as an effective means to create baseline requirements for operations, as well as effective oversight. CoinFlip currently holds approximately 14 money transmitter licenses or virtual currency licenses associated with its kiosk business and numerous additional applications currently pending. As a licensee, CoinFlip is required to undergo periodic audits in each jurisdiction with reviews of its compliance, finance, and cybersecurity programs.

Consumer Protection

As a company, one of CoinFlip's key priorities is consumer protection. Our company will not succeed unless our customers believe we provide them with a safe and secure platform from which to transact virtual currency. CoinFlip's compliance and consumer protection efforts are currently overseen by its Chief Legal Officer, General Counsel, BSA Officer, and Consumer Protection Officer. To effectively manage the risks associated with its operations, CoinFlip implements both traditional consumer protection efforts such as clear disclosures and warnings, as well as state-of-the-art technology to detect and prevent fraudulent transactions.

When transacting with a CoinFlip kiosk, customers are warned numerous times regarding scam-related activity prior to initiating *every* transaction. The customer must attest that they were not sent to the kiosk in order to make a payment; that they are transacting with a digital wallet they own; and that they understand all transactions are final and irreversible. This screen is customizable and is updated with warnings about common scams to alert customers and help prevent fraud.

Additionally, CoinFlip has 24/7 live customer service and lists its number both on the physical kiosk as well as its transaction screens. Customers are instructed to call CoinFlip in the event a third-party sent them to transact at the kiosk. CoinFlip customer service receives training at least twice annually on AML/BSA requirements and how to be the first line of defense in compliance efforts. As a result of these efforts, between December 2023 and February 2024 alone, CoinFlip halted over 300 transactions due to our customer service identifying a potential scam.

Traditional consumer protection efforts, such as highly visible, consumer alerts prior to initiating and completing transactions, are effective. However, CoinFlip believes it is essential that virtual currency kiosk operators also implement technology solutions to prevent fraud before it can occur.

CoinFlip implements state-of-the-art blockchain analytics and compliance tools to block fraudulent transactions and investigate suspicious activity. It is a technology that works. Since April 2022, CoinFlip has automatically blocked more than 1,230 transactions using blockchain analytics. 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. Implementing these technology measures, in conjunction with highly visible consumer alerts are important and highly effective tools in preventing fraud at digital currency kiosks.

Lastly, it is imperative that an MSB continuously monitor patterns in fraud. As a result, CoinFlip appointed a Consumer Protection Officer whose job includes managing and maintaining its Consumer Protection Policy. As part of these efforts, CoinFlip periodically conducts cross functional meetings between its legal, compliance, and fraud investigation teams to monitor customer behavior and to identify any consumer protection issues. As any financial institution can attest to, consumer protection and compliance require continuous effort and cannot be left to static policies and procedures.

H.F. No. 4717

Minnesota recently introduced H.F. No. 4717 in order to regulate virtual currency kiosk disclosures, transaction limits, and transaction fees. Unfortunately, H.F. 4717 relies on faulty policies such transaction limits, fee caps, and refund language that create a false sense of consumer safety while not addressing the root cause of scams and fraud.

First, the proposed transaction limits do not adequately consider existing federal reporting requirements. Arbitrarily low transaction limits create an unintended consequence of encouraging the structuring of transactions to further obscure federal reporting requirements, creating less transparency and information being reported to law enforcement. Current federal reporting requirements require the filing of Suspicious Activity Report ("SAR") for any suspicious transaction over $2,000 and a Currency Transaction Report ("CTR") for any transaction over $10,000. CTRs specifically are implemented for physical currency deposits and are required for not only single transactions, but the aggregation of currency transactions as well. These reports allow law enforcement to quickly and efficiently request supporting documentation that can be essential in quick moving investigations. However, virtual currency kiosk operators (and law enforcement) will be unable to determine if a customer transacted more than $2,000 or $10,000 across multiple operators. As a result, virtual currency kiosk operators will be less able to detect suspicious activity, worrisome transactions will be spread over multiple operators, and federal reporting requirements will not be triggered.

Second, the addition of fee caps does nothing to prevent customer fraud and in combination with transaction limits, inadvertently creates incentives for less transparency. At this time, it is unclear how the 10% proposal was determined and whether it took into consideration the unique costs of virtual currency kiosk operators. Unlike an exchange, virtual currency kiosk operators must purchase, install, and operate physical equipment; pay rent to small businesses to host their kiosks; pay armored car services to service their kiosks; and maintain an inventory of virtual currency to sell to customers. Similar to other virtual currency businesses, virtual currency kiosk operators must also pay for bank fees, blockchain network fees, BSA/AML compliance tools and employees, customer service, cybersecurity tools and employees, and transaction monitoring tools. Put simply, virtual currency kiosk operators have more operational expenses than other virtual currency companies.

Lastly, the refund provision displays a misunderstanding of blockchain technology and creates an unintended consequence, as scam artists will seek to game the refund period and defraud virtual currency kiosk operators. Virtual currency kiosk operators allow for the purchase of virtual currency via physical fiat currency rather than any previously authorized transaction. Despite this fact, the Minnesota statute mistakenly suggests that customers be allowed to "stop payment of a preauthorized virtual currency transfer…" The statute further confusingly requires virtual currency kiosk operators to disclose that transactions are irreversible while simultaneously instructing kiosk operators to refund specific transactions. It is noted there are no qualifications or requirements for the customer to receive a refund.

The current proposed language makes virtual currency kiosk operators the insurer of all first-time transactions. Customers are given a non-discretionary 72-hour period to determine whether they still want the purchased virtual currency, and do not have to return the virtual currency if they do request a refund. CoinFlip is unaware of any other institution that has similar requirements. In fact, the legislation goes as far as to encourage wrongdoers to defraud virtual currency kiosk operators by purchasing virtual currency, sending it to their own digital wallet, and requesting a refund so they can keep both the virtual currency purchased and the cash used to purchase it.

Proposed Consumer Protections

Despite disagreements over the contents of H.F. 4717, CoinFlip is committed to working with Minnesota in order to implement further consumer protections. The following is a brief overview of proposed changes that CoinFlip believes will implement consumer protections in a meaningful manner:

1. **Require Licensure with the State**. Although the proposed Minnesota legislation repeatedly refers to a "virtual currency kiosk licensee," there is this nothing in the proposed legislation or current Minnesota law that requires virtual currency kiosk operators to be licensed. CoinFlip encourages language be added to the bill that would require virtual currency kiosk operators be licensed for proper oversight, including obtaining a Money Transmitter License ("MTL"). The MTL would implement baselines requirements similar to other financial institutions operating in the State. It additionally would allow state oversight and periodic audits to determine the adequacy of compliance, finance, and cybersecurity programs.
2. **Require a Focus on Compliance**. Require virtual currency kiosk operators to directly employ an in-house Chief Compliance Officer that does not have a large ownership interest in the company.
3. **Require Disclosures.** Require virtual currency kiosk operators to clearly display, at the physical location and on any electronic screens, prior to the initiation of a transaction, information about potential scams. Require operators to provide a Customer Service phone number that is clearly displayed at the location.
4. **Require Fee Disclosures**. Require digital currency kiosk operators to clearly disclose, prior to completion of a transaction, all fees associated with the transaction. Require operators to provide a receipt (physical or digital) of the transaction details.
5. **Require Blockchain Analytics**. Require the use of blockchain analytics technology in order to prevent fraud before the customer transaction by automatically blocking transactions that are attempting to be sent to wallets flagged as high risk because of an association with criminal or fraudulent activity. Since April 2022, CoinFlip has automatically blocked more than 1,230 transactions using blockchain analytics.

6. **Require Robust Policies and Procedures**. Require an Anti-Fraud Policy and Consumer Protection Policy that outline specific risk areas of the virtual currency kiosk operators, how they will protect against such risks, and a company refund policy.
7. **Require Live Customer Service**: Virtual currency kiosk operators are required to implement live customer service for a minimum of 8:00 AM – 10:00 PM CST in order to identify and prevent fraud. Between December 2023 and February 2024, CoinFlip customer service halted transactions for over 300 customers before they could occur due to indications the customer was involved in a scam.
8. **Tiered Transaction Limits**: In the event the legislature still believes transaction limits are appropriate, a distinction should be made between new customers and existing customers. Transaction limits are based on if you are a New Customer or an Existing Customer. These limits provide protection for a new customer who may be the victim of a scam by limiting the amount they can transact, while allowing an existing customer who has transacted with the company additional purchasing access once they are no longer at an increased scam risk. These limits should be in line with federal reporting requirements for Suspicious Activity Reports ($2,000) and Currency Transaction Reports ($10,000).

Conclusion

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. The best defense for consumers is to be well-informed and well-alerted at the point of transaction. The best defense for companies is to have the tools in place to help identify and prevent fraud and help law enforcement catch the bad actors. It is more important than ever that we do not simply treat the symptoms but attack the root of financial fraud and arm consumers with the knowledge they need to stay one step ahead of the scammers.

Unlike some others in the industry, CoinFlip believes smart regulation is good for business. We believe that a regulatory framework is necessary to protect consumers and encourage innovation. CoinFlip and Minnesota share a similar goal: consumer protection. CoinFlip looks forward to continuing to work together with Minnesota in order to best determine how to achieve that common goal.

Sincerely,
/s/ Larry Lipka

Larry Lipka
General Counsel

Enclosures

Dr Shannon May October 2023 Scam Statement

On October 17, 2024, me and my family's life was greatly altered with trauma and great financial upheaval that we will be digging out of for many years to come.

I am a Naturopathic Doctor and Acupuncturist (ND, Lac) with my clinic in Duluth, MN. I was at work seeing patients when I received a voicemail from the phone number of Carlton County Sheriff's Office. The voicemail said it was Chief Deputy Dan Danielson from Carlton County Sheriff's office and they need me to call him as soon as possible as a legal matter in regards to me came across his desk that morning. They said to call him directly at (218) 503-3873. So I looked up their Chief Deputy and it was indeed Dan Danielson. Since this added up I called.

When I called "Chief Dan Danielson" he asked if I was sitting down? My heart dropped because my husband drives through Carlton County every day on the way to his work in Moose Lake. I immediately thought something had happened to him on the highway, like an accident, and potentially worse case scenario, he was hospitalized or even dead. I told him I was sitting down and then he proceeded to tell me that there is a legal issue in the means of some felony charges on me because I failed to show up for a court hearing Monday, October 16, 2023 at 9am, as an expert witness for a federal juvenile case (potentially one of my patients, they could not get me that information at that time) with the Honorable Judge Schiltz. I checked online and saw the Honorable Judge Schiltz was indeed a U.S. District Court judge in Carlton County.

They said I was court ordered with a formal subpoena presented to me by officers September 8, 2023. I confirmed that that was my house address on September 8th (however, we moved that following week to our current residence), but that I was away since about 2pm that day as I was out of town. I did recall, however, that when talking to my daughter that evening on September 8th, that she had mentioned police stopped by asking for me. I thought that was strange, but wrote it off as maybe related to something happening in the neighborhood and were checking in with neighbors.

They proceeded to tell me that the problem is that they have a signature on the subpoena form that I signed, or potentially someone else signed, so there is proven consent of the court hearing and document received. They said if what I say is true then there may be plagiarism involved. They said if the police on that day did anything wrong then rest assured that would be addressed and proper action would be taken. At that point I was unsure if maybe the baby-sitter (17 years old) or my daughter (10 years old) had mistakenly signed something and forgot to show me the document. We were in the throws of moving and mail was being placed all over the place by my kids and the house was filled with packing boxes here and there. I could see a scenario where a document made its way into one of the boxes. At this point the story they gave me was sounding real, but I told them I never saw or encountered police and never signed a subpoena order to even know I was supposed to be at this federal court hearing with Judge Schiltz. They were empathetic about this and told me that there is a process to get this cleared up if indeed I did not sign the document.

They said they then need to discuss the citations involved with my case. The first one was Failure to Appear in Court (FTA-CV-4747). They said this stems from the signed subpoena and that not appearing in court. They said the second one was Contempt of Court (COC-V-5740). They also explained that there was a third citation given by the Honorable Judge Schiltz, Avoiding Civil Duty (ACD) (missing court appearance pertaining to my profession), which is a Class 6 felony and the Civil Surety bond posted by the Honorable Judge Schiltz.

They went on to tell me there are two procedures that I can consider to rectify this matter and would explain both of them. The first procedure would be a civil process. The civil process has two orders placed. The first order is a Suppression Order (eg. Gag order). They said it's similar to HIPPA, and it's restricting information being made public or being passed onto any unauthorized third party. They said because this is an ongoing federal trial that I have delayed, this order has been put in place at this point. They said it is okay to tell others that a work related issue has come up and you're working on it and that I can let them know once it's been completed. The second order put in place has been a Make and Maintain Contact Order and that I must maintain continued contact at all times. They said if a call dropped or loss mobile monitoring it would need to be immediately re-established. They said with this first process, the civil process, they would get me to the signature verification process at Carlton County Sheriff's office and compare signature with a professional signature analyst they have on site that is 99.9% accurate. They would fingerprint me as well, show me the case file, and at that point I could also request body cams from the police officers that day to see if it was not me who signed, then see who then plagiarized my name.

The second procedure as an option would be to disconnect this call at any time and seek legal course and then he'd need to go through that attorney. I would then need to turn myself in and would be put in custody for at least 72 hours.

This was the point where since everything they said had added up, I placed this whole situation as REAL in my mind and that I needed to get to the other side of this as quickly and smoothly as possible. This involved getting the surety bonds paid so that I could freely enter the Carlton County Sheriff's Office and meet with the signature analyst to prove that wasn't my signature and essentially prove my freedom. They had told me at that point when I prove my innocence I would immediately get the surety bonds returned to me from the US Dept of Treasury. Over the next two days I spent my time trying to collect these monies and sending it through these CoinMe Coinstar kiosks (FDIC approved 3rd party retailer to the US Department of Treasury's Account).

At the end of the day, I felt figuratively held hostage for 48hrs with what I thought was Carlton County and the Federal Government collecting my ransom (surety bonds) for over $80,000 and on a sort of house arrest that whole time maintaining an open line connection on my phone to keep me and my family's safety and freedom. At the end of the day it was a very well orchestrated professional scam. My sister and brother-in-law drove from over 2 hours away to help pay for a portion of it as well.

What we would like to see is more legislative support around these Coinme CoinStar kiosks. Since they are new and support cryptocurrency there is not a lot of regulation around them. For instance, as people are continuing to get scammed (we recently heard on MPR that these scammers have reached earnings in the billions – on MPR the week of March 4th, 2024) if there was at a minimum of a 48 hour hold on those funds, that would be enough time for so many of these scams to get "saved" financially. Also, we have tried to reach out to the CEO of these Coinme CoinStar kiosks to make them aware of what is going on but to date they have not returned any of our calls. Our understanding, looking into these kiosks, is that they have 11% interest gains on these transactions. That means that this company earned over $8,000 from just our one scam. Ultimately, they currently do not have incentive to change how these kiosks are being used in scams when they have a financial gain with each scammed transaction.

In conclusion, we do not want to see these scams affect other families the way it has negatively impacted ours. We feel we are speaking for ourselves and all those who have been and may still be affected by these type of scams that we appreciate any and all support and ideas you have around legislation involving these kiosks and scams today.

March 12, 2024

Commerce, Finance, and Policy Committee
Minnesota House of Representatives
100 Rev. Dr. Martin Luther King Jr. Blvd.
Saint Paul, MN 55155

RE: HF 4717, an act concerning virtual currency

Committee Chair Zack Stephenson, Co-Chair Calie Kotyza-Witthuhn and Members of the Committee,

RockItCoin, LLC ("RockItCoin", or "the Company") applauds the legislature's efforts to properly define expectations and regulations for the cryptocurrency kiosk operators in the state. Unfortunately, HF4717 appears to borrow heavily from a bill passed in Connecticut last year. The Connecticut law demonstrated a lack of understanding of the cryptocurrency kiosk business, and its attempts to strengthen consumer safety and knowledge in this space, ironically, did the exact opposite.

HF4717 should take the opportunity to correct and enhance the Connecticut law, otherwise HF4717 will have a negative effect on the emerging crypto industry, fail to properly address consumer safety, place undue burdens on the small businesses running the kiosks, and penalize consumers wishing to purchase cryptocurrency.

Please note RockItCoin fully supports regulation in this space. We have met personally with individuals across the country in an effort towards substantive dialogue and mutual understanding about our industry. Independent of governmental guidance, our Company has developed a strong compliance program that includes customer interactions and interruptions of transactions as methods to best protect our customers.

Arbitrary limits do not protect the customer - communication, education, and interaction do.

We work with law enforcement to combat the negative actors in our space, offering insights and guidance. We identify risk typologies and proactively involve ourselves with customers prior to a transaction being consummated, speaking with them directly and at times holding transactions altogether until definitive discussions can be had. Transactions that are not deemed legitimate are refused and money, if collected, is returned.

As an example, RockItCoin's protocols interrupted a $5,800 transaction by a customer until extra due diligence could be performed. Such intervention is critical to identify and contain possible scam victims and fraudulent transactions. It was determined the customer was indeed the victim of a scam, and consequently the transaction was refused by RockItCoin which resulted in the entire $5,800 being returned to the customer.

Kristen McKnight, a member of the US Secret Service Task Force in Louisiana, observed in an email to the Company,

> *"If RockItCoin did not have the protocols in place, the victim could have potentially lost those funds and not been recovered. I would like to note that four different Bitcoin ATM companies were involved in the scam and only one, RockItCoin, suspended the victim's transaction. Thank you RockItCoin for your protocols in place, which prevented additional loss to my victim."*

As McKnight explained in her email, the victim used multiple operators to perform her large transaction, but only RockItCoin interrupted its transaction. If the other operators exercised a similar level of diligence or a law had been in place mandating such actions, perhaps this victim would have been made whole. It is here where the illusion of transaction caps fail the customer – they can simply visit as many different operators as they choose. Customers will continue to be at risk without proper framework around the operators, such as intervention, education, and communication.

Kristofer Carlson of the Minnesota Commerce Fraud Bureau similarly praised the protocols developed and utilized by RockItCoin. After observing the Company's diligence and processes, he said in an unsolicited email:

> *"Thank you for your due diligence. As a sworn member in law enforcement investigating these crimes and seeing the devastation and significant financial impact it's having, it's reassuring to know that we've got support in combating this in companies like RockItCoin. Please pass along to whomever you can and want to that the law enforcement community sees and appreciates the work you're doing."*

And we know the protocols described above are workable solutions that can be adopted by operators – because RockItCoin is doing it now, going well beyond what is regulatorily required to do what is right. Rather than legislating arbitrary caps and controls that stand to stifle and choke the very businesses it is aiming to regulate, a well-crafted law can instead encourage growth and investment while protecting the customer.

Ironically, by introducing transaction and fee caps the bill as written disincentivizes the protection of the customer. By capping revenue and inadvertently pushing transaction thresholds below reporting requirements, operators will gravitate towards lower standards which consequently exposes customers to the very dangers the bill hopes to eliminate. It is better to raise the floor to a higher standard and hold operators accountable than lower the ceiling and push everyone towards lower standards and fewer protections.

Three operators in our space, Bitcoin Depot, CoinFlip, and ourselves, testified last week in front of the Connecticut Joint Committee on Banking and yesterday met with representatives from the Connecticut State Police and the Department of Banking to further discuss our findings and concerns. The meeting was quite productive, with industry submitting proposed changes for committee consideration.

The Connecticut law and the Minnesota counterpart here require corrections too numerous and important to leave for a future legislative session. It is worthy of attention and discussion prior to passage in order to provide an opportunity to strengthen the bill by including some of the protocols and best practices developed by RockItCoin. An enhanced bill would go a long way towards the protection and safety of your constituents while simultaneously giving the industry the guidance, direction, and framework it desperately needs.

Every kiosk operator that does not address the safety of the customer and instead does the bare minimum required puts customers at risk and our industry's reputation on the line. Bringing expectations up to a defined standard is something we should strive to do.

And looking beyond Minnesota, RockItCoin envisions such a law serving as a template for other states as they try to address cryptocurrency in general and specifically the kiosks found within their own borders. RockItCoin so believes in our compliance model that we would welcome it to be implemented nationwide.

Inconsistencies and Issues Within HF 4717

Kiosk operators do not have accounts with their customers.

Sec 5, Subd 2 addresses opening "accounts" with customers, which a kiosk operator does not do. We do not act as custodians of any customer assets or cryptocurrency, nor do we hold them for the customer's future use. This section of the law demonstrates a general lack of understanding about what the kiosk aims to do, which is to provide a cryptocurrency retail solution. This is precisely what the regulatory departments in Minnesota already know about what we do - if the kiosk operators were holding money or assets of the customer, they would be under the jurisdiction of other laws in the state.

With no accounts, how can kiosk operators provide "statements"?

Sec 5, Subd 2,(2)(ii) requires the kiosk operator to give the customer periodic statements and valuations of the non-existent accounts described in Sec 5, Subd 2. As there are no "accounts" with the customer, here the legislature has confused the kiosk operators with custodial exchanges. The wallets presented at the kiosk are the customers' wallets and under their control, not the kiosk operator's. The kiosk operator does not have any insights into the acquisitions and activities of the customer's personal wallets being used at the kiosks, and certainly would be unable to provide "periodic statements and valuations."

A “stop payment” feature is not a possibility in a cryptocurrency transaction.

Sec 5, Subd 2,(2)(i) addresses a "virtual currency transfer" without ever having defined such a term. This is significant because whatever assumptions have been made about this “transfer” have a great impact on the kiosk operator. Specifically, this section creates a customer's right to the "stop payment" of a transfer. It appears at a minimum the law is requiring kiosk operators to do something that can't be accomplished in the crypto world: undo or claw back a transaction after it has been authorized or set in motion on the blockchain.

The law requires a warning to the customer that transactions cannot be undone once executed, in direct conflict with the prior “stop payment” requirement.

Paradoxically, Sec 5, Subd 3,(4) requires kiosk operators to warn the customer that once a transaction is executed it cannot be undone.

Undefined term aside, under this law kiosk operators are required to disclose to the customer that a transaction cannot be undone, but yet the customer has the right to "stop payment" of one. This confusion will certainly lead to problems (consumer expectations of rights or actions that cannot exist) if not further defined. It again demonstrates the misunderstandings of the law’s supporters and illustrates exactly why such a law needs to be addressed in the raised bill currently pending.

The bill places prohibitions on the collection of fees for our service.

Sec 5, Subd 5 is concerning. It places a cap on the amounts the kiosk operator may charge. The service provided by the kiosk operators carries many unique costs such as inventory procurement, kiosk deployment and maintenance, cash logistics providers, customer service interactions, and compliance requirements, to mention a few. The definition of a maximum revenue potential without regard to a Company’s costs puts the power to shut an entire industry down with no input from nor protection or rights offered to the kiosk operator.

The law establishes a daily limit on transactions a customer can do, to our knowledge unprecedented in the retail or investing community.

Sec 5, Subd 3,(5) establishes an arbitrary daily limit an individual can transact at the machine. This seems like a figure hastily put in place to "protect" consumers while negatively affecting those who transact higher amounts safely. Kiosk operators are unaware of other industries similarly targeted and, lacking context on the decision-making process, do not understand why its activity is curtailed. We cannot see similar limits placed on consumer-based retail or investments, and as such believe this portion of the law can be interpreted as discriminatory.

The law creates a wholly unworkable and unrealistic situation wherein a first-time customer under certain circumstances can request a “refund” of a cryptocurrency transaction.

Despite demonstrating an understanding that cryptocurrency transactions cannot be undone (see Sec 5, Subd 3,(4) wherein kiosk operators have to warn such a fact), the bill attempts to magically legislate into existence a “refund” scenario.

Sec 5, Subd 6 places many unworkable and unreconcilable scenarios in play. First, it gives the right of the first-time customer to "cancel and receive a full refund for the virtual currency transaction", which again is in direct conflict with earlier warnings. That issue aside, it fails to define what a "refund" would look like – does the kiosk operator get its cryptocurrency back when money is returned to the customer, or is the kiosk operator expected to simply hand over money and let the customer keep both the crypto and the cash? The latter option is most decidedly not a refund by any standard definition.

Such a "refund," unprecedented in the cryptocurrency space, creates a moral hazard.

Most concerning is the bill places the cost of such a "refund" squarely on kiosk operator. Again, in Sec 3(h) it states (emphasis added), "A virtual kiosk licensee must, ***at the licensee's cost*** and within seventy-two hours after a virtual currency transaction, allow the person to cancel and receive a full refund…" With no accountability or cost associated to the customer (it having been borne entirely by the operator per the language), abuse of such a provision is a real possibility.

Thus, the "refund" scenario creates a moral hazard. Allowing the customer 72 hours to decide whether or not they wish to keep an asset whose price fluctuates is decidedly unfair to the kiosk operator. Imagine a scenario wherein an investor can purchase Google stock, but then have three days to observe price direction and decide whether or not they wish to keep their purchase.

And paradoxically, should bad actors understand that Minnesota will not be seeking justice from them and will instead hold the operator liable for all "refunds", the likelihood of scam activity actually increases.

Even worse, the "refund" criteria is created within another fundamental misunderstanding of how the cryptocurrency space operates.

The criteria for being eligible for this "refund" contains an interesting "and" in the bill which sets up yet another conflict: the transaction must be to "a virtual currency wallet or exchange located outside of the United States." The bill's authors are clearly unaware that the physical location of, or the exchange affiliation with, a particular wallet address is simply not known with certainty.

Aside from being impossible to know each time and difficult to "prove," such a situation would be in violation of our Terms of Service. Oddly, this portion of the law sets up a scenario wherein a customer can violate our Terms of Service and be rewarded for doing so by becoming eligible for a refund which we warned them couldn't happen, but we are required to make it happen, again with no protections for ourselves, the kiosk operator.

Ways to strengthen HF 4717

We have attached a markup of the proposed legislation to this document as "Exhibit A." Rather than restate all of our comments here, please see the exhibit for both our redline suggestions and commentary.

Working through the bill, you will note that we first address several of the required warnings and attestations. Some are inapplicable and should be removed while others need modified to bring them more in line with the industry. Some of the "disclosures" are also problematic, as what they describe cannot be accomplished in the cryptocurrency world.

The transaction cap in the bill has the appearance of consumer safety in that on the surface it appears to limit the amount a consumer can be scammed. However, in practice it is not as effective as one would believe and has other implications as well. Instead of an individual being limited to the "safety" of a cap, they can merely visit another operator's kiosk and continue to transact, as described earlier. Even a diligent operator will never see the overall transaction pattern that could suggest intervention is needed.

And no Federal rules exist requiring the specific identification of the customer for a $1,000 transaction. Larger transactions, such as $3,000, require, per Federal code, not only photo identification verification but also the collection of the social security number of the individual transacting. These are vital pieces of information for law enforcement but are now not required to be collected under a $1,000 cap.

Currency Transaction Reports (CTRs) are filed with the IRS for a currency transaction(s) individually or cumulatively exceeding $10,000 in a day. These reports carry identifying information of the individual transacting. Law enforcement uses these reports as documented evidence of a suspect spending cash. The $1,000 transaction cap prevents the CTR threshold from being reached and consequently prevents CTRs from ever being filed, depriving law enforcement of possible documented evidence.

Circumvention of the CTR reporting requirements would necessitate a Suspicious Activity Report (SAR) filing with FINCEN, but without the ability to see the full customer activity, it cannot be done. Previously reportable activity is now unreported. Customers are forced to return day after day, transacting $1,000 each time, to purchase larger amounts of cryptocurrency. Therefore, the proposed Bill obscures what would otherwise have been a large transaction reportable via a CTR or perhaps a SAR.

The law puts the operators in the impossible situation of guessing whether or not the customer activity should be interpreted as a circumvention of Federal reporting rules or that it simply was a product of the customer following the laws of the State of Minnesota. The proposed Bill would diminish the effectiveness and validity of a previously effective process.

Therefore, a $1,000 transaction limit obscures true customer activity, reduces the amount of identification information required to be collected, and eliminates valuable intelligence heading to law enforcement – all things that truly protect consumers.

The ineffectiveness of a transaction cap is also evident in California, where a $1,000 kiosk transaction cap has now encouraged kiosk manufacturers to produce a one way “safe” instead of a kiosk in an effort to circumvent the rules. The product is marketed specifically as a work around of the California law. Other kiosk operators in California have instead opted to open actual storefronts where people can transact. Instead of protecting consumers with rational, well thought out solutions, the law passed in California simply fails those consumers that need protection the most.

We need to address a very small subset of customers who find themselves at risk among the literally thousands upon thousands of transactions processed each day by the cryptocurrency kiosk industry. Inconveniencing the entire group for the protection of this subset by limiting transactions or access is not an effective solution.

The most effective form of customer safety is intervention and communication. Our proposals include mandates for this: new customers need contacted if transacting over a certain threshold and elderly customers need contacted prior to their first transaction being consummated. A live customer service staff is required for operators to communicate with customers, not text messages and chatbots. Robust compliance policies and procedures, run by actual employees of the company and not disinterested third parties, should be part of any true plan for customer safety.

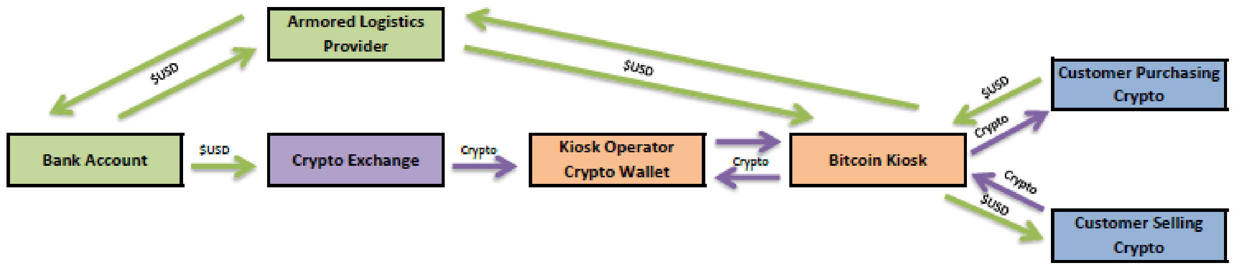
All FINCEN registered MSBs are required to have a risk-based approach to customer due diligence and transaction monitoring. Such a risk-based approach to money laundering would necessitate focusing on higher dollar transactions. Our proposal addresses this fact by requiring more direct consumer interactions and protections. A cap on fees is addressed in a similar manner - those required to allocate more resources towards customer protections should be permitted to charge a higher fee to pay for it.

The model that both sets and incentivizes the compliance of the operator by allowing both larger fees and transactions is a solution that we can support. An impossible scenario would be to place transaction and fee caps on the operators while simultaneously requiring the additional compliance protections. Customers being safe would find themselves needlessly inconvenienced while the industry would find itself with an unfunded mandate – a position detrimental to the growth and investment in what we believe to be the future of payments, peer to peer transactions, and wealth storage.

Bitcoin Kiosk Industry

Based upon the Connecticut law and the proposed Minnesota bill’s inconsistencies and flaws within it, we have reason to believe the legislature does not fully understand what the kiosk operators do.

Please see the kiosk operator Flow of Funds diagram below:



Moving left to right, the kiosk operator bank account sends USD to a crypto exchange to purchase crypto that is sent to the kiosk operator's wallet inventory for use in the kiosks. Note the Armored Logistics Provider takes money from the kiosks (obtained through customer crypto purchases) and deposits it back into the bank account, and vice versa for money dispensed from the kiosk (to pay for customer crypto sales to the kiosk operator).

Moving right to left, a customer approaches the machine and either purchases or sells cryptocurrency and only interacts with the kiosk. This transaction is contained within itself and does not include third parties per our Terms of Service and customer attestation. The transaction represents the customer's entire relationship with the Company's kiosk.

Upon approaching the kiosk, the customer must identify themselves, declare how much they wish to buy or sell, and provide whatever KYC documentation is necessary. The customer must present a digital wallet that they attest is theirs and under their control. This wallet is immediately screened by a blockchain analytics company that alerts RockItCoin if it has been involved with suspicious or sanctioned activity. Upon satisfaction of the requirements, the customer can then determine if they wish to proceed. Customers who purchase cryptocurrency insert cash into the kiosk to pay for their purchase and in turn receive the cryptocurrency on the wallet they presented, and customers intending to sell cryptocurrency instead send cryptocurrency to the kiosk and receive cash dispensed from the machine as payment for the cryptocurrency.

It is critical to understand the transaction is consummated at the machine and that the kiosk operator is NOT:

1. Holding customer funds for future use.
2. Holding cryptocurrency for the benefit of the customer.
3. Transacting with anyone else but the identified customer at the kiosk.

The bitcoin kiosk industry arose out of the need for individuals to obtain cryptocurrency.

Acquiring crypto from online exchanges takes time – funding an account, purchasing, and moving crypto for use is historically fraught with delays and roadblocks for the consumer. First of all, funding has to come from an established account through wire or ACH, which immediately eliminates the underbanked and poses logistical challenges for others. After funding, many online exchanges have a grace period before you can use the deposited funds as a way to combat fraud, but this simply increases the inefficiencies of the process. Lastly, many online exchanges require yet another grace period after acquiring crypto before you can use or move it from the exchange.

To the individual wanting to make a purchase or pay for a service in the short term, online exchanges offer a service that does not mesh with the needs of the consumer. RockItCoin fills that gap with its cryptocurrency kiosks.

In crypto's early days, people would meet in parking lots and exchange cash for their crypto. This is neither safe nor efficient and most importantly, outside of regulatory purview. RockItCoin kiosks are the solution to acquiring cryptocurrency quickly, in person, and most importantly, under regulation.

The negative news associated with exchange failures like FTX and crypto lenders such as Celsius is not a reflection on our business. As mentioned previously, kiosk operators do not take custody of customer funds or assets and therefore the possibility of customer loss from company malfeasance is small. Quite simply, although we all deal in cryptocurrency, our businesses are not the same because we do not have control over our customers' assets.

Legitimate cryptocurrency kiosk operators, such as RockItCoin, desire regulatory oversight and welcome the opportunity to operate under clear guidelines and true customer protections that are well thought out and fair to all parties. Such rules serve to enhance, protect, and grow the space; contradictory or flawed Bills stifle, confuse, and choke the growth out of an industry.

Company Background

RockItCoin operates a nationwide network of approximately 2,300 cryptocurrency kiosks in 48 states and Puerto Rico. These kiosks allow the customer to purchase, and in some cases sell, cryptocurrency in person and directly with the Company. While the Company's operations began in Chicago, Illinois, in late 2015, our first kiosk in Minnesota went live in February, 2020.

Michael Dalesandro founded RockItCoin with the vision to bring cryptocurrency to the masses. For many, and especially those in the underbanked community, cryptocurrency access is quite limited and available only through third parties. RockItCoin solves this by allowing customers to purchase cryptocurrency immediately, in person, without minimums, and with the cash they have in their pockets.

Customers approach a kiosk and identify themselves with a phone number and valid state identification. At increasing levels of activity, we require additional information including social security numbers, source of funds documentation, various attestations, and enhanced due diligence.

On a federal level, RockItCoin is a registered money service business (MSB). With that comes the necessary requirements for having a robust Anti-Money Laundering policy that is independently audited annually, an education program targeted for employees, the designation of an AML officer at the firm, the creation of risk-based customer monitoring processes, and the filing of Suspicious Activity Reports and Currency Transaction Reports – all of which we do.

States make their own determination on licensing, and several require money transmission licenses for our kiosk activity. We carry licenses in 21 states, all of whom conducted due diligence on our activities and business plan. RockItCoin has also undergone and passed two MSB Title 31 Examinations (in 2017 and 2021) conducted on behalf of FINCEN by the Internal Revenue Service. We are proud of our commitment to, and our track record of, compliance.

We proactively combat fraud, interrupting transactions and speaking directly with customers whom we believe are at risk for being scammed. The approaches we take are not mandated by regulation but rather guided by our own internal policies. We have identified risk typologies and actively seek to protect our customers from harm.

Additionally, RockItCoin has a live customer service department available to answer phones between 7:00 am and midnight CST Monday through Friday and from 8:00 am to 10:00 pm on the weekends. We understand crypto can be confusing and requires information resources. We strive to be that resource and foster a trusted relationship with our customers.

RockItCoin Kiosks in Minnesota

In late 2018 and prior to RockItCoin's first Minnesota kiosk installation, we requested a licensing opinion. We were given guidance that our business activity did not require licensure. We repeatedly sought updates from Minnesota on this guidance.

RockItCoin applied for a money transmission license in September, 2023 based upon further guidance. As we await the approval of our application, we carry a $250,000 surety bond for our Minnesota activity.

Enforcement

It is our hope that any enacted legislative regulation runs parallel with an enforcement framework. Operators in the cryptocurrency space that purposely choose to ignore or operate outside the rules should be held accountable for the protection of the consumer, integrity of the law, and reputation of the industry.

Conclusion

It is the Company's firm belief that cryptocurrency is game changing and here to stay.

For Minnesota to simultaneously protect its citizens, encourage participation, and be at the forefront of this potentially world-changing industry, a fair, proper, and thought-out regulatory framework is necessary. RockItCoin is willing to help the legislature identify, address, and perfect both processes and best practice requirements by which Minnesota can safely embrace the cryptocurrency space with kiosk operators.

True engagement and eventual success must begin through conversations and commitments to listen, learn, and lead. Amending and enhancing HF 4717 prior to passage is a proper first step to clear the way for the development of effective laws, not unfair, emotionally driven, contradictory rules that will serve to confuse the consumer and kiosk operator alike. I would be happy to discuss my thoughts further in person or meet via Zoom at your convenience.

Thank you in advance for your time, and I look forward to hearing from you.

Sincerely,

John Carroll, CCO
RockItCoin, LLC

enclosure

Exhibit A

A bill for an act
relating to commerce;
defining terms relating to virtual currency;
adding additional disclosure requirements for virtual currency transactions;
amending Minnesota Statutes 2023 Supplement, section 53B.69, by adding subdivisions;
proposing coding for new law in Minnesota Statutes, chapter 53B.

BE IT ENACTED BY THE LEGISLATURE OF THE STATE OF MINNESOTA:

Section 1. Minnesota Statutes 2023 Supplement, section 53B.69, is amended by adding a subdivision to read:

Subd. 3a. Transaction hash. "Transaction hash" means a unique identifier made up of a string of characters that act as a record of and provides proof that the transaction was verified and added to the blockchain.

Sec. 2. Minnesota Statutes 2023 Supplement, section 53B.69, is amended by adding a subdivision to read:

Subd. 6a. Virtual currency address. "Virtual currency address" means an alphanumeric identifier representing a destination for a virtual currency transfer that is associated with a virtual currency wallet.

Sec. 3. Minnesota Statutes 2023 Supplement, section 53B.69, is amended by adding a subdivision to read:

Subd. 10. Virtual currency kiosk. "Virtual currency kiosk" means an electronic terminal acting as a mechanical agent of the licensee to enable the licensee to facilitate the exchange of virtual currency for money, bank credit, or other virtual currency, including but not limited to by (1) connecting directly to a separate virtual currency exchanger that performs the actual virtual currency transmission, or (2) drawing upon the virtual currency in the possession of the electronic terminal's licensee.

Sec. 4. Minnesota Statutes 2023 Supplement, section 53B.69, is amended by adding a subdivision to read:

Subd. 11. Virtual currency wallet. "Virtual currency wallet" means a software application or other mechanism providing a means to hold, store, or transfer virtual currency.

Sec. 5. [53B.75] VIRTUAL CURRENCY KIOSKS.

Subdivision 1. Disclosures on material risks.

(a) Before entering into an initial virtual currency transaction for, on behalf of, or with a person, the virtual currency kiosk licensee must disclose in clear, conspicuous, and legibly written English all material risks generally associated with virtual currency. The disclosures must be displayed on the screen of the virtual currency kiosk with the ability for a person to acknowledge the receipt of the disclosures. The disclosures must include at least the following information:

(1) 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;

(2) some virtual currency transactions are deemed to be made when recorded on a public ledger, which may not be the date or time when the person initiates the transaction;

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

~~(4) a person who accepts a virtual currency as payment today is not required to accept and might not accept virtual currency in the future;~~

~~(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;~~

~~(6) the nature of virtual currency may lead to an increased risk of fraud or cyber attack;~~

~~(7) the nature of virtual currency means that any technological difficulties experienced by the licensees may prevent access to or use of a person's virtual currency; and~~

~~(8) any bond maintained by the licensee for the benefit of a person may not cover all losses a person incurs.~~

(5) Virtual currency transactions are irreversible and are used by scammers, including those impersonating loved ones, threatening jail time, stating your identity was stolen, insisting you withdraw money from your bank account and purchase cryptocurrency, or alleging your personal computer has been hacked.

(b) The virtual currency kiosk licensee must provide an additional disclosure, which must be acknowledged by the person, written prominently and in bold type, and provided separately from the disclosures above, stating: "WARNING: LOSSES DUE TO FRAUDULENT OR ACCIDENTAL TRANSACTIONS ~~MAY NOT BE~~ARE NOT RECOVERABLE AND TRANSACTIONS IN VIRTUAL CURRENCY ARE IRREVERSIBLE."

Subd. 2. New account disclosures. When opening an account for a person a virtual currency kiosk licensee has not previously opened an account for, and before entering into an initial virtual currency transaction for, on behalf of, or with the person, a virtual currency kiosk licensee

Commented [JC1]: This is a warning about a customer's possible future virtual currency transaction that has nothing to do with the current transaction between the operator and the customer.

Commented [JC2]: The kiosk operator does not have a fiduciary relationship with the customer and therefore is not in any way obligated to provide investment advice on specific risks a customer might have apart from the transaction with the kiosk.

Commented [JC3]: This has no basis in fact and is inappropriate.

Commented [JC4]: This is a misstatement or misunderstanding of the role of the kiosk operator. It does not accurately explain the relationship between operator and customer and is confusing. Operators do not hold custody of customer funds or crypto.

Commented [JC5]: Confusing and completely unclear. Just because a bond is maintained for the benefit of the customer does not mean it could be used to cover losses incurred by the customer. Such verbiage implies a possible "insurance" policy for some of the transaction that the customer does not really have.

Commented [JC6]: Kiosk operators should be obligated to warn customers on scams prevalent in the industry.

Commented [JC7]: The use of word "may" implies chances for recovery exist that most likely do not. Amend references to reflect changes, and change "may not be" to "are not".

must disclose all relevant terms and conditions generally associated with the products, services, and activities of the licensee and virtual currency. A virtual currency licensee must make the disclosures in clear, conspicuous, and legibly written English, using a reasonable size and type font~~at least 48-point sans serif type font~~. The disclosures under this subdivision must address at least the following:

~~(1) the person's liability for unauthorized virtual currency transactions;~~

Commented [JC8]: "Virtual currency transaction" was never defined in the law, let alone what an "unauthorized" one would entail. References to it or dependent upon it should be removed.

(2) the person's right to:
~~(i) stop payment of a preauthorized virtual currency transfer and the procedure to stop payment;~~
~~(ii) receive periodic account statements and valuations from the licensee;~~
(iii) receive a receipt, trade ticket, or other evidence of a transaction at the time of the transaction; and
(iv) ~~prior notice of a~~consent to a change in the licensee's rules or policies prior to performing a subsequent transaction;

Commented [JC9]: "Virtual Currency transfer" was never defined in the law and references to it or dependent upon it should be removed. Additionally, the concept of a "stop payment" is at complete odds with virtual currency transactions.

Commented [JC10]: Again, customers do not have an "account" with the kiosk owner or operator and utilize their own digital wallets in transactions. Therefore, the operator would have no idea what such customer may or may not have done outside the kiosk transactions, making "statements and valuations" impossible.

(3) ~~under what circumstances the licensee, without a court or government order, discloses a person's account information~~The owner or operator's mandated privacy policy to communicate what customer information may be disclosed to third parties; and

(4) other disclosures that are customarily provided in connection with opening a person's
account.

Subd. 3. Prior to transaction disclosures. Before each virtual currency transaction for, on behalf of, or with a person, a virtual currency kiosk licensee must disclose the transaction's terms and conditions in clear, conspicuous, and legibly written English, using a reasonable size and type font~~at least 48-point sans serif type font~~. The disclosures under this subdivision must address at least the following:

(1) the amount of the transaction;

(2) any fees, expenses, and charges, including applicable exchange rates;

(3) the type and nature of the transaction;

(4) a warning that once completed, the transaction may not be reversed, if applicable;

(5) a daily virtual currency transaction limit of no more than $~~1,000~~15,000;

Commented [JC11]: As discussed previously, transaction caps (especially those far below reporting thresholds) are the least effective solution for customer protection. The licensee requirements proposed later in this bill in conjunction with the larger limit here will allow operators to properly identify suspicious activity, interrupt transactions for the protection of the customer, and educate those interested in cryptocurrency.

(6) the difference in the virtual currency's sale price versus the current market price; and

(7) other disclosures that are customarily given in connection with a virtual currency transaction.

Subd. 4. Acknowledgment of disclosures. A virtual currency kiosk licensee must ensure that each person who engages in a virtual currency transaction using the virtual currency licensee's kiosk acknowledges receipt of all the disclosures required under this section. Additionally, upon a transaction's completion, the virtual currency licensee must provide a person with a receipt, virtual or physical, containing the following information:

(1) the licensee's name and contact information, including a telephone number to answer questions and register complaints;

(2) the type, value, date, and precise time of the transaction, transactional hash, and each virtual currency address;

(3) the fee charged;

(4) the exchange rate, if applicable;

(5) a statement of the licensee's liability for nondelivery or delayed delivery;

(6) a statement of the licensee's refund policy; and

(7) any additional information the commissioner of commerce may require.

Subd. 5. Fees. The licensee of a virtual currency kiosk is prohibited from collecting fees, whether direct or indirect, from a person related to a single digital financial asset transaction that exceeds the greater of either:

(1) $5; or

(2) ~~ten~~ twenty percent of the United States dollar equivalent of digital financial assets involved in the transaction, according to the publicly quoted market price of the digital asset on a licensed digital financial asset exchange at the time the person initiates the transaction.

Commented [JC12]: The service provided by the kiosk operators carries many unique costs such as inventory procurement, kiosk deployment and maintenance, cash logistics providers, customer service interactions, and compliance requirements, to mention a few. The definition of a maximum revenue potential without regard to a Company's costs is unfair to the licensee. Twenty percent is a good compromise, acknowledging the higher costs of the operator while addressing the potential cost to the customer.

Subd. 6. Cancellation and refund. A virtual currency kiosk licensee must ~~, at the licensee's cost and within 72 hours after a virtual currency transaction,~~ allow the person to cancel and receive a full refund for the virtual currency transaction if ~~the virtual currency transaction is~~:

(1) It is the person's first virtual currency transaction with the licensee; and

(2) The customer returns the purchased cryptocurrency back to the owner or operator; and ~~to a virtual currency wallet or exchange located outside of the United States.~~

(3) No more than 72 hours have passed since the virtual currency transaction occurred.

Subd. 7. Additional Requirements. A virtual currency kiosk licensee must:

(1) obtain government issued identification for all customers, regardless of transaction size.

(2) have restrictions in place that prevent two customers from using the same digital wallet.

(3) have the ability to blacklist or prevent designated wallets from use at the kiosk.

(4) preemptively perform blockchain analytics from an established third party company specializing in such tasks to identify and prevent high risk scored or sanctioned wallets from being used by a customer at the kiosk.

(5) have defined in their policies and procedures a risk-based method to monitor customers on a post-transaction basis.

(6) offer, between 8 AM and 10 PM EST Monday through Friday, live telephone-based customer support from a number prominently displayed at or on the kiosk.

(7) identify and communicate with any new customer over 70 years of age prior to performing a first transaction. During this communication, the owner or operator must 1. Reconfirm kiosk attestations, 2. Discuss the transaction, and 3. Discuss scam typologies. Approval of the customer to transact is dependent upon the owner or operator's assessment of the answers given.

(8) identify and communicate with any new customer attempting to perform, either once or cumulatively, a transaction that breaches a predesignated large transaction amount before such transaction can be released to the blockchain. During this communication the owner or operator 1. must positively identify the customer, 2. review the stated purpose of the transaction, and 3. discuss scam typologies. Approval of the customer to transact is dependent upon the owner or operator's assessment of the answers given.

(9) use a blockchain analytics software in order to assist in the prevention of sending purchased virtual currency from a virtual currency kiosk operator to a virtual currency wallet known to be affiliated with fraudulent activity at the time of a transaction.

(10) designate and employ a compliance officer with the following considerations:

(a) the individual must be qualified to coordinate and monitor compliance with this Act and all other applicable Federal and State laws, rules, and regulations;
(b) the individual must be employed full-time by the virtual currency kiosk operator; and
(c) the designated compliance officer cannot be any individual who owns more than 20% of the virtual currency kiosk operator by whom the individual is employed.

(11) utilize full-time employees of the licensee for compliance responsibilities required under Federal and State laws, rules and regulations.

(12) use a properly registered armored car carrier to handle the collection and transportation of cash from the kiosk to the licensee’s banking solution.