03/21/2024

Senate Commerce and Consumer Protection Committee
Minnesota Senate
95 University Avenue, W
Saint Paul, MN 55155

Re: ***Opposition to S.F. No. 4909 as written***

Chair Klein, Vice-Chair Seeberger, Ranking Minority Member Dahms, and honorable members of the Commerce and Consumer Protection Committee. Thank you for the opportunity to express our concerns on S.F. 4909. CoinFlip opposes S.F. 4909 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, New Zealand, 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 25 money transmitter licenses or virtual currency licenses in the U.S. and numerous additional applications currently pending—CoinFlip is also licensed or registered internationally where needed. 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, who is also an experienced attorney, 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.

S.F. No. 4909

Minnesota recently introduced S.F. No. 4909 in order to regulate virtual currency kiosk disclosures, transaction limits, and transaction fees. Unfortunately, S.F. 4909 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. Further, when a transaction is $3,000 or more, the BSA requires MSBs to collect and store additional info about customers, including social security numbers which helps the government detect and prevent money laundering. 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 immediate 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 S.F. 4909, 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), collection of social security numbers ($3,000) 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 small non-compliant kiosk operators, 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