

Interplay of Federal and State Control in Cryptocurrency Space

FEDERAL:

- Bank Secrecy Act (1970)
- Money Laundering Control Act (1986)

Cryptocurrency ATMs

- A Money Services Business subject to BSA

Administration By FinCEN

- Examined by IRS

Federal FinCEN Regulation

Federal Registration

BSA Compliance Program:

- Designated BSA Compliance Officer
- Internal controls specific to registered business
- BSA/AML training
- Independent testing of BSA/AML program
- Customer Due Diligence

Compliance with applicable State(s) law

As a MSB under
federal law, a
bitcoin ATM
business is (likely)
a money
transmitter in
Kentucky

Kentucky Money Transmitters Act of 2006

- KRS 286.11

Kentucky Department of Financial Institutions

- KDFI's Division of Non-Depository Institutions

KDFI's Licensing Guidance:

- 2013 adoption of NMLS System for Money Transmitters
- September 2022 application of our Money Transmitters Act to Virtual Currency operators



Majority of states
regulate virtual
currency kiosks
under their state
money
transmitter
regime

MTL Application:

1. Provide its BSA Compliance Program documents
2. Data about its itself:
 - ~ Business plan
 - ~ Audited financial statements
 - ~ Information on Executives
3. NMLS System

On-going Monitoring :

1. Surety Bond
2. Periodic audits (compliance, cyber security, and finance programs)
3. Enforcement authority

Bitcoin ATMs in Kentucky

417 (known)
Virtual
Currency
Kiosks
currently
operating in
Kentucky

COINFLIP

BEST PRACTICES TO EDUCATE, ALERT & PREVENT SCAMS

NOVEMBER 2024



About CoinFlip

CoinFlip is a leading digital asset technology company hyper-focused on providing consumers with a simple and secure platform to buy and sell digital currency. Headquartered in Chicago, CoinFlip was founded in 2015 on the belief that enabling safe access to digital currencies will foster the development of a more inclusive, stable and equitable global financial system for consumers. Today, CoinFlip operates a global network of digital currency ATMs, with more than 5,000 locations across the continental United States, Puerto Rico, Canada, Australia, New Zealand, Panama, Brazil, South Africa, Spain, Mexico and Italy.



Focus on Consumer Protection and Compliance

CoinFlip prioritizes consumer protection and legal compliance in all our products and services through annual risk assessments and independent audits, a risk-based AML program with robust KYC requirements, industry-leading third-party blockchain analytics, and rigorous adherence to state and federal laws. When a customer interacts with CoinFlip's state-of-the-art kiosks, identification confirmation is the first step. We implement additional safeguard checks aimed at protecting consumers and preventing fraud. CoinFlip is the industry leader in consumer protection and compliance, collaborating with policymakers and public safety organizations to further state and federal legislation that prioritizes consumers and protects technology innovation.

COINFLIP IN KENTUCKY

Total Employees

201

Total Number of KY Customers:

1,033

KY State Taxes Generated in 2023

\$41.3K

Total rent and fees paid to KY host locations:

\$870K

Total fees paid to local CIT services and technicians:

\$184K

CoinFlip Digital Currency Kiosk Locations



69

Total Locations
in **Kentucky**

How It Works: Making Transactions Simple, Safe & Transparent

CoinFlip controls transactions from end to end, with robust AML and KYC protocols, and efficient fulfillment of customer orders to reduce consumer's bitcoin price risk



- 1. SAFETY FIRST.** When customers visit the kiosk, CoinFlip provides education and warnings on common scam tactics to empower users to make informed decisions. The company also collects required KYC information, a vital safeguard for the financial ecosystem.



- 2. TRANSPARENT.** The price, inclusive of the transaction and network fee, is fully displayed and customer places the order.



- 4. RELIABLE.** CoinFlip offers 24/7 live customer support to assist users every step of the way. The team receives ongoing training related to compliance requirements and financial crime typologies with an emphasis on fraud prevention.

- 3. EFFICIENT.** CoinFlip sends the crypto to the customer for the order minus network and transaction fees.

Consumer Protection

- An estimated 40% of the U.S. adults own a virtual currency asset.
- Criminal scams include directing victims to transfer funds via virtual currency kiosks and other financial platforms. We see this with gift cards and peer-to-peer payment platforms as well.
- The industry must be laser-focused on providing a secure physical platform for our customers to buy and sell digital currency. We want to stop fraud before a consumer initiates a transaction at kiosks.
- As such, CoinFlip has created our “Safe in Six” program to educate consumers and law enforcement on how to spot and stop scams in six questions. These questions are displayed on each of CoinFlip’s virtual currency kiosks. We also partner with law enforcement so they can educate consumers using this program.



**SAFE
inSiX**

SIX QUESTIONS DESIGNED TO
KEEP YOU SAFE FROM SCAMS

COINFLIP



Are you being asked to make an unsolicited financial transaction by an unknown third-party? If so, **STOP**.



Are you being urged to act quickly and/or in secrecy, under the threat of harm in order to satisfy a request from someone unfamiliar? Are you being instructed to lie? If so, **STOP**.



Are you being asked to pay a government fine or a utility bill using a new and unfamiliar payment method like cryptocurrency or gift cards? If so, **STOP**.



Does the offer sound “too good to be true” or feel like an “easy money” investment? If so, **STOP**.



Is someone you’ve initiated a romantic relationship with online now asking you to transfer or deposit money into a kiosk or other bank account as a condition of the relationship? If so, **STOP**.



Is someone asking you to pay or use cryptocurrency to secure a job offer, clear a virus from your computer, clear an arrest warrant, jury duty notice, or to secure your bank account? If so, **STOP**.

What Now?

- If you've gone through this check list and are concerned about what to do next, immediately **STOP** initiation of any transaction.
- **Immediately contact the local law enforcement authorities.**
- Criminals will often tell you to operate in secrecy, tell no one and do not contact the authorities. They will intimidate you and tell you that if you alert family members or police you will put yourself in danger. **DO NOT** listen to them.
- Scammers are sophisticated and persistent operators. They also can sound friendly and helpful. **Follow your gut and the checklist.** If you suspect any of these conditions exist. **STOP.**

Clear, visible scam alerts are highly effective

- ✓ Consumer and scam warnings should be presented and acknowledged by the consumer before initiating every transaction.
- ✓ Customers should also be required to agree to Terms of Service and Privacy Policy during the transaction process.
- ✓ Clear disclosures about transactions being final and irreversible should be prominently displayed and acknowledged by the consumer.



CoinFlip Safeguards: How we prioritize consumer protection

CoinFlip deploys a number of anti-fraud safeguards that are visible and invisible to the consumer. Below are some of CF's best practices for protecting consumers who transact with our products:



Blockchain Analytics

We use leading third-party software to scan and rate digital wallet addresses, auto-blocking transactions that attempt to send to OFAC sanctioned wallets or wallets directly associated with criminal or fraudulent activity.



Identification Verification

We use leading technology to determine if an ID matches the person at the kiosk



Automated case Management

We use case management tools that integrate automated alerts and allows compliance to build case files and file suspicious activity reports directly to FinCEN



Transaction Monitoring

We use technology tools and automated alerts to detect and identify potentially suspicious transactions



Compliance Team

We employ a trained compliance team with over ten Anti-Money Laundering Analysts who identify, investigate and report on potentially suspicious transactions

A stack of several colorful notebooks (red, yellow, blue, green) is placed on a dark laptop keyboard. The image is partially obscured by a white, torn-edge border on the right side.

Consumer Protection Best Practices Work

- Using its blockchain analytics tools, CoinFlip has proactively blocked more than one thousand customer transactions related to suspicious or blacklisted digital wallets.
- CoinFlip's customer experience agents who are all located in the U.S. are trained to identify potential scams and have prevented hundreds of suspicious transactions from going forward.

Effective Regulations for Consumer Protection

The following consumer protection best practices should be considered as part of any digital currency kiosk legislation:

- 1. Licensure with the state creates a strong foundation from which to enforce consumer protective practices.** A state money transmitter license like in Kentucky is the best way to regulate virtual currency kiosk operators. This gives the state an opportunity for oversight (including audit and other enforcement) of kiosk operators.
- 2. Robust internal compliance is necessary.** 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.
- 3. Clear, highly visible scam warnings are effective consumer protection tools.** Warnings should be required to be prominently displayed and acknowledged by the customer prior to the initiation and completion of any transaction. Virtual currency kiosk operators should be required to clearly disclose, prior to completion of a transaction, all fees associated with the transaction.
- 4. Innovative technologies like blockchain analytics are necessary consumer protection tools.** The use of blockchain analytics technology should be required to prevent fraud by automatically blocking customer transactions to high-risk digital wallets.
- 5. Customer service is the first line of defense for consumer protection.** Live, human intervention is a proven successful tool at preventing scams. Virtual currency kiosk operator should be required to provide trained, live customer service.

THANK YOU

