CS FOR HOUSE BILL NO. 324(JUD)

IN THE LEGISLATURE OF THE STATE OF ALASKA

THIRTY-FOURTH LEGISLATURE - SECOND SESSION

BY THE HOUSE JUDICIARY COMMITTEE

Offered: 3/27/26
Referred: Labor and Commerce

Sponsor(s): REPRESENTATIVE MOORE

A BILL

FOR AN ACT ENTITLED

"An Act relating to virtual currency kiosks; relating to transactions involving virtual currency; and relating to unfair trade or deceptive acts or practices."

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

*** Section 1.** AS 06.55 is amended by adding new sections to read:

Article 1A. Virtual Currency Kiosks.

Sec. 06.55.115. Virtual currency kiosk operator licensing and reporting. (a) A virtual currency kiosk operator may not engage in a virtual currency kiosk transaction or hold itself out as being able to engage in virtual currency kiosk transactions with or on behalf of another person unless the virtual currency kiosk operator holds a money transmission license.

(b) A virtual currency kiosk operator may not locate a virtual currency kiosk in the state unless the virtual currency kiosk operator registers with and obtains the prior approval of the department.

Sec. 06.55.120. Mandatory hold for first transaction. If a user has not

previously engaged with a virtual currency kiosk operator, the virtual currency kiosk operator shall put a 48-hour hold on the first virtual currency kiosk transaction that the user engages in with the virtual currency kiosk operator before completing the transaction. The virtual currency kiosk operator may not engage in another transaction with the user until the 48-hour hold has expired.

Sec. 06.55.125. Reporting. (a) Within 45 days after the end of each calendar quarter, a virtual currency kiosk operator shall submit a quarterly report to the department for each location in the state at which the person operates a virtual currency kiosk. The report must include the following:

(1) the legal name of the virtual currency kiosk operator;

(2) any fictitious or trade name used by the virtual currency kiosk operator;

(3) the virtual currency kiosk operator's physical address;

(4) the date that operation of a virtual currency kiosk began at the location;

(5) if applicable, the date the virtual currency kiosk operator ceased operating a virtual currency kiosk at the location;

(6) virtual currency addresses used by the virtual currency kiosk operator to service users at every location in the state; and

(7) the number of transactions declined because of suspicion of illicit activity.

(b) On or before March 31 of each year, a virtual currency kiosk operator shall submit an annual report to the department relating to the virtual currency kiosk operator's business conducted in the state during the previous calendar year. The report shall be on a form prescribed by the department and must include

(1) the gross revenue attributable to virtual currency transactions conducted through virtual currency kiosks in the state;

(2) copies of each complaint filed by a user against the virtual currency kiosk operator with the Better Business Bureau or a state or federal agency other than the department and a description of the resolution, if any, of each complaint;

(3) the total number and value of virtual currency transactions the

virtual currency kiosk operator conducted through virtual currency kiosks in the state;

(4) the total number of refunds requested by users, including the number of requests granted and the number denied by the virtual currency kiosk operator;

(5) the total dollar amount of refunds the virtual currency kiosk operator provided to users;

(6) contact details for the virtual currency kiosk operator's compliance officer;

(7) the total number of virtual currency kiosk locations; and

(8) the total number and dollar amount of suspicious transaction reports the virtual currency kiosk operator was required to file under 31 U.S.C. 5311 - 5336.

(c) Upon request, a virtual currency kiosk operator shall make available to the department information on any transaction processed by the virtual currency kiosk or any user of the virtual currency kiosk, including information related to transactions that were attempted but denied.

(d) Data collected by the department under this section is confidential and is not a public record for purposes of AS 40.25.110 - 40.25.140 but may be released in composite form. The department shall prepare and make available to the public an annual report summarizing the data reported to the department under this section.

Sec. 06.55.130. Disclosures. (a) A virtual currency kiosk operator shall disclose in a clear, conspicuous, and easily readable manner in the chosen language of the user all relevant terms and conditions generally associated with the products, services, and activities of the virtual currency kiosk operator and virtual currency, including transaction charges collected and exchange rates used by the virtual currency kiosk operator.

(b) When a user engages with a virtual currency kiosk, the virtual currency kiosk operator shall obtain acknowledgment of receipt of all disclosures required under this section.

(c) The disclosures required under this section must address the following:

(1) a warning, written prominently and in bold type stating

WARNING: this technology can be used to defraud you. If someone asked you to deposit money in this machine or is on the telephone with you and claims to be a friend or family member, government agent, computer software representative, bill collector, law enforcement officer, or anyone you do not know personally IMMEDIATELY STOP THIS TRANSACTION and contact your local law enforcement and the kiosk operator. This may be a scam. NEVER SEND MONEY to someone you don't know;

(2) a warning of the material risks associated with virtual currency, including a warning that virtual currency is not issued or backed by the United States government; is not legal tender in the United States; is not subject to protections by the Federal Deposit Insurance Corporation, National Credit Union Administration, or Securities Investor Protection Corporation; and that its value relative to the United States dollar may fluctuate significantly;

(3) the name, address, and telephone number of the owner of the kiosk and the days, time, and means by which a user can contact the owner for assistance;

(4) the address and telephone number of the Alaska state troopers, local law enforcement, and the department, along with a message that a user may report fraud to any of those entities, shall be displayed on or at the location of a virtual currency kiosk or on the first screen of a kiosk; and

(5) other disclosures that the department requires by regulation.

(d) The disclosures required under this section do not affect the obligation of a virtual currency kiosk operator to issue a refund under AS 06.55.160.

(e) After each transaction, the virtual currency kiosk operator shall provide users with paper and electronic receipts. In addition to the information required under AS 06.55.830, the receipt must include the following information:

(1) the virtual currency kiosk operator's name and toll-free customer service telephone number;

(2) relevant contact information to report fraud to the Alaska state troopers, local law enforcement, and the department;

(3) the type, value, date, and time of the transaction;

(4) each applicable virtual currency address and transaction hash, if applicable;

(5) all charges incurred in the transaction;

(6) the exchange rate used between the virtual currency and United States dollar;

(7) if the transaction is subject to a first transaction hold required under AS 06.55.120, notice of the hold and when the hold expires;

(8) a statement of the virtual currency kiosk operator's refund policy;

(9) any additional information the department requires by regulation.

Sec. 06.55.135. Fraud and anti-money laundering policy. A virtual currency kiosk operator shall take reasonable steps to detect and prevent fraud and money laundering, including establishing and maintaining a written anti-fraud policy and abiding by 31 U.S.C. 5311 - 5336 (Bank Secrecy Act). The anti-fraud and money laundering policy must, at a minimum,

(1) identify and assess fraud-related and money laundering-related risk areas;

(2) establish procedures and controls to protect against identified risks of fraud and money laundering;

(3) allocate responsibility for monitoring risks of fraud and money laundering; and

(4) require periodic evaluation and revision of the anti-fraud and money laundering procedures, controls, and monitoring mechanisms.

Sec. 06.55.140. Blockchain analytics. A virtual currency kiosk operator shall use blockchain analytics and tracing software to assist in the prevention of sending virtual currency to a virtual currency wallet known or likely to be affiliated with fraudulent activity at the time of a transaction and to detect transaction patterns indicative of fraud or other illicit activities. Virtual currency kiosk operators shall block transactions to virtual currency wallets associated with overseas exchanges that are inaccessible to users in the United States. A virtual currency kiosk operator shall make available to the department, upon request, evidence of their current use of blockchain analytics.

Sec. 06.55.145. Posted warnings. A virtual currency kiosk operator shall post a conspicuous written warning in plain view of the virtual currency kiosk providing notice to users that criminals may direct victims of fraud or scams to send money by way of virtual currency kiosks. This warning must include the virtual currency kiosk operator's toll-free customer service telephone number.

Sec. 06.55.150. User identification. (a) A virtual currency kiosk operator or their authorized delegate shall verify the identity of a user before accepting payment from the user for a virtual currency transaction. A virtual currency kiosk operator or their authorized delegate shall obtain a copy of a government-issued identification card that identifies the user and shall collect additional user information, including the user's name, date of birth, telephone number, address, and electronic mail address, before accepting a payment from the user at a virtual currency kiosk.

(b) A virtual currency kiosk operator may not allow a user to engage in a transaction at a virtual currency kiosk under any name, account, or identity other than the user's own true name and identity.

(c) A virtual currency kiosk operator is strictly liable for a violation of this section.

Sec. 06.55.155. Training. On an annual basis, a virtual currency kiosk operator shall provide the store or location where the kiosk is located with staff training materials approved by the department. The training materials must outline how criminals may exploit virtual currency kiosks in illicit activity, including red flag indicators that a virtual currency kiosk user may be the victim of fraud or scams as well as signs of financial abuse and exploitation. The virtual currency kiosk operator may not prohibit or prevent staff at the location of the virtual currency kiosk from educating virtual currency kiosk users on fraud and scams.

Sec. 06.55.160. Refunds. (a) For cases related to fraud, a virtual currency kiosk operator shall issue a full refund to a user if the user

(1) engaged in a transaction involving the virtual currency kiosk that was affected by fraud;

(2) informed the virtual currency kiosk operator of the fraudulent nature of the transaction or transactions at issue within 90 days after the last

transaction or within 90 days after the user became aware of the fraud, whichever is later; and

(3) within 120 days after contacting the virtual currency kiosk operator, submitted to the virtual currency kiosk operator a police report, report by the department, or a sworn statement detailing the fraudulent nature of the transaction.

(b) If a user requests that a transaction be cancelled during a first transaction hold required under AS 06.55.120, the virtual currency kiosk operator shall cancel the transaction and provide the user with a full refund.

(c) If the conditions for a refund under (a) or (b) of this section are met, the virtual currency kiosk operator shall issue the refund to the user

(1) in the original currency provided by the user;

(2) in the full amount of all transactions paid by the user at the time of the transaction, including transaction charges, regardless of any acknowledgment the user may have made before finalizing the transactions; and

(3) within 72 hours after receiving a copy of the police report, report by the department, or sworn statement for a refund required under (a) of this section or a request that the transaction be cancelled during a first transaction hold for a refund required under (b) of this section.

Sec. 06.55.165. Communication. For all communication between the virtual currency kiosk operator and the user, the virtual currency kiosk operator shall provide written notices in both English and Spanish and communicate with the user in their preferred language through staff, oral interpretation services, or auxiliary aids and services.

Sec. 06.55.170. Transaction limit. (a) A virtual currency kiosk operator may not accept transactions totaling more than $1,000, or the equivalent in virtual currency, from a user in one calendar day.

(b) A virtual currency kiosk operator may not accept transactions totaling more than $10,000, or the equivalent in virtual currency, from a user in a 30-day period.

(c) The limits in this section apply to all products offered by a virtual currency kiosk operator. The use of alternative products, including online purchasing or over-

the-counter platforms, may not be employed to circumvent or exceed the limits in this section.

Sec. 06.55.175. Transaction fees. A virtual currency kiosk operator may not collect fees from a user for a transaction that total more than three percent of the transaction value in United States dollars or the equivalent in virtual currency.

Sec. 06.55.180. Customer service. A virtual currency kiosk operator shall provide live customer service during operating hours, including the hours between 8:00 a.m. and 10:00 p.m. Alaska time. A customer service toll-free number must be displayed on the virtual currency kiosk or the virtual currency kiosk screen.

Sec. 06.55.185. Law enforcement access to investigative information. A virtual currency kiosk operator shall provide a dedicated communications line for government agencies to contact the virtual currency kiosk operator. The dedicated line must be an electronic mail address or telephone number based in the United States. A law enforcement agency or a regulatory agency, including the department, may use the dedicated line to communicate with the virtual currency kiosk operator in the event of a fraud report from a user. The dedicated line must be regularly monitored. Upon request from a law enforcement agency or regulatory agency, a virtual currency kiosk operator must provide the agency with trace findings and grant the agency assistance with blockchain analytics to assist in an investigative matter related to potential fraud.

Sec. 06.55.190. Penalties. (a) A virtual currency kiosk operator that violates AS 06.55.115 - 06.55.200 commits an unfair trade or deceptive act or practice in violation of AS 45.50.471.

(b) A virtual currency kiosk operator operating in this state without a money transmission license or that otherwise violates AS 06.55.115 - 06.55.200 is subject to administrative action, including civil penalties, that may, notwithstanding AS 06.55.605, include the seizure of any virtual currency kiosk and the forfeiture of all fees received from customers in the state during the period of unlicensed activity or noncompliance.

Sec. 06.55.195. Municipal regulations. Nothing in AS 06.55.115 - 06.55.200 may be interpreted to preempt or nullify a municipal ordinance that provides greater protections, requirements, or restrictions if the municipal ordinance does not directly

conflict with AS 06.55.115 - 06.55.200.

Sec. 06.55.200. Definitions. In AS 06.55.115 - 06.55.200,

(1) "blockchain analytics" means the analysis of data from blockchains or public distributed ledgers, including associated transaction information;

(2) "blockchain analytics and tracing software" includes a software service that uses blockchain analytics to provide risk-specific information and tracing of virtual currency wallet addresses;

(3) "charges" include

(A) fees or expenses paid by a user; and

(B) the difference between the market price of the virtual currency and the price of the virtual currency charged to the user;

(4) "user" means an individual or entity that initiates, authorizes, or completes a transaction involving virtual currency through a virtual currency kiosk for the purpose of purchasing, selling, transferring, or otherwise exchanging virtual currency;

(5) "virtual currency" means an electronic asset that confers economic, proprietary, or access rights or powers and is recorded using cryptographically secured distributed ledger technology, or any similar analogue;

(6) "virtual currency address" means an alphanumeric identifier associated with a virtual currency wallet that identifies the location to which a virtual currency transaction can be sent;

(7) "virtual currency kiosk" means a person acting on the behalf of, or a mechanical agent of, the virtual currency kiosk operator to enable the virtual currency kiosk operator to facilitate the exchange of virtual currency for money, bank credit, or other virtual currency by connecting directly to a separate virtual currency exchange, drawing on virtual currency in the possession of the electronic terminal's operator, or by another method;

(8) "virtual currency kiosk operator" means a person that engages in virtual currency business activity by way of a virtual currency kiosk located in the state or a person that owns, operates, manages, or provides custodial or noncustodial services for a virtual currency kiosk located in the state through which virtual currency

business activity is offered;

(9) "virtual currency kiosk transaction" means a transaction conducted or performed, in whole or in part, by electronic means through a virtual currency kiosk or a transaction made at a virtual currency kiosk to purchase virtual currency with United States dollars or to sell virtual currency for United States dollars;

(10) "virtual currency wallet" means a software application or other mechanism providing a means to hold the keys necessary to access and transfer virtual currency.

*** Sec. 2.** AS 06.55.840 is amended by adding a new subsection to read:

(b) This section does not apply to a refund requested for a virtual currency kiosk transaction under AS 06.55.115 - 06.55.200.

*** Sec. 3.** AS 06.55.990(15) is amended to read:

(15) "money transmission"

(A) means

(i) selling or issuing payment instruments or stored value, or receiving money or monetary value for transmission**; or**

(ii) operating a virtual currency kiosk;

(B) [, BUT] does not include the provision solely of delivery, online services, telecommunications services, or network access;

*** Sec. 4.** AS 45.50.471(b) is amended by adding a new paragraph to read:

(58) violating AS 06.55.115 - 06.55.200 (virtual currency kiosks).

Alaska State Legislature

Representative Elexie Moore
House District 28
907-465-4833

120 4th Street
Alaska State Capitol
Room 432
Juneau, AK 99801

Sponsor Statement: House Bill 324
"An Act relating to virtual currency kiosks"

House Bill 324 addresses a growing gap in our state's financial regulatory framework: the unregulated rise of virtual currency kiosks, commonly known as "Bitcoin ATMs." While Alaska embraces technological innovation, we must ensure that these new financial tools are not weaponized by bad actors to defraud Alaskans, particularly our seniors and those most vulnerable.

In recent years, law enforcement agencies across the country have reported a massive surge in scams involving virtual currency kiosks. Because these machines allow for the near-instantaneous transfer of cash into untraceable digital assets, they have become the preferred vehicle for "grandparent scams," government imposter schemes, and romance fraud. Under current law, these kiosks often operate in a legal "gray area," leaving victims with no recourse and the state with no oversight.

House Bill 324 establishes a comprehensive "Consumer Bill of Rights" for virtual currency transactions:

- Licensing and Oversight: Requires all kiosk operators to hold a money transmission license and register each physical location with the Department of Commerce, Community, and Economic Development.
- Mandatory Fraud Warnings: Requires clear, bold physical and digital warnings on every machine to alert users that government agencies and legitimate businesses will never ask for payment via a Bitcoin kiosk.
- Transaction Limits: Implements sensible daily and monthly limits—$1,000 per day and $10,000 per month—to slow down the rapid "draining" of life savings that often occurs during a high-pressure scam.
- Fee Transparency: Protects consumers from predatory pricing by capping transaction fees at 3%, ensuring that Alaskans are not losing a massive portion of their principle to hidden exchange rate spreads or exorbitant service charges.
- Right to Refund: Establishes a strict liability pathway for refunds in cases of documented fraud, holding operators accountable for verifying the identity of users and maintaining robust anti-money laundering (AML) protocols.
- Law Enforcement Cooperation: Mandates the use of blockchain analytics and creates a dedicated communications line for law enforcement to track illicit transfers in real-time.

By passing HB 324, we are sending a clear message: Alaska is open for innovation, but we will not be a safe harbor for exploitation. This bill provides the Department and law enforcement the tools they need to protect Alaskans' hard-earned money while bringing a rapidly growing industry into the light of common-sense regulation.

Alaska State Legislature

Representative Elexie Moore
House District 28
907-465-4833

120 4th Street
Alaska State Capitol
Room 432
Juneau, AK 99801

Sectional Analysis CSHB 324(JUD) \N
"An Act Relating to Virtual Currency Kiosks"

Section 1: Regulation of Virtual Currency Kiosks (AS 06.55) – Page 1, ln. 4 through Page 9, ln. 27

This section creates a new regulatory framework specifically for operators of virtual currency kiosks (commonly known as Bitcoin ATMs).

- **Sec. 06.55.120. Licensing and Registration:** * Mandates that kiosk operators hold a valid money transmission license. (Page 1, lines 6-13)
    - Requires prior department approval for every physical kiosk location in the state.
- **Sec. 06.55.120 Mandatory Hold for First Transaction:** Places a 48-hour hold on the release of cryptocurrency funds for first time users who have not previously engaged with virtual currency kiosks.
- **Sec. 06.55.125. Reporting:** * Quarterly Reports: Operators must disclose locations, virtual currency addresses used, and the number of transactions declined due to suspicion of illicit activity. (Page 1, ln. 14 through Page 3, ln. 14)
    - Annual Reports: Operators must report gross revenue, total transaction volume/value, refund statistics, and the number of Suspicious Transaction Reports (STRs) filed under federal law.
- **Sec. 06.55.130. Disclosures:** * Requires clear, conspicuous warnings about fraud risks (e.g., "WARNING: this technology can be used to defraud you"). (Page 3, ln. 15 through Page 5, ln. 3)
    - Mandates detailed receipts (paper and electronic) including transaction hashes, exchange rates, and law enforcement contact information.
- **Sec. 06.55.135 – 06.55.140. Fraud Prevention & Blockchain Analytics:** * Requires operators to maintain written anti-fraud and anti-money laundering (AML) policies. (Page 5, lines 4-25)
    - Mandates the use of blockchain analytics and tracing software to block transactions to fraudulent wallets or inaccessible overseas exchanges.
- **Sec. 05.55.145 Posted Warnings:** This requires kiosk operators to post conspicuous written warnings regarding potentially fraudulent activity. (Page 5, lines 26-30)
- **Sec. 06.55.150. User Identification:** * Requires identity verification (KYC) via a government-issued ID for all transactions. (Page 5, ln. 31 through Page 6, ln. 11)
    - Establishes strict liability for operators who allow transactions under false names or identities.
- **Sec. 06.55.155 Training:** Requires kiosk operators to annually provide training to staff and may not prohibit staff from educating kiosk users on fraud and scams. (Page 6, lines 12-19)
- **Sec. 06.55.160. Refunds:** * Grants victims of fraud a statutory right to a full refund (including fees) if they notify the operator within 90 days and provide a police report. (Page 6, ln. 60 through Page 7, ln. 6)
    - Operators must issue refunds within 72 hours of receiving the documentation.

- **Sec. 06.55.165. Communication:** Stipulates that kiosk operators must have written notices in English and Spanish and provide interpretation services as necessary. (Page 7, lines 7-11)
- **Sec. 06.55.170 – 06.55.172. Limits on Transactions and Fees:** * Daily Limit: $1,000 per user. (Page 7, lines 12-24)
    - 30-Day Limit: $10,000 per user.
    - Fee Cap: Total transaction charges (including exchange rate spreads) cannot exceed 3% of the transaction value.
- **Sec. 06.55.175. Customer Service:** * Requires kiosk operators to provide live customer service between the hours of 8:00 am and 10:00 PM AST including a toll-free number. (Page 7, lines 25-28)
- **Sec. 06.55.180. Law enforcement access to investigative information:** An operator is required to provide a dedicated line for government agencies, and the dedicated line must be regularly monitored. In addition, operators must provide a law enforcement or regulatory agency with trace finding and blockchain analytics. (Page 7, ln. 29 through Page 8, ln. 7)
- **Sec. 06.55.185. Penalties:** * Violations are classified as unfair or deceptive acts under the Alaska Consumer Protection Act.
    - Operators are subject to civil penalties, seizure of kiosks, and forfeiture of all fees collected during the period of noncompliance.
- **Sec. 06.55.190. Municipal Regulations:** * Allows Alaska municipalities to adopt stricter ordinances that state statute if it is not in conflict with state statute. (Page 8, lines 17-20)
- **Sec. 06.55.195. Definitions:** It provides definitions relevant to this chapter. (Page 8 ln. 21 through Page 9, ln. 27)
    - Definitions in this section include:
        - Blockchain analytics
        - Blockchain analytics and tracing software
        - Charges
        - User
        - Virtual currency
        - Virtual currency address
        - Virtual currency kiosk
        - Virtual currency kiosk operator
        - Virtual currency kiosk transaction
        - Virtual currency wallet

Section 2: Conforming Amendment (AS 06.55.840) – Page 9, lines 28-30

- Exempts virtual currency kiosk transactions from general money transmission refund rules to ensure the specific, more consumer-friendly refund protections in HB 324 take precedence.

S**ection 3: Conforming Amendment (AS 06.55.990)** – Page 9, ln. 31 through Page 10, ln. 9

- Amends AS 06.55.990(15) to include operating a virtual currency kiosk.

Fiscal Note

State of Alaska
2026 Legislative Session

Bill Version: HB 324
Fiscal Note Number:
() Publish Date:

Identifier: HB324-DCCED-DBS-02-27-26
Title: VIRTUAL CURRENCY KIOSKS
Sponsor: MOORE
Requester: (H) JUDICIARY

Department: Department of Commerce, Community and Economic Development
Appropriation: Banking and Securities
Allocation: Banking and Securities
OMB Component Number: 2808

Expenditures/Revenues

Note: Amounts do not include inflation unless otherwise noted below. (Thousands of Dollars)

	FY2027 Appropriation Requested	Included in Governor's FY2027 Request	Out-Year Cost Estimates				
OPERATING EXPENDITURES	**FY 2027**	**FY 2027**	**FY 2028**	**FY 2029**	**FY 2030**	**FY 2031**	**FY 2032**
Personal Services							
Travel							
Services							
Commodities							
Capital Outlay							
Grants & Benefits							
Miscellaneous							
Total Operating	**0.0**	**0.0**	**0.0**	**0.0**	**0.0**	**0.0**	**0.0**

Fund Source (Operating Only)

None							
Total	**0.0**	**0.0**	**0.0**	**0.0**	**0.0**	**0.0**	**0.0**

Positions

Full-time							
Part-time							
Temporary							

Change in Revenues

None							
Total	**0.0**	**0.0**	**0.0**	**0.0**	**0.0**	**0.0**	**0.0**

Estimated SUPPLEMENTAL (FY2026) cost: 0.0 *(separate supplemental appropriation required)*

Estimated CAPITAL (FY2027) cost: 0.0 *(separate capital appropriation required)*

Does the bill create or modify a new fund or account? No

(Supplemental/Capital/New Fund - discuss reasons and fund source(s) in analysis section)

ASSOCIATED REGULATIONS

Does the bill direct, or will the bill result in, regulation changes adopted by your agency? Yes
If yes, by what date are the regulations to be adopted, amended or repealed? 12/31/26

Why this fiscal note differs from previous version/comments:

Not applicable, intial version.

Prepared By: Tracy Reno, Division Director — Phone: (907)269-8112
Division: Division of Banking and Securities — Date: 02/27/2026
Approved By: Hannah Lager, Administrative Services Director — Date: 02/27/26
Agency: Department of Commerce, Community, and Economic Development

FISCAL NOTE ANALYSIS

STATE OF ALASKA **BILL NO. HB 324**
2026 LEGISLATIVE SESSION

Analysis

HB 324, Virtual Currency Kiosks, establishes a regulatory framework for virtual currency kiosks in Alaska to enhance consumer protection and prevent fraud and money laundering. HB 324 creates a new section in AS 06.55 to regulate virtual currency kiosks ("kiosk"). This bill requires kiosk operators to obtain a money transmitter license and provide periodic reports. This bill requires a money transmission licensee ("licensee") to provide clear disclosures to users, limit transaction dollar amounts each day and month, and provide receipts with detailed transaction information including fees, exchange rates, fraud warnings, and risks associated with virtual currency. This bill requires licensees to combat illicit activity by implementing anti-fraud and anti-money laundering policies, to utilize blockchain analytics to detect suspicious transactions, and block transfers to wallets linked to fraud. Licensees are required to prioritize consumer protection, are liable for fraudulent transactions, and are required to refund the transaction amount and fees to a user after receiving appropriate documentation. Violations of these provisions are classified as unfair trade or deceptive acts under AS 45.50, subject to civil penalties, seizure of kiosks, and forfeiture of fees.

The Division of Banking and Securities ("Division") is the primary regulator for money services businesses regulated under Alaska Uniform Money Services Act ("Act") AS 06.55 and 3 AAC 13 and has oversight over virtual currency kiosks as registered agent locations. The division licenses, examines, conducts investigations, and enforces statutes for money service businesses in Alaska. The division conducts periodic examinations to ensure that money service businesses operate in compliance with state and federal law and are operating in a safe and sound manner.
There are approximately 76 active virtual currency kiosks in the state of Alaska currently and the companies that utilize the kiosks for money transmission already hold a license in Alaska. No new revenue is expected from licensing.

The fiscal impact of this legislation is indeterminate. The division expects a significant increase in complaints being filed by users who are victims of fraud utilizing a virtual currency kiosk, but the volume and complexity of those complaints and resulting investigations is not known. Additional staff may be needed to conduct investigations into reports of fraud. For each investigation, staff would work through the administrative process, which includes a complaint form filed by a user, an investigation, and if warranted staff draft an order with a written option for an administrative hearing with 30 days to request a hearing. An order would be required for the division to order a licensee to issue refund for cases related to fraud. If the licensee chooses to proceed to a hearing the division would enlist Department of Law ("DOL") to represent them at hearing; this would likely increase operating expenditures for legal services, but those costs cannot be estimated at this time. If an order or a hearing result in a civil penalty paid by the licensee there would be a contribution to the general fund resulting in an unknown amount of revenue.

At this time, the division submits a zero fiscal note and will continue to reassess should additional funding or position may be needed.

IN THE SUPERIOR COURT OF THE DISTRICT OF COLUMBIA
Civil Division

DISTRICT OF COLUMBIA, a municipal corporation, 400 6th Street, NW Washington, DC 20001, *Plaintiff*, v. **ATHENA BITCOIN, INC.** 1 SE 3rd Avenue, STE 2740 Miami, Florida 33131 *Defendant*.	Civil Action No.: _____ **COMPLAINT** **JURY TRIAL DEMANDED**

Plaintiff District of Columbia ("District"), by its Office of the Attorney General, brings this action against Defendant Athena Bitcoin, Inc. ("Athena") for failing to disclose excessive fees and to protect consumers from scams in violation of the District's Consumer Protection Procedures Act ("CPPA"), D.C. Code §§ 28-3901, *et seq*. and Abuse, Neglect, and Financial Exploitation of Vulnerable Adults and the Elderly Act (the "Financial Exploitation Act"), D.C. Code §§ 22-933.01 and 22-937. In support of its claims, the District states as follows:

INTRODUCTION

1. District seniors and other residents have been scammed out of life-altering amounts of cash through Athena Bitcoin Automated Teller Machines ("BTMs"). Most deposits to Athena BTMs in the District—93% during the first five months of operation—are the product of outright fraud. Not only has Athena done little to nothing to prevent this fraud, but it has instead pocketed hundreds of thousands of dollars in undisclosed fees on the backs of scam victims and adopted policies to prevent these victims from recovering any of their losses.

2. Athena—one of the country's largest BTM operators—has maintained seven BTMs in the District. These BTMs ostensibly allow consumers to purchase cryptocurrencies, such as Bitcoin, using cash.[1] But Athena's machines are primarily used to facilitate fraudulent schemes that exploit the elderly and result in huge sums of money being transferred directly to scammers.

(*Athena BTM image via https://athenabitcoin.com/host-an-atm*)

3. Bitcoin is digital "money" that is stored in a digital "wallet"—like a bank account but without the oversight or security provided by a financial institution. Bitcoin wallets are identified by long strings of letters and numbers called "addresses." Each transaction with a Bitcoin wallet is recorded on a public ledger called the "blockchain."

4. In the typical BTM scam, foreign fraudsters contact victims posing as representatives of trusted institutions—banks, law enforcement agencies, technology companies—and falsely claim that the victim's finances are at risk. Scammers tell victims to withdraw cash from their bank or retirement accounts and deposit the funds into a BTM to protect their money or to cooperate with an official investigation.

[1] For simplicity, this Complaint generally uses the term "Bitcoin" to refer to the cryptocurrencies that users can purchase using BTMs. That term should be understood to refer to any cryptocurrency that a user attempts to purchase using a BTM.

5. Upon receiving this directive, victims locate an Athena BTM, often in a gas station, and insert their cash into the BTM. They direct the cash to a Bitcoin wallet—usually by scanning a QR code provided by the fraudsters—where their converted cash is to be deposited as Bitcoin. Athena then purchases the Bitcoin on an open exchange and, sometime later, transfers that Bitcoin to the wallet address scanned by the user.

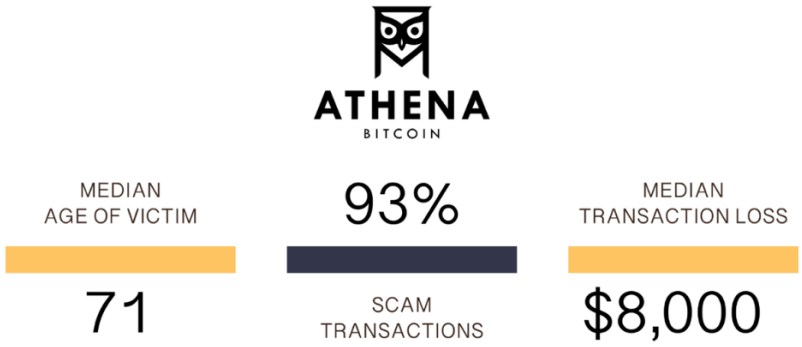
6. The scammer in control of the wallet may then transfer the money to another wallet controlled by the scammer or convert the Bitcoin to cash via offshore Bitcoin exchanges, such as Binance, Bybit, or KuCoin. Once the money has been deposited into the scammer's wallet, the transaction cannot be reversed.

7. Rather than take the steps necessary to prevent these fraudulent transactions from overrunning its machines, Athena has intentionally profited from the fraud by imposing excessive, undisclosed fees on BTM transactions—up to 26% of each transaction. Athena also has allowed elderly consumers to deposit very large amounts of cash over short time periods into wallets that Athena *knew* had already been used by other scam victims. Athena's ineffective oversight procedures have created an unchecked pipeline for illicit international fraud transactions.

8. Once the fraud is discovered, Athena has given consumers no recourse to recover their funds. Athena has systematically told scam victims that *all their money* is unrecoverable even while Athena has retained up to 26% of the scam as a fee, which could be easily returned. Exacerbating these problems, Athena has misrepresented its refund policy in every direction—imposing a no refunds policy in its Terms of Service while arbitrarily capping the fee refunds when victims diligently force the issue.

9. An analysis of complaint and transaction data from Athena's first five months of operations within the District—from May 2024 to September 2024—revealed that at least 93% of

all Athena BTM deposits were the product of fraud, as noted above. The data also revealed that the median age of victims was 71 years, and the median loss per transaction was $8,000.



10. Athena violates the CPPA by engaging in unfair and deceptive trade practices, including by failing to adequately disclose transaction fees, utilizing unconscionable contract provisions, unfairly denying fraud victims the ability to recover stolen funds, operating without a money transmission license, and failing to implement adequate consumer protection measures.

11. Athena's conduct also violates the Financial Exploitation Act by facilitating the financial exploitation of elderly and vulnerable District residents while actively deceiving them regarding the existence and magnitude of the company's excessive fee structure and its ability (or inability) to refund those fees. Athena has permitted and profited from transactions in which victims are coerced, misled, and manipulated into depositing their life savings into Athena's machines under fraudulent pretenses.

12. The District of Columbia brings this enforcement action to stop Athena's predatory business practices, protect vulnerable and elderly consumers, and obtain financial relief for Athena's victims. The District seeks injunctive relief, restitution, damages, civil penalties, attorneys' fees, and all other appropriate relief to ensure that Athena fully discloses its fee structure, implements effective fraud prevention measures, and provides an adequate refund process for victims of scams.

PARTIES

13. Plaintiff District of Columbia is a municipal corporation empowered to sue and be sued and is the local government for the territory constituting the permanent seat of the government of the United States. The District is represented by and through its chief legal officer, the Attorney General for the District of Columbia. The Attorney General has general charge and conduct of all legal business of the District and all suits initiated by and against the District and is responsible for upholding the public interest. *See* D.C. Code § 1-301.81(a)(1). The Attorney General is specifically authorized to enforce the CPPA and the Financial Exploitation Act under D.C. Code §§ 28-3909 and 22-937, respectively.

14. Defendant Athena Bitcoin, Inc. is a Delaware corporation formed on September 18, 2015. Athena maintains its headquarters at 1 SE 3rd Ave, Suite 2740, Miami, FL 33131. Athena operates BTMs across the United States, including within the District and internationally, enabling consumers to purchase Bitcoin using cash. Athena is registered to do business in the District but does not have the required money transmission license. Athena trades over the counter (outside a national exchange but subject to SEC oversight) as Athena Bitcoin Global with a total market capitalization of more than $200 million and yearly revenue of $192 million.

JURISDICTION

15. This Court has subject matter jurisdiction over the claims in this Complaint through D.C. Code § 11-921 and under the District's Financial Exploitation Act, D.C. Code § 22-937(a), and the CPPA, D.C. Code § 28-3909.

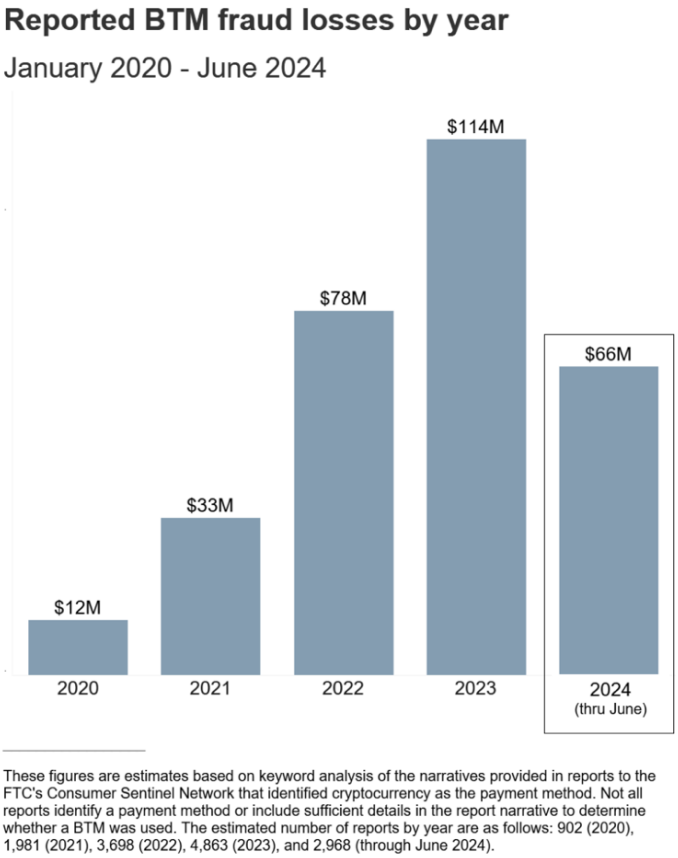
16. This Court has personal jurisdiction over the Defendant under D.C. Code §§ 13-422 and 13-423.

FACTUAL ALLEGATIONS

I. BTMs Primarily Serve as a Scammer Payment Portal

17. BTMs have rapidly become a preferred tool for scammers worldwide—particularly those targeting elderly and vulnerable consumers. The speed, anonymity, cross-border functionality, and irreversibility of cash-to-crypto transactions make BTMs an ideal tool for scammers.

18. The Federal Trade Commission ("FTC") and the Federal Bureau of Investigation ("FBI") have both documented the escalating role of BTMs in financial scams. According to the FTC, reported fraud losses involving BTMs increased nearly tenfold from 2020 to 2023, reaching $66 million in the first half of 2024 alone:



(*BTM losses by year as reported by the FTC*)

19. The FBI's data paints an even darker picture. Its 2023 Cryptocurrency Fraud Report notes that the Internet Crime Complaint Center ("IC3") received more than 5,500 fraud complaints in 2023 involving BTMs with total reported losses *exceeding $189 million*.

20. The impact on elderly consumers is particularly severe. The FTC reports that in 2024, individuals over 60 were more than three times as likely as younger adults to report fraud losses involving BTMs, accounting for about 71% of all reported losses at these machines. Similarly, the FBI's analysis of intakes from its Internet Crime Complaint Center from 2023 shows that the overwhelming majority of both BTM complaints and losses were concentrated among the elderly:

USE OF CRYPTOCURRENCY KIOSKS REPORTED IN IC3 COMPLAINTS – 2023

Age Range	Complaints	Losses
Under 20	65	$252,198
20 - 29	416	$3,529,680
30 - 39	451	$8,651,706
40 - 49	391	$9,634,346
50 - 59	476	$11,409,372
Over 60	2,676	$124,332,127

(*2023 IC3 data as reported by the FBI*)

21. This stands in stark contrast to nationwide cryptocurrency usage trends. According to the Federal Deposit Insurance Corporation's ("FDIC") National Survey of Unbanked and Underbanked Households, individuals 65 or older are the *least likely* age cohort to use cryptocurrency:

TABLE 6.1 Use of Crypto by Bank Account Ownership and Selected Household Characteristics, 2023

All Households, Row Percent

Characteristic	Crypto
Age Group	
15 to 24 Years	6.5
25 to 34 Years	9.8
35 to 44 Years	7.1
45 to 54 Years	5.8
55 to 64 Years	2.7
65 Years or More	1.2

(*2023 crypto usage data as reported by the FDIC*)

22. Losses from scams utilizing BTMs far exceed those reported for most other types of fraud, with the median reported loss per scam involving a BTM at $10,000 compared to $447 for fraud more generally. Criminals take advantage of the BTM industry's lack of mandatory transaction holds, minimal fraud screening, and weak internal consumer protections to convince elderly victims to withdraw their entire life savings and deposit the cash into a BTM.

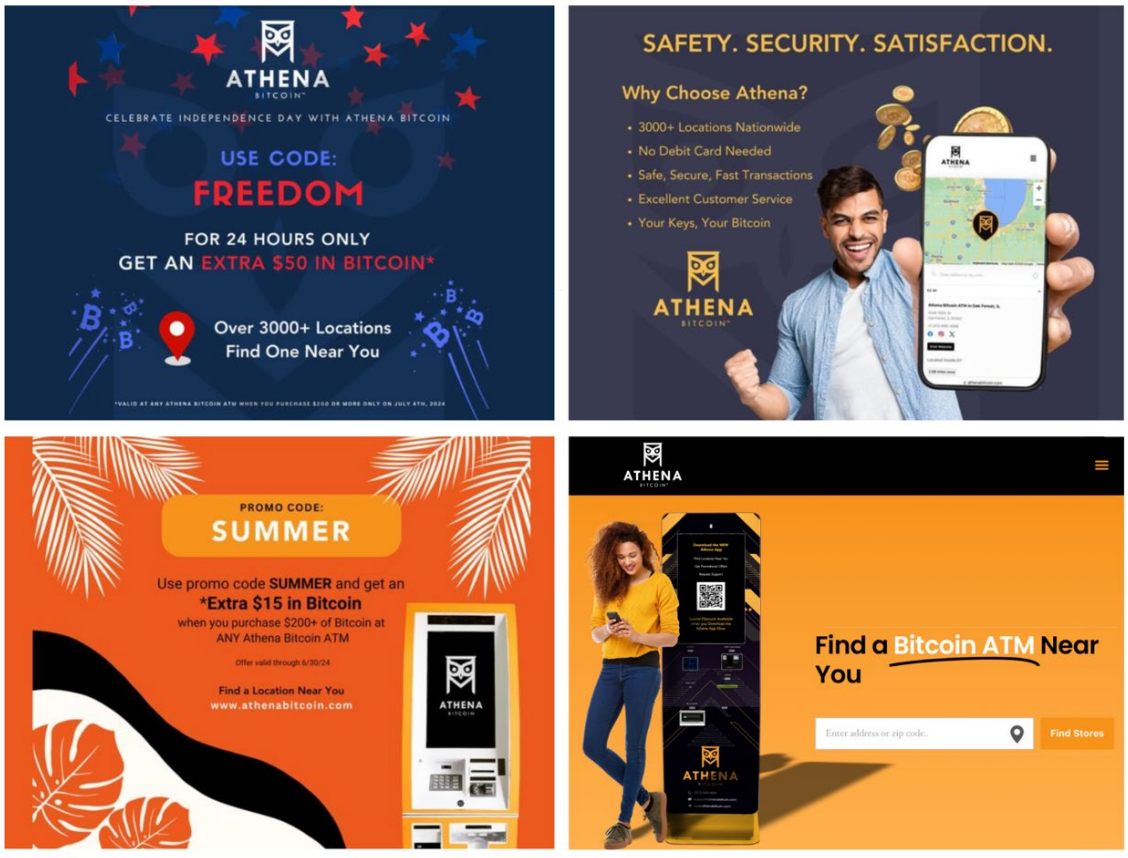
23. Scammers do not select these BTMs randomly. They direct victims to specific operators, favoring those with lax security measures and weak fraud prevention protocols—providing victims precise instructions on where to find BTMs in each city.

24. Athena plays a major part in this expanding crisis—operating 3,500 BTMs worldwide, including having operated seven locations in DC. Transaction records show that Athena's kiosks in the District average $4,592 per transaction—far more cash than most people would be comfortable carrying into a gas station. Athena takes an average of 20% per transaction:

II. Athena's Profits Are Derived from Undisclosed Fees

25. Through apps and exchanges, Bitcoin can be purchased online for fees ranging from 0.24% to 3%. But Athena BTMs charge District consumers exorbitant fees of up to 26%—without ever disclosing those fees to the consumer. Athena's markup is hidden within a fee-inclusive price that Athena misleadingly displays as the "exchange rate."

26. None of Athena's online marketing efforts disclose the fact that Athena charges transaction fees, much less their magnitude. Athena's online advertisements direct consumers to the nearest BTM for "freedom," "security," and "satisfaction." Athena's website, which is available to consumers in the District, makes no mention of the existence of the fee:



(*Sample of Athena's online advertisements*)

27. Athena's fees are also not clearly disclosed at the BTM. Consumers are not told that they will receive significantly less in cryptocurrency than the cash they insert at any point before or during the process and may only learn they have been charged a large fee after the transaction—if at all.

28. Before June 2024, Athena's BTMs made no mention of the steep transaction fees. After June 2024, Athena amended its Terms of Service, which are only presented to consumers in a text box the first time they use a machine. The Terms of Service do not use the word "fee" at all. Instead, the Terms of Service speak of a "Transaction Service Margin," which is buried deep within a 700+ word wall of text that is only accessible by scrolling the BTMs' digital interface. Athena's Terms of Service state that:

> A margin (the difference between the market price and the actual selling or buying price at the kiosk) will be assessed on your purchase or sale of cryptocurrencies in an amount disclosed to you at the time you make the offer to purchase or sell cryptocurrency.

29. The Terms of Service falsely claim that the magnitude of the Transaction Service Margin will be disclosed at the time of purchase when, in fact, Athena never discloses the margin. In order to determine the margin, a user must independently compare the spot price of Bitcoin to the "exchange rate" charged at the machine or compare the Bitcoin received to the amount of cash deposited into the BTM.

30. The Terms of Service present an example of the fee that obfuscates rather than elucidates:

> For example, in the context of a purchase transaction, if you tender a $100 bill and the Transaction Service Margin is $4, the Transaction Service Margin will be assessed and deducted from the $100 and the remaining $96 will be used to calculate the quantity of any cryptocurrencies purchased by you at the quoted price.

31. This hypothetical example confusingly misstates the process as a flat fee taken prior to the purchase at the quoted price rather than a fee hidden within the quoted price. In addition, this example is grossly misleading in the context of a 26% markup.

32. A real-world example provides a more accurate illustration of how the fee functions. On August 21, 2024, a scam victim deposited $10,000 cash into an Athena BTM located inside the Exxon station at 3535 Connecticut Ave NW. The price of Bitcoin at the time of the transaction was $59,936 for one Bitcoin, but Athena marked up the Bitcoin price by 25.4% and charged the victim an "exchange rate" of $80,315 per Bitcoin. So, of the $10,000 cash fed into the BTM, Athena transferred just $7,463 worth of crypto (or 0.1245 of a Bitcoin) to the scammer's wallet identified by the victim. Athena retained the remaining $2,537 as a fee, which was not disclosed to the victim.

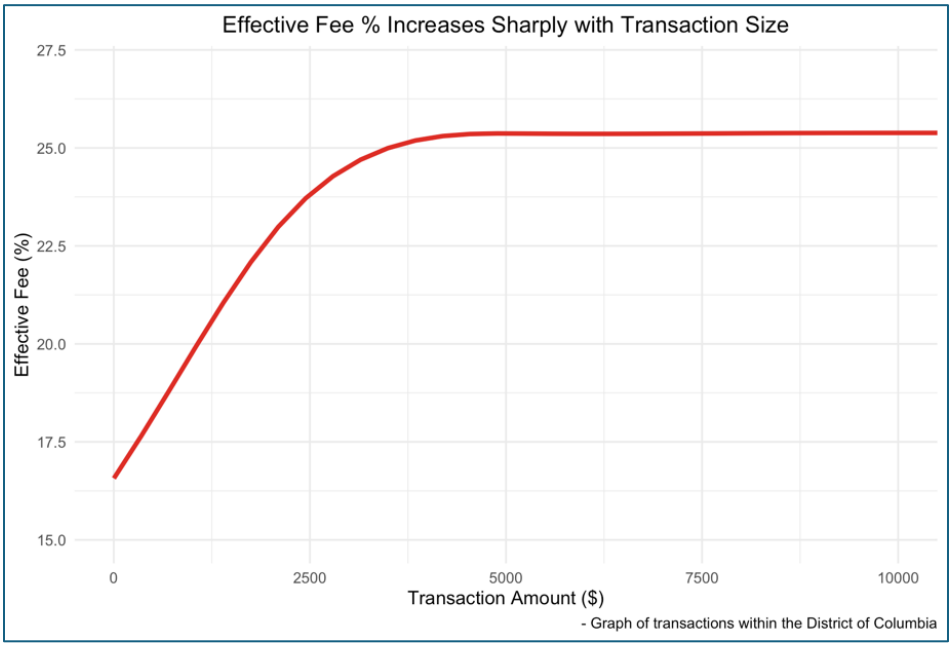
33. In SEC filings, Athena describes the primary source of its revenue much more plainly:

> We charge a fee per crypto asset available through our Athena Bitcoin ATM, equal to the prevailing price at U.S.-based exchanges plus a markup that typically ranges between 13% and 26%. The prices shown to customers on our Bitcoin ATM are inclusive of this price spread...The markup varies by location. It is determined by a proprietary method that is maintained as a trade secret.

Athena does not disclose the breakdown of the markup during the transaction. Instead, Athena hides these fees in the price of the cryptocurrency displayed during the transaction. Athena's fees are excessive, inconsistent, undisclosed, and "maintained as a trade secret" to the detriment of District consumers.

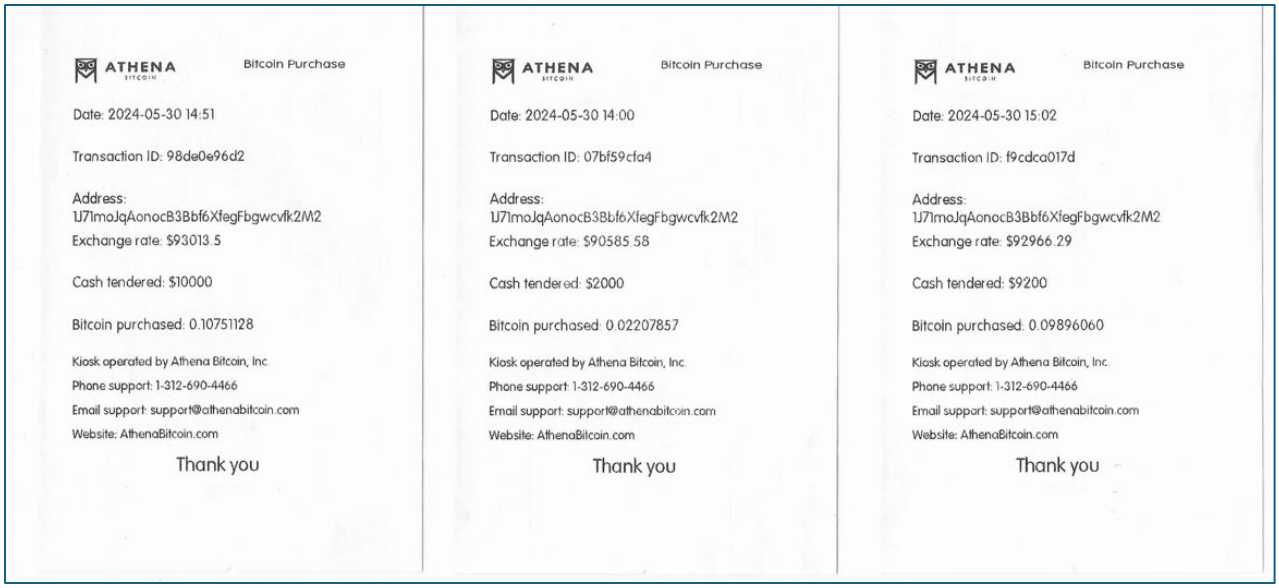
34. Part of the "secret" of Athena's fee method is that the more Bitcoin a user buys, the higher the fee percentage. In the District, small transactions are assessed a fee as low as 13%,

and then steadily increase until maxing out at approximately a 26% fee for the largest transactions.



35. Even after a transaction is complete, Athena still does not disclose the fee to the consumer. After completing a transaction, a consumer receives a receipt from Athena that shows the cash tendered and the Bitcoin received. Athena's BTM receipts do not itemize transaction fees and leave consumers with no clear idea of the exorbitant markup they were charged. The only way for users to determine the amount of the fee is to compare the highly volatile market price of Bitcoin at the exact moment of the transaction with the fee-inclusive "exchange rate" charged by Athena or by examining the amount of Bitcoin that ultimately appears in the user's wallet (which is likely controlled by a scammer).

36. The receipts below show an elderly District resident being charged three different "exchange rates," between $90,585 and $93,013 per Bitcoin, when depositing $21,200 into a scammer's wallet across three transactions over the course of an hour. The actual cost of Bitcoin on the date of these transactions was less than $70,000.



ATHENA BITCOIN — Bitcoin Purchase

Date: 2024-05-30 14:51

Transaction ID: 98de0e96d2

Address: 1J71moJqAonocB3Bbf6XfegFbgwcvfk2M2

Exchange rate: $93013.5

Cash tendered: $10000

Bitcoin purchased: 0.10751128

Kiosk operated by Athena Bitcoin, Inc.
Phone support: 1-312-690-4466
Email support: support@athenabitcoin.com
Website: AthenaBitcoin.com

Thank you

ATHENA BITCOIN — Bitcoin Purchase

Date: 2024-05-30 14:00

Transaction ID: 07bf59cfa4

Address: 1J71moJqAonocB3Bbf6XfegFbgwcvfk2M2

Exchange rate: $90585.58

Cash tendered: $2000

Bitcoin purchased: 0.02207857

Kiosk operated by Athena Bitcoin, Inc.
Phone support: 1-312-690-4466
Email support: support@athenabitcoin.com
Website: AthenaBitcoin.com

Thank you

ATHENA BITCOIN — Bitcoin Purchase

Date: 2024-05-30 15:02

Transaction ID: f9cdca017d

Address: 1J71moJqAonocB3Bbf6XfegFbgwcvfk2M2

Exchange rate: $92966.29

Cash tendered: $9200

Bitcoin purchased: 0.09896060

Kiosk operated by Athena Bitcoin, Inc.
Phone support: 1-312-690-4466
Email support: support@athenabitcoin.com
Website: AthenaBitcoin.com

Thank you

37. Athena's failure to disclose these fees in a clear and transparent manner prevents consumers from making informed financial decisions and results in unsuspecting users paying excessive hidden charges. The company's deceptive pricing structure is particularly harmful to elderly consumers, who are often unfamiliar with cryptocurrency transactions and are unlikely to recognize that they are paying an exorbitant markup.

38. For scam victims, the lack of fee disclosures eliminates a critical opportunity to recognize that their money is, in fact, not being "protected" before completing the transaction. Many victims are tricked into believing they must deposit cash into a BTM to "protect" their money from hackers or fraudsters or other assorted pretextual villains. But if Athena clearly disclosed its 26% fee before the transaction, some victims may consider the potential loss of a quarter of their savings and realize that their money is not being protected before it is too late.

III. Athena's Refund Policy is Misleading and Unfair

39. Athena enforces an opaque refund policy that either denies refunds to scam victims altogether or caps them arbitrarily, even though, at a minimum, Athena could easily return the hidden transaction fees that it charges and retains.

40. Athena's Terms of Service tell a story of zero refunds, except in what Athena suggests are limited circumstances required by state law.

> Your transaction will be final once you have inserted cash into a kiosk... All Transaction Service Margins are fully earned when assessed. Unless required by applicable law, no Transaction Service Margins or any amounts paid for cryptocurrencies will be refunded **for any reason**. In the event that a refund needs to be issued, Athena will refer to the legal requirements established in each state and adhere to its respective refund policies. (emphasis added)

41. In practice, Athena actively avoids issuing refunds to victims who have clearly been defrauded. Athena's logs of complaints from District customers show that Athena customer service representatives misrepresent to caller after caller that no refunds are available and instead point victims to disclaimers, terms and conditions, and law enforcement agencies. As reflected in Athena's contemporaneous logs:

- On June 1, 2024, an Athena representative informed a relative of District elder S.K. that: "Then I confirmed to him that the transaction was already completed and explained why it cannot be reversal or refunded, then I suggested that he should submit a report to the local police or the FBI."

- On July 16, 2024, an Athena representative informed District elder C.S. that: "I told her how this Bitcoin transaction works, and I explained all the terms and conditions of the service, and told her that report the case with the police…"

- On July 25, 2024, an Athena representative informed District elder S.H. that: "I told her how this bitcoins transaction works and explained the terms and conditions and recommended submit a report with the local police or FBI…"

- On August 17, 2024, an Athena representative informed District elder M.H. that: "i confirmed to him that the transaction was already completed and explained why it cannot be reversal or refunded, then i suggested that he should submit a report to the local police or the FBI." [errors original]

42. Athena does not disclose to elderly (and other) fraud victims at any point during or after the transaction, including when they report fraud and request a refund, that Athena retains a significant percentage of a victim's losses as a transaction fee.

43. For example, on July 15, 2024, a 78-year-old District resident was scammed into cashing out $18,500 worth of her retirement savings and feeding it into an Athena BTM. Later that same evening, after discussing the matter with some friends, she realized that she had been scammed. The following day, less than 24 hours after the transaction, the elderly victim called Athena to report the fraud. Athena informed her that the transaction was final and said there was nothing to be done but file a report with the police. Athena did not reveal, and the elderly victim never discovered, that Athena had retained $4,694 of the fraudulent proceeds—funds that Athena could have immediately refunded.

44. Even when Athena provides refunds after consumers repeatedly follow-up and involve law enforcement, Athena arbitrarily caps them. According to Sam Nazzaro, Athena's Chief Compliance Officer and Regulatory Counsel, Athena's "Board of Directors has instituted a limited fee refund policy even though there is no legal or statutory obligation to do so..." and that policy "caps the potential gross profit refunds at $7500" because "gross profit reflected on any purchase does not take into account the various costs with running this business."

45. Under this policy, a District resident who was scammed into feeding $98,000 into an Athena BTM while paying almost $26,000 in undisclosed fees along the way received a capped fee refund of $7,500—just 30% of the fee paid and less than 10% of the total losses.

46. As a condition of receiving the arbitrarily capped fee refund, Athena requires a fraud victim to sign a confidential release, "under penalty of perjury in accordance with 28 USC sec. 1746," that frees the company from "any and all claims, demands, damages, actions, causes

of action or suits of any kind or nature whatsoever." The release requires the victim to agree that they:

> …accepted the Terms of Service and attested to our Pledge of Ownership of the digital wallet... However, it is now alleged, after presenting a complaint to a law enforcement agency, that the acceptance to the Terms of Service and the Pledge of Ownership were made in apparent deceit from a third party despite the warnings provided by the kiosk.

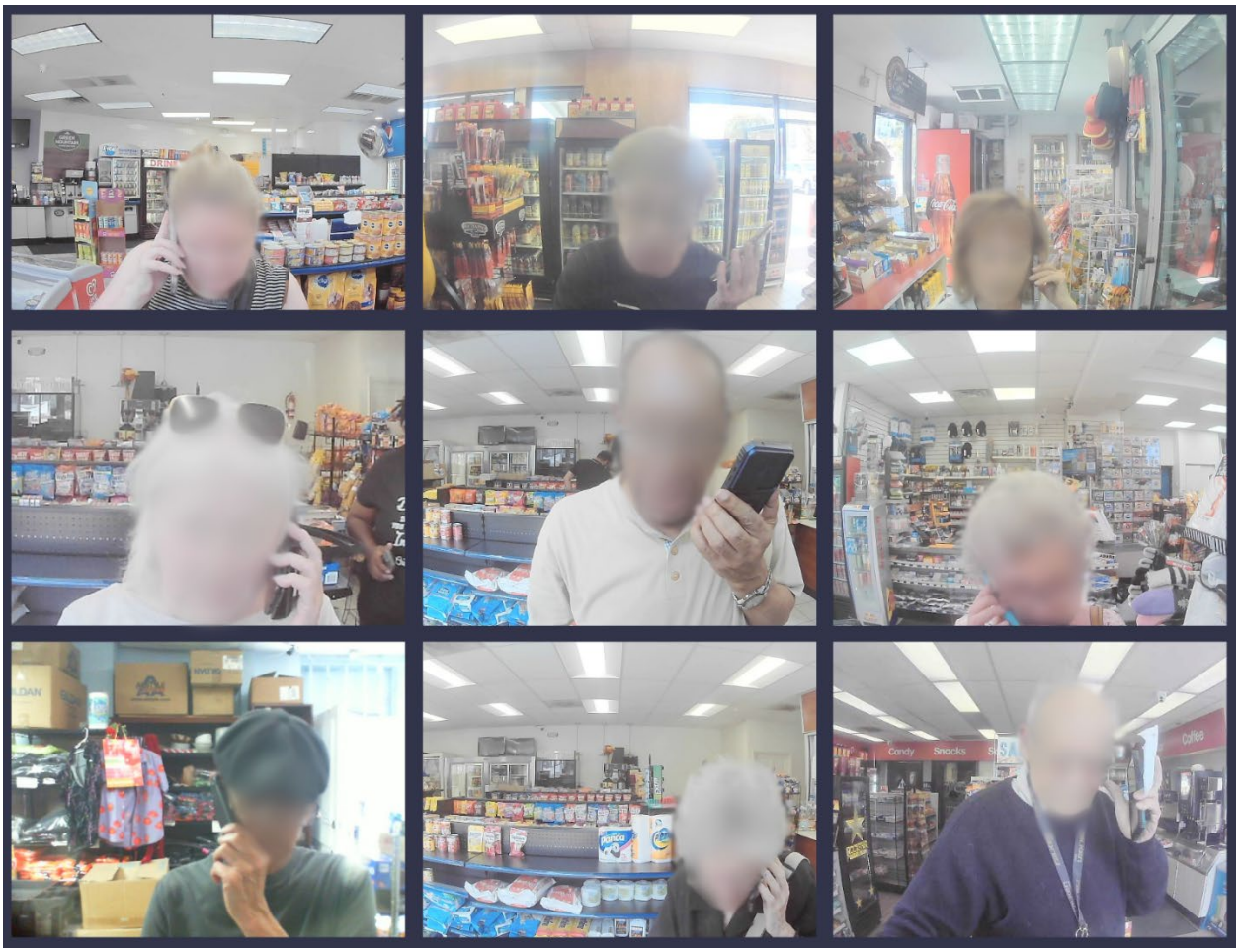
47. The release attempts to free Athena of all future liability while requiring the victim to blame themselves "under penalty of perjury" for not sufficiently heeding the onscreen warnings.

IV. Athena Knows Its Fraud Warnings Are Ineffective

48. Athena's BTMs contain warning screens featuring stock photos of people receiving bad news over the phone. The warnings specifically allude to tech support, bank, and government imposter scams, and offer a hollow directive: "REACT BEFORE YOU TRANSACT."

49. The warnings make clear that Athena knows its BTMs are used in scams where victims are directed to a BTM by someone else, tricked into "protecting" their money from a supposed account compromise, threatened with fake arrest, or convinced that they are assisting with an important government investigation.

50. But scammers don't let victims think about warnings. As depicted in the photos below, they keep victims *on the phone* and off balance throughout the entire scam—talking victims through the visit to their bank, the trip to the BTM, clicking through its many screens, and that terrifying moment when a lifetime's worth of cash is inserted one bill at a time.



(*Athena security camera photos of District scam victims*)

51. Scammers tell victims to do as they're told and not talk to anyone until the deposit is complete. Scammers explicitly warn victims not to read the on-screen warnings or tell them that the warnings don't apply to their situation.

52. The rapid prompts, wordy warnings, and long, complicated legal disclaimers that Athena uses at its BTMs exacerbate the confusion and pressure that scammers create for their victims.

53. Athena knows that its scam warnings are ineffective because most of the money deposited into Athena's District BTMs—and 93% of dollars deposited in the first five months of Athena's operation in the District—comes from people who are the victims of just these sorts of scams.

54. Athena is aware its BTMs are commonly used for scams because victims frequently self-report the scams to Athena. Victims repeatedly describe the same pattern in their complaints to Athena:

- "someone who pretended to be from Wells Fargo"
- "the scammer impersonated a bank and made me deposit USD 98,120"
- "someone was pretending to be an agent from the Bank of America and said to her bank account was hacked"
- the scammer said "she was accused in Texas for 3 different counts related to drugs trafficking, money laundering and identity theft"
- "someone who pretended to be from [a] software company that provide antivirus software contacted him"
- "someone was impersonating US Government and said to him that he needed to protect his money"
- "she said that someone who pretended to be from Chase Bank and Apple contacted her"

- "she said that an inspector officer from the US Marshall told her that she was related with drug traffic" [errors original]

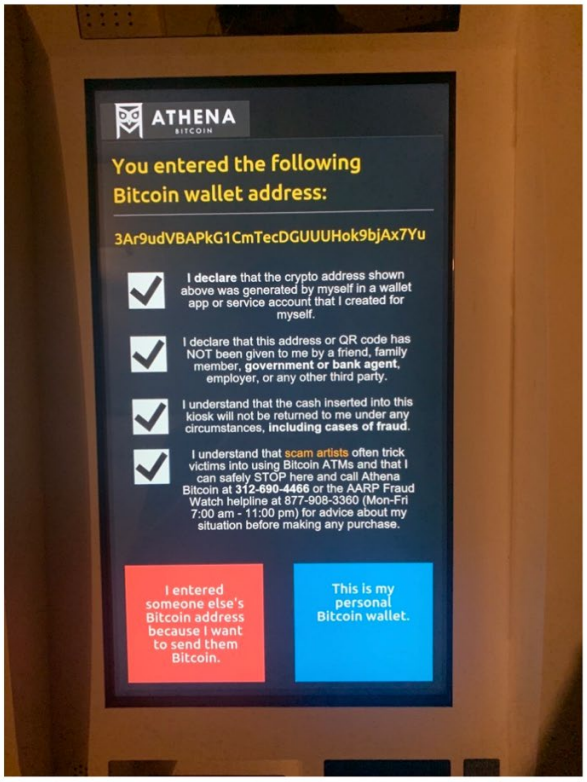
55. Despite clear data showing that its warnings do nothing to stop the imposter scams driving most of its revenue, Athena has continued operating unchanged—attempting to insulate itself behind ineffectual warnings and allowing its network of machines to grow into a pipeline for large-scale elder financial exploitation.

56. There are obvious measures Athena knows it could take to protect users from scams. For instance, Athena could adopt reasonable transaction limits to prevent users—especially first-time users—from being duped into giving away substantial savings all at once. Recognizing the dangers of unregulated BTMs, certain jurisdictions, including the State of California, where Athena operates, have enacted such protections. *See* Cal. Fin. Code §§ 3902, 3905 (imposing fee disclosure requirements and a $1,000 daily transaction limit). However, Athena has failed to implement any such protections on a national level and continued to operate in the District in a manner that exposed consumers to predictable and preventable financial harm.

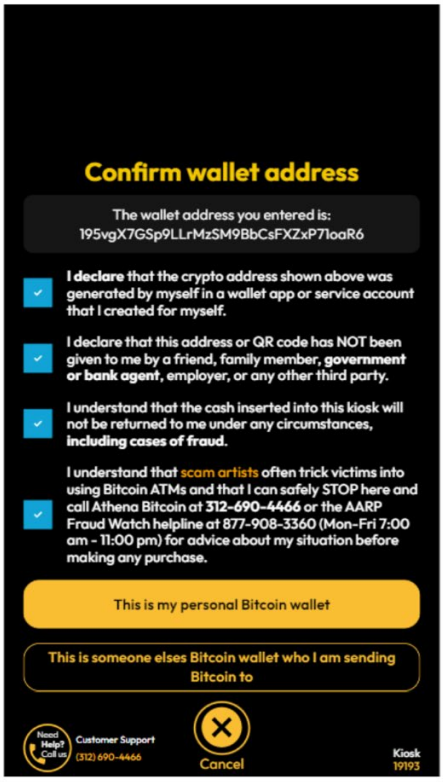
57. For example, on July 10, 2024, a 75-year-old District resident lost $27,600 in a single BTM transaction; on July 15, 2024, a 79-year-old District resident lost $18,500 in a single BTM transaction; and on August 30, 2024, a 73-year-old District resident lost $24,500 in a single BTM transaction. Athena could have—and should have—prevented each of these scams. Instead, the company allowed the transactions to proceed and pocketed a combined total of $17,913 in undisclosed fees on the backs of three District elders who lost more than $70,000 combined.

V. Athena Requires Users to Complete Wallet Attestations That It Knows Are Ineffective and Processes Clearly Fraudulent Transactions That Are Linked to a Single Scam Wallet

58. Like its ineffectual "warning" screens, Athena further attempts to shield itself from liability by requiring its BTM users to tick a series of boxes confirming that the Bitcoin wallet address was "generated by myself"—a process that the company terms a "Pledge of Ownership" after a transaction is completed.



(*Athena wallet confirmation before June 2024*)



(*After June 2024*)

59. The on-screen prompts (shown above) instruct a user to tick boxes stating, "I declare that the crypto address shown above was generated by myself" and that the address or QR Code was not "given to me by a friend, family member, government or bank agent, employer, or any other third party." The user completes the screen by clicking a button that states "This is my personal Bitcoin wallet."

60. But elderly scam victims standing terror-stricken in gas stations, pockets stuffed with uncomfortable amounts of cash, do not understand what it means to "generate" a cryptocurrency wallet or have their own "personal Bitcoin wallet." In reality, scam victims are provided a QR code by the scammer that they use to identify the (scammer's) wallet that should receive the Bitcoin deposit. Scam victims are unlikely to be familiar with the technical details of Bitcoin wallet creation and generation, are unaware that they don't own or control that wallet, and are unaware that they are, in fact, transferring money directly to the scammer.

61. Given this Pledge of Ownership, Athena knows or should know when a wallet has been claimed by a consumer; however, Athena processed transactions when a user requested money be deposited into a Bitcoin wallet that has already been used by someone else. Athena could have prevented many of the scams by implementing an obvious fraud prevention measure: it could have declined to process these transactions. In these instances, Athena knew for a fact that the wallet was not "generated" by the person depositing the funds and that the wallet is not that individual's "personal Bitcoin wallet." But Athena failed to implement these protections, enabling it to continue to collect thousands of dollars in transaction fees on the back of fraud victims.

62. An example is illustrative: For the five days starting May 28, 2024, across 56 different transactions, scammers manipulated multiple victims into depositing an aggregate of $297,143 into a single Bitcoin wallet the scammers controlled. More than 20 of the transactions originated through Athena BTMs, helping the fraudsters direct $184,871 of the total losses into that wallet. Two of the victims were elderly District residents, who Athena permitted to deposit huge sums of cash into the *same* wallet.

63. By June 1, 2024, the wallet had been completely emptied through KuCoin—a Seychelles-based crypto exchange that recently agreed to exit the U.S. market after pleading guilty

in the Southern District of New York to charges related to violating U.S. anti-money laundering laws.

64. This was not an isolated incident. On August 14, 2024, scammers convinced a 74-year-old District resident that her money was at risk due to a malicious hack on her bank accounts. At the scammers' direction, she brought $6,000 cash to an Athena BTM inside the Exxon at 420 Rhode Island Ave NW (pictured below) to deposit her cash into a crypto wallet using a QR code as instructed. But the wallet belonged to the scammers, and after Athena took its 25% cut of the scam, $4,446 worth of Bitcoin was transferred directly into the scammers' wallet.

(*ExxonMobil station at 420 Rhode Island*)

65. In the five days leading up to this fraudulent transaction, Athena had already transferred more than $90,000, across at least seven different transactions, into the same scam wallet. Multiple victims had already clicked through Athena's Pledge of Ownership screen and confusedly claimed to own that same wallet. Despite having knowledge that the elderly District resident could not actually own this wallet that had been previously claimed by other victims, Athena processed and profited from her transaction. By September 11, 2024, the scam wallet had been completely emptied, and all the money was gone.

66. Athena continued to process transactions even after multiple victims have pledged ownership of the very same wallet—ignoring an obvious indicator of fraud.

67. Athena has forced victims to pledge wallet ownership to protect itself—to deflect from the fact that it does not know, or care, who owns the wallets, or where the money is going, as long as they get to keep their undisclosed cut.

CAUSES OF ACTION

COUNT ONE
Deceptive Trade Practices in Violation of the Consumer Protection Procedures Act, D.C. Code § 28-3901 *et seq.*

68. The District re-alleges the foregoing paragraphs of this Complaint as if fully set forth herein.

69. The CPPA is a remedial statute that is to be broadly construed. It establishes an enforceable right to truthful information from merchants regarding consumer goods and services that are or would be purchased, leased, or received in the District of Columbia.

70. Athena's cryptocurrency transaction services through its BTMs are for personal, household, or family purposes and, therefore, are consumer goods and services.

71. Athena, in the ordinary course of business, offers to sell or supply, either directly or indirectly, consumer goods and services and is therefore a merchant as defined by the CPPA.

72. Users of Athena machines purchase consumer goods and services from Athena through its BTMs and are therefore consumers as defined by the CPPA.

73. The deceptive trade practices that the CPPA prohibits in connection with the sale of consumer goods and services include:

a. Representing that goods or services have a source, sponsorship, approval, certification, accessories, characteristics, ingredients, uses, benefits, or quantities that they do not have, D.C. Code § 28-3904(a);

b. Misrepresenting as to a material fact which has a tendency to mislead, D.C. Code § 28-3904(e); and

c. Failing to state a material fact if such failure tends to mislead, D.C. Code § 28-3904(f).

74. Athena has violated the CPPA, including one or more of the foregoing CPPA provisions, by:

a. Failing to disclose its excessive transaction fees before consumers insert cash. Consumers are not informed that they will be charged a fee of up to 26%, nor are they provided with a clear explanation of how the fee is calculated. Instead, Athena buries the fee within a misleading "exchange rate," which prevents consumers from understanding the true cost of their transaction.

b. Misleading scam victims who call to report fraud by failing to disclose that the company has retained a significant portion of their losses as a transaction fee. Instead of informing victims that Athena collected up to 26% of the transaction in fees, Athena implies or directly states that nothing can be refunded because cryptocurrency transactions are irreversible. This misleading representation creates the false impression that Athena has no ability to provide restitution, when in reality it has retained a substantial portion of the victim's money.

c. Failing to disclose to consumers when they are depositing funds into a wallet that has already been associated with one or more previous transactions with other consumers. Transaction records show that Athena allows multiple consumers to pledge ownership of the same wallet and send repeated payments to fraudsters using that wallet. Athena does not warn consumers when a wallet has already been associated with another transaction.

d. Impliedly representing to consumers that it has a money transmission license to operate in the District when in fact it does not. District consumers insert money into Athena BTMs for transmission, and Athena transmits money on their behalf. Athena is thus a money transmitter and is required to possess a money transmission license under D.C. Code § 26-1002. It does not have one. Nevertheless, by doing business in the District, it implicitly holds itself out to consumers as having one.

75. Each of these deceptive acts or practices constitutes a separate violation of the CPPA.

COUNT TWO
Unfair Trade Practices in Violation of the
Consumer Protection Procedures Act, D.C. Code § 28-3901 *et seq.*

76. The District re-alleges the foregoing paragraphs of this Complaint as if fully set forth herein.

77. The CPPA requires merchants to treat consumers fairly in connection with the sale, lease, or transfer of consumer goods and services.

78. Athena has violated the CPPA by engaging in the unfair acts and practices alleged herein. Those unfair acts or practices cause District consumers substantial injury that those consumers cannot reasonably avoid and that is not outweighed by countervailing benefits to those consumers or to competition.

79. Athena engages in an unfair trade practice, prohibited by D.C. Code § 28-3904, by including in its Terms of Service and enforcing an unconscionable provision that states no refunds will be given under any circumstances, even when a consumer is the victim of fraud. This provision unfairly shifts all risk to the consumer while shielding Athena from accountability, despite the company's ability to refund its excessive transaction fees.

80. Athena engages in an unfair trade practice, prohibited by D.C. Code § 28-3904, by systematically preventing scam victims from recovering their stolen funds. When fraud victims contact Athena shortly after a scam transaction, the company refuses to refund any portion of the transaction, instead directing victims to law enforcement while retaining a substantial portion of the stolen funds as fees.

81. Athena engages in an unfair trade practice, prohibited by D.C. Code § 28-3904, by arbitrarily capping any refunds it provides at $7,500. This arbitrary cap on fee refunds is unfair because it prevents District consumers from fully recovering funds lost to Athena's undisclosed fee collection process.

82. Athena engages in an unfair trade practice, prohibited by D.C. Code § 28-3904, by failing to implement adequate fraud prevention measures to protect consumers from scams. Despite knowing that its BTMs are routinely used in fraud schemes and that its warnings are ineffective, Athena does not take reasonable steps to prevent financial exploitation. It fails to

implement effective consumer warnings and permits large cash deposits from elderly consumers without intervention.

83. Athena has engaged in unlawful and unfair trade practices affecting District consumers, in violation of D.C. Code § 28-3904, by engaging in trade practices that violate the District's money transmitter laws, including by operating without the money transmitter license required by D.C. Code § 26-1002.

84. The substantial injury that Athena's BTMs inflict on consumers from its unfair acts and practices includes significant loss of funds through both scams and Athena's undisclosed fees.

85. As a direct result of the unfair practices described above, Athena obtained income, profits, and other benefits that it would not otherwise have obtained.

86. Athena continues to cash in on undisclosed BTM fees despite knowing the harm its BTMs cause to the District and District residents.

87. Each instance in which Athena engaged in an unfair act or practice as alleged in this Count constitutes a separate violation of the CPPA.

88. Athena's violations present a continuing harm, and the unlawful acts and practices complained of here affect the public interest.

COUNT THREE
Violations of the Abuse, Neglect, and Financial Exploitation of Vulnerable Adults and the Elderly Act, D.C. Code § 22-931 *et seq*.

89. The District re-alleges the foregoing paragraphs of this Complaint as if fully set forth herein.

90. The Financial Exploitation Act, D.C. Code § 22-933.01, prohibits the financial exploitation of vulnerable adults and the elderly, including "[using] deception . . . to obtain the property, including money, of a vulnerable adult or elderly person, with the intent to deprive the

vulnerable adult or elderly person of the property or use it for the advantage of anyone other than the vulnerable adult or elderly person."

91. Athena violates D.C. Code § 22-933.01 by systematically withholding material information about its exorbitant transaction fees, preventing consumers—especially elderly users unfamiliar with cryptocurrency—from understanding how much money they are losing in each transaction. By failing to disclose its fees clearly and instead embedding them in a misleading exchange rate, Athena deceives elders into overpaying, extracting substantial sums from individuals who are already being defrauded.

92. Athena also violates D.C. Code § 22-933.01 by knowingly benefiting from fraudulent transactions in which scammers coerce elderly consumers into depositing their money into Athena's BTMs. Athena receives numerous complaints from scam victims and is aware of the prevalence of scam victims utilizing its machines based on its ineffective warnings. In addition, Athena routinely allows consumers to deposit money into wallets previously used by a different Athena consumer, which increases the likelihood of scams. Despite these flags, Athena continues processing these transactions and retaining the fees generated from them.

93. Athena also violates D.C. Code § 22-933.01 by falsely claiming that nothing can be refunded because "cryptocurrency transactions are final" when elderly scam victims contact the company to report fraud. In reality, Athena retains a substantial portion of scam victims' funds in the form of excessive fees but either refuses to return these funds or sets an arbitrary cap on any refund.

94. Through its actions, Athena intentionally and knowingly has obtained the money or property of elderly and vulnerable adults by deception with the intent to use the funds for the

benefit of someone other than those vulnerable and elderly adults (i.e., Athena), in violation of D.C. Code § 22-933.01(a)(1).

PRAYER FOR RELIEF

WHEREFORE, Plaintiff the District of Columbia respectfully requests that the Court:

a. Declare that Athena's conduct violates the CPPA and Financial Exploitation Act, as described herein.

b. Permanently enjoin Athena, pursuant to D.C. Code § 28-3909(a), from violating the CPPA, including requiring the company to:

   i. Remove unconscionable contract terms, including its no-refunds policy, its cap on refunds, and its liability limitation clauses;

   ii. Fully disclose all transaction fees, including the actual percentage markup above the market rate, at the point of sale before consumers insert cash;

   iii. Institute and implement adequate fraud prevention measures, including appropriate daily and monthly transaction limits and effective fraud detection protocols.

c. Permanently enjoin Athena, pursuant to D.C. Code § 22-937(a)(1), from violating the Financial Exploitation Act;

d. Enjoin Athena from engaging in money transmissions in the District of Columbia until Athena has the licenses required by D.C. Code § 26-1002(a);

e. Order Athena to pay damages and restitution pursuant to D.C. Code §§ 28-3909(a), 28-3909(b)(3), and 22-937(a)(2), for the entire transaction amounts it collected in connection with fraudulent transactions conducted within the District of Columbia in violation of the CPPA and Financial Exploitation Act, in an amount to be proven at trial;

f. Order Athena to pay damages and restitution, pursuant to D.C. Code §§ 28-3909(a), 28-3909(b)(3) and 22-937(a)(2), for all undisclosed fees it collected within the District of Columbia in violation of the CPPA and Financial Exploitation Act, in an amount to be proven at trial;

g. Award civil penalties of $10,000 for each violation of the Financial Exploitation Act pursuant to D.C. Code § 22-937(a)(5), in a total amount to be proven at trial;

h. Award civil penalties of $5,000 for each violation of the CPPA pursuant to D.C. Code § 28-3909(b), in a total amount to be proven at trial;

i. Award the District the costs of this action and reasonable attorneys' fees pursuant to D.C. Code §§ 28-3909(b)(4) and 22-937(a)(3); and

j. Grant such further relief as the Court deems just and proper.

JURY DEMAND

The District of Columbia hereby demands a trial by jury.

Date: September 8, 2025

Respectfully submitted,

BRIAN L. SCHWALB
Attorney General for the District of Columbia

COTY MONTAG
Deputy Attorney General
Public Advocacy Division

WILLIAM F. STEPHENS
BETH MELLEN
Assistant Deputy Attorneys General
Public Advocacy Division

/s/ Alicia M. Lendon
ALICIA M. LENDON [1765057]
Chief, Civil Rights & Elder Justice Section
Public Advocacy Division

/s/ Anabel M. Butler
ANABEL M. BUTLER [90006593]
JASON JONES [90003354]
Assistant Attorneys General
400 6th Street, NW, Suite 10100
Washington, DC 20001
(202) 841-6061
anabel.butler@dc.gov

Attorneys for the District of Columbia

IN THE IOWA DISTRICT COURT FOR POLK COUNTY

STATE OF IOWA, *ex rel.* BRENNA BIRD, ATTORNEY GENERAL OF IOWA, Plaintiff, v. **LUX VENDING, LLC (d/b/a Bitcoin Depot, Inc.); BITCOIN DEPOT OPERATING, LLC (d/b/a Bitcoin Depot),** Defendants.	Equity No. _____ **PETITION**

Table of Contents

The Appendix filed as an attachment to this complaint is incorporated here by reference.

"It's definitely interesting how we are selling a digital product. But the thing is when you can actually touch this machine, and know there is a real company behind it, versus just a random website that can vanish at any time- It gives you the sense of trust and credibility that this company is legitimate" -Interview with Brandon Mintz, CEO of Bitcoin Depot (available at https://www.youtube.com/watch?v=M7VvbM04qnM.)

Introduction

1. Fraudsters and scammers update their deceptive practices to reflect new technology. Here, Defendants are misusing the popular excitement around technologies like Bitcoin and other cryptocurrencies to unfairly and deceptively put Iowa consumers in harm's way and take their piece of Iowans hard-earned money before sending the rest to scammers.

2. Cryptocurrencies are technologies often centered around recording transactions on a public register, or blockchain. The details of that technology can be complicated and nuanced. But what is not nuanced is using a veneer of association with cryptocurrencies to defraud consumers.

3. Defendants Lux Vending, LLC, and Bitcoin Depot Operating, LLC (collectively, "Bitcoin Depot") profit when scammers profit because of the unfair and unsafe business practices easily allowing Iowans to send their money to scammers—with a kickback to Bitcoin Depot. So far, Iowa has identified more than $7 million in fraudulent, scam payments processed through Bitcoin Depot.

4. A cryptocurrency kiosk is a physical kiosk or automated machine that allows consumers to insert physical cash to buy purely digital or virtual cryptocurrencies. Bitcoin Depot runs a type of cryptocurrency kiosk that it refers to as a Bitcoin ATM, or BTM. Bitcoin Depot's BTMs—at issue in this Petition—allow consumers to buy Bitcoin—a specific cryptocurrency. BTMs allow a consumer to insert cash into the machine, convert that

cash into Bitcoin, and then send that Bitcoin to a "Bitcoin address" associated with a "digital wallet"—all for a fee(s).

5. A Bitcoin address can be thought of as an account holding all Bitcoin sent to it. Each Bitcoin address is (i) a string of letters and numbers and (ii) associated with a digital wallet. The owner of the digital wallet is the owner of each Bitcoin address associated with that wallet.

6. Although Bitcoin Depot states that it requires consumers to send Bitcoin they buy through a BTM to a Bitcoin address owned by the consumer, Bitcoin Depot regularly allows purchased Bitcoin to be sent to Bitcoin addresses owned by third parties.

7. Bitcoin Depot's CEO Brandon Mintz said, "[c]ompared to many other crypto companies, we have delivered consistent year-over-year financial growth and profitability in an industry where that can be quite difficult to find." That is because Bitcoin Depot does not profit from investing in Bitcoin as a valued digital asset.

8. Instead, Bitcoin Depot profits from the fees it charges to buy Bitcoin and send it to someone else. Bitcoin Depot gets paid when a scammer tricks an Iowan into using a BTM to send Bitcoin. Some scams that brutally victimize Iowans and send them to a BTM are: (i) romance scams-- sending Bitcoin to a fake love interest met online, (ii) law enforcement scams—sending Bitcoin to a fake sheriff or U.S. Marshal to avoid criminal charges or arrest, (iii) refund scams—sending Bitcoin to return the fake overpayment of a refund from a large company, or (iv) tech-virus scams—sending Bitcoin to save the consumer's laptop from a fake virus.

9. Scam calls and text messages targeting Iowans (and all Americans), particularly the elderly, are on the rise. BTMs are one of the key tools used to scam Iowa consumers. And each successful scam using a BTM is revenue for Bitcoin Depot.

10. Bitcoin Depot is the largest cryptocurrency kiosk selling Bitcoin in North America. It has placed its BTMs at around 100 Iowa locations. Its machines can be found in small gas stations, large chain gas stations, convenience stores, and even grocery stores.

11. Bitcoin Depot knows scammers frequently send fraud victims to its BTMs, but it fails to take meaningful action to protect Iowa consumers. That is because it is not in Bitcoin Depot's economic interest to take meaningful actions to decrease fraudulent transactions. While Bitcoin Depot reaps profits from Iowa consumers who are the victims of fraud, Iowa consumers are embarrassed and even worse, face financial hardship, bankruptcy, social isolation, stress, or depression after being scammed into using BTMs. Consumers overwhelmingly fail to receive any consumer or competitive benefit from BTMs. Bitcoin Depot profits from every scam transaction completed—whether it denies a consumer a refund, a scam is completed and the embarrassed consumer does not even seek a refund, or the money associated with the transaction is not seized by law enforcement.

12. Bitcoin Depot's business model is so co-dependent on the success of scammers that there is likely no way to operate a profitable BTM in Iowa that is not an unlawful act under Iowa's Consumer Fraud Act. Bitcoin Depot even announced a 25% reduction in its revenue for the third quarter of 2024 as compared to the third quarter of 2023 because of "unfavorable legislation that was passed in California." That unfavorable legislation limited how much scammers and Bitcoin Depot could collectively extract from California consumers to $1,000 per day.

13. Offering Iowans an unsafe money transfer service through a physical machine located in a gas station or vape shop to buy purely digital assets at unclear exchange rates and for high fees is not innovative or beneficial to consumers. Instead, it is an unlawful, "unfair practice" under the Act: "an act or practice which causes substantial, unavoidable injury to consumers that is not outweighed by any consumer or competitive benefits which the practice produces."

14. The Attorney General's Office has found that scam transactions processed through Iowa BTMs between October 10, 2021, and July 26, 2024, totaled at least $7,243,991.

15. Bitcoin Depot profited from those scam transactions. Bitcoin Depot's policies for use of its BTMs do not adequately protect Iowa consumers or prevent scam transactions. Bitcoin Depot also fails to follow its own inadequate policies. The existing policies; lack of their enforcement; and lack of additional, needed safeguards create an environment

where the "substantial unavoidable injury to consumers" far outweighs any "consumer or competitive benefits" that BTMs offer (if any). Iowa Code § 714.16(2)(a).

16. Bitcoin Depot's business model also employs deceptive practices in its Bitcoin pricing. The cost to purchase Bitcoin at a BTM is often much higher than the cost to purchase on a cryptocurrency exchange, and Bitcoin Depot does not want consumers to know the true cost. Bitcoin Depot hides the cost to BTM consumers in a way that has a "tendency or capacity to mislead a substantial number of consumers as to a material fact or facts." Bitcoin Depot's nominal fee of $3.00 is clear, but an additional cost known as a "spread" increases the total fee to Iowa consumers to an additional amount up to 23% of the total transaction amount.

17. Bitcoin Depot harms Iowa consumers by deceptively designing its refund policy and misrepresenting the policy such that no consumer would know of or access it. Bitcoin Depot talks out of both sides of its mouth as it tells consumers there is no ability for a refund when they've been scammed while telling regulators concerned with fraud that it does have a refund policy in instances of fraud. Since 2021, hundreds of Iowans complained to Bitcoin Depot about using its BTMs due to being victims of scams. Bitcoin Depot largely denied these consumers relief and kept its share of the fraudulent proceeds.

18. At best, Bitcoin Depot is a willfully blind participant in the victimization of hundreds of Iowans. At worst, it is a silent partner to many scammers' preying on Iowans, taking a cut of each scam with its excessive and deceptive BTM fees that are further paired with a lack of refunds.

19. The State seeks a preliminary and permanent injunction under the Act to (i) enjoin Defendants from engaging in the deceptive and unfair acts described in this Petition whether that be by (a) a permanent ban from doing business in Iowa or (b) placing additional safeguards and scam prevention requirements on the operation of BTMs in; and (ii) impose all other injunctive relief the Court finds equitable.

20. The State also seeks civil penalties, reimbursement, disgorgement, and other costs and fees permitted by the Act given Bitcoin Depot's deceptive and unfair conduct, which has harmed and continues to harm Iowa consumers.

I. Jurisdiction

21. This Court has jurisdiction over this matter under Iowa Code § 714.16(7).

22. This Court has jurisdiction over the Defendants under Iowa Code § 714.16 because they have transacted business within the state of Iowa at all times relevant to this complaint.

23. Polk County is the proper venue under Iowa Code § 714.16(10) because Defendants transact business in Polk County through numerous physical BTM locations in Polk County. Also, transactions that serve as the factual basis for this action occurred in and some victims reside in Polk County.

II. Parties

24. Plaintiff is the State of Iowa, *ex rel*. Brenna Bird, Attorney General of Iowa. Under Iowa Code § 714.16(7), the Attorney General may seek civil enforcement of the Iowa Consumer Fraud Act.

25. Defendant Lux Vending, LLC (d/b/a Bitcoin Depot, Inc.) is a for-profit entity incorporated in Delaware. It is headquartered in Georgia with its executive offices located at 3343 Peachtree Road NE, Suite 750, Atlanta, GA 30326. Lux Vending, LLC is registered with the Iowa Secretary of State to do business in the State of Iowa under business number 648043. The company lists its registered agent as "CORPORATION SERVICE COMPANY" located at 505 5th Avenue, Suite 729, Des Moines, IA 50309.

26. Bitcoin Depot, Inc. is a publicly traded company on the National Association of Securities Dealers Automated Quotations (NASDAQ) stock market, an American stock exchange based in New York City.

27. Defendant Bitcoin Depot Operating, LLC, is a foreign limited liability company registered to do business in the State of Iowa. According to public filings by Bitcoin Depot, Inc., Bitcoin Depot Operating, LLC, is a wholly owned subsidiary of BT HoldCo, LLC, of which Bitcoin Depot, Inc. is the sole managing member. Bitcoin Depot

Operating, LLC is registered with the Iowa Secretary of State to do business in the State of Iowa under business number 648043. The company lists its registered agent as "CORPORATION SERVICE COMPANY" located at 505 5th Avenue, Suite 729 Des Moines, IA 50309.

28. At all relevant times, Bitcoin Depot transacted business in Iowa by marketing, promoting, advertising, and offering for sale its services/products, including the sale of Bitcoin to Iowa consumers at Iowa locations.

III. Factual Allegations

29. Bitcoin Depot claims to be the largest cryptocurrency kiosk network selling Bitcoin in North America. As of November 2024, Bitcoin Depot purports to operate a network of more than 8,400 BTMs across the U.S., Canada, and Puerto Rico. From October 10, 2021, to July 26, 2024, the company operated approximately 118 BTMs in Iowa.

30. Bitcoin Depot uses retail partnership contracts to place its BTMs in national, regional, and independently owned convenience stores, grocery stores, liquor stores, and gas stations.

31. The company reported total annual revenue of $688.97 million for 2023. Bitcoin Depot reports it has conducted at least $2.4 billion in transactions since its inception, including at least [redacted] in Iowa between October 10, 2021 and July 26, 2024.

32. The Attorney General's office has spoken to 34 of the top 50 Bitcoin Depot users in Iowa between October 10, 2021, and July 26, 2024, based on total transaction(s) size. All 34 confirmed they used Bitcoin Depot's machines because of a scam. These individuals alone collectively represent over $2.4 million in BTM transactions in Iowa.

33. The Attorney General's office reasonably believes that amount will only grow as more consumers are contacted.

34. Also, based on an analysis of data provided from Bitcoin Depot and other data related to Bitcoin addresses and digital wallets, the Attorney General's office has reason to believe that more than half of all money taken in by Bitcoin Depot in Iowa between October 10, 2021, and July 26, 2024, are transactions completed because of a scam.

A. BTMs and Scams Go Hand-in-Hand

35. Cryptocurrency surged as a payment method for scams in recent years because it is portable and difficult to trace.

36. Widespread access to cryptocurrency kiosks including BTMs helps make this possible. Reported losses using cryptocurrency kiosks are overwhelmingly related to government impersonation, business impersonation, and tech-support scams. Fed. Trade Comm'n, *New FTC Data Shows Massive Increase in Losses from Bitcoin ATM Scams* (Sept. 2024), https://www.ftc.gov/news-events/news/press-releases/2024/09/new-ftc-data-shows-massive-increase-losses-bitcoin-atm-scams.

37. Since most fraud is not reported, these numbers likely represent only a fraction of the actual harm. One study showed only 4.8% of people who experienced mass-market consumer fraud complained to the Better Business Bureau or a government entity. *See* Keith B. Anderson, *To Whom Do Victims of Mass-Market Consumer Fraud Complain?*, at 1 (May 2021), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3852323.

38. The Federal Trade Commission estimates that fraud losses at cryptocurrency kiosks have skyrocketed, increasing nearly tenfold from $12 million in 2020 to $114 million in 2023 and topping $65 million in the first half of 2024.

39. In the first six months of 2024, the median reported loss was $10,000 when using cryptocurrency kiosks, $5,400 when cryptocurrency was the reported payment method (including reports with and without using cryptocurrency kiosks), and $447 in general fraud cases. FTC data shows that older adults are less likely to report fraud than younger adults and have even higher individual median dollar losses. Fed. Trade Comm'n, *Protecting Older Consumers 2023-2024: A Report of the Federal Trade Commission*, at 17 (Oct. 18, 2024), https://www.ftc.gov/system/files/ftc_gov/pdf/federal-trade-commission-protecting-older-adults-report_102024.pdf. This is significant; as noted above, most Iowans using BTMs are age 60 or older.

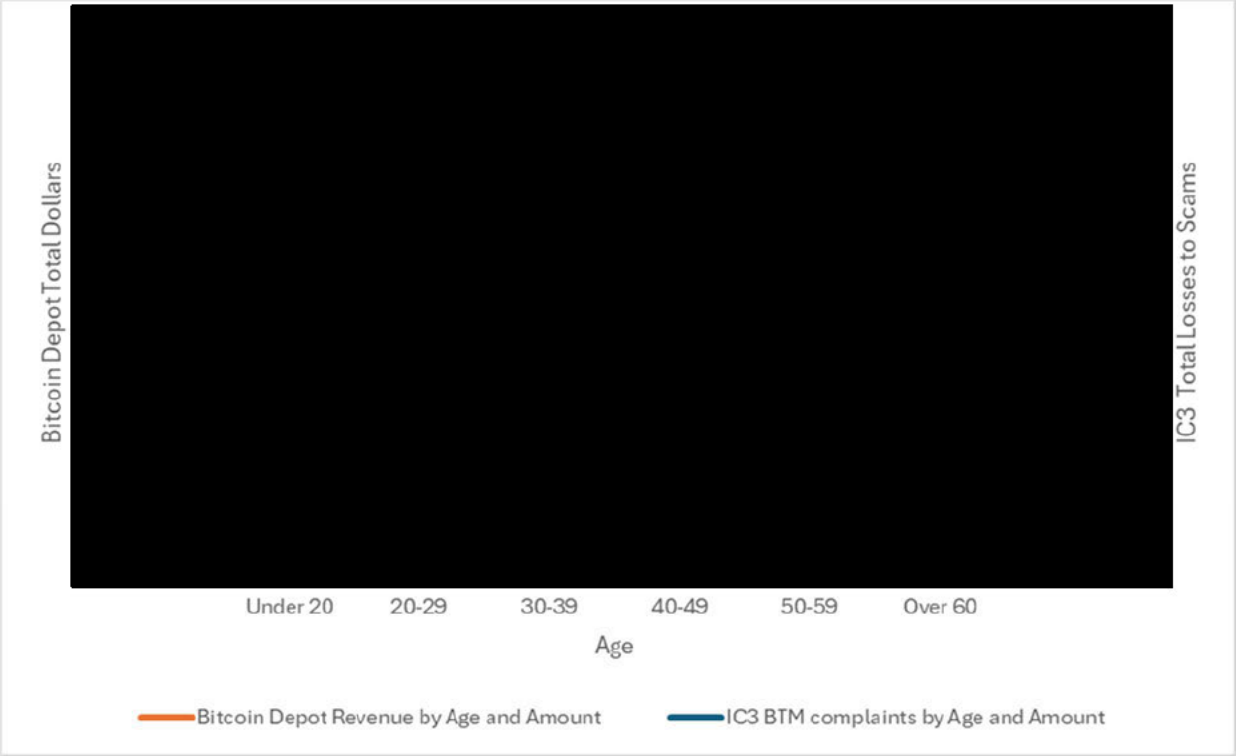
40. The following chart, created by the FBI's Internet Crime Complaint Center, shows reported scams and losses increase with age.

USE OF CRYPTOCURRENCY KIOSKS REPORTED IN IC3 COMPLAINTS – 2023

Age Range	Complaints	Losses
Under 20	65	$252,198
20 - 29	416	$3,529,680
30 - 39	451	$8,651,706
40 - 49	391	$9,634,346
50 - 59	476	$11,409,372
Over 60	2,676	$124,332,127

Internet Crime Complaint Ctr., *2023 IC3 Annual Report: Cryptocurrency Report*, *available at* https://www.ic3.gov/annualreport/reports/2023_ic3cryptocurrencyreport.pdf.

41. Similarly, Bitcoin Depot's transaction amounts increase by age as shown by the following chart that provides an overlay of what Iowa BTM transactions and IC3's Reported Losses to Fraud look like when broken into the IC3 chart's age brackets. As the chart shows, the trends for IC3 scam victims and Iowa BTM users closely and sadly align.



B. Bitcoin Depot Allows Pervasive Scam Transactions Across Iowa BTMs While Representing That BTMs Are Safe and Trustworthy

42. Contrary to its stated focus on fraud prevention, Bitcoin Depot's records show its inability to prevent scam transactions processed through its Iowa BTMs. Bitcoin Depot's internal data supports that Bitcoin Depot's policies and BTMs are causing Iowa consumers "substantial, unavoidable injury" that far outweighs any consumer or competitive benefits. Iowa Code § 714.16(1)(i).

43. Bitcoin Depot stated to Vice Media on May 27, 2018, "Bitcoin Depot has outstanding compliance policies and strives to go above and beyond all know your customer (KYC) and monitoring requirements at its ATMs." *Bitcoin ATM's Could Be Coming to a Gas Station or Vape Store Near You (HBO)*, VICE News (May 29, 2018), https://www.youtube.com/watch?v=M7VvbM04qnM.

44. Bitcoin Depot CEO Brandon Mintz stated the company's central objective is to "safely, securely, bring Bitcoin to the masses." *Crypto ATM Provider Bitcoin Depot Announces Nasdaq Listing for July 3***,** CRYPTOSLATE (July 2, 2023), https://cryptoslate.com/crypto-atm-provider-bitcoin-depot-announces-nasdaq-listing-for-july-3/.

45. Bitcoin Depot knows that many of the transactions it is asked to process are coerced or unwilling transactions initiated by or at the behest of scammers. In a recent SEC filing, the company stated:

> Our risk management efforts may not be effective, which could expose us to losses and liability and otherwise harm our business.
>
> We offer payments and other products and services to a large number of users. We have programs designed to vet and monitor these users and the transactions we process for them as part of our risk management efforts, **but such programs require continuous improvement and may not be effective in detecting and preventing fraud and illegitimate transactions.** When our services are used to process illicit transactions, and we settle those funds to users and are unable to recover them, we suffer losses and liability. Additionally, illicit transactions can also expose us to governmental and regulatory enforcement actions.

> The highly automated nature of, and liquidity offered by, our services make us and our users a target for illegal or improper uses, including scams and fraud directed at our users, fraudulent or illegal sales of goods or services, money laundering, and terrorist financing. **Our risk management policies, procedures, techniques, and processes may not be sufficient to identify all risks to which we are exposed, to enable us to prevent or mitigate the risks we have identified, or to identify additional risks to which we may become subject in the future**."

(emphasis added) Bitcoin Depot Inc., Form 10-K Annual Report for the Period Ended December 31, 2023**,** *available at* https://ir.bitcoindepot.com/sec-filings/all-sec-filings/content/0000950170-24-044405/btm-20231231.htm.

46. Mintz wrote in a February 14, 2024, article that "as the crypto industry shifts toward more regulatory compliance, it also looks to increase fraud prevention measures. These efforts include improving consumer protection protocols, mitigating risks, and enhancing transparency." Brandon Mintz, *Opinion: Changing Regulatory Dynamics for Bitcoin ATMs*, BITCOIN MAG. (Feb. 14, 2024), https://bitcoinmagazine.com/legal/changing-regulatory-dynamics-for-bitcoin-atms. According to Mintz, "there is a concerted effort to provide as much security as possible to BTMs and other crypto-related financial services." Id.

47. Despite Bitcoin Depot's public-facing statements about its concern for fraud or scams, reality paints a different picture. [redacted]

48. Bitcoin Depot's records include many other obvious warning signs of fraud, including:

a. *Bitcoin Depot's consumer base is overwhelmingly older.* As noted below, older adults are more likely to be targeted for scams, more likely to lose large sums of money, and less likely to report their losses. [redacted] Bitcoin Depot has not reasonably questioned why so many older Iowans use its service. It has not implemented any policies to protect this vulnerable population. And it is not true in Iowa that Bitcoin Depot's purported target user—people without bank accounts or that want to send remittances abroad—are the typical user. Instead, the typical Iowa Bitcoin Depot

customer is 60 or older, does not remit money to family abroad, and does not lack banking services. Whether intended or not, Bitcoin Depot's typical user in Iowa is a scam victim.

b. *Many Bitcoin Depot users have multiple accounts.* [redacted] VoIP providers are known tools for scammers and allow individuals to far more easily circumvent Bitcoin Depot's anti-money laundering and know your customer rules. *See FTC Warns 19 VoIP Service Providers That 'Assisting and Facilitating' Illegal Telemarketing or Robocalling Is Against the Law*, FTC Press Release (Jan. 30, 2020), https://www.ftc.gov/news-events/news/press-releases/2020/01/ftc-warns-19-voip-service-providers-assisting-facilitating-illegal-telemarketing-or-robocalling.

[redacted]

c. *Multiple Bitcoin Depot users sent money to the same Bitcoin address.* Anyone who knows the string of numbers and letters for a Bitcoin address can send Bitcoin to that address. Bitcoin Depot makes users verify that they own and control the Bitcoin address to which they send Bitcoin. Its website states, "Bitcoin Depot ATMs are to be used for personal purchases of cryptocurrency. Once your crypto reaches your digital wallet, you can send crypto to anyone else's wallet using the Bitcoin Depot app." Bitcoin Depot, *Can I Send Money to Someone Through a Bitcoin ATM?*, https://bitcoindepot.com/faq/.

It further explains, "Unlike cash in a bank account, you hold the keys to where your Bitcoin is held. It is virtually impossible for someone else to access your Bitcoin wallet unless they have your wallet's credentials. For this reason, it is crucial that you keep your wallet information private." Bitcoin Depot, *Should I send Bitcoin to a Stranger?,* https://bitcoindepot.com/faq/. [redacted]

d. *Users that have a large amount of Bitcoin addresses are connected to multiple wallets.* [redacted]

e. *Bitcoin Depot ignores red flags related to email.* [redacted]

C. Bitcoin Depot's Policies Are Insufficient to Address the Known Issues Related to Scams

49. Bitcoin Depot has several policies and programs related to fraud including, but not limited to, its "Compliance Program," its "Know Your Customer Policy," and its "Enhanced Due Diligence Policy." These programs failed to adequately and effectively detect and prevent consumer fraud and scam transactions processed through BTMs.

50. In addition to its anti-fraud program, Bitcoin Depot is required by the Bank Secrecy Act to have an effective anti-money laundering ("AML") program to prevent money laundering. 31 C.F.R. § 1022.210.

51. That prevention responsibility includes, but is not limited to, the flow of illicit funds, such as funds derived from fraud. As part of its AML program, Bitcoin Depot has developed "Know Your Customer" guidelines and policies along with policies and procedures for monitoring transactions, customers, and agent activity for risks, including suspicious activity.

52. AML legal requirements are distinct from compliance responsibilities under Iowa's Consumer Fraud Act. But all policies implemented under the umbrella of AML have failed in preventing Bitcoin Depot's business acts and practice from causing "substantial, unavoidable injury" to Iowa consumers. Those policies are either inadequate or ineffective due to Bitcoin Depot's failure to enforce and follow the policies. Either way, Bitcoin Depot's money-transfer system is an unfair or deceptive act or practice that is unlawful under Iowa's Consumer Fraud Act.

53. [redacted]

54. [redacted]

55. Bitcoin Depot's policy is designed to process transactions even when it has enough information to determine the transaction is fraudulent. [redacted]

D. Bitcoin Depot Fails to Address Red Flags and Allows Scam Transactions to Run Rampant

56. [redacted]

57. [redacted]

58. [redacted]

59. [redacted]

[redacted]

60. [redacted]

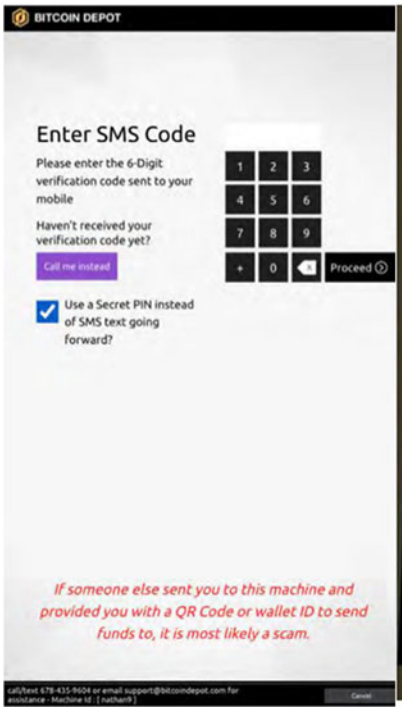
61. [redacted]

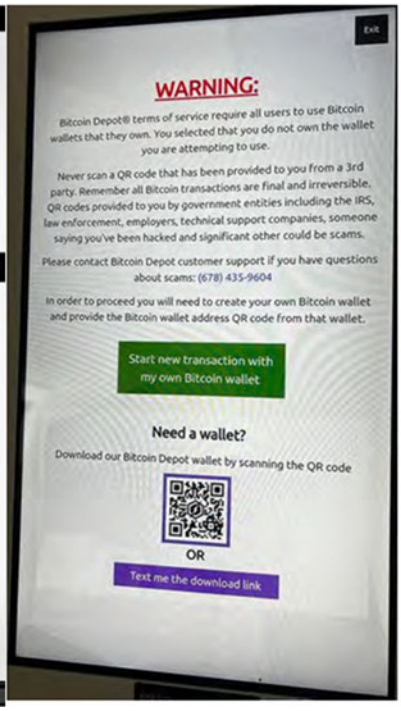
62. Repeating the same ineffective warnings and references to the Terms of Service is less effective than Bitcoin Depot's approach to those it suspects to be scam victims. Blocking the wallet does little to help the scam victim, as scammers often have dozens of wallets at their disposal and can send the victim a new address. [redacted]

E. Bitcoin Depot's Warnings are Ineffective at Preventing Scam Transactions

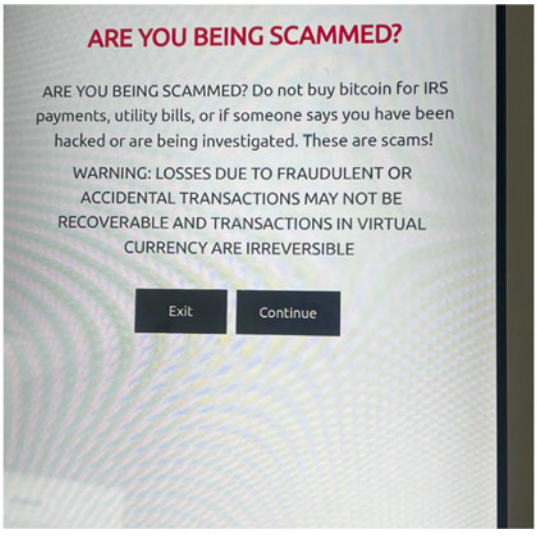
63. Bitcoin Depot's primary method of preventing Iowa scam victims from using a BTM is to place onscreen warnings and sticker warnings on the machine. Below are examples of the warnings taken from a letter addressed to the State of California from Mark J. Smalley, Bitcoin Depot's Chief Compliance Officer, (Jan. 12, 2024), https://dfpi.ca.gov/wp-content/uploads/sites/337/2024/02/Bitcoin-Depot-1.12.24.pdf:


WARNING: Have you received a phone call from someone demanding payment in Bitcoin? THIS IS LIKELY A SCAM. All Bitcoin transactions are irreversible. Send to your own wallet only. NOT SURE if you are being scammed? CALL US for assistance at (678) 435-9604.


BITCOIN DEPOT
Enter SMS Code
Please enter the 6-Digit verification code sent to your mobile
Haven't received your verification code yet?
Call me instead
Proceed
Use a Secret PIN instead of SMS text going forward?
If someone else sent you to this machine and provided you with a QR Code or wallet ID to send funds to, it is most likely a scam.


Exit
WARNING:
Bitcoin Depot® terms of service require all users to use Bitcoin wallets that they own. You selected that you do not own the wallet you are attempting to use.
Never scan a QR code that has been provided to you from a 3rd party. Remember all Bitcoin transactions are final and irreversible. QR codes provided to you by government entities including the IRS, law enforcement, employers, technical support companies, someone saying you've been hacked and significant other could be scams.
Please contact Bitcoin Depot customer support if you have questions about scams: (678) 435-9604
In order to proceed you will need to create your own Bitcoin wallet and provide the Bitcoin wallet address QR code from that wallet.
Start new transaction with my own Bitcoin wallet
Need a wallet?
Download our Bitcoin Depot wallet by scanning the QR code
OR
Text me the download link


BITCOIN DEPOT
Scan your digital wallet
Wallet Already in Use
This wallet is already associated with another customer account. Please continue with a different wallet address or call or text Customer Support at (678) 435-9604 if you believe it's yours.
Continue transaction with a new wallet address that belongs to you
If you need a wallet, see the instructions below if you'd like to download our Bitcoin Depot mobile app.
Need a wallet?
Download our Bitcoin Depot wallet by scanning the QR code
OR


ARE YOU BEING SCAMMED?
ARE YOU BEING SCAMMED? Do not buy bitcoin for IRS payments, utility bills, or if someone says you have been hacked or are being investigated. These are scams!
WARNING: LOSSES DUE TO FRAUDULENT OR ACCIDENTAL TRANSACTIONS MAY NOT BE RECOVERABLE AND TRANSACTIONS IN VIRTUAL CURRENCY ARE IRREVERSIBLE
Exit
Continue

64. These warnings are insufficient to protect Iowa scam victims and Bitcoin Depot knows it. A review of the best studies on warnings, shows that scammers disrupt a person's ability to reason and in the moment warnings often fail. *A Review of Scam Prevention Messaging Research, Federal Trade Commission*, available at https://consumer.ftc.gov/system/files/consumer_ftc_gov/pdf/A%20Review%20of%20Scam%20Prevention%20Messaging%20Research.pdf.

65. Bitcoin Depot only needs to look at its data as the proof is in the pudding. The sheer volume of transactions confirmed as scams to date show this method is ineffective. Also, even red flag scenarios trigger some of the warnings above Bitcoin Depot allows the customer in those scenarios to enter a different address and complete the transaction. Bitcoin Depot does not call to speak with its customers to prevent a scam even in most scenarios raising a red flag.

F. The Demographic Markets in Iowa for Scam Victims and BTMs Are Older Iowans

66. Bitcoin Depot competes with online exchanges, which sell consumers Bitcoin at a significantly lower net cost than Bitcoin Depot's BTMs. The primary competitive advantages Bitcoin Depot touts over online exchanges are that BTMs (i) don't require a bank account, (ii) allow individuals to use cash, and (iii) process the transactions more quickly. The company also promotes its usefulness in helping immigrants remit money. *See* Bitcoin Depot Blog, *Crypto Remittance and Bitcoin ATMs: The Unbanked's New Bank*, October 22, 2024, https://bitcoindepot.com/bitcoin-atm-info/crypto-remittance-and-bitcoin-atms-the-unbankeds-new-bank/.

67. Bitcoin Depot's website states, "Bitcoin Depot was founded in 2016 with the mission to connect those who prefer to use cash to the broader, digital financial system." Bitcoin Depot, *Company Information*, https://ir.bitcoindepot.com/company-information

68. In a May 2018 interview with Vice Media, Bitcoin Depot's founder and CEO Brandon Mintz stated he does not have exact metrics on demographics, but "it's really diverse, I mean there's low-income people using the machines because it's a better source of money transfer than Western Union. There are investors going to the machine…" *Bitcoin ATM's Could Be Coming to a Gas Station or Vape Store Near You (HBO)*, VICE NEWS (May 29, 2018), https://www.youtube.com/watch?v=M7VvbM04qnM.

69. In a December 2020 interview, Mintz stated the "majority of the demographic" for Bitcoin Depot services was "more in that lower middle-income range. Blockworks Macro, *Bringing the Unbanked into the Financial World W Brandon Mintz of the Bitcoin ATM Empire*, YouTube (Dec. 29, 2020), https://www.youtube.com/watch?v=W8gJRkSDNlA.

70. He stated in the same interview that many people who are underbanked and unbanked prefer to use cash, so we try to focus on those areas. Additionally, Mintz, acknowledged that BTM users are unlikely to be "super sophisticated" and that the very sophisticated users would most likely use online exchanges. *Id*.

71. According to the FDIC, the unbanked represent 3% of Iowa's households. Most of these households are single parent, non-home owning, and or non-US citizens. Federal Deposit Insurance Corporation, *FDIC National Survey of Unbanked and Underbanked Households*, https://www.fdic.gov/household-survey.

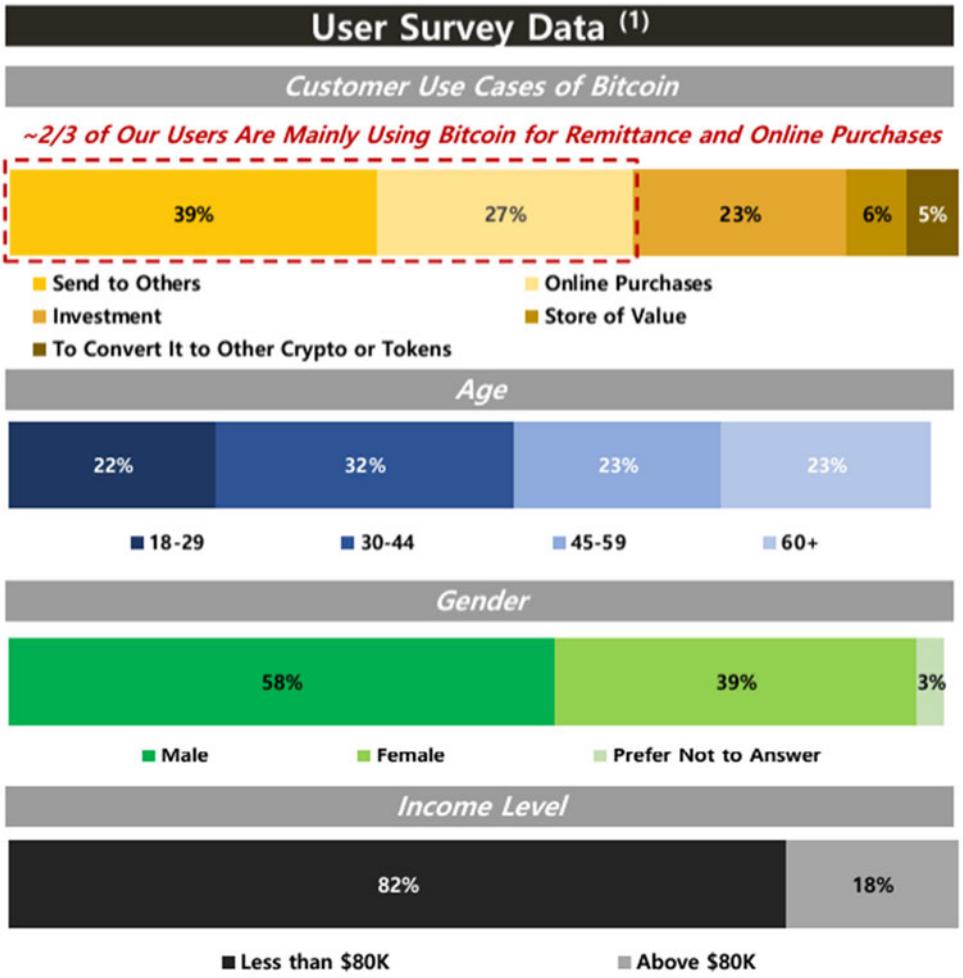
72. When asked a similar question about demographics during a 2023 interview, Mintz stated, "There's really three different buckets I like to break it into."

    a. The first "bucket," is made up of people who just prefer to use cash. An important part of this group, according to Mintz, are the underbanked and unbanked.

    b. The second bucket is filled with, "anyone who wants pure convenience and doesn't mind paying a markup." Mintz explains, "maybe they got fed up waiting on verification on an exchange."

    c. The third bucket, is "baby boomers." Mintz explains, "As crypto has been adopted more and more, the baby boomer demographic has come into play as well, so you have people who aren't that great with technology, they don't want to try and figure out how to use an online exchange, and they want a familiar experience, something they can see touch and feel, that gives them a lot more comfort than just completing the transaction through the website. Especially with all the news that came out the last year, a lot of people may feel you go to a website to buy bitcoin, they could just disappear or say, 'hey we're not allowing withdrawals.' You go to a BTM, you are getting your bitcoin essentially instantly. There's a lot less to worry about." Thinking Crypto, "Brandon Mintz Talks Bitcoin Depot ATMs, Going Public in 2023, Bitcoin Adoption & Bear Market," https://www.youtube.com/watch?v=LUnt2AgClDk.

73. Bitcoin Depot submitted the following chart to California regulators, created from data obtained from an internal survey of 625 BTM users conducted between August 15, 2022, and December 15, 2022: Letter from Mark J. Smalley, Chief Compliance Officer, Bitcoin Depot, to the State of California (Jan. 12, 2024), https://dfpi.ca.gov/wp-content/uploads/sites/337/2024/02/Bitcoin-Depot-1.12.24.pdf.



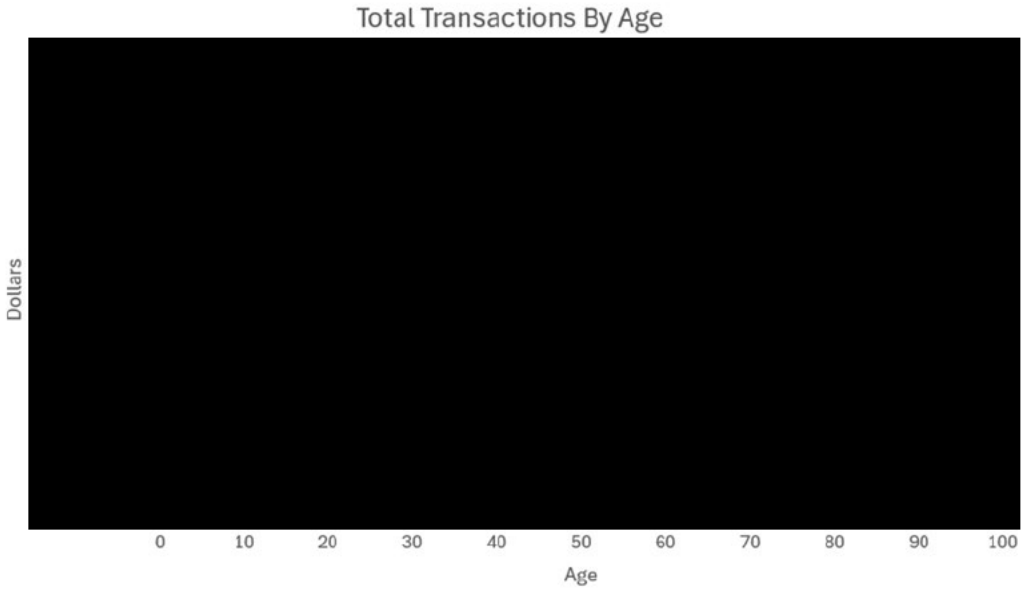
74. While Bitcoin Depot tells California that its business model depends on younger individuals, lower-income individuals, and a large volume of users, Bitcoin Depot's data tells a different story.

75. In Iowa, Bitcoin Depot's business model depends on a small number of high-volume users and its primary audience is, in fact, older individuals with significant assets. [redacted]

[redacted]

76. Contrast the California data with Iowa. The chart below shows the percentage of Iowans who used a BTM by age group for the period of October 10, 2021, to July 26, 2024.

77. Bitcoin Depot's dependency on older Iowa consumers is clearer when shown as the total amount of money placed into machines by Iowan consumers based on age.



78. Older Iowans use BTMs the most. [redacted]

[redacted] Coincidentally, the FTC reports that the average loss for scam victims to BTMs is approximately $10,000. Emma Fletcher, *Bitcoin ATMs: A payment portal for scammers*, FTC (Sept. 3, 2024), https://www.ftc.gov/news-events/data-visualizations/data-spotlight/2024/09/bitcoin-atms-payment-portal-scammers.

G. Bitcoin Depot's Profitability in Iowa Depends on Iowa Scam Victims

79. Bitcoin Depot could do more to prevent scam transactions, but such policies would reduce its profits:

a. *Bitcoin Depot Underutilizes Bitcoin Tracking Capabilities***.** Inherent in Bitcoin is the ability to track Bitcoin transactions, as every transaction is recorded in the currency. [redacted]

b. *Bitcoin Depot Fails to Use its Machine's Surveillance Abilities.* Each BTM has an internet-connected video camera that can be accessed by Bitcoin Depot remotely. [redacted]

[redacted]

c. *Bitcoin Depot does nothing to protect elderly populations*. Bitcoin Depot has no policies designed to assist or protect Iowans aged 60 or over (its most prevalent users) from fraud. One example of a potential protective policy is to call older customers before they use the machine. Other cryptocurrency kiosk companies have such a policy. In fact, while one company stopped an older Iowan from processing a scam transaction through its machine, Bitcoin Depot processed $15,000 (over two transactions) for that same Iowan, sending $11,525 to a scammer and retaining about $3,475 in fees and transaction costs. App. 1.

d. *Bitcoin Depot Does Not Want Stores to Stop Scams.* Store clerks could be a key line of defense against fraud. [redacted]

[redacted] More recent contracts actually prohibit a store from preventing a scam transaction; the store must agree that [redacted] A store clerk or manager must stand by and witness an older Iowan placing his or her hard-earned cash into a BTM that is destined for the scammer's and Bitcoin Depot's pockets.

H. Bitcoin Depot Profits From Iowa Scam Victims

80. [redacted] Under Bitcoin Depot's newest terms of service published in January 2025, its cut of transactions processed through BTMs may reach 50% of the total transaction amount.

81. In a competitive landscape with multiple direct competitors who charge far less and alternative methods of buying bitcoin such as exchanges that charge even less, Bitcoin Depot has doubled its rates over night. It can only do this because its users are (i) unaware of the charges being assessed, (ii) using its services involuntarily as part of a scam, or (iii) both. Even Bitcoin Depot admits this is too much money to charge, stating to California regulators that it "believes that a 28% fee cap and $15,000 daily transaction limit support economic growth in California while allowing kiosk operators to invest in meaningful compliance efforts." *Letter addressed to the State of California from Mark J. Smalley*, Bitcoin Depot's Chief Compliance Officer, (Jan. 12, 2024),https://dfpi.ca.gov/wp-content/uploads/sites/337/2024/02/Bitcoin-Depot-1.12.24.pdf.

82. Though it is difficult to know exactly how much revenue Bitcoin Depot received in Iowa due to the deceptive way Bitcoin Depot conflates transaction costs and fees, [redacted]

I. Bitcoin Depot Hides the True Cost of Using a BTM From Iowa Consumers

83. Bitcoin Depot engages in deceptive practices to conceal what it really charges an Iowa consumer to buy Bitcoin, including by:

a. Combining both its online and BTM services in one Terms of Service document, so BTM users find it harder to determine which sections apply to them.

b. Calling the product a "Bitcoin ATM" and charging a $3 service fee, which confuses consumers into thinking they are paying only $3.

c. Burying any explanation of the total actual fees (currently "up to 23%" and averaging close to that at more than 22%) on page 20 of 47 in the Terms of Service.

d. Displaying information on screens and receipts in a way that obscures the true cost of the service.

84. The cost of a product or service is a material term to a transaction. Bitcoin Depot hides that material term related to its BTMs transactions in fine print that is confusing and designed to go unnoticed by Iowa consumers. Bitcoin Depot interacts with Iowa consumers in three ways: at a BTM, online, and through the Bitcoin Depot app. Bitcoin Depot's Terms of Service are different for each service, but rather than have separate terms of service for each, Bitcoin Depot combines all three into one document. This forces consumers to scan an array of terms in an attempt to understand which may apply to their transaction. It is one of the reasons Bitcoin Depot's Terms of Service document is 47 pages and 12,500 words. Assuming an average reading speed of 300 words per minute, it would take a person about 41 minutes to read the entire document.

85. The Terms of Service is the only place where Bitcoin Depot discloses its true fee structure, which it does on page 20 of 47.

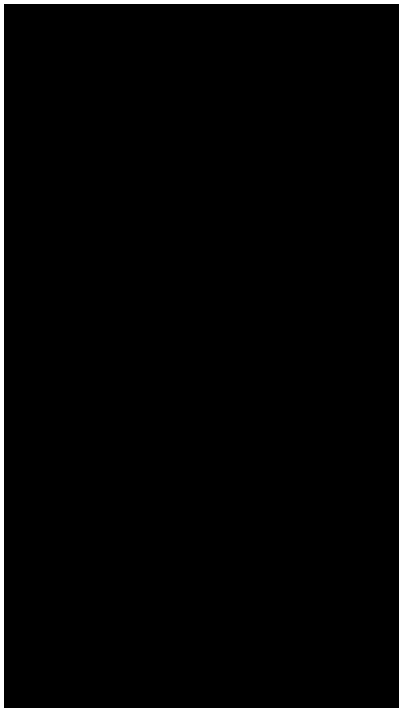
86. Bitcoin Depot's Terms of Service are regularly updated, but the document in effect for most of October 10, 2021, to July 26, 2024, included this:

> *Exchange Service Fee. A service fee shall be applied to all exchange transactions and such fee will be communicated to the Customer prior to confirmation of the transaction. The transaction value and service fees are calculated/quoted in "USD" for U.S. Dollar transactions and may be calculated/quoted in USD equivalents for transactions in all other currencies, or in the currency of the transaction. The service fee will be a flat fee of three dollars [$3.00] and Bitcoin Depot shall charge a spread of up to twenty three percent [23%] of the total transaction amount calculated in USD. The spread refers to the difference between the cash inserted into the kiosk and the current market value of Bitcoin received, excluding the $3.00 flat fee.* App. 96-97.

87. Bitcoin Depot hides the true cost of its service in the "spread." [redacted]

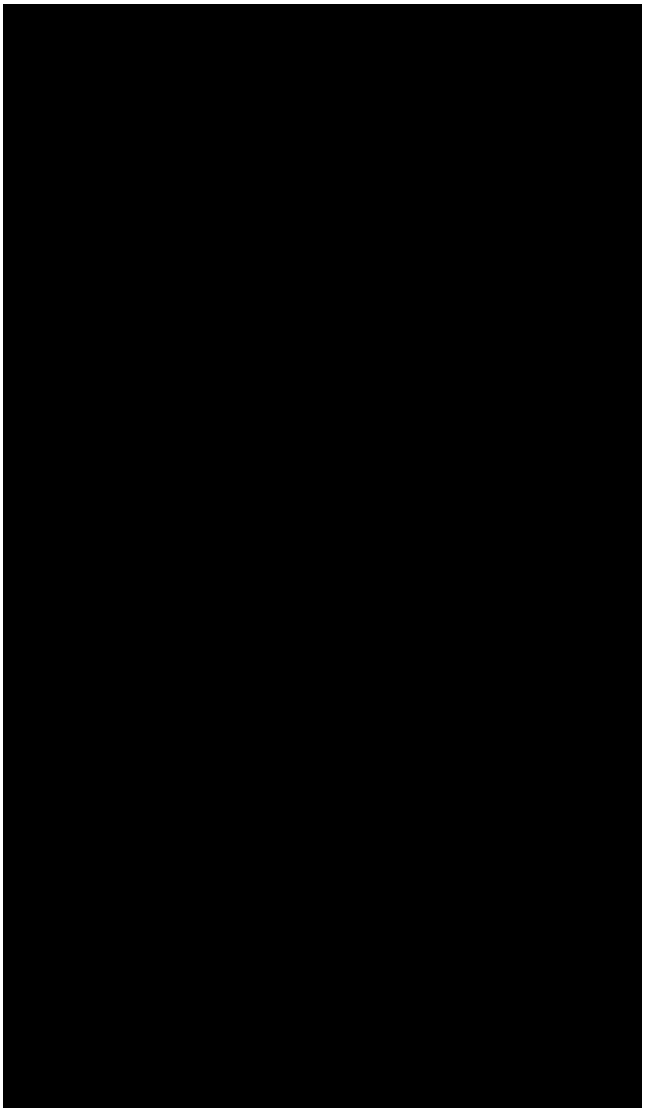
88. Consumers were unaware of the amount of money Bitcoin Depot charged them to use BTMs or believed that they paid a small service fee. Bitcoin Depot deceives consumers by obfuscating an excess charge known as the spread that is hidden within Bitcoin Depot's Terms of Service and is not clearly relayed to Iowa consumers even after the transaction is completed.

89. The following images demonstrate how Bitcoin Depot hides the cost of purchasing Bitcoin, and the images are taken from Bitcoin Depot training documents, unless otherwise noted.



90. The first screen asks the consumer “How much would you like to buy today?” and gives him or her a range of options. The choices offered are: $20-$250, $251-$2,999, or $3,000-$ 15,000.

91. Consumers then must enter their “mobile number” and agree to the terms and conditions.



92. Consumers have the option of scrolling through the 47-page Terms of Service viewed through a narrow portion of the overall screen, or they can click "I accept these terms and conditions."

93. This design makes reading the Terms of Service tedious and difficult and skipping the experience of reading easy. Even the choice to place the terms of service on a black background with white font contributes to the overall design goal of stopping the consumer from reading the document.

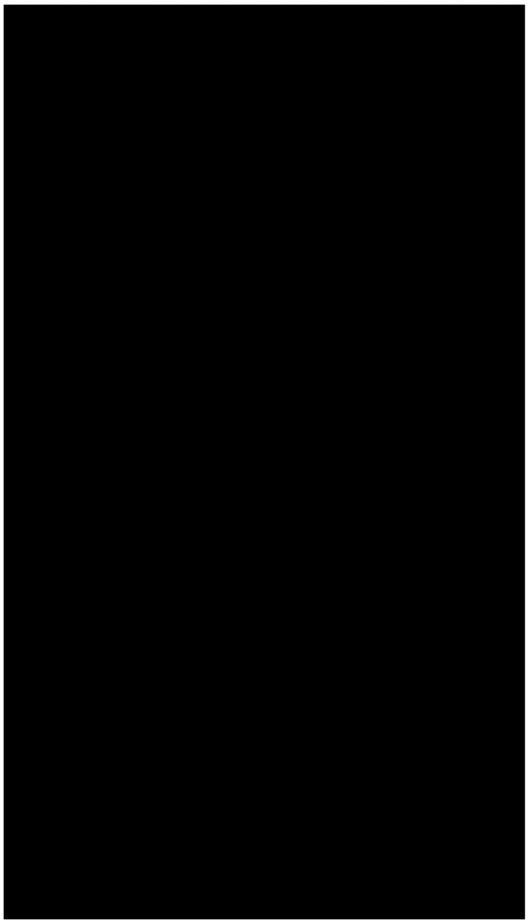
94. After accepting the terms and entering a phone number, consumers must provide additional verifications depending on the money level the consumer wishes to send.

95. For transactions under $250, the machine requires a name, phone number, and email address. Level 2, for transactions between $251 and $3,000, adds a requirement scanning an ID with

the machine. Finally, Level 3, including transactions between $3,001 and $15,000 requires a picture of the front and back of the ID and a social security number. The BTM is supposed to automatically send a link to consumers to verify their ID.

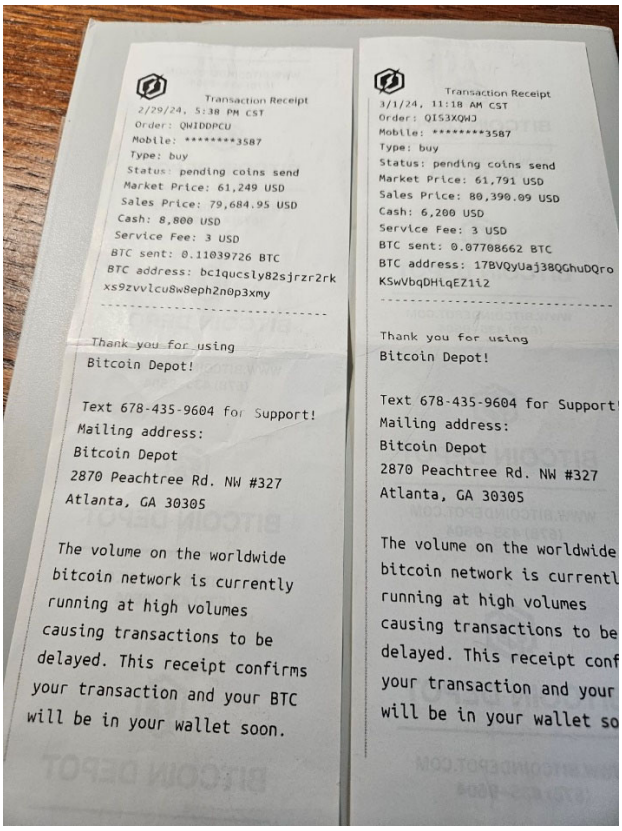
96. Consumers may then insert cash.

97. The above, example from Bitcoin Depot's training materials, also includes instructions for what customer service representatives should say to the consumer if assisting a transaction remotely. In the example, the user put in $60 into the machine, which shows he or she is about to purchase 0.00171722 BTC. On the top right of the screen is the transaction limit, the "service fee" of $3 and "1 BTC 33,193.10 USD." This is not the market price of Bitcoin at the time of the sale, but the Bitcoin Depot sales price of Bitcoin (with the extra charge of a spread included). Though noted in the above photo from Bitcoin Depot's training manual, this feature no longer appears during BTM transactions – further obscuring the true cost of the transaction to consumers.



98. The above example (which again includes the addition of a customer service representative script that is not present on the actual machine) shows that when consumers complete the transaction, they can choose to print a receipt. The screen displays only the cash inserted and the Bitcoin sent.

99. One confirmed scam victim provided the following picture of his receipts:



The relevant portions of the receipt located on the left states:

Transaction Receipt

2/29/24, 5:38 PM CST

Order: QWIDDPCU
Mobile: ********3587
Type: buy
Status: pending coins send
Market Price: 61,249 USD
Sales Price: 79,684.95 USD
Cash: 8,800 USD
Service Fee: 3 USD
BTC Sent: 0.11039726 BTC
BTC address: bc1qucsly82sjrzr2rkxs9zvvlcu8w8eph2n0p3xmy

100. The Iowa consumer's receipt lists a "Market Price," which he was supposed to know is the market price of one Bitcoin. He was given a "Sales Price" which he is supposed to know is the price at which Bitcoin Depot is selling one Bitcoin. The receipt then lists the cash the consumer is putting into the machine, the service fee ("3 USD"), and finally the amount of Bitcoin sent and where it was sent.

101. Assuming the Iowa consumer read and understood the terms of conditions, the only way for the Iowa consumer to know how much Bitcoin Depot charged in total fees is to go through the following steps:

    a. Multiply the market price ($61,249) by the BTC Sent (0.11039726). This tells the consumer that the present-day value of the Bitcoin he has purchased is $6,761.72.
    b. Subtract $6,761 from the inserted cash amount ($8,800) to obtain the total fee amount retained by Bitcoin Depot of $2,038.28.
    c. The Iowa consumer knows there is a $3 flat fee, so he subtracts that from the total fee amount of $2,038.28 to know the Iowa consumer paid (i) a $3 service fee, plus (ii) an extra charge equal to $2,035.28.
    d. The extra charge of $2,035.28 (which is the spread) is equal to slightly more that 23% of his total money inserted.

102. Bitcoin Depot has taken recent steps to make this even less clear. Recent consumer receipts from BTMs provided to the Attorney General's office do not include the market price. The machines also no longer come with the option of printing a receipt instead opting to text consumers a link to a digital receipt.

103. Bitcoin Depot does not express the full cost of its service as a US dollar amount on the screen and receipt, as many of its competitors do, because consumers would be less likely to use its service. This lack of transparency becomes even more important for Iowa scam victims who are often unfamiliar with Bitcoin values and directed by scammers to use BTMs. Scammers often use threats and emotional manipulation to fluster their victims and place them in a heightened emotional state. They then instruct the victims to skip screens quickly, not giving them time to read the 47-page Terms of Service or warnings on the screen. Many victims say they were unaware of the prices Bitcoin Depot charged, and if they had known, they would have further questioned the transaction and may not have put money into the machine.

J. Bitcoin Depot Hides the Cost of Using a BTM Behind Iowans' Experience with ATM Fees

104. Bitcoin Depot's use of the term "Bitcoin ATM" in its marketing and advertising further deceives consumers about its fees. People associate the term "ATM" with the more common bank automated teller machines that often charge a small service fee for its use. Consumers assume that the $3 service fee prominently displayed on the Bitcoin Depot ATM screen is similar a regular ATM fee. In that way, consumers are tricked into thinking the $3 is the extent of the fees they must pay.

105. Bitcoin Depot encourages this confusion. In a recent blog post on its website entitled "Bitcoin ATMs vs. Traditional ATMs," the company states about traditional ATMs: "Many ATM-specific businesses allow users like you to grab cash on the go for a small fee. In fact, the total ATM market is estimated at a value of $24 billion." The article goes on to compare traditional ATMs and Bitcoin ATMs, discussing items like functionality, transaction types, accessibility, and regulatory framework. Conspicuously absent from the article is a cost comparison of using a Bitcoin ATM, despite mentioning the low fees associated with traditional ones. The post concludes, "Bitcoin ATMs and traditional ATMs represent distinct yet interconnected facets of the financial landscape. As financial technology continues to evolve, the interplay between these two types of ATMs signals a dynamic shift in how individuals interact with and understand the concept of money in the digital age." Bitcoin Depot, *Bitcoin ATMs vs. Traditional ATMs* (last updated Jan. 10, 2025), https://bitcoindepot.com/bitcoin-atm-info/bitcoin-atms-vs-traditional-atms/.

106. Bitcoin Depot recently updated the Exchange Service Fee portion of its Terms of Service to say that the spread will range between 17.3% and 50% of the total transaction. The same document notes that these fees "may be significantly greater than other available options for converting fiat currency to Digital Currency." Bitcoin Depot, *Terms and Conditions*, https://bitcoindepot.com/terms-and-conditions/.

K. Bitcoin Depot's Internal Training Documents Show Bitcoin Depot Wants to Hide Its Total Fees

107. Bitcoin Depot's internal training documents reveal that if a consumer asks about fees, customer service representatives are to say, [redacted]

[redacted] This lack of transparency means Iowa consumers and Iowa scam victims may never realize how much of the cash they insert into a BTM that Bitcoin Depot keeps.

108. If asked why its service costs so much, Bitcoin Depot customer service representatives are told to give [redacted]

109. [redacted]

110. When victims do not realize that Bitcoin Depot currently retains between 17.3% and 50% of their money, they are more likely to continue to use the machine and less likely to request a refund from Bitcoin Depot—an intentional design choice that protects Bitcoin Depot's profits and the flow of Bitcoin to scammers.

L. Bitcoin Depot Lies to Iowans About Its Refund Policy

111. Bitcoin Depot keeps a separate "secret" refund policy that is only accessible through law enforcement and does not inform consumers of its existence.

112. If consumers read Bitcoin Depot's publicly available "Refund Policy" (last updated 10/30/23), they will see, in bold:

> "**Completed transactions and transactions to a wallet that you do not control are not eligible for a refund.**"

Bitcoin Depot, *Refund Policy*, https://bitcoindepot.com/refund-policy/.

113. Likewise, the Terms of Service states:

> *Moreover, Customer acknowledges that Bitcoin Depot cannot retrieve or return any funds (including, but not limited to, cryptocurrencies) once sent to the designated address and, therefore, Bitcoin Depot does not provide any refunds after such point. Bitcoin Depot, Terms and Conditions, https://bitcoindepot.com/terms-and-conditions/.*

114. At any rate, Bitcoin Depot's official "Consumer Refund Policy," [redacted]

115. Bitcoin Depot at no point informs consumers of the existence of this hidden refund policy despite the policy's stating,

116. If Iowa consumers ask how much they can get back, or makes any inquiries about refunds, the document tells the customer representative to say:

And it continues:

[redacted]

Id.

117. It is unclear how consumers are expected to know or use Bitcoin Depot's refund policy, and it is unclear whether law enforcement is aware that its involvement is necessary for any refund.

118. Of the Iowa consumers the Attorney General's office has interviewed who tried getting a refund from Bitcoin Depot, very few have been successful. Some report being told that all transactions are final. Others read online that no refunds are available. Many reported their scams to police and were not given a refund.

119. [redacted]

120. Bitcoin Depot often denies refunds based on company policies that consumers do not know and cannot access. For example, one individual provided the company with a picture, a scam-related document, a receipt, a police report, and a letter from the Lyon County Sheriff's Department. Bitcoin Depot's analysis shows that the deposits occurred close to the victim's home address, the amount alleged to have been scammed matches the police report, and the report is consistent with a "hacked" scam. The individual reported the scam to police on April 25, 2024, the day of the transaction. Yet the officer did not report the fraud to Bitcoin Depot within its secret 30-day reporting window, and thus Bitcoin Depot retained all funds related to this obvious victim of fraud. *Id.*

121. Bitcoin Depot cannot afford to advertise refunds or give refunds to all Iowa scam victims using its BTMs without sacrificing its profitability.

IV. Violations of the Iowa Consumer Fraud Act

122. Under the Act:

> The act, use or employment by a person of an unfair practice, deception, fraud, false pretense, false promise, or misrepresentation, or the concealment, suppression, or omission of a material fact with intent that

> others rely upon the concealment, suppression, or omission, in connection with the lease, sale, or advertisement of any merchandise or the solicitation of contributions for charitable purposes, whether or not a person has in fact been misled, deceived, or damaged, is an unlawful practice.

Iowa Code § 714.16(2)(a).

123. Bitcoin Depot sells merchandise as defined by the Act. *Id*. Merchandise "includes any objects, wares, goods, commodities, intangibles, securities, bonds, debentures, stocks, real estate or services." *Id*. § 714.16(1)(e). BTMs provide money transmitter services as well as sell Bitcoin, which could be considered a good, commodity, or intangible under the Act.

124. Bitcoin Depot has and is engaged in an "unfair practice, deception," and "misrepresentation" as follows:

A. Selling Bitcoin Through a Kiosk That Allows for Prevalent Scam Transactions is an Unfair Practice

125. Bitcoin Depot's practice of selling Bitcoin through its BTMs in a manner that allows for prevalent scam transactions to be processed constitutes an "unfair practice" that is unlawful under Iowa Code § 714.16(2). An "unfair practice" is defined as an act or practice which causes substantial, unavoidable injury to consumers that is not outweighed by any consumer or competitive benefits which the practice produces." Iowa Code § 714.16(1)(i).

126. The amount of money for the period of October 10, 2021, to July 26, 2024, processed through Iowa BTMs related to confirmed scam transactions totaled a staggering $7,243,991. This number is only expected to grow as the Attorney General's office has only been able to contact or confirm data related to $7,418,024 of the total $18,816,893 of transactions processed during the above period.

127. Bitcoin Depot's policies comprise a paradigmatic "unfair practice." BTMs are causing "substantial, unavoidable injury" to Iowa consumers. Iowans are losing their life savings, going bankrupt, getting depression, and a myriad of other injuries because of BTMs.

128. The injuries caused by BTMs far outweigh any consumer or competitive benefits under any equitable weighing test. Any benefit in the vast pile of scams, high transaction fees, and hidden refund policies is scant. Bitcoin Depot's expressed goal extending

cryptocurrency access to the unbanked or helping people send money abroad is not the typical case in Iowa.

129. BTMs that operate under Bitcoin Depot's current policies and practices that allow BTMs to primarily operate as a gateway for scammers violate Iowa consumer protection laws. Bitcoin Depot BTMs create a path to financial ruin for Iowans, and especially older Iowans. Bitcoin Depot's deficiencies include, but are not limited to, failing to take timely, appropriate, and effective action to detect and prevent fraud-induced money transfers through its BTM system, as described above.

130. Bitcoin Depot knows that its BTMs are frequently used by scammers to defraud older and vulnerable Iowa consumers, both within this State and elsewhere, but it does not institute adequate safeguards relate to BTM operations to prevent scam transactions that could avoid "substantial, unavoidable injuries" to Iowa consumers.

131. Rather, Bitcoin Depot continues to employ practices related to BTMs that are akin to putting a loaf of bread known to be poisonous on the store shelf with a warning label slapped on to avoid liability. Both are unlawful under the Iowa Consumer Fraud Act and both cause "substantial, unavoidable injuries" that are not outweighed by consumer or competitive benefits.

132. Bitcoin Depot's practice of selling Bitcoin through a BTM in a manner that allows for prevalent scam transactions is a violation of the Act. The State is entitled to civil penalties of up to $40,000 per violation of the Act under Iowa Code § 714.16(7). There is a violation with respect to each BTM located in Iowa.

B. Bitcoin Depot Deceived Iowans About the Price of Bitcoin Purchased Through BTMs

133. Bitcoin Depot's practices of failing to conspicuously present Iowa consumers with either the price of Bitcoin or the fees they pay, hiding the terms regarding the cost of Bitcoin and fees in lengthy, complex documents with inapplicable terms, and instructing its customer service representatives to evade and misdirect questions about cost are deceptive acts or practices that are unlawful under the Act.

134. "Deception" under the Act is "an act or practice which has the tendency or capacity to mislead a substantial number of consumers as to a material fact or facts." Iowa Code § 714.16(1)(c). The price of a good or service is a material fact.

135. Bitcoin Depot only advertises the $3.00 service fee associated with its BTMs in a clear and conspicuous manner. The extra charge known as the "spread" that Bitcoin Depot charges is hidden and made unclear to Iowa consumers.

136. Additionally, Bitcoin Depot buries its extra charge in its Terms of Service and does not provide an example to Iowa consumers of how to calculate the charge themselves. It takes sophisticated math skills to back into determining the total fees associated with the purchase of Bitcoin BTM.

137. Bitcoin Depot does not even offer clear information to an Iowa consumer about how it determines how much Bitcoin will be delivered.

138. Bitcoin Depot further muddies the water by instructing its customer service representatives to evade and misdirect the few Iowa consumers who may realize there are additional fees.

139. Bitcoin Depot's deception regarding the pricing and fees associated with the purchase of Bitcoin through a BTM is a violation of the Act. The State is entitled to civil penalties not to exceed $40,000 per violation of the Act under Iowa Code § 714.16(7). There is a violation with respect to each BTM located in Iowa. There is also a violation for each version of Bitcoin Depot's Terms of Service delivered to Iowa consumers, and a violation for the practice of customer service representatives in deceiving Iowa consumers on the telephone.

C. Bitcoin Depot Misrepresents to Iowa Consumers Its Refund Policy

140. Bitcoin misrepresents the existence of its refund policy in certain circumstances to Iowa consumers.

141. Bitcoin Depot tells Iowa consumers it does not have a refund policy in certain cases such as transactions where Bitcoin is sent to a Bitcoin address not owned by the Iowa consumer. This is false; it does have a refund policy that can be applied in those instances to return Bitcoin or cash to Iowa consumers.

142. Bitcoin Depot's misrepresentation regarding its refund policy violates the Act. The State is entitled to civil penalties of up to $40,000 per violation of the Act under Iowa Code § 714.16(7). There is a violation with respect to each BTM located in Iowa.

D. Bitcoin Depot's Refund Policy Is Deceptive

143. Bitcoin Depot's refund policy and its implementation of the policy is deceptive and unlawful under the Act as both have a "tendency or capacity to mislead a substantial number of consumers" as to the material fact of obtaining a refund to which the Iowa consumer is entitled.

144. Bitcoin Depot instructs its customer service representatives to avoid explaining that there is a refund policy and how it works. Bitcoin Depot does not explain to the consumer that she needs to involve law enforcement on a specific timeline to be entitled to receive a refund under the refund policy. Indeed, none of the necessary components to get a refund are conveyed to consumers.

145. Bitcoin Depot actively tries to hide its refund policy from Iowa consumers and takes steps to deceive Iowa consumers as to a material fact or facts.

146. Bitcoin Depot's deception regarding its refund policy violates the Act. The State is entitled to civil penalties of up to $40,000 per violation of the Act under Iowa Code § 714.16(7). There is a violation with respect to each BTM located in Iowa. There is also a violation for the practice of customer service representatives in deceiving Iowa consumers on the telephone.

E. Bitcoin Depot's Violations of the Act Were Committed Against Iowa Consumers Sixty Years of Age or Older

147. The violations alleged in this Petition were committed against "older individuals" as defined under Iowa Code § 714.16A—those who are "sixty years of age or older." *Id*.

148. The State is thus entitled to additional civil penalties of up to $5,000 for each violation of the Act that was committed against an older individual.

V. Conclusion and Prayer

The State of Iowa, *ex rel.* Attorney General Brenna Bird, requests that the Court render judgment in the State's favor and:

A. Declare that Defendants have engaged in misrepresentations, deceptions, and unfair practices against Iowa consumers in violation of the Iowa Consumer Fraud Act, Iowa Code § 714.16, *et seq.*;

B. Preliminarily and permanently enjoin Defendants from engaging in the deceptive and unfair acts described in this Petition whether that be by (i) a permanent ban from doing business in Iowa; (ii) placing additional safeguards and scam prevention requirements on the operation of BTMs in Iowa; or (iii) any other injunctive relief the Court deems necessary and equitable;

C. Adjudge the Defendants liable for civil penalties of $40,000 for each violation of the Iowa Consumer Fraud Act;

D. Adjudge the Defendants liable for additional civil penalties of $5,000 for each violation of the Iowa Consumer Fraud Act committed against an older individual; and

E. Order the Defendants to reimburse the full transaction amounts—including but not limited to the full cash or card amount processed through a BTM—to all Iowa consumers who (i) purchased Bitcoin through a BTM because they were a scam victim, (ii) would have been entitled to a refund under Bitcoin Depot's written refund policy, or (iii) attest they did not understand the total fees or price of Bitcoin at the time of their BTM transaction;

F. For all Iowa consumers entitled to reimbursement who cannot be located through reasonable efforts, order the Defendants to disgorge all related funds and property they acquired from those Iowa consumers through misrepresentations, deceptions, and unfair practices, and award the funds and property to the State to be used by the Attorney General under Iowa Code § 714.16(7);

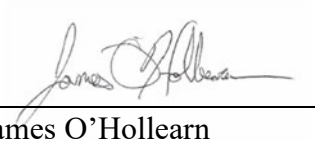
G. Award the State its costs and fees under Iowa Code § 714.16(11), including expert-witness expenses; costs incurred in pursuing this action and investigation, including reasonable attorneys' fees; and prejudgment and post-judgment interest at the highest lawful rates; and

H. Grant all other relief necessary or appropriate to remedy the effects of Defendants' acts or to which the State may be entitled.

Date: February 26, 2025,

Respectfully submitted,

BRENNA BIRD
ATTORNEY GENERAL



James O'Hollearn
Assistant Attorney General
William R. Pearson
Assistant Attorney General
Daniel L. Barnes
Deputy Attorney General for Consumer Protection
Hoover Building
1305 E. Walnut St.
Des Moines, Iowa 50319
(515) 281-6411
james.ohollearn@ag.iowa.gov
william.pearson@ag.iowa.gov
daniel.barnes@ag.iowa.gov

IN THE IOWA DISTRICT COURT FOR POLK COUNTY

STATE OF IOWA, *ex rel.* BRENNA BIRD, ATTORNEY GENERAL OF IOWA, Plaintiff, v. **GPD HOLDINGS LLC d/b/a COINFLIP,** Defendant.	Equity No. _____ **PETITION**

Table of Contents

The Appendix filed attached to this complaint is incorporated here by reference.

Introduction

1. Fraudsters and scammers update their deceptive practices to reflect new technology. Here, Defendants are misusing the popular excitement around technologies like Bitcoin and other cryptocurrencies to unfairly and deceptively put Iowa consumers in harm's way and take their piece of Iowans hard-earned money before sending the rest to scammers.
2. Cryptocurrencies are technologies often centered around recording transactions on a public register, or blockchain. The details of that technology can be complicated and nuanced. But what is not nuanced is using a veneer of association with cryptocurrencies to defraud consumers.
3. Defendant GPD Holdings LLC d/b/a CoinFlip (hereinafter "CoinFlip") profit when scammers profit because of the unfair and unsafe business practices easily allowing Iowans to send large sums of money to scammers—with a kickback to CoinFlip. So far, Iowa has identified more than $13 million in fraudulent, scam payments processed through Coinflip "Bitcoin ATMs" (defined below).
4. A cryptocurrency kiosk is a physical kiosk or automated machine that allows consumers to insert physical cash to buy purely digital or virtual cryptocurrencies. CoinFlip runs a type of cryptocurrency kiosk that it refers to as a Bitcoin ATM, or BTM. CoinFlip's BTMs—at issue in this Petition—allow consumers to buy various crypto currencies, including Bitcoin. BTMs allow a consumer to insert cash into the machine, convert that cash into Bitcoin, and then send that Bitcoin to a "digital wallet"—all for a fee(s).
5. Although CoinFlip states that it requires consumers to send Bitcoin they buy through a BTM to a digital wallet owned by the consumer, CoinFlip regularly allows purchased Bitcoin to be sent to a third party's digital wallet.
6. CoinFlip profits from the fees it charges to buy Bitcoin and send it to someone else. CoinFlip gets paid when a scammer tricks an Iowan into using a BTM to send Bitcoin. Some scams that brutally victimize Iowans and send them to a BTM are: (i) romance scams-- sending Bitcoin to a fake love interest met online, (ii) law enforcement scams—sending Bitcoin to a fake sheriff or U.S. Marshal to avoid criminal charges or arrest, (iii) refund scams—sending Bitcoin to return the fake overpayment of a refund from a large company, or (iv) tech-virus scams—sending Bitcoin to save the consumer's laptop from a fake virus.

7. Scam calls and text messages targeting Iowans (and all Americans), particularly the elderly, are on the rise. BTMs are one of the key tools used to scam Iowa consumers. Each successful scam using a BTM is revenue for CoinFlip.

8. CoinFlip is the second largest BTM operator in the world. It has placed BTMs at around 54 Iowa locations. Its machines can be found in gas stations, grocery stores, and vape shops. Based on the total amount of transactions at Iowa BTMs from January 1, 2021, to June 10, 2024, CoinFlip is the largest BTM operator in Iowa.

9. CoinFlip knows scammers frequently send fraud victims to its BTMs, but it fails to take meaningful action to protect Iowa consumers. That is because it is not in CoinFlip's economic interest to take meaningful actions to decrease fraudulent transactions. While CoinFlip reaps profits from Iowa consumers who are the victims of fraud, Iowa consumers are embarrassed and, even worse, face financial hardship, bankruptcy, social isolation, stress or depression after being scammed into using BTMs. Consumers overwhelmingly fail to receive any consumer or competitive benefit from BTMs.

10. CoinFlip's business model is so co-dependent on the success of scammers that there may be no way to operate a profitable BTM in Iowa that is not an unlawful act under Iowa's Consumer Fraud Act ("the Act").

11. Offering Iowans an unsafe money transfer service through a physical machine located in a gas station or vape shop to buy purely digital assets at unclear exchange rates and for high fees is not innovative or beneficial to consumers. Instead, it is an unlawful, "unfair practice" under the Act: "an act or practice which causes substantial, unavoidable injury to consumers that is not outweighed by any consumer or competitive benefits which the practice produces." Iowa Code § 714.16(1)(i).

12. The Attorney General's Office has reasonably found that scam transactions processed through Iowa BTMs between January 1, 2021, to June 10, 2024, totaled at least $13,182,625.

13. CoinFlip profited from those scam transactions. CoinFlip's policies for use of its BTMs do not adequately protect Iowa consumers or prevent scam transactions. CoinFlip also fails to follow its own inadequate policies. The existing policies; lack of their enforcement; and lack of additional, needed safeguards create an environment where the

"substantial unavoidable injury to consumers" far outweighs any "consumer or competitive benefits" that BTMs offer (if any). Iowa Code § 714.16(2)(a).

14. CoinFlip's business model also employs deceptive practices in its Bitcoin pricing. The cost to purchase Bitcoin at a BTM is often much higher than the cost to purchase on a cryptocurrency exchange, and CoinFlip does not want consumers to know the true cost. CoinFlip hides the cost to BTM consumers in a way that has a "tendency or capacity to mislead a substantial number of consumers as to a material fact or facts." Iowa Code § 714.16(1)(c). CoinFlip's flat fee of around $3.00 is relatively clear, but an additional "Transaction Fee" (as described below) increases the total fee to Iowa consumers to an additional amount in excess of 20% of the total transaction amount.

15. CoinFlip offers no refund policy related to scam transactions, further cementing CoinFlip's profits from Iowa scam victims and showing there is no release valve that could undo a portion of the harm Iowa consumers face from CoinFlip's unfair and deceptive acts or practices.

16. After increased complaints from consumers and law enforcement regarding Iowa scam victims who placed large sums of money into BTMs in the course of their victimization, the Attorney General's office initiated an investigation into the BTM operators in the State, including CoinFlip.

17. At best, CoinFlip is a willfully blind participant in the victimization of hundreds of Iowans. At worst, it is a silent partner to many scammers preying on Iowans, taking a cut of each scam with its excessive and deceptive BTM fees that are further paired with a no refund policy.

18. The State seeks a preliminary and permanent injunction under the Act to (i) enjoin Defendant from engaging in the deceptive and unfair acts described in this Petition whether that be by (a) a permanent ban from doing business in Iowa or (b) placing additional safeguards and scam prevention requirements on the operation of BTMs in Iowa; and (ii) impose all other injunctive relief the Court finds equitable.

19. The State also seeks civil penalties, reimbursement, disgorgement, and other costs and fees permitted by the Act given CoinFlip's deceptive and unfair conduct, which has harmed and continues to harm Iowa consumers.

I. Jurisdiction

20. This Court has jurisdiction over this matter under Iowa Code § 714.16(7).

21. This Court has jurisdiction over the Defendant under Iowa Code § 714.16 because the Defendant has transacted business within the state of Iowa at all times relevant to this complaint.

22. Polk County is the proper venue under Iowa Code § 714.16(10) because Defendant transacts business in Polk County through numerous physical BTM locations in Polk County. Additionally, transactions upon which this action is based occurred in and some victims reside in Polk County.

II. Parties

23. Plaintiff is the State of Iowa, *ex rel*. Brenna Bird, Attorney General of Iowa. Under Iowa Code § 714.16(7), the Attorney General may seek civil enforcement of the Iowa Consumer Fraud Act.,

24. Defendant GPD HOLDINGS LLC (d/b/a CoinFlip, Inc.) is a Delaware corporation with its principal place of business in Illinois and its executive offices located at 433 W. VAN BUREN STREET, SUITE 1050N, CHICAGO, IL, 6060. GPD HOLDINGS LLC is registered with the Iowa Secretary of State to do business in the State of Iowa under business number 638151. The company lists its registered agent as "UNITED AGENT GROUP INC." located at 3106 INGERSOLL AVENUE Des Moines, IA 50312.

25. At all relevant times, CoinFlip transacted business in Iowa by marketing, promoting, advertising, offering its services/products for sale which include allowing consumers access to its BTMs to purchase Bitcoin.

III. Factual Allegations

26. CoinFlip advertises itself as the owner of one of the largest BTM networks worldwide. CoinFlip claims that it operates a network of over 5,500 BTMs around the US and several other countries. *About Us*, CoinFlip, 2022, available at https://coinflip.tech/about (last visited Feb. 17, 2025). From January 1, 2021, to June 10, 2024, the company operated approximately 54 BTMs in Iowa.

27. CoinFlip uses retail partnership contracts to place its BTMs in convenience stores, grocery stores, liquor stores, vape shops, and gas stations.

28. CoinFlip reports it has conducted at least $4 billion in transactions since the company's inception with more than 500,000 customers. *Id*.

29. From January 1, 2021, to June 10, 2024, CoinFlip processed more than [redacted] transactions, totaling more than [redacted] in the state of Iowa. Over $13 million in transactions processed through a CoinFlip BTM have been identified as a scam transaction. The Attorney General has spoken to or analyzed data related to the top 20 users of CoinFlip's BTMs in Iowa (based on total BTM deposits during the time period). The transactions of all 20 users occurred because of a scam. These individuals alone represent over $7.3 million in transactions.

30. The Attorney General's office reasonably believes the number of scam transactions will only grow as more consumers are contacted.

31. Also, based on an analysis of data provided from CoinFlip and other data related to Bitcoin addresses and digital wallets, the Attorney General's office has reason to believe that at least [redacted] of CoinFlip's transactions are either fraudulent, sent from accounts that were later banned, or were sent to addresses later blacklisted (meaning flagged for fraud) by the company itself.

A. BTMs and Scams Go Hand-in-Hand

32. Cryptocurrency surged as a payment method for scams in recent years because it is portable and difficult to trace.

33. Widespread access to cryptocurrency kiosks including BTMs helps make this possible. Reported losses using cryptocurrency kiosks are overwhelmingly related to government impersonation, business impersonation, and tech-support scams. "New FTC Data Shows Massive Increase in Losses to Bitcoin ATM Scams." Federal Trade Commission, 3 Sept. 2024, www.ftc.gov/news-events/news/press-releases/2024/09/new-ftc-data-shows-massive-increase-losses-bitcoin-atm-scams.

34. Since most fraud is not reported, these numbers likely represent only a fraction of the actual harm. One study showed only 4.8% of people who experienced mass-market consumer fraud complained to a Better Business Bureau or a government entity. Anderson, Keith B. "To Whom Do Victims of Mass-Market Consumer Fraud Complain?" *SSRN Electronic Journal*, 2021, https://doi.org/10.2139/ssrn.3852323.

35. The Federal Trade Commission estimates that fraud losses at cryptocurrency kiosks have skyrocketed, increasing nearly tenfold from $12 million in 2020 to $114 million in 2023 and topping $65 million in the first half of 2024. Emma Fletcher, Bitcoin ATMs: A payment portal for scammers, FTC (Sept. 3, 2024), https://www.ftc.gov/news-events/data-visualizations/data-spotlight/2024/09/bitcoin-atms-payment-portal-scammers.

36. In the first six months of 2024, the median reported loss was $10,000 when using cryptocurrency kiosks, $5,400 when cryptocurrency was the reported payment method (including reports with and without using cryptocurrency kiosks), and $447 in general fraud cases. FTC data shows that older adults are less likely to report fraud than younger adults and have even higher individual median dollar losses. Protecting Older Consumers 2023-2024, A Report of the Federal Trade Commission at 17 (Oct. 18, 2024), https://www.ftc.gov/system/files/ftc_gov/pdf/federal-trade-commission-protecting-older-adults-report_102024.pdf. This is significant; as noted below, most Iowans using BTMs are age 60 or older.

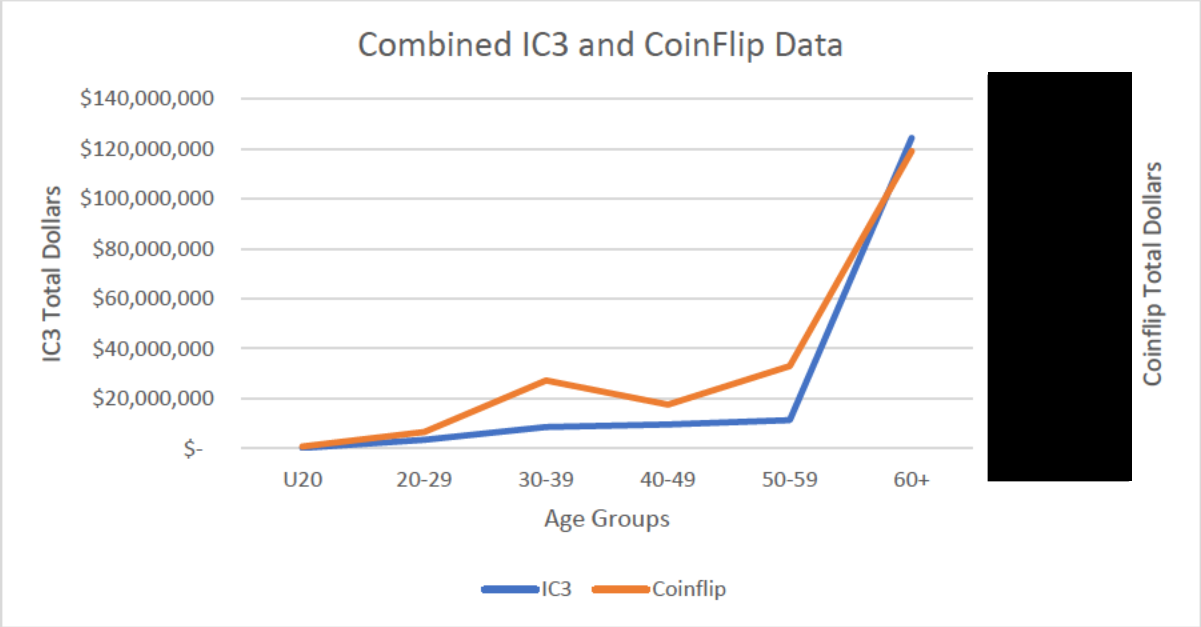
37. The following chart, created by the FBI's Internet Crim Complaint Center, shows reported scams and losses increase with age.

USE OF CRYPTOCURRENCY KIOSKS REPORTED IN IC3 COMPLAINTS – 2023

Age Range	Complaints	Losses
Under 20	65	$252,198
20 - 29	416	$3,529,680
30 - 39	451	$8,651,706
40 - 49	391	$9,634,346
50 - 59	476	$11,409,372
Over 60	2,676	$124,332,127

"2023 Cryptocurrency Fraud Report Contents," Internet Crime Complaint Center, available at https://www.ic3.gov/annualreport/reports/2023_ic3cryptocurrencyreport.pdf

38. Similarly, CoinFlip's transaction amounts increase by age as shown by the following chart that provides an overlay of what Iowa BTM transactions and IC3's Reported Losses to Fraud look like when broken into the IC3 chart's age brackets. As the chart shows, the trends for IC3 scam victims and Iowa BTM users closely and sadly align.



B. CoinFlip Represents Its BTMs are Safe and Trustworthy, But Allows Pervasive Scam Transactions Across Its Iowa BTMs

39. Contrary to its stated focus on fraud prevention, CoinFlip's records show its inability to prevent scam transactions processed through its Iowa BTMs. It is clear from CoinFlip's internal data that its policies and BTMs are causing Iowa consumers "substantial, unavoidable injury" that far outweighs any consumer or competitive benefits. Iowa Code § 714.16(1)(i).

40. CoinFlip publicly states the safety of its BTMs while scam transactions at Iowa BTMs continue to occur regularly.

41. In a blog post entitled, "Are Bitcoin ATMs Safe?" published on the company's website, the author states, "If you have cash and want to buy bitcoin, an ATM is a safe option."

42. In another blog post titled, "How to Buy Bitcoin with Cash Safely: Coinflip Bitcoin ATMs, the CoinFlip team writes: "CoinFlip Bitcoin ATM terminals are the safest and easiest solutions for cash cryptocurrency investments."

43. CoinFlip also states, "About 40% of Americans own crypto, and some like to use cash to buy and sell it. Crypto kiosks give consumers a safe and convenient way to do just that." The company claims it has robust controls: "Coinflip controls transactions from end to end, with robust Anti-Money Laundering and Know your Customer protocols, and efficient fulfillment of customer orders to reduce consumer's bitcoin price risk."

44. The following graphic sums up CoinFlip's position that its BTMs are safe and even goes a step further to state that CoinFlip's scam education at its machines "empower users to make informed decisions."

App. 4.

45. CoinFlip knows that many of the transactions it is asked to process are coerced or unwilling transactions initiated by or at the behest of scammers. CoinFlip's training and compliance documents speak at length about the dangers of money transfers, the prevalence of scams, and the various ways to identify potential scams.

46. Despite CoinFlip's public-facing statements about its concern for fraud or scams, reality paints a different picture.

47. Transactions where an individual sends money to a digital wallet that a different consumer has already sent money to are processed regularly, despite CoinFlip stating the wallet must be controlled by the person sending the money.

48. CoinFlip's records also show that from January 1, 2021, to June 10, 2024, $16,531,995 was transferred by Iowa BTM users who were later banned by the service. Many of these individuals simply created new accounts and continued using the service.

49. $12,955,025 was transferred by Coinflip during January 1, 2021, to June 10, 2024, to digital wallets that CoinFlip later placed on a blacklist. Coinflip's general operating

procedure for when an individual attempts to send money to blacklisted wallets is to simply ask them to use a different wallet.

50. CoinFlip's records include many other obvious warning signs of fraud, including:

a. *CoinFlip's consumer base is overwhelmingly older.* CoinFlip acknowledges in its training documents that, "one of the fastest-growing forms of fraud is elder financial exploitation." The document continues, stating, "people who are manipulated in this way often don't realize that they are victims." Despite this awareness and even though a large percentage of its Iowa BTM revenue comes from Iowans aged 60 or older, CoinFlip has failed to implement adequate policies to protect this vulnerable population. Whether intended or not, CoinFlip's typical user in Iowa is an older Iowan and a scam victim.

b. *Many CoinFlip users have multiple accounts.* CoinFlip knows that at least 311 Iowa BTM users with the same first and last name have at least two accounts. Most of these people have indicators that would suggest they are the same person (for example the same home address). One Iowa user has what appears to be 21 different distinct customer IDs. Coinflip records show that Iowa user used the same Coinflip machine (located in Des Moines) 21 times on 2 different days. Each transaction, occurring minutes apart, was for $900. Due to CoinFlip's poor screening, the user placed a total of $18,760 into a CoinFlip machine without ever triggering any higher review, or even the requirement to provide a government ID.

CoinFlip claims to apply heightened scrutiny to accounts over lifetime usage and must under the law make reports for unusual and/or suspicious activities involving transactions over certain amounts. Allowing a user to deceptively open multiple accounts enables him or her to evade such scrutiny.

c. *Multiple CoinFlip users sent money to the same Bitcoin address.* A Bitcoin address is a string of letters and numbers that functions like an email address. Bitcoin can be sent to that specific string of letters and numbers and the user at the other end can receive Bitcoin at that address. Like an email address, anyone who knows the address can send Bitcoin to that address. CoinFlip makes users verify that they own and control the Bitcoin address to which they send money. Every user must affirm the following: "I attest that I am sending my funds to a wallet I own or directly have

control over." The reason for this is because unlike cash in a bank account, a person holds the keys to where his or her Bitcoin is held. It is virtually impossible for someone else to access a Bitcoin wallet unless they have the wallet's credentials. Once Bitcoin is given over to someone it is very hard to take it back.

Nevertheless, CoinFlip routinely ignores the red flags it has identified to consumers and transfers money to addresses that (i) multiple users have claimed to "own" and (ii) CoinFlip's own data shows is claimed by multiple users and thus likely fraudulent.

From January 1, 2021, to June 10, 2024, Coinflip sent money from 10 distinct users to the same two Bitcoin addresses. The first address had 45 associated transactions from different users of $900 each transaction, for a total of $40,489. The second address had 51 associated transactions from different users of $900 each, for a total of $45,860. Data related to each address shows that the money was quickly transferred out of the wallet each time. Despite these clear violations of CoinFlip's user agreements and red flags for fraud, all 10 users were never flagged or banned from using CoinFlip services. All but one of the users was never required to enter a date of birth. Rather than notify the users, freeze the accounts, blacklist the wallets, or take any action to protect Iowans, the company continued to process the transactions making over $7,000 in fees to look the other way.

In data provided to the Attorney General's office, there are 586 Bitcoin addresses which had more than one distinct Iowa BTM user sending money to the address. If Iowa transactions were cross-referenced against CoinFlip's data from around the country that number will almost certainly increase. This is because the data examined by the Iowa Attorney General's office includes transactions occurring in Iowa at BTMs. It doesn't include the data CoinFlip has from its online sales, app sales, or from the other 5,500 or so BTMs not located in Iowa.

d. *Users have a large amount of Bitcoin addresses and are connected to multiple wallets.* A Bitcoin address can be thought of as an account holding all Bitcoin sent to it. Each Bitcoin address is associated with a digital wallet. The owner of the digital wallet is the owner of each Bitcoin address associated with that wallet. Of the more than 4,206 distinct user IDs who used CoinFlip's machines in Iowa from January 1,

2021, to June 10, 2024, approximately 2,025 of those Iowa consumers used more than one Bitcoin address, with 513 using 10 addresses or more. For example, one Iowa user and confirmed scam victim (age 74), was eventually blacklisted by CoinFlip, but not before he sent $291,075 on a CoinFlip BTM using 205 distinct addresses.

One reason for a person to have so many wallets is to ensure that if law enforcement finds or shuts one down, that the damage is limited. Or, if a company actually performing consumer protection duties flagged a wallet as likely belonging to a scammer, having more than 80 alternative wallets could be one way to skirt enforcement. For CoinFlip, a company by its own admission which typically serves less sophisticated users of cryptocurrency, older users depositing their money into numerous addresses linked to multiple wallets at CoinFlip BTMs should trigger further investigation by CoinFlip.

e. *CoinFlip allows users who are under 18 years old to use its services, despite its Terms of Service*. From January 1, 2021, to June 10, 2024, CoinFlip processed 36 transactions for Iowa BTM users who identified themselves as under 18. There is an additional $3,373,000 in transactions where CoinFlip did not require the user to provide a date of birth at all. It is clear that this is a feature of the service, and not a bug. In an interview, (then) Head of Business Development at Coinflip, Dustin Wei stated, "I got into crypto and ATM's specifically, because as someone who was under 18, it's kind of hard to buy crypto because I don't have a bank account, and when I did, they actually banned me because I was buying crypto with my bank account. So, my only resort was bitcoin ATMs. [CEO Daniel Polotsky interjects] "Was Coinflip" [Wei] Yeah exactly, was Coinflip." Crypto Campfire Podcast, *Crypto ATMs vs. Face-To-Face Bitcoin Trading, Finance Regulation, & 7-Toed Cats W/ CoinFlip* ATMs, YouTube, 1 Sept. 2019, www.youtube.com/watch?v=dcz3hrlqYps. This shows that CoinFlip is asleep at the wheel and not looking to enforce the policies in its Terms of Service including scam prevention.

C. CoinFlip's Policies Are Insufficient to Address the Known Issues Related to Scams

51. CoinFlip has several policies and programs related to fraud including, but not limited to, its "Compliance Program," its "Know Your Customer Policy," and its "Enhanced Due

Diligence Policy." These programs fail to adequately and effectively detect and prevent consumer fraud and scam transactions processed through CoinFlip's Iowa BTMs.

52. In addition to its anti-fraud program, CoinFlip is required by the Bank Secrecy Act to have an effective anti-money laundering ("AML") program to prevent money laundering. 31 C.F.R. § 1022.210. That prevention responsibility includes, but is not limited to, the flow of illicit funds, such as funds derived from fraud. As part of its AML program, CoinFlip has developed "Know Your Customer" guidelines and policies along with policies and procedures for monitoring transactions, customers, and agent activity for risks, including suspicious activity.

53. AML legal requirements are distinct from compliance responsibilities under the Act. But all policies implemented under the umbrella of AML have failed in preventing CoinFlip's business acts and practice from causing "substantial, unavoidable injury" to Iowa consumers. Iowa Code §714.16(1)(i). Those policies are either inadequate or ineffective due to CoinFlip's failure to enforce and follow the policies. Either way, CoinFlip's money-transfer system is an unfair or deceptive act or practice that is unlawful under the Act.

54. CoinFlip's primary training documents for employees outline its approach to scams. In its training on [redacted]

55. However, CoinFlip's practices make it clear that CoinFlip's goal is not to stop or interrupt scams, unless and until the scam victim admits to CoinFlip that he or she is in fact the victim of a scam (and it may take multiple admissions). If an individual does not admit so, CoinFlip's policy appears to be to disclaim and warn the user but to allow future transactions. Warnings are frequently given to consumers who are caught sharing accounts, using multiple accounts, and using wallets known to belong to third parties.

56. For example, CoinFlip's training document provides:

App. 78.

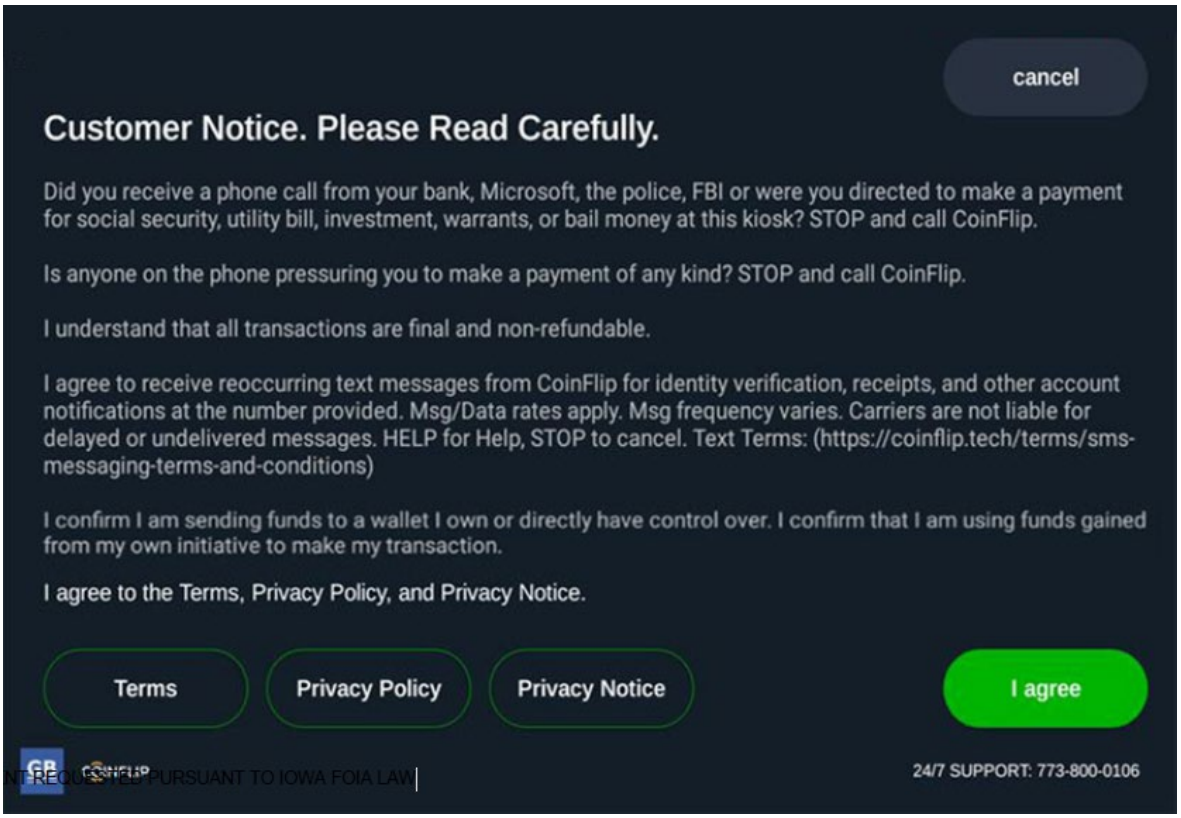
57. Even when an Iowa user is "banned" from using CoinFlip, he or she need only provide a new telephone, and even if he or she uses the same home address and date of birth, the user will be allowed to continue his or her use of CoinFlip's services.

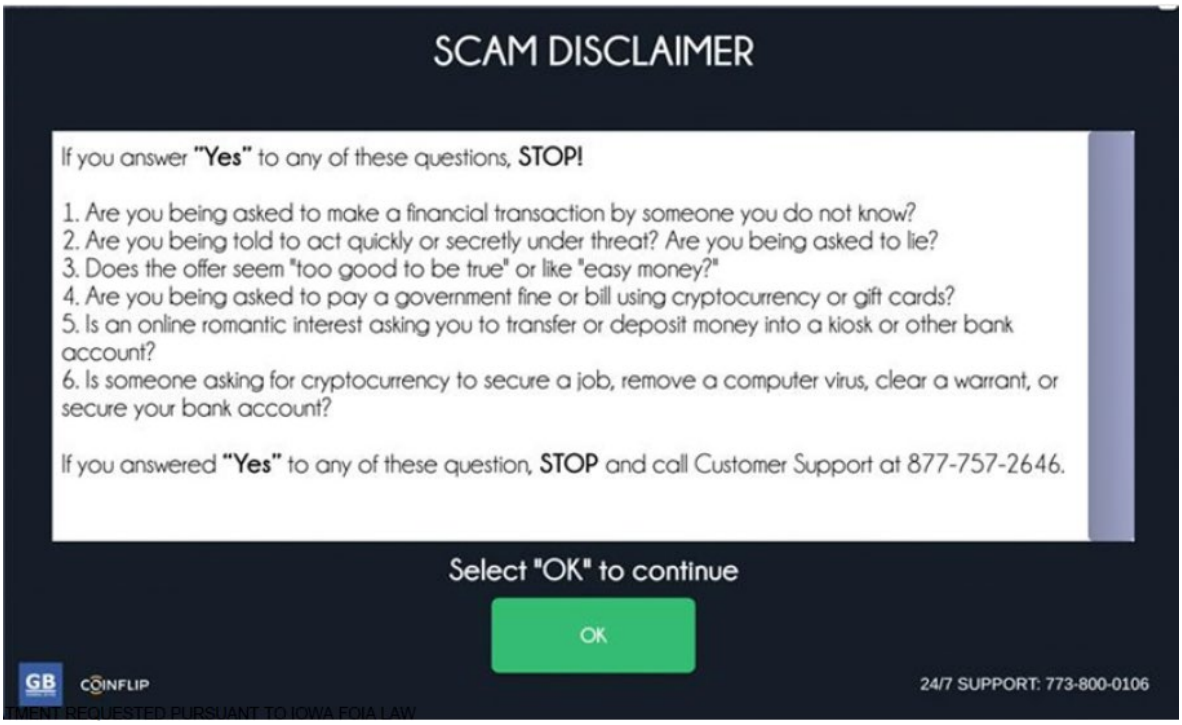
58. Further, CoinFlip is more interested in protecting itself (and its bottom line) than protecting Iowa consumers and preventing scams.

59. Rather than take a protective and proactive approach to preventing prevalent scam transactions across Iowa BTMs, CoinFlip chooses to simply show a vague warning to victims and make clear to them that there will be no recourse or refund for them when they eventually realize that they are another Iowa scam victim that used a CoinFlip BTM. *Id*.

D. CoinFlip's Warnings Are Ineffective at Preventing Scam Transactions

60. CoinFlip's primary method of preventing scam victims from using a BTM is to place onscreen warnings and sticker warnings on the machine. Below are examples of the warnings:





61. These warnings are insufficient to protect Iowa scam victims and CoinFlip knows it. CoinFlip only needs to look at its data as the proof is in the pudding. A review of the best studies on warnings, shows that scammers disrupt a person's ability to reason and in the moment warnings often fail. A Review of Scam Prevention Messaging Research, Federal Trade Commission, available at: https://consumer.ftc.gov/system/files/consumer_ftc_gov/pdf/A%20Review%20of%20Scam%20Prevention%20Messaging%20Research.pdf. The sheer volume of transactions confirmed as scams to date show this method is ineffective. CoinFlip does not often call to speak with its customers to prevent a scam even in most scenarios raising a red flag. Something as easy as a call could make a major difference as noted by a scam victim in a recent news story who (i) said it was possible there was a warning on the machine he skipped passed, and (ii) went on to state "If somebody called me and said, 'Wait a second, what are you doing? Why are you putting in so much money, and do you have more money you're going to put in?' that would have saved me. . . ." "To fight scams, Senate bill would limit transactions at crypto ATMs," *available at*, https://www.nbcnews.com/news/us-news/senate-crypto-atm-bitcoin-scam-rcna193495 (last accessed February 25, 2025).

E. The Demographic Markets in Iowa for Scam Victims and BTMs Are Older Iowans

62. CoinFlip competes with online exchanges, which sell consumers Bitcoin at a significantly lower net cost than CoinFlip BTMs. CoinFlip targets less sophisticated users who prefer to use cash. It often describes its target audience as the unbanked or underbanked.

63. Then Chief Operating Officer and Current CEO and cofounder of the company, Ben Weiss, described the target audience as follows:

> "There was this issue of how hard it is to get bitcoin, especially if you don't have a bank account, or if you're unbanked or if you just want to buy fifty dollars, a hundred dollars. So, we saw the need for the ATMs and we saw all these unbanked and underbanked communities who were kind of being left out of this financial revolution that was supposed to be a democratizing force, so that's why we went the ATM route instead of the exchange route." Crypto Coin Show, *Blockchain Interviews - Ben Weiss, COO of CoinFlip Bitcoin ATMs*," *YouTube*, 13 Oct. 2020, www.youtube.com/watch?v=iBORlRY6sm4.

64. In the same interview, he states, "A lot of these people who are going to the ATMs are beginning investors, they want to get into bitcoin, but you know they need more support, more customer service than someone who's been doing this for five or six years." *Id*.

65. Mr. Weiss has also stated, "We wanted to make it for the average consumer. Like my mom, she writes checks. She goes into bank branches. We didn't see any equivalent of that for cryptocurrency." Fintech Nexus, "Podcast #77: Ben Weiss of Coinflip." *YouTube*, 25 Jan. 2023, www.youtube.com/watch?v=HyCNY6rv02Q.

66. Cofounder and (at the time CEO) Daniel Polotsky stated, "I would say a plurality of people, like 40 to 50 % are just buying and holding. And not doing anything, just speculating on the price, and using it as their bank, which I think is cool." Polotsky explained "I don't think bitcoin is ready to be spent on low ticket items because the price is too volatile.... It's a little too volatile."

67. Polotsky also stated, "I think right now, that people definitely do use bitcoin to buy things, but it's more like high ticket items like Ferraris or Lambos or houses, you know, it's not like for a bag of chips."

68. However, the data from CoinFlip tells a starkly different story:

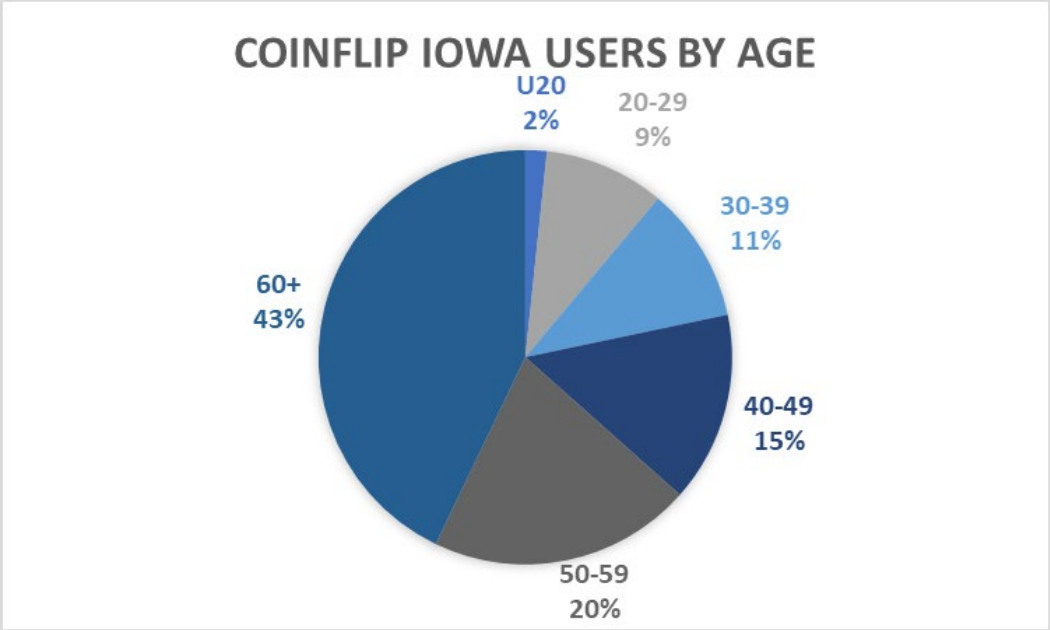
a. Its business model depends on a small number of high-volume users;

b. Its primary audience is, in fact, older individuals with large sums of assets who bank; and

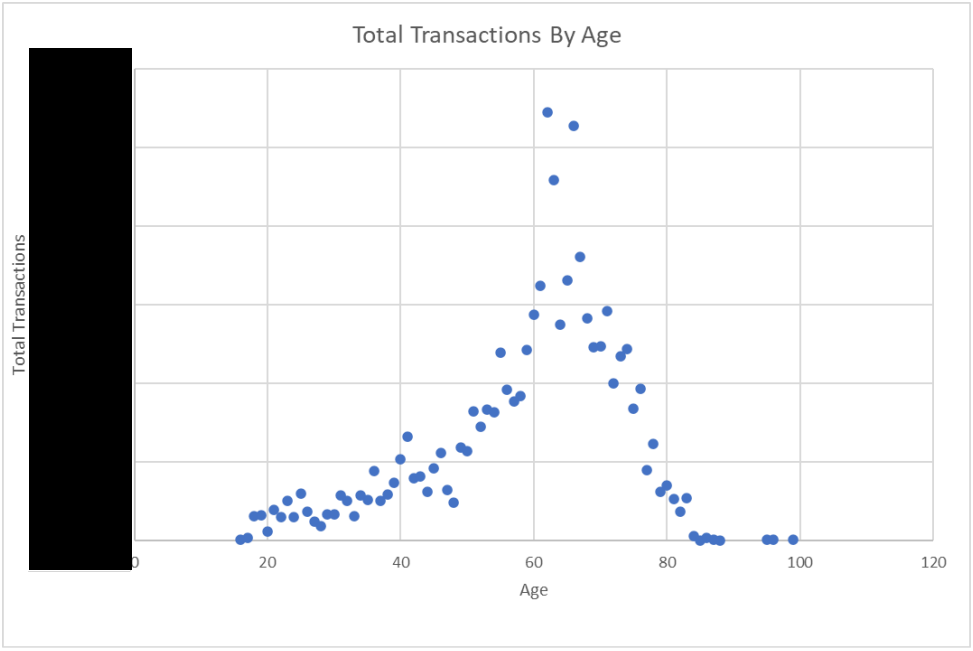
c. Most of its largest customers (by total transaction amount) use dozens of bitcoin addresses and wallets, often quickly transferring the money out of the wallets into a wide variety of foreign based exchanges.

69. The top 20 percent of Iowa users by total transaction(s) size accounted for [redacted] of all money processed through CoinFlip's Iowa BTMs from January 1, 2021, to June 10, 2024. The bottom 60% of Iowa users account for 15% of all money put into CoinFlip's BTMs.

70. The chart below was created using CoinFlip's data provided to the Attorney General's office. It shows a breakdown of CoinFlip's Iowa users from January 1, 2021, to June 10, 2024, by age. Approximately 43% of its users in Iowa are 60 years old or older.



71. The targeting of older Iowans becomes even more evident when shown as the total amount of money placed into CoinFlip's Iowa BTMs between from January 1, 2021, to June 10, 2024, based upon the age of the customer, as shown below:



72. Older Iowans use BTMs the most. Though Iowans who are 60 years old or older represent 43% of users, 58% of the money CoinFlip took from Iowans from January 1, 2021, to June 10, 2024, came from individuals in this group. 62-year-olds put the most money into Iowa Coinflip BTMs, accounting for approximately [redacted]. The average age of CoinFlip's top twenty users in Iowa is 67.4 years old. 78-year-olds were the age group with the highest average amount per customer of approximately [redacted].

73. CoinFlip and scammers are both profiting from older Iowans.

F. CoinFlip's Profitability in Iowa Depends on Iowa Scam Victims

74. CoinFlip could do more to prevent scam transactions, but such policies would reduce its profits:

a. *CoinFlip Underutilizes Bitcoin Tracking Capabilities***.** Inherent in Bitcoin is the ability to track Bitcoin transactions, as every transaction is recorded in the currency. CoinFlip has access to Elliptic software, which traces Bitcoin transactions. Elliptic uses a mix of proprietary and publicly available tools to follow the money. CoinFlip could use Elliptic to identify and stop scams faster and at a higher rate. But rather than stopping suspicious transactions, employing blockchain analytics software to analyze transaction patterns, or questioning users, CoinFlip collected fees.

CoinFlip's internal data provides examples of how easily it could detect and stop scams, even using publicly searchable digital wallet databases instead of the

expensive software CoinFlip already has. The Attorney General's office has employed similar software on many of CoinFlip's largest customers and identified many clear indicators of fraud. For example, one older Iowan interviewed by the Attorney General's office claimed he was not a victim of fraud. He claimed that he put $151,000 into a CoinFlip BTM to help fund orphanages in Africa. The Attorney General's office analyzed the five Bitcoin addresses he sent the most money to and found the addresses were tied to a porn site, an online gambling site, and Russian and Iranian based fraud shops. When the Attorney General approached the elderly man with this information, he admitted he was in a romance scam and was too ashamed to initially tell the truth.

b. *CoinFlip Fails to Use its Machine's Surveillance Abilities.* Each BTM has an internet-connected video camera that can be accessed by CoinFlip remotely. Its policies allow CoinFlip's compliance teams to monitor transactions and prevent people who are posing as others or using multiple aliases from using the machine.

Many fraudsters maintain continuous phone contact with their victims so that they can keep them in a state of emotional distress. Few willing users attempt to use a BTM while on the phone, as entering information and placing physical bills into the machine generally requires two hands and the machine sends a text message as part of the transaction. CoinFlip could monitor Iowa consumers to identify clear red flags – such as being on the phone while using the machine – and further verify the transaction is legitimate in those circumstances.

c. *CoinFlip Provides No Training to Its Store Locations on How to Spot Scams.* Store clerks could be a key line of defense against fraud. The Attorney General's office spoke with a store clerk who said she often sees older people attempting to use the BTM located in her store. When she sees an older person with a stack of $100 bills come in and he or she is on the phone or looks scared, she will speak to the individual and convince them that he or she is being scammed.

Yet, CoinFlip's lease agreements with these stores show that their focus is on making sure the stores protect CoinFlip's BTMs, not its customers. The contracts come with many requirements to make sure the BTM is available to consumers and none requiring the store to assist Coinflip in identifying scam victims. CoinFlip does

not appear to warn these locations of the danger that its machines are utilized in fraud or provide any training documents for the stores to be better equipped to help CoinFlip protect its consumers. Though CoinFlip doesn't help the stores protect its consumers from fraud, CoinFlip is quick to use its agreement to protect itself from liability for such fraud. The lease agreement attempts to protect CoinFlip from liability to the stores in the event of theft, vandalism, criminal acts, or a host of other eventualities.

G. CoinFlip Profits From Iowa Scam Victims

75. From January 1, 2021, to June 10, 2024, CoinFlip retained 10.86% of all money processed through its machines in Iowa. In total CoinFlip made more than $5.4 million from Iowans, with millions of that money likely coming directly from scam victims.

76. So far, the Attorney General's office has reviewed data for CoinFlip's self-identified scam victims and contacted CoinFlip's Iowa BTM users. Of hundreds of people contacted, approximately 90% reported they were victims of a scam. All 20 of CoinFlip's top 20 users of Iowa BTMs by total transaction(s) size for January 1, 2021, to June 10, 2024, have been confirmed by the Attorney General's office to be scam victims.

77. Currently the total transaction value of confirmed scam transactions in Iowa from January 1, 2021, to June 10, 2024, is $13,182,625.

78. The Attorney General's office reasonably believes this amount to rise significantly as more individuals are contacted and further forensic analysis is completed.

79. CoinFlip started as a business that attempted to compete on price. One of the inspirations for starting the company was that competitors charged such excessively high fees. Talking about his first time using a bitcoin ATM prior to starting the business, CoinFlip CEO Daniel Polotsky said "I went to the first ever bitcoin atm. The fees were crazy, it was probably like 12 percent." Funky Crypto Podcast, 39: Daniel Polotsky CEO and Founder of the Fastest Growing Crypto ATM Company Coinflip ATM., Sep. 17, 2020. https://open.spotify.com/episode/5AWInN4d5eRO3WERNBNJ3p.

80. Most businesses as they mature and are faced with competition must respond with lower prices. CoinFlip has more than doubled its rates (raising it six times) in the last 4 years without meaningfully changing the services offered at its BTMs.

81. CoinFlip's combined fees to purchase Bitcoin through its machines is currently up to 21.90%, more than triple what the fees were when CoinFlip was a startup company.

82. At the same time, it has never been easier to buy Bitcoin elsewhere. Direct competitors have dramatically expanded their footprints (Bitcoin Depot, Athena, and RockitCoin to name a few), online crypto exchanges (Coinbase, Kraken, Binance) have improved their services, popular investment platforms (Fidelity, Charles Schwab, Robinhood) have added the ability to buy cryptocurrency, and payment apps (CashApp, Venmo, and PayPal) have added options to buy and sell crypto.

83. Current CEO and cofounder of the CoinFlip, Ben Weiss, explains CoinFlip's growth and competitive advantage to charge high fees are a result of: "The ethos of being there for the customer every step of the way no matter how much or how little they know about crypto and about technology, and having our 24/7 customer support, I think it's that unique white glove service that we offer that has allowed us to continue to grow throughout these years." Fintech Nexus. "Podcast #77: Ben Weiss of Coinflip." *YouTube*, 25 Jan. 2023, www.youtube.com/watch?v=HyCNY6rv02Q.

84. However, CoinFlip's own internal data makes it clear that its "competitive advantage" is its symbiotic relationship with scammers. The scammers manipulate unwitting Iowans into using CoinFlip's BTMs, unaware that they are being scammed and unaware they are being charged exorbitant rates. The scammers get the lion's share of an Iowa victim's money. CoinFlip, acting as the getaway vehicle, retains an ever-increasing percentage of the stolen money.

H. CoinFlip Hides the True Cost of Using a BTM From Iowa Consumers

85. CoinFlip engages in deceptive practices to conceal what it really charges an Iowa consumer to buy Bitcoin, including by:

a. Combining all three of its online, app, and kiosk services in its Terms of Service document presented to BTM users, so BTM users find it harder to determine which sections apply to them.

b. Calling the product a "Bitcoin ATM" and charging a "flat fee" around $3, which confuses Iowans into thinking they are paying only around $3.

c. Burying any explanation of the total actual fees (currently up to 21.90%) in the Terms of Service.

d. Displaying information on screens and receipts in a way that increases the likelihood a consumer will not learn the true cost of the service.

86. Many Iowa consumers we interviewed were unaware of the amount of money they were charged to use the CoinFlip machines or under the impression that they paid a small service fee similar to a traditional bank ATM. CoinFlip encourages this belief by hiding the fees in an ambiguous "Transaction Fee" that is buried in its complex Terms of Service. However, CoinFlip makes sure to clearly highlight it's small "flat fee."

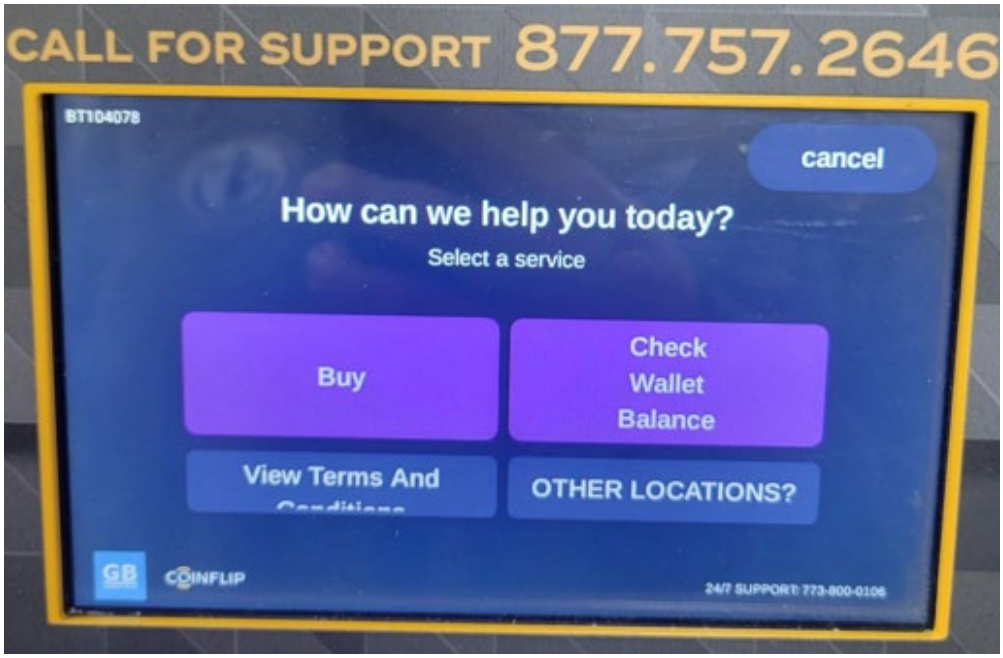
87. The cost of a product or service is a material term to a transaction. CoinFlip hides that material term related to its BTMs transactions in fine print that is confusing and designed to go unnoticed by Iowa consumers. CoinFlip interacts with Iowa consumers in three ways: at a BTM, online, and through its app. CoinFlip's Terms of Service are different for each service, but rather than have separate terms of service for each, CoinFlip combines all three into one document. This forces consumers to scan an array of terms in an attempt to understand which may apply to their transaction.

88. Pew Research estimates that 22% of Americans either always or often read terms of service. 36% say they never read the terms of service. Auxier, Brooke, et al. "Americans' Attitudes and Experiences with Privacy Policies and Laws." Pew Research Center: Internet, Science & Tech, Pew Research Center: Internet, Science & Tech, 15 Nov. 2019, www.pewresearch.org/internet/2019/11/15/americans-attitudes-and-experiences-with-privacy-policies-and-laws/.

89. CoinFlip has the capability, if it wants, to track the time a person spends on screen and can monitor the person in real time using a camera on the machine, if desired. It knows that the vast majority of CoinFlip customers are not reading the Terms of Service to learn of the true fee structure. CoinFlip counts on consumers assuming the machine is like most traditional bank ATMs and that the fee to purchase Bitcoin at an Iowa BTM is the prominently displayed "flat fee."

90. It is useful to view what a CoinFlip transaction looks like to an Iowa consumer. The following images were taken by the Attorney General's office at a CoinFlip BTM.

91. After the BTM asks an Iowan to select a "Crypto Currency," it shows the user the following screen, which includes an obscured "View Terms and Conditions" button.



92. If the Iowa user clicks the partially obscured button, he or she can then scroll through the lengthy Terms of Service viewed through a narrow portion of the overall screen to learn the details of the fee schedule.

93. Assuming an Iowan clicked on the "View Terms and Conditions" button, he or she would need to scroll to page 9 of 33 to locate the appropriate fee language. The Terms of Service include three different Fee schedules: "Fees at Kiosks and Cashiers," "Fees for Coinflip Preferred Order Desk," "Fees in the App." There is then a paragraph that is titled "Market Price" that presumably applies to all three of the different Fee schedules included. The Fee and Market Price sections are as follows:

Fees

Fees at Kiosks and Cashiers

You agree that by transacting at a Kiosk the Company may charge, and You will pay, a Transaction Fee and a Network Fee for each transaction You make. The Transaction Fee is calculated as a percentage of Your total transaction amount and ranges from 4.99% to 21.90% of the total transaction amount. The Network Fee is a fixed fee that does not depend on the size of Your transaction. The Transaction Fee and Network Fee are included in the exchange rate applicable to Your transaction. Before You make a transaction, we will tell You the exchange rate applicable to Your transaction. By proceeding with the transaction, You agree to

pay the exchange rate, including the Transaction Fee and Network Fee, and You agree to the other terms applicable to the transaction as set forth in these Terms. If You do not agree, You may not proceed with the transaction and must immediately discontinue Your use of the Services for that transaction.

The Transaction Fee is calculated as a percentage over the Market Price, as discussed fully in the paragraph above. The Transaction Fee and Network Fee are included in the exchange rate applicable to Your transaction. Before You make a transaction, we will tell You the exchange rate applicable to Your transaction. In other words, the Company will tell You: (1) the amount You must pay in fiat currency to purchase a certain amount of cryptocurrency from the Company or (2) the amount the Company will pay You in fiat currency to purchase a certain amount of cryptocurrency from You. By proceeding with the transaction, You agree to pay the exchange rate, including the Transaction Fee and Network Fee, and You agree to the other terms applicable to the transaction as set forth in these Terms of Service. If You do not agree, You may not proceed with the transaction and must immediately discontinue Your use of the Services for that transaction.

Fees for Coinflip Preferred Order Desk

You agree that CoinFlip Preferred may charge, and you will pay between 0.50% to 9.99% over the Market Price for purchases and be paid approximately 0.50% to 9.99% under the Market Price for sales of cryptocurrency (the "Transaction Fees"). The Transaction Fee and Network Fee are included in the exchange rate applicable to your transaction. Before you make a transaction, we will tell you the exchange rate applicable to your transaction. In other words, CoinFlip Preferred will tell you: (1) the amount you must pay in fiat currency to purchase a certain amount of cryptocurrency from CoinFlip Preferred or (2) the amount CoinFlip Preferred will pay you in fiat currency to purchase a certain amount of cryptocurrency from you. By proceeding with the transaction, you agree to pay the exchange rate, including the Transaction Fee, and you agree to the other terms applicable to the transaction as set forth in these Terms of Service. If you do not agree, you may not proceed with the transaction and must immediately discontinue your use of the CoinFlip Preferred service for that transaction. By completing your

transaction, you acknowledge that you have been presented the exchange rate applicable to your transaction and have agreed to it, including the Transaction Fee.

Fees in the App

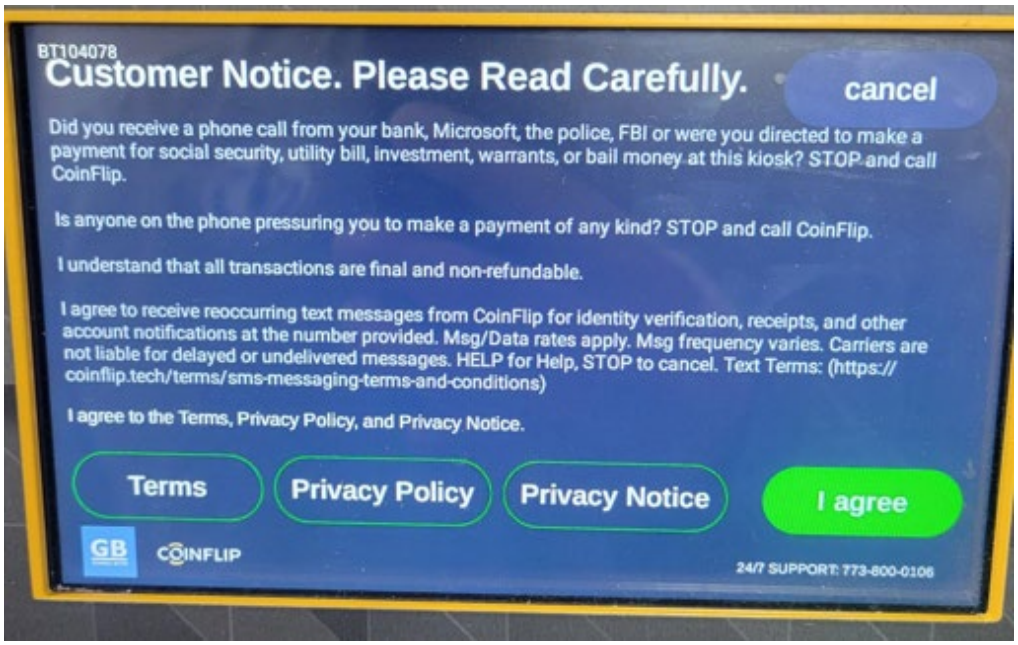
For purchases in the App, You will be required to pay a Processing Fee, a Transaction Fee, and a Network Fee. The Processing Fee is calculated as a percentage over the Market Price, as discussed fully below. The Processing Fee will be different based on whether You complete a transaction using debit, credit, or ACH. Before You make a transaction, we will tell You the exchange rate applicable to Your transaction and all applicable fees, including the Processing Fee, Transaction Fee, and Network Fee. By proceeding with the transaction, You agree to pay the exchange rate, including the Transaction Fee, Processing Fee, and Network Fee, and You agree to the other terms applicable to the transaction as set forth in these Terms of Service. If You do not agree, You may not proceed with the transaction and must immediately discontinue Your use of the Services for that transaction.

Market Price

The Company uses CoinAPI indexing to determine the Market Price. The Company reserves the right to use a different source without notice to determine Market Price for any reason. By transacting with the Company, You waive any claims or liability against the Company based on the manner in which the Company determines the Market Price.The Company also charges a minimum $2.49 Network Fee. "Network Fee" shall mean the minimum $2.49 fee applied towards the required payment to use the applicable blockchain to send Your selected cryptocurrency to Your cryptocurrency wallet. Due to the nature of how the Company processes customer transactions, the Company may periodically profit from the Network Fee. During times of high transaction volume, the Network Fee may be increased. By transacting with the Company, You waive any claims or liability against the Company based on the charged Network Fee." App. 113-114.

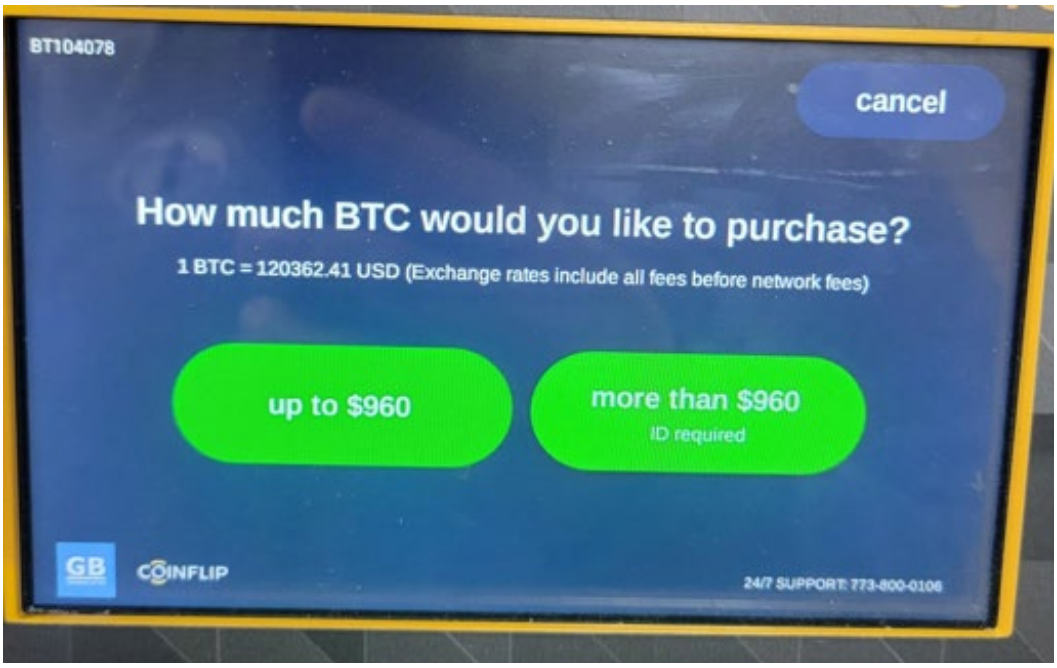
94. It is not easy for an Iowan consumer to decipher the cost of purchasing Bitcoin through a CoinFlip BTM.

95. The next screen (below) shows more signs of confusing Iowa consumers. It has a lengthy "Customer Notice," along with options to view "Terms," "Privacy Policy," and "Privacy Notice." The button to continue is bright green and placed in a position most likely to be pushed.



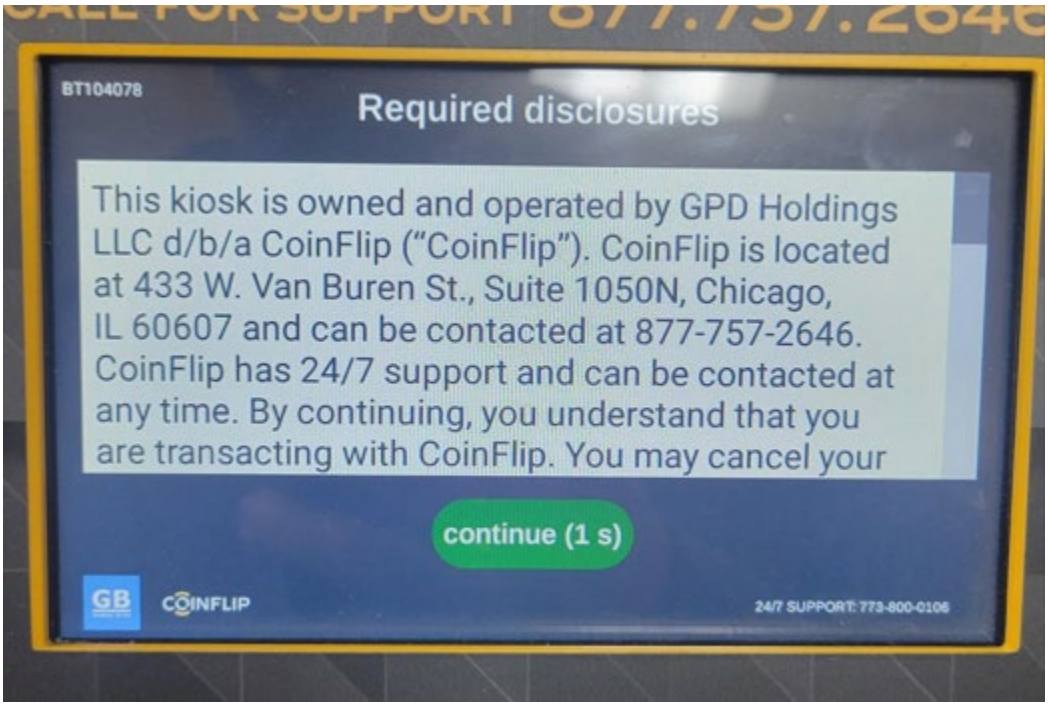
96. Next is the "Scam Disclaimer" screen (included earlier in this Petition) followed by a screen that asks the Iowa consumer how much Bitcoin he or she would like to purchase. The screen (below) notably tells the consumer that "the exchange rates include all fees before network fees." It is unclear what exchange rates this refers to or why the word

"rates" is pluralized.

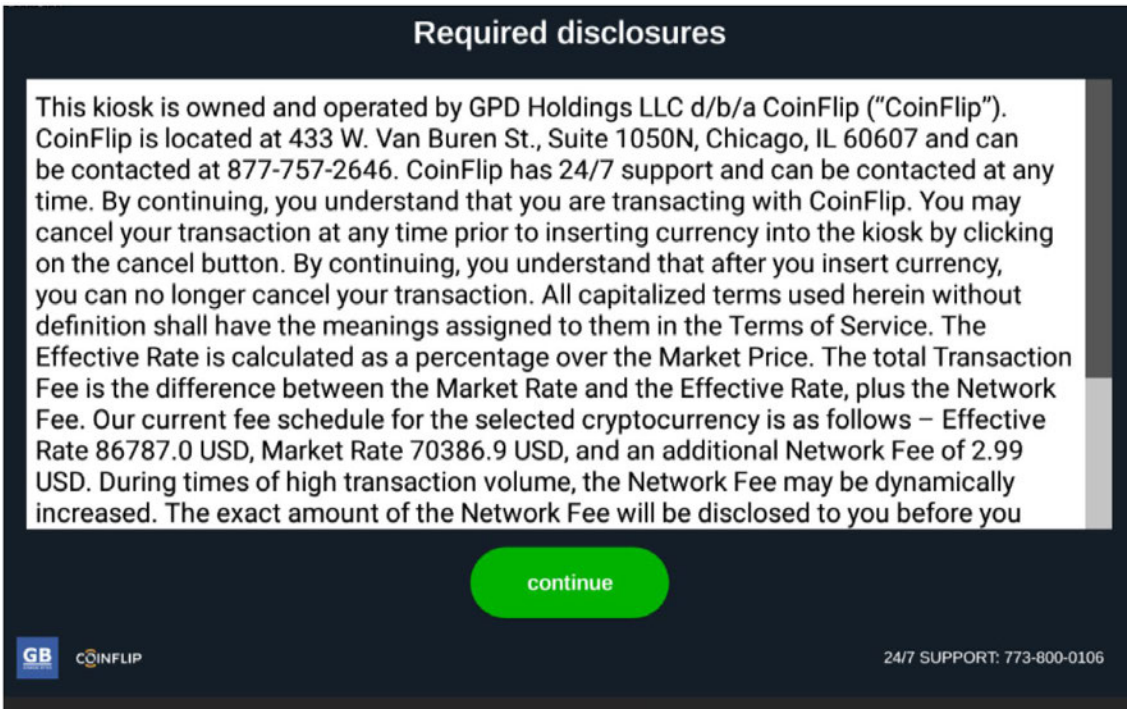


97. The Iowa user must then enter his or her "mobile number," a one-time SMS passcode the machine sends to the number, and the Iowan's name and a date of birth.

98. Iowans are then shown the following screen which again gives the user the option between scrolling through dense language or clicking a bright green button:



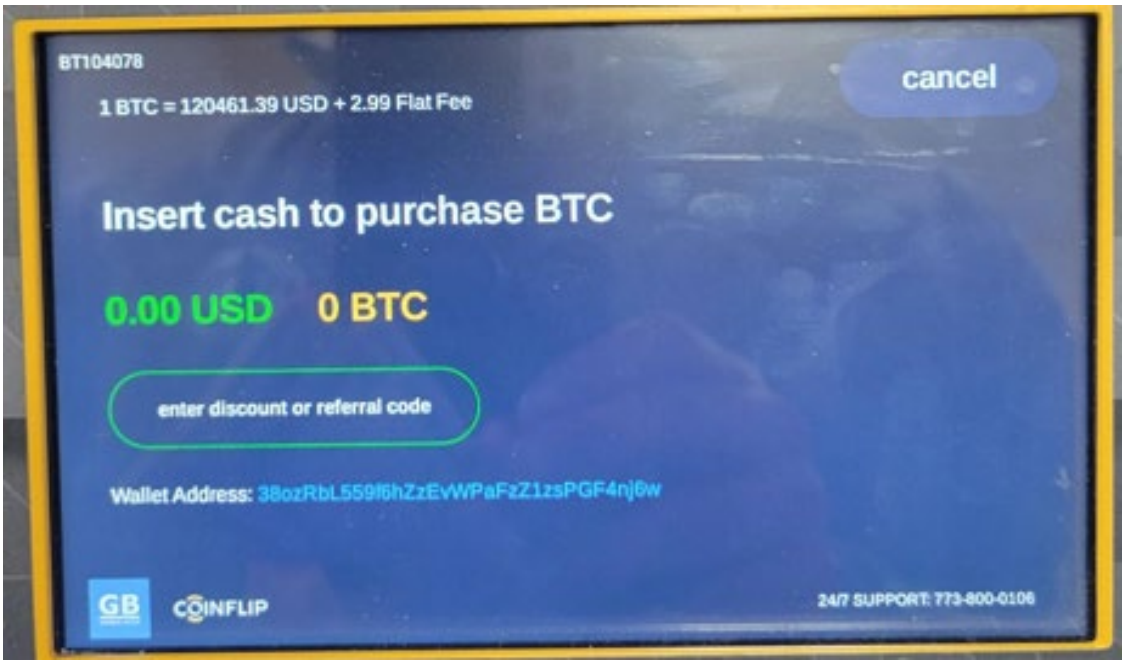
99. If the consumer were to scroll down, the Iowan would find something like the following: "All capitalized terms used herein without definition shall have the meanings assigned to them in the Terms of Service. The Effective Rate is calculated as a percentage over the Market Price. The Total Transaction Fee is the difference between the Market Rate and the Effective Rate, plus the Network Fee. Our current fee schedule for the selected crypto currency is as follows – Effective Rate 86787.0 USD, Market Rate 70,386.9 USD, and an additional Network Fee of 2.99 USD." The below photo is from CoinFlip's documentation submitted to the Attorney General's office.



100. Assuming the consumer scrolled through and understood the complex information, the consumer now has all of the variables needed to complete the Algebraic equation to calculate the fees to purchase Bitcoin.

101. To calculate the fees, an Iowan consumer must take the money to be inserted into the BTM (in this example $20) and subtract the $2.99 network fee (to get 17.01). The consumer then needs to divide the market rate of bitcoin (70,386.9) by the effective rate that Coinflip is charging 86,787 (which is 0.81103). Lastly, the Iowan needs to multiply $17.01 by 0.81103 to learn that Coinflip will be sending $13.80 in Bitcoin to an address and retaining $6.20 for themselves in fees.

102. The next screen prompts the user to scan in a Bitcoin address using a QR code scanner. After the address is inputed, the consumer is prompted to enter money into the machine.

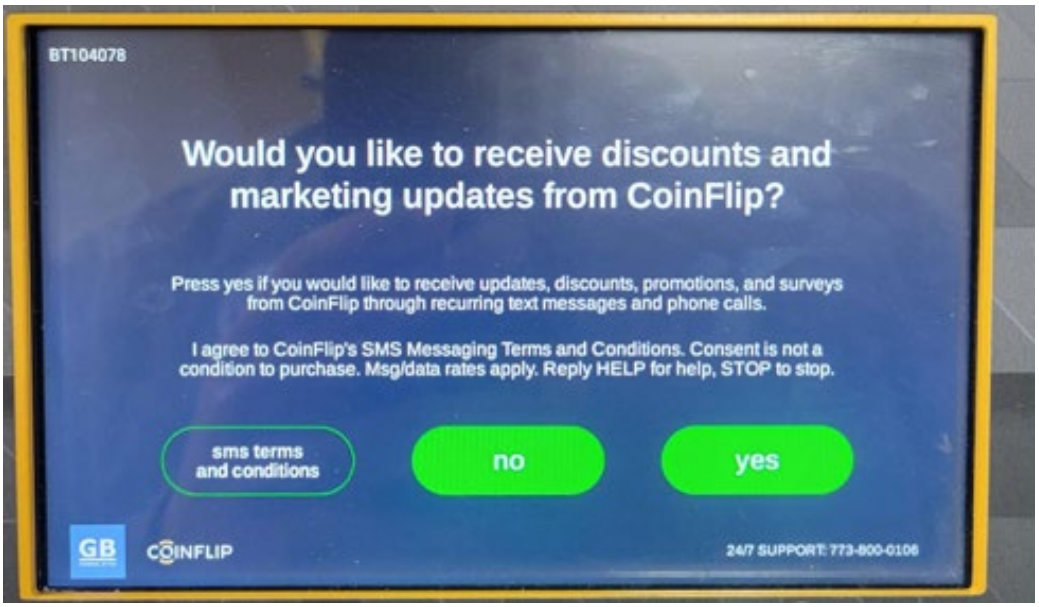


103. The top of the screen reads 1BTC=120461.39 USD +2.99 ***Flat Fee***. The term "Flat Fee" is not found anywhere in the Terms and Conditions or any other disclosure.

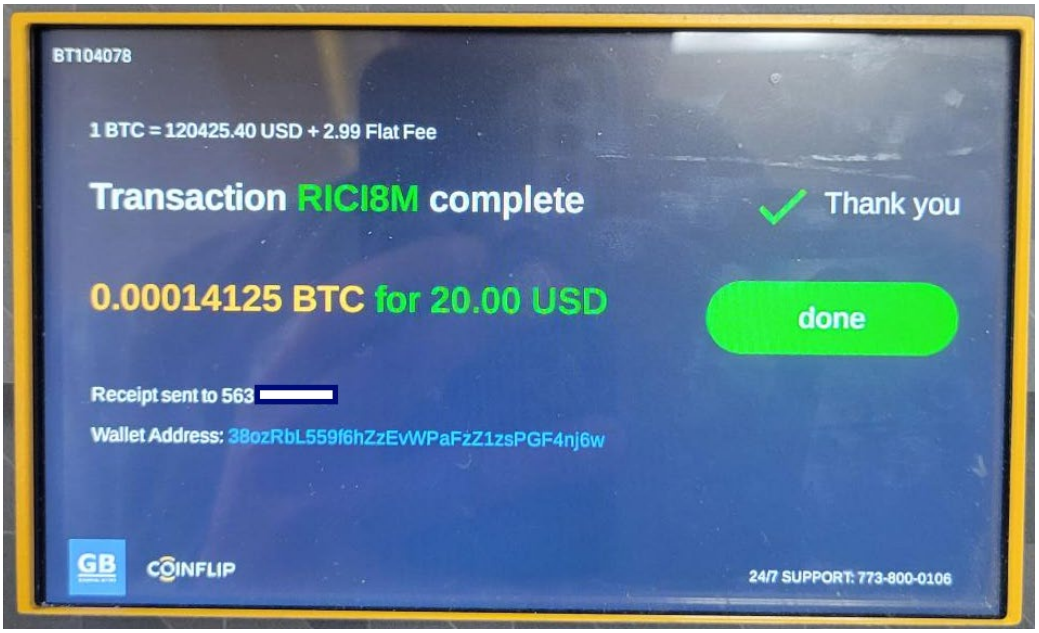
104. Presumably, CoinFlip is referring to the "Network Fee." However, by using the phrase "Flat Fee," an Iowan could easily believe he or she is being charged only $2.99 as a flat fee to use a CoinFlip BTM.

105. So not only is the calculation to determine the fees of Bitcoin at a Coinflip BTM deceptive by virtue of being hidden and subject to a string of complex math formualas, CoinFlip uses the phrase "flat fee" to further hide the cost.

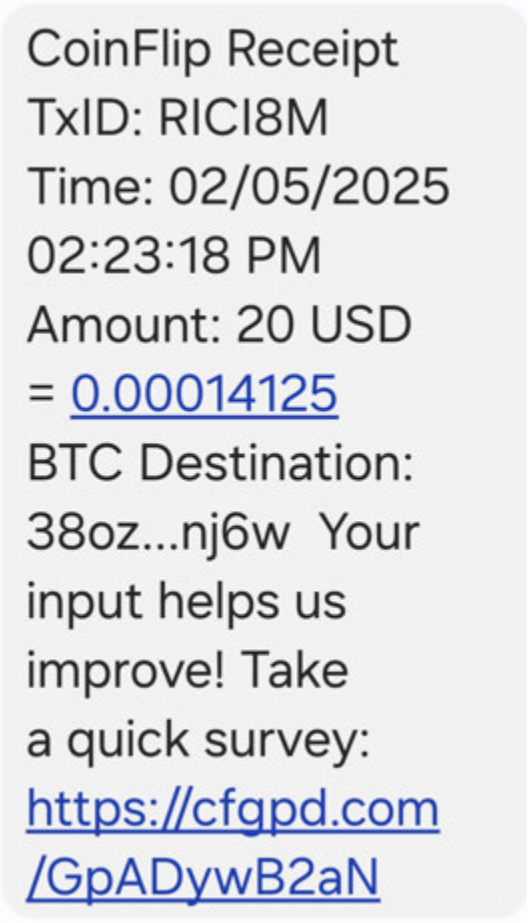
106. The consumer is then asked to opt in to marketing updates and offered the opportunity to read yet another legal document (the "SMS terms and conditions").



107. Finally, an Iowa user sees a screen showing a total transaction where $20.00 was translated into .00014125 of bitcoin.



108. A text "Receipt" is sent to the user's phone. The receipt does not contain any information regarding the fees paid by the consumer. (See below).



109. Coinflip's user interface is designed to make reading the Terms of Service tedious and difficult, while simultaneously making it easy and intuitive for the consumer to skip the terms entirely.

110. CoinFlip's leadership acknowledges that many of its customers are not sophisticated when it comes to their understanding of Bitcoin, and yet it hides material details of the transaction among legal jargon and behind partially obscured buttons.

111. CoinFlip could easily express the full cost of its service as a US dollar amount on the screen and receipt, as many of its competitors do, but it doesn't because doing so would alert the consumer to the high cost of the service and make them less likely to use CoinFlip's service.

112. CoinFlip's website shows its obfuscation of the fees is intentional. The Terms of Service states the fee ranges from 4.99% to 21.90% and the fee you will pay is unknowable until you are at the machine (which as stated above is hidden below a scrollable window and long legal jargon). Outside of the Terms of Service which an Iowan can find through a

small link near the very bottom of the website, there is no place on CoinFlip's website where an Iowan can locate a fee schedule. The cost of a transaction is not mentioned in the "FAQ" or the "Bitcoin ATMs" section of the website. The site has dozens of blog posts, and not a single one addresses the cost of the service. The cost of purchasing Bitcoin through a CoinFlip BTM is effectively hidden from the consumer.

113. This lack of price transparency is important for scam victims who are often using a Coinflip ATM at the direction of the scammers. These people are typically unfamiliar with Bitcoin values or exchange rates. These scammers often use threats and emotional manipulation to fluster their victims and place them in a heightened emotional state. They then instruct the victims to skip screens quickly, not giving them the time to read the 33 or so pages of the terms of service or warnings on the screen.

114. Some Iowa scam victims have said they were unaware of the high prices being charged and if they had known about the price CoinFlip charges, it would have made them question the transaction. It could have been what have stopped Iowa users from putting their money into the machine entirely.

I. CoinFlip Hides the Cost of Purchasing Using a BTM Behind Iowans' Experience with ATM Fees

115. CoinFlip's use of the term "Bitcoin ATM" in its marketing and advertising further deceives consumers about its fees.

116. Iowans associate the term "ATM" and associate it with the more common bank ATMs that often charge a small service fee for their use.

117. When Iowans see CoinFlip's around $3 "network fee" or "flat fee" prominently displayed on the Coinflip ATM screen is similar a regular ATM fee, they are tricked into thinking the around $3 fee is the extent of the fees they must pay.

118. CoinFlip has made a strategic decision to bury all other fees in its Terms of Service, clearly display a nominal fee, and call its kiosks Bitcoin ATMs. All three of those facts lead to deception about the BTM fees CoinFlip charges Iowa consumers.

IV. Violations of the Iowa Consumer Fraud Act

119. Under the Act:

> The act, use or employment by a person of an unfair practice, deception, fraud, false pretense, false promise, or misrepresentation, or the

> concealment, suppression, or omission of a material fact with intent that others rely upon the concealment, suppression, or omission, in connection with the lease, sale, or advertisement of any merchandise or the solicitation of contributions for charitable purposes, whether or not a person has in fact been misled, deceived, or damaged, is an unlawful practice.

Iowa Code § 714.16(2)(a).

120. CoinFlip sells merchandise as defined by the Act. *Id*. Merchandise "includes any objects, wares, goods, commodities, intangibles, securities, bonds, debentures, stocks, real estate or services." *Id*. § 714.16(1)(e). BTMs provide money transmitter services as well as sell Bitcoin, which could be considered a good, commodity, or intangible under the Act.

121. CoinFlip has and is engaged in an "unfair practice", deception," and "misrepresentation" as follows:

A. Selling Bitcoin Through a Kiosk That Allows for Prevalent Scam Transactions is an Unfair Practice

122. CoinFlip's practice of selling Bitcoin through its BTMs in a manner that allows for prevalent scam transactions to be processed constitutes an "unfair practice" that is unlawful under Iowa Code § 714.16(2). An "unfair practice" is defined as an act or practice which causes substantial, unavoidable injury to consumers that is not outweighed by any consumer or competitive benefits which the practice produces." Iowa Code § 714.16(1)(i)

123. The amount of money for the period of January 1, 2021, to June 10, 2024, processed through Iowa BTMs related to confirmed scam transactions totaled a staggering $13,182,625. This number is only expected to grow as the Attorney General's office has only been able to contact or confirm data related to $ 13,888,625 of the total $50,058,825 of transactions processed during the above period.

124. CoinFlip's policies comprise a paradigmatic "unfair practice." BTMs are causing "substantial, unavoidable injury" to Iowa consumers. Iowans are losing their life savings, going bankrupt, getting depression, and a myriad of other injuries because of BTMs.

125. The injuries caused by BTMs far outweigh any consumer or competitive benefits under any equitable weighing test. Any benefit in the vast pile of scams, high transaction fees, and insufficient refund policies is scant. CoinFlip's expressed benefit of extending cryptocurrency to the unbanked underbanked is not the typical case in Iowa.

126. BTMs that operate under CoinFlip's current policies and practices allow BTMs to primarily operate as a gateway driver for scammers violates Iowa consumer protection laws. CoinFlip BTMs create a path to financial ruin for Iowans, and especially older Iowans. CoinFlip's deficiencies include, but are not limited to, failing to take timely, appropriate, and effective action to detect and prevent fraud-induced money transfers through its BTM system, as described above.

127. CoinFlip knows that its BTMs are frequently used by scammers to defraud older and vulnerable Iowa consumers, both within this State and elsewhere, but it does not institute adequate safeguards relate to BTM operations to prevent scam transactions that could avoid "substantial, unavoidable injuries" to Iowa consumers.

128. Rather, CoinFlip continues to employ practices related to BTMs that are akin to putting a loaf of bread known to be poisonous on the store shelf with a warning label slapped on to avoid liability. Both are unlawful under the Iowa Consumer Fraud Act and both cause "substantial, unavoidable injuries" that are not outweighed by consumer or competitive benefits.

129. CoinFlip's practice of selling Bitcoin through a BTM in a manner that allows for prevalent scam transactions is a violation of the Act. The State is entitled to civil penalties of up to $40,000 per violation of the Act under Iowa Code § 714.16(7). There is a violation with respect to each BTM located in Iowa.

B. CoinFlip Deceived Iowans About the Price of Bitcoin Purchased Through Its BTMs

130. CoinFlip's practices of failing to conspicuously present Iowa consumers with either the price of Bitcoin or the fees they pay, hiding the terms regarding the cost of Bitcoin fees in lengthy, complex documents with inapplicable terms, and using the term "flat fee" are deceptive acts or practices that are unlawful under the Act.

131. "Deception" under the Act is "an act or practice which has the tendency or capacity to mislead a substantial number of consumers as to a material fact or facts." The price of a good or service is a material fact.

132. CoinFlip only advertises the around $3 network fee associated with its BTMs in a clear and conspicuous manner.

133. The extra charge known as the "Transaction Fee" that CoinFlip charges is buried in a complex Terms of Service and made unclear to Iowa consumers. It takes sophisticated math skills to back into determining the total fees associated with the purchase of Bitcoin from a CoinFlip BTM.

134. CoinFlip further muddies the water by using the phrase "flat fee" on the screens that Iowa consumers view during their purchase experience.

135. CoinFlip's deception regarding the pricing and fees associated with the purchase of Bitcoin through a BTM is a violation of the Act. The State is entitled to civil penalties not to exceed $40,000 per violation of the Act under Iowa Code § 714.16(7). There is a violation with respect to each BTM located in Iowa. There is also a violation for each version of CoinFlip's Terms of Service delivered to Iowa consumers, and a violation for the practice of customer service representatives in deceiving Iowa consumers on the telephone.

C. CoinFlip Misrepresents to Iowa Consumers That it Charges a Flat Fee

136. Although not include in its Terms of Service, CoinFlip advertises to Iowans during their transaction experience that there is a flat fee of around $3 when purchasing Bitcoin at a CoinFlip BTM.

137. There is not a flat fee, but rather multiple fees often unknown. Most consumers would understand a flat fee to be a singular fee representing the total purchase price.

138. CoinFlip's misrepresentation regarding the flat fee to purchase Bitcoin at its BTMs violates the Act. The State is entitled to civil penalties of up to $40,000 per violation of the Act under Iowa Code § 714.16(7). There is a violation with respect to each BTM located in Iowa.

D. CoinFlip's Violations of the Act Were Committed Against Iowa Consumers Sixty Years of Age or Older

139. The violations alleged in this Petition were committed against "older individuals," as defined under Iowa Code Section 714.16A, those who are "sixty years of age or older." *Id*.

140. The State is thus entitled to additional civil penalties of up to $5,000 for each violation of the Act that was committed against an older individual.

V. Conclusion and Prayer

The State of Iowa, *ex rel.* Attorney General Brenna Bird, requests that the Court render judgment in the State's favor and:

A. Declare that Defendant has engaged in misrepresentations, deceptions, and unfair practices against Iowa consumers in violation of the Iowa Consumer Fraud Act, Iowa Code § 714.16, *et seq.*;

B. Preliminarily and permanently enjoin Defendant from engaging in the deceptive and unfair acts described in this Petition whether that be by (i) a permanent ban from doing business in Iowa; (ii) placing additional safeguards on the operation of BTMs in Iowa, (3) refunding the full transaction amount to any scam victim whose transaction was processed through a BTM in Iowa, (4) total fee caps to exceed no more than a set percentage of the total transaction amount as determined by the Court; or (iii) any other injunctive relief the Court deems necessary and equitable;

C. Adjudge the Defendant liable for civil penalties of $40,000 for each violation of the Iowa Consumer Fraud Act;

D. Adjudge the Defendant liable for additional civil penalties of $5,000 for each violation of the Iowa Consumer Fraud Act committed against an older individual;

E. Order the Defendant to reimburse the full transaction amounts—including but not limited to the full cash or card amount processed through a BTM—to all Iowa consumers who (i) purchased Bitcoin through a BTM because they were a scam victim, (ii) would have been entitled to a refund under CoinFlip's written refund policy, or (iii) attest they did not understand the total fees or price of Bitcoin at the time of their BTM transaction;

F. For all Iowa consumers entitled to reimbursement who cannot be located through reasonable efforts, order the Defendant to disgorge all related funds and property they acquired from those Iowa consumers through misrepresentations, deceptions, and unfair practices, and award the funds and property to the State to be used by the Attorney General under Iowa Code § 714.16(7);

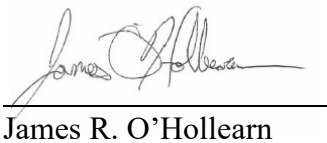
G. Award the State its costs and fees under Iowa Code § 714.16(11), including expert-witness expenses; costs incurred in pursuing this action and investigation, including reasonable attorneys' fees; and prejudgment and post-judgment interest at the highest lawful rates; and

H. Grant all other relief necessary or appropriate to remedy the effects of Defendant's acts or to which the State may be entitled.

Date: February 26, 2025

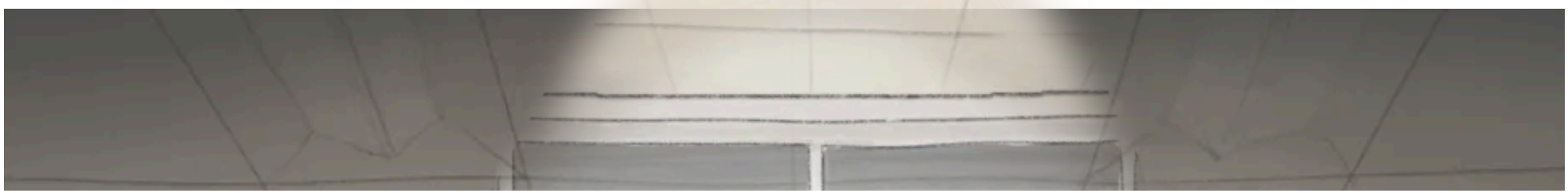
Respectfully submitted,

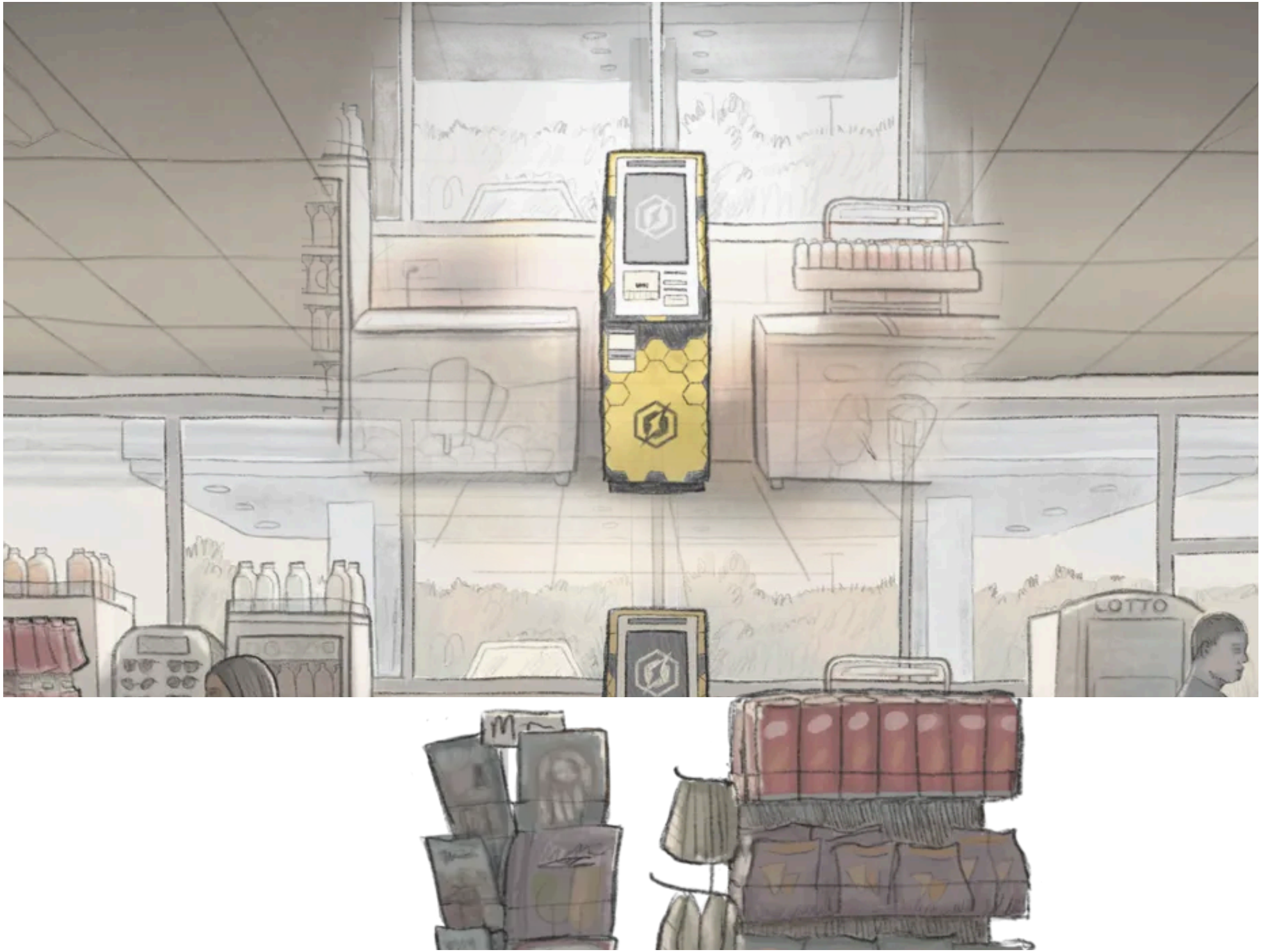
BRENNA BIRD
ATTORNEY GENERAL

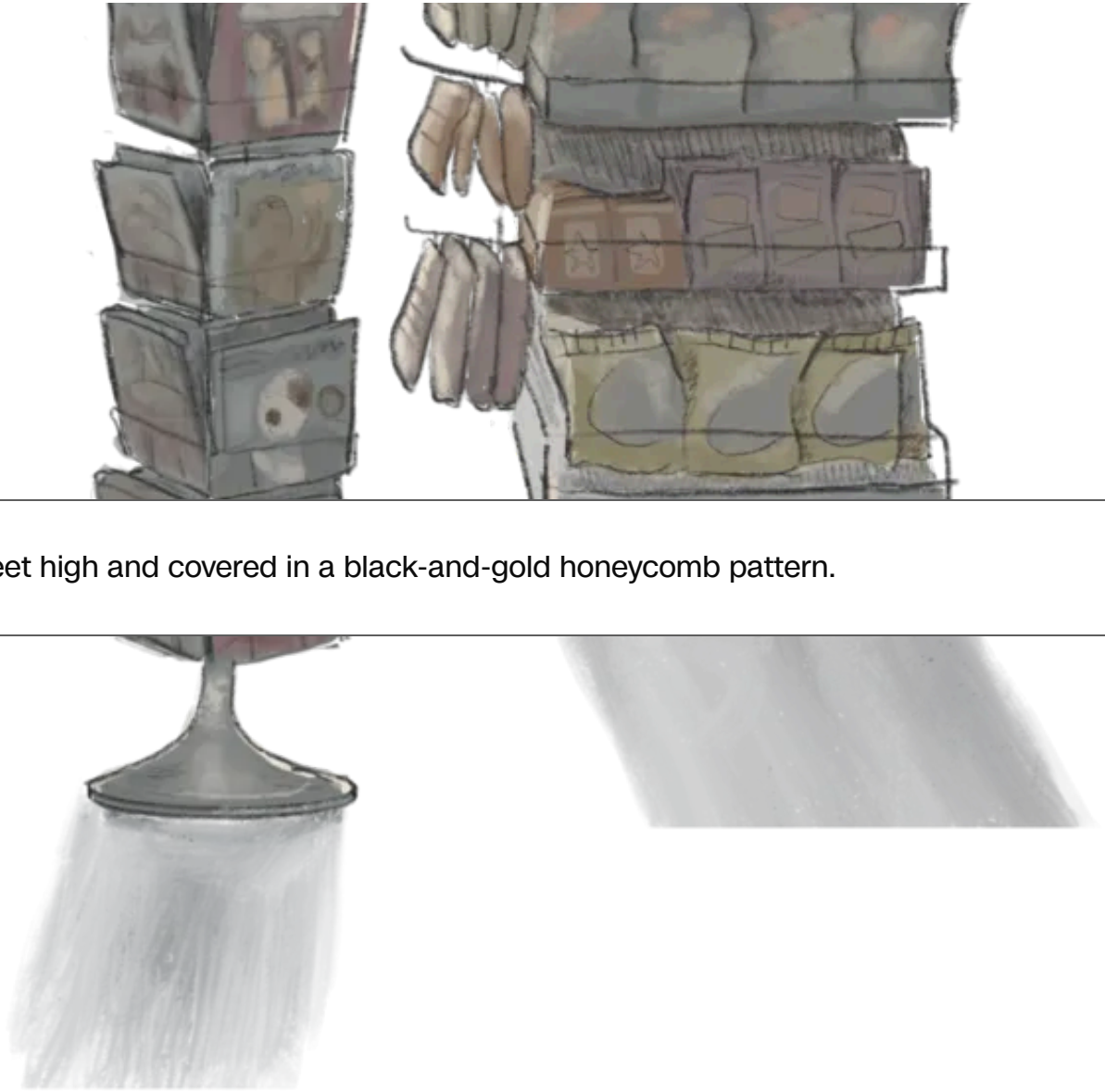


James R. O'Hollearn
Assistant Attorney General
Laura L. Mommsen
Assistant Attorney General
Daniel L. Barnes
Deputy Attorney General for Consumer Protection
Hoover Building
1305 E. Walnut St.
Des Moines, Iowa 50319
(515) 281-6411
james.ohollearn@ag.iowa.gov
laura.mommsen@ag.iowa.gov
daniel.barnes@ag.iowa.gov

The machine sits near the front door inside a convenience store on a busy street in Prescott, Arizona, wedged next to an ice cream cooler and a rack of bottled water.




LOTTO



It’s about five feet high and covered in a black-and-gold honeycomb pattern.

There’s a touchscreen, a keypad and a slot to feed in cash.

At first glance it looks like an ordinary ATM – but it’s not. It’s a perpetual crime scene, a key tool in a sinister web of international scams that bilk people out of their savings.

In just four days earlier this summer, four people were defrauded by scammers here. A woman named Jeanne lost $18,000, fed bill by bill into the machine.

Hours later, Patricia lost $3,000 in the same spot.

The next day, $25,000 was stolen from Heather.

Lily walked in two days later and was fleeced out of nearly $8,000.

Since last year, at least a dozen victims were duped out of a total of $118,000 at this machine – a crypto ATM, which turns cash into cryptocurrency.

Crypto crime scene

How the companies behind crypto ATMs profit as Americans lose millions to scams

By Curt Devine, Majlie de Puy Kamp, Yahya Abou-Ghazala, Casey Tolan, Kyung Lah, Amy O’Kruk, Byron Manley and Eleanor Stubbs, CNN

Published October 14, 2025

The victims were led to the Arizona convenience store by an increasingly familiar scam: Crooks had tricked them into believing they were in legal trouble, their bank accounts were hacked or that they had to pay off debts. To fix the "crisis," they were told to feed cash into the crypto ATM – where it was promptly routed to scammers' accounts.

This crime wave was no secret. Local police knew all about it.

But they were all but powerless to stop the scammers.

And what truly frustrates investigators is that US companies, which own and operate crypto ATMs around the country, profit from the fraud while doing too little to help stop it. Prosecutors have likened the machines to a "getaway vehicle" exploited by thieves to quickly escape with the money.

A CNN investigation, which included a review of more than 700 criminal cases and complaints, has found that crypto ATM companies make money by often marking up the price of cryptocurrency by 20% to 30% or more on transactions, including the illicit ones. Despite public claims, they often fail to refund money to victims and aggressively fight police to claw back scam money seized from machines.

The companies have also largely failed to adopt measures that could stifle scammers, such as strict transaction limits, and have heavily lobbied state legislatures to neuter laws that would force them to better protect victims. Some states have passed or proposed laws that closely match model legislation with fewer protections pushed by industry lobbyists.

"These machines are nothing more than conduits for fraud and criminal activity. Period," said New Jersey state Sen. Paul Moriarty, who sponsored a bill in his state to outright ban the machines. "There's no other use for them, because if you wanted to buy cryptocurrency you could buy it somewhere else for less."

The story is increasingly common around the nation. Americans, often retirees, lost around $240 million to crypto ATM scams in the first six months of this year, according to the FBI – about double the pace of similar scams last year.

Crypto ATM companies charge significant markups on the price of cryptocurrency

---

TRANSACTION RECEIPT

Status: Pending coins

Market price: $67,000
Sales price: $83,400
Service fee: $3

Cash: $4,300
Bitcoin sent: 0.05155024 BTC

THANK YOU FOR USING BITCOIN DEPOT!

This is a receipt for an actual Bitcoin Depot transaction from March of last year. Numbers have been rounded.

Bitcoin Depot Transaction
3/18/24 10:02 AM PDT

While it looks as though Bitcoin Depot only charges a $3 service fee, the company is selling Bitcoin at **24 percent higher** than the market rate on this transaction.

On this $4,300 transaction, Bitcoin Depot would have issued the customer around $3,450 worth of Bitcoin, pocketing around **$850** on top of the $3 service fee.

In interviews with CNN, four former crypto ATM company employees said that companies are not doing enough to prevent fraud or help victims.

One former senior staffer at a crypto ATM company who spoke anonymously for fear of reprisal described the general philosophy at his former employer as, “it’s not my problem if someone is stupid and gets scammed.”

Another former staffer said, "If there was a way to prevent 100% of scams there is no way this industry would survive."

Crypto ATM companies strongly disputed allegations they profit from scams and listed various efforts to protect consumers, such as multiple warnings about scams that are shown whenever their machines are used.

Like the other major crypto ATM operators who responded to CNN, Bitcoin Depot pointed out that users agree to terms of service before transferring money, including a promise to only send money to their own Bitcoin accounts and an acknowledgement of company fees.

"Scams, unfortunately, target every financial service, from banks to wire transfers to gift cards, but they are not representative of our business. The vast majority of our customers use our kiosks for legitimate purposes," Bitcoin Depot said in a statement, adding that "scams account for only a very small share of overall transactions."

A spokesperson for CoinFlip, another major crypto ATM firm, said the company also has multiple layers of consumer protections and noted "third-party analysis and reporting have shown our scam rate to be below what's associated with traditional financial institutions."

Multiple investigations from attorneys general and financial regulators have concluded many crypto ATM deposits involve scams, findings that came after interviewing hundreds of victims and reviewing thousands of transactions. Last month, the DC attorney general alleged that more than 90% of deposits in one company's ATMs came from fraud.

Law enforcement officials also say that victims under great duress rarely read terms of service or on-screen warnings as scammers guide them around the company protections.

The proliferation of crypto ATM scams has alarmed authorities. In recent months, the Secret Service has even visited shops where the ATMs are located to hand out

paper warnings about scams, while the Treasury Department issued an alert to banks in August, urging vigilance against the fraud.

Some nations have cracked down harder. Authorities in New Zealand, Australia and the UK have all taken steps to limit or outright ban the devices to battle financial crimes.

Local police officers, meanwhile, are seething as they respond again and again to the same machines and find themselves unable to help victims. One sheriff’s deputy in Texas even wielded a power saw to break into a crypto ATM to retrieve cash a victim deposited.

The company with the most crypto ATMs, in response, has mocked and lashed out at police who have seized money.

“Glorious day,” a manager for Bitcoin Depot wrote in an email to one sheriff's office after a court ruled it could take back money deposited in one of its machines by a scam victim. “Which one of you would like to coordinate... the return of our cash?”

That manager chastised another sheriff, saying that he displayed “ignorance and arrogance,” and sent a copy of the US Constitution to officers at another police department, suggesting they need to read it.

Asked for comment, Bitcoin Depot said those messages and others to law enforcement were “unacceptable” and did “not reflect who we are,” adding that the employee who sent them was no longer with the company.

"We've reinforced with our team that all law enforcement interactions must be handled with professionalism and respect," the company said.

The employee's separation from the company occurred shortly after CNN asked Bitcoin Depot about the messages.

Rise of the scams

The man on the phone told Shelby 'Gus' Cason he would be arrested if he didn't quickly follow instructions.

He told him a convoluted but convincing tale that involved incriminating information and his bank account in jeopardy.

As a panicked Cason listened at home in Coggon, Iowa, the man directed him to withdraw $15,000 from his bank and then to drive to a liquor store, where he told him to deposit the money into a Bitcoin ATM.

"I was under duress big time," said Cason, who was 69 at the time and added that he had recently suffered a stroke and wasn't thinking clearly.

Cason's story is a familiar one that's been going on for years.

The first crypto ATMs popped up in 2013 with a simple premise, as Daniel Polotsky, the cofounder of CoinFlip, later said on a podcast: "We make the process really, really easy: Go insert cash. Get Bitcoin."

The trio of Bitcoin Depot, CoinFlip and Athena Bitcoin operate more than half of all crypto ATMs in the US, with more than 16,000 machines between them, according to Coin ATM Radar, which tracks the devices.

The machines offer an alternative to buying cryptocurrency online — but charge significantly more for each transaction.

As crypto has gone more mainstream, the devices have multiplied and spread from major cities into suburban and even rural areas – like the shop near Cason's home in eastern Iowa. Convenience stores, gas stations and other shops often charge a fee to crypto ATM operators to host the machines.

As the ATMs have spread, so have scams that use them.

Crypto ATMs are ideal tools for financial scammers, according to police who have investigated the crimes, because they offer a quick way to turn cash into hard-to-recover cryptocurrency.

Scammers coach their often-elderly victims step-by-step to use the machines and convert their cash to cryptocurrency, which then gets deposited into anonymous crypto wallets controlled by the criminals. From there, the scammers can swiftly route the funds to offshore crypto platforms.

"Many agencies don't even initiate investigations," said Boise police Detective Brad Thorne. He has worked dozens of cases involving scam suspects around the world but has only helped successfully seize cryptocurrency once.

Across the US, the Federal Trade Commission found fraud losses involving crypto ATMs jumped from about $12 million in 2020 to $114 million in 2023 – nearly a tenfold increase. FBI data suggests the rate of the losses is only increasing.

CNN's review of hundreds of incident reports and consumer complaints – which totaled more than $11 million in losses, with the average victim losing more than $15,600 – revealed many cases follow roughly the same script that ensnared Cason. Scammers often start by alerting victims to a fabricated problem, then offer a hasty solution that ends with cash funneled into a crypto ATM.

Body-cam footage shows police officers responding to scams in progress

WESTLAKE, OHIO

0:00 / 0:32

Video transcript

Officer

Ma'am, listen to your police department. We're here to help you. He's scamming you.

No, no, no, no, no, no. Don't do that.

Victim

Excuse me? Excuse me, sir? Samuel what? Oh.

f law
s, who
y personal.

e got footage of you doing filthy things in your house,” one scam email reviewed by CNN states. “With just a single click, I can send this garbage to all of your contacts.”

To further understand how these frauds work, CNN reporters called the phone numbers listed in scam emails without immediately identifying themselves as journalists. The scammers who answered posed as tech support and bank staffers and shared spoofed websites of real businesses. One scammer urged a reporter to stuff nearly $10,000 into a Bitcoin Depot ATM.

When confronted by the reporter, the scammer ultimately dropped his cover story and admitted to working with colleagues to transfer millions in cryptocurrency each month before briefly apologizing and hanging up.

Police try to assist when victims call for help – but often have little recourse. That’s what happened to Cason, the Iowa victim.

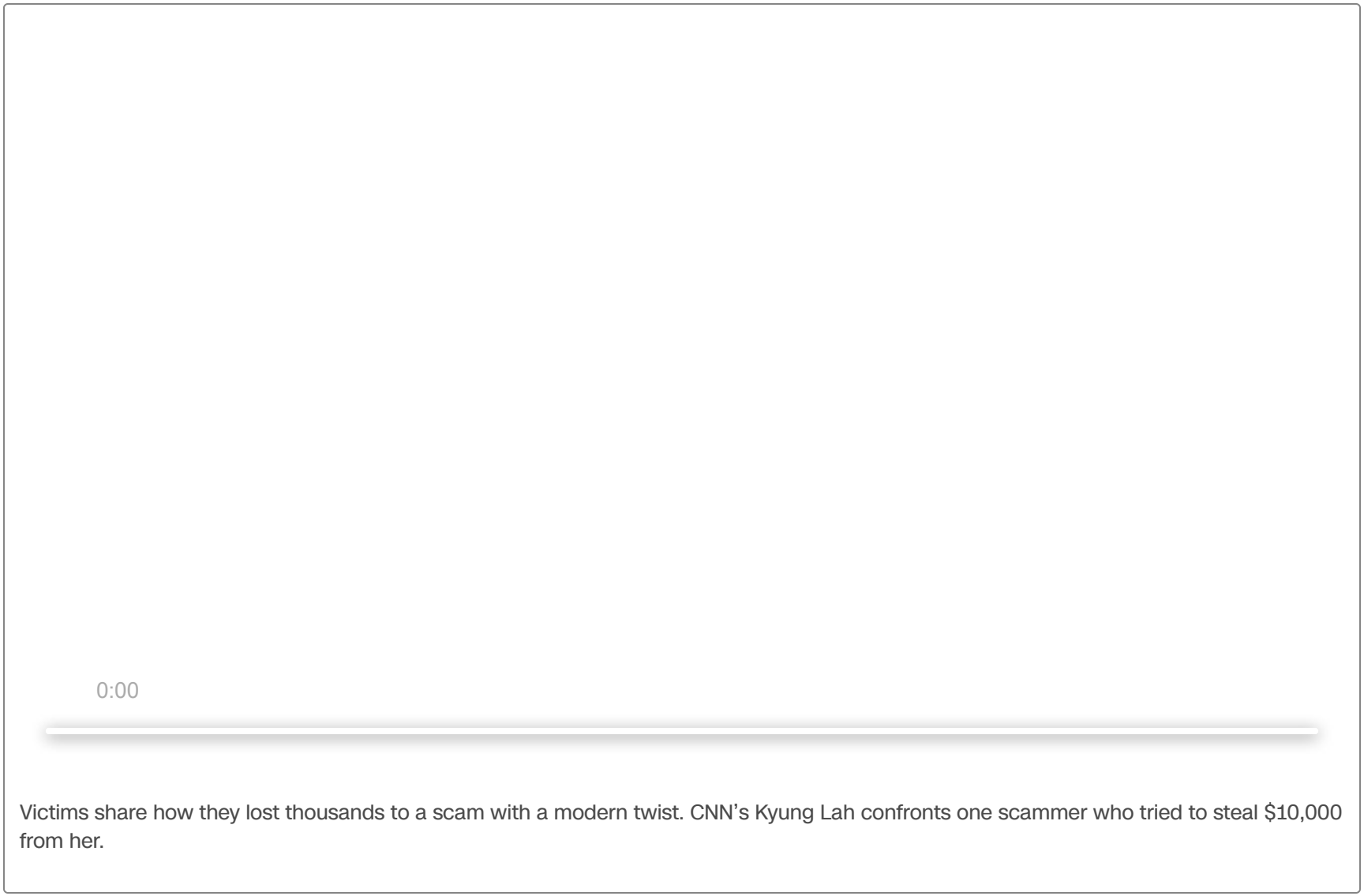
When Cason contacted the sheriff’s office in July 2023, investigators got a search warrant for the machine and seized the cash he had deposited, intending to return the money to him.

But Bitcoin Depot argued in court that Cason had authorized the transaction and had agreed to the company’s terms of service when he used the machine. His cash had already been turned into cryptocurrency and transferred away, the company said.

The case went all the way to Iowa's state Supreme Court, which ruled in favor of Bitcoin Depot in the spring. Because scammers had convinced Cason to bypass company requirements that users only send funds to crypto wallets they control, the court found Bitcoin Depot wasn’t liable.

Cason never saw the cash again.

Watch how scammers convince victims to give up their savings



Victims share how they lost thousands to a scam with a modern twist. CNN’s Kyung Lah confronts one scammer who tried to steal $10,000 from her.

What's driving business

Crypto ATM companies have argued fraud is not a significant driver of business, with some highlighting a report by the analytics group TRM Labs, which found that 1.2% of cash-to-crypto transactions were illicit in 2023.

But even the analytics group behind that report acknowledged in a statement to CNN that "the reality is clear: a significant share of scams and fraud move through these machines."

Another leading analytics firm recently noted a "surge" of crypto ATM scams last year. Bitcoin Depot itself has warned its investors of the issue as early as 2022, disclosing in financial records that its machines and services could facilitate "fraud, money laundering, gambling, tax evasion, and scams."

For police who have investigated crypto ATMs, there's little doubt: scammers love to use the machines.

"This is running rampant all over our country," said John Altman, commander of a Woodbury, Minnesota police team that has investigated multiple crypto ATM scams.

Iowa's attorney general sued Bitcoin Depot this year, alleging that scams accounted for "more than half of all money taken in by Bitcoin Depot in Iowa" over a roughly three-year period ending in 2024, more than $7 million in scam transactions. The attorney general said in another suit that CoinFlip's top 20 users

in the state were all scam victims. The companies have disputed the claims in court.

Documents show a regulator in Maine denied a license application from Bitcoin Depot in April on the grounds that its crypto ATMs "caused an unacceptably high number of Maine consumers to suffer financial loss." The state concluded that elderly consumers accounted for more than 70% of money transmitted on its machines in the state over about two years. The regulator also found the company's ATMs lack "necessary controls, warnings, and safeguards."

Bitcoin Depot told CNN it disagreed with that finding, pointing to its scam warnings on machines. They also noted that more protections for seniors were being rolled out. The company has appealed, the Maine regulator said.

In September, the District of Columbia's attorney general filed a lawsuit against Athena Bitcoin, another major operator of crypto ATMs, alleging that 93% of deposits on its machines in DC over a five-month period came from scams.

In a statement, Athena Bitcoin disputed the suit's allegations. "The foundation of our business is providing a safe and convenient customer experience. We have strong safeguards against fraud including transparent instructions, prominent warnings and consumer education," the company said.

The problem extends beyond US borders.

In June, Australian authorities said they contacted 90 people who were among the biggest crypto ATM users and found that around 85% were scam victims or

“money mules” who had been coerced into moving suspected illicit funds through the ATMs, according to AUSTRAC, the country’s financial intelligence unit.

Police say the money stolen in crypto ATM scams usually ends up in foreign countries that are less likely to cooperate with US investigations – making it extremely difficult to recover.

Those anecdotal findings are echoed by a CNN analysis of blockchain data over the last decade, which shows that the bulk of all cash deposited in ATMs operated by the biggest US companies has ended up on exchanges based overseas.

Some law enforcement officials said the prevalence of such overseas transfers raises questions about the companies’ claims that a small minority of their users’ transactions are illegitimate.

Most of the top 10 exchanges that received funds say their services aren’t accessible to US users, and many are based in jurisdictions with historically weak anti-money laundering laws, such as the Cayman Islands and Nigeria, CNN’s analysis found.

“It's a red flag to us, knowing that a large majority of financial crimes that are happening in the United States are run by overseas actors,” said a Secret Service official who requested anonymity due to the sensitivity of their position. “It likely is a money laundering indicator if large fees are charged and people are willing to pay those when there are other options that are much cheaper and just as convenient.”

Crypto ATM operators say their devices offer a fast and easy way to send money internationally, and that many customers use the machines to send remittances

abroad. "Bitcoin is a global asset, so many transactions naturally flow to international exchanges," Bitcoin Depot said in a statement.

A CoinFlip spokesperson added that "the farther away in the transaction chain you look, the less it reflects anything related to the original CoinFlip customer activity."

'Slap in the face'

Crypto ATM companies say they have layers of consumer protections to ensure they are not in the business of profiting from fraud.

Bitcoin Depot highlighted its protections including real-time screening for questionable transactions and requirements for users to provide ID. A spokesperson for CoinFlip described related safeguards, such as live customer service agents and holds placed on transactions deemed high-risk.

But more than two dozen state regulators and members of law enforcement interviewed by CNN said the companies could take immediate steps to crack down harder, such as adopting stricter transaction limits and more aggressively placing holds on suspicious deposits, among other measures.

Others questioned whether the companies have incentives to fully stop the scams.

"I'm not sure these companies really believe it's in their own monetary interest," said James Brown, Montana's state auditor.

While some crypto ATM companies such as Bitcoin Depot and CoinFlip say they refund transaction fees for scam victims, the firms’ websites do not clearly publicize that policy, but rather stipulate that transactions are nonrefundable.

Iowa’s attorney general has accused CoinFlip of having no refund policy for scam victims and Bitcoin Depot of having a "secret” refund policy that the company has shared with regulators — but not victims. The companies dispute this.

CNN spoke with ten victims who lost thousands on Bitcoin Depot ATMs and never received fees and markups back from the company. Some said they were rebuffed by the company when they reached out after being scammed, but others said they had no idea they could try to get fees back.

Jacob Arnold of New Mexico said he got “nothing at all” from the company when he reached out after being scammed out of $10,000 that he had set aside for his daughter's education. “There was no recourse for me,” he said.

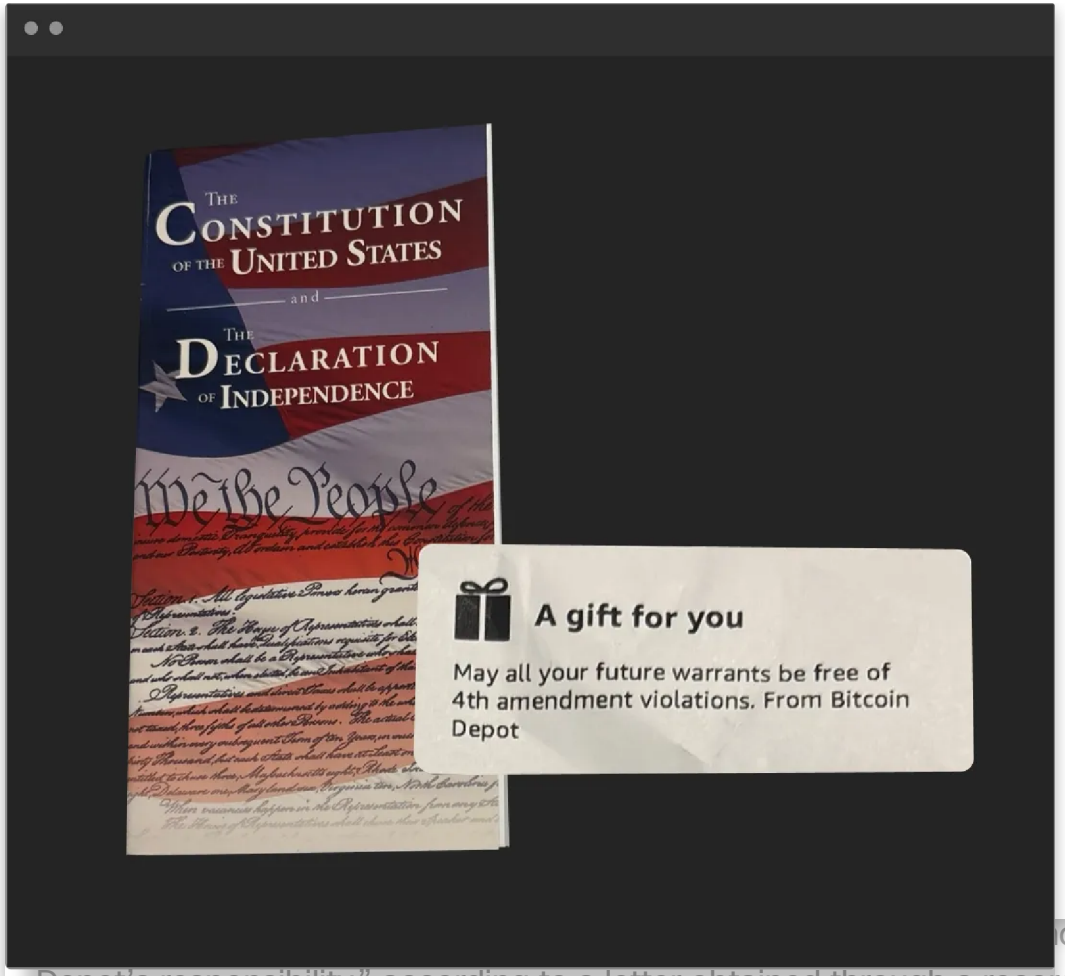
"It is a somewhat convoluted process with very limited reports of success in getting a refund,” said Nathan VanCleave, a financial investigator with police in Evansville, Indiana. “It’s all discretionary, case-by-case, company-by-company.”

Bitcoin Depot reviews scam cases individually and has refunded millions of dollars in attempted scam transactions, the company said in a statement. “Because crypto is irreversible once transferred, publishing a one-size-fits-all refund policy risks creating confusion,” the company said.

When local authorities have obtained search warrants and seized cash on behalf of victims, crypto ATM companies have pushed in court to keep the money – arguing they’ve already used that cash to purchase the crypto sent to scammers.

In Colorado, for example, CoinFlip reached a settlement last year to reclaim money seized by a sheriff’s office after a couple was scammed out of $38,000. In North Carolina, Bitcoin Depot successfully petitioned a few months later for the return of about $13,000 that police held after a 74-year-old woman was defrauded. An Iowa judge issued a similar ruling last year on a petition from another company.

One crypto ATM company's tone and tactics with law enforcement



A Bitcoin Depot staffer sent a copy of the Constitution to the Centralia Police Department in Washington state along with a note suggesting the police had violated the 4th Amendment during a seizure of cash from a crypto ATM. Credit: Centralia Police

"The idea is that when we have these rogue agencies that don't want to listen to law or logic, putting pressure on them from their peers will hopefully curb that behavior," a Bitcoin Depot manager wrote in an email to another police

department. Records show the company has used similar pressure tactics in Georgia and Texas, though Bitcoin Depot said in a statement to CNN its refund policy has never been paused.

Police in Centralia ultimately returned the cash to Bitcoin Depot. The company then mailed a copy of the US Constitution to the department with a note that read, "A gift for you. May all your future warrants be free of 4th amendment violations," according to a photo of the package.

The message to Centralia police was among those sent by the employee Bitcoin Depot said is no longer with the company.

"It was kind of a slap in the face to the victims," Chad Withrow, a detective with the Centralia Police Department, said of the package. "There was no consideration for the victims... They don't care. It's about money."

'Pushing' language to lawmakers

With crypto fraudsters outpacing police, state lawmakers around the country have drafted legislation that aims to blunt scams. But crypto ATM companies have hired lobbyists to sway the regulations in their favor – sometimes even getting lawmakers to file bills with language proposed by the industry.

Since 2023, at least 18 states have passed laws or rules specifically focused on crypto ATMs and scams. The laws impose requirements such as daily transaction

limits, refund obligations for fraud victims or other stipulations.

Across the US, crypto ATM companies have collectively deployed more than 150 lobbyists in the last three years, government records show. Those lobbyists have successfully watered down legislation in multiple states by convincing lawmakers on both sides of the aisle to loosen proposed requirements.

In Minnesota, for example, the legislature proposed a bill with a blanket transaction cap of $1,000 per day to cut scam victims' potential losses.

But the bill that eventually passed last year raised the limit to $2,000 for new users only. The law also added requirements for scam victims to get refunds, including contacting crypto ATM companies and law enforcement within two weeks.

An attorney for CoinFlip, Larry Lipka, testified that he "helped draft" Minnesota's legislation and wrote in a February email that he "added" language related to refunds to the bill.

Asked by CNN whether industry lobbyists loosened the bill's requirements, Minnesota state Rep. Amanda Hemmingsen-Jaeger, a sponsor of the legislation and a Democrat, replied, "It really came down to compromise."

She said outright rejecting the industry's perspective could have jeopardized the bill's passage, though she said she insisted on having some form of transaction limit, which crypto ATM companies resisted. "I think the industry cares about their bottom line," she said.

Because the bill only applied that transaction limit to new users, some scammers have circumvented the rule by directing victims to preexisting crypto accounts, Lucas Rogers, a detective in Woodbury, Minnesota, told CNN.

Bills in states including Arizona, Colorado, Maryland, North Dakota and Rhode Island followed similar patterns, where proposed transaction limits were softened in the legislation that ultimately passed.

"As soon as I had it drafted, the crypto people came out of the woodwork," said Rhode Island state Rep. Julie Casimiro, a Democrat. "They wanted much less restrictions."

In some states, lawmakers have backed bills with language promoted by the industry.

In Missouri, legislators passed regulations this year that match nearly word-for-word model legislation shared by CoinFlip in another state, with no transaction limits or refund requirements, records show.

Lobbyists have pushed some of the legislative language governing crypto ATMs

CNN analyzed one state bill — signed into law by Missouri's governor in July — and found many parts matched language pushed by lobbyists nearly word-for-word.

Bill text matching language promoted by industry lobbyists

(3) Transactions in virtual currency may be irreversible, and, accordingly, losses due to fraudulent or accidental transactions may not be recoverable;

Missouri Senate Bill 98

"This is language that we've been pushing in 25, 30 states," Lipka, the CoinFlip attorney, said in March when he testified in support of the Missouri bill.

Bills proposed in states including Illinois, Massachusetts and New Jersey contain language that's nearly identical to that model legislation in various sections, though some have other requirements the companies must now abide by.

A spokesperson for Republican Massachusetts state Sen. Patrick O'Connor, a bill sponsor, acknowledged that the law's language "is industry backed."

Some states – including California, Maine and Iowa – have enacted strict $1,000 daily transaction caps and other limits. Vermont temporarily banned new crypto ATMs in the state.

CoinFlip has openly touted its engagement with government officials. CEO Ben Weiss visited the White House in July, played kickball with Florida legislators last year and met with federal lawmakers on Capitol Hill the year before, according to photos he or the company posted on social media. In April, two months after his company was sued by Iowa's attorney general, CNN spotted Weiss with multiple other state attorneys general on a luxury trip in Rome.

A CoinFlip spokesperson said the company "has a long history of engaging with a wide range of public and private stakeholders, including attorneys general, to provide education and industry-specific guidance to ensure consumers remain protected in an evolving space." The spokesperson added the company supports requirements for live customer service and other safety features.

In an interview, Bitcoin Depot's president and chief operating officer, Scott Buchanan, said his company has also suggested regulations to state lawmakers.

"In some states we've proposed the bills in the first place," he said, noting that he supports certain regulations, such as requirements to add warnings to machines that alert users to look out for scams.

"Our advocacy is for rules that are effective in practice," the company said.

'Protect these people'

As the Trump administration has relaxed oversight of the crypto industry, some US senators have sought tighter regulations for crypto ATMs – largely without success.

A proposal that included transaction limits spearheaded by Illinois Sen. Dick Durbin, a Democrat, was ultimately not included in crypto legislation President Donald Trump signed into law in July. Wyoming Sen. Cynthia Lummis, a Republican, posted on X last month that she hoped to address the scams.

Some Bitcoin ATM lobbyists have referenced Trump's pro-crypto policies as they've sought to advance their own cause.

"The federal government is looking to promote this and here we are overregulating it," Dan Claitor, a lobbyist for CoinFlip, said in May during a Louisiana Senate

hearing on a crypto ATM bill that later passed. Referencing Trump, Claitor said, “There’s no question he is for cryptocurrency.”

On the state level, at least six other legislatures have introduced bills that could stiffen crypto ATM regulations.

Law enforcement authorities said even without new legislation, crypto ATM companies should change their policies to better stifle scams and help victims.

“If they truly care and they're running a legitimate business, they'd do something to try and protect these people,” said Chad Colston of the Linn County Sheriff’s Office, which seized the cash deposited by Cason, the Iowa scam victim.

Cason told CNN he believes he was stiffed twice – once by a scammer and again when Bitcoin Depot successfully pushed in court to reclaim the cash he deposited.

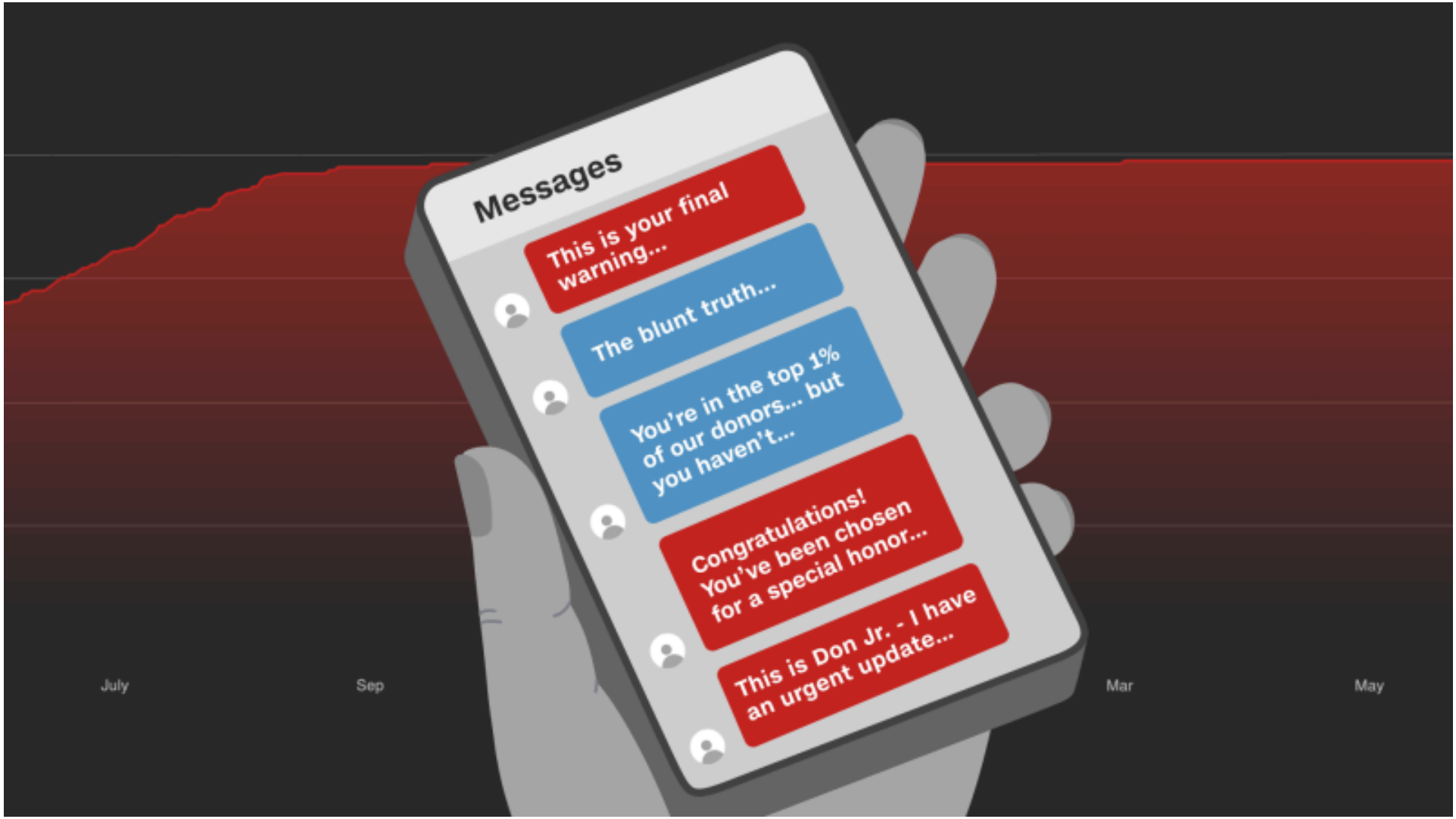
In July, he filed a lawsuit against Bitcoin Depot that alleges the company has failed to protect users from fraud. Bitcoin Depot has rejected his arguments and asked the court to dismiss the case.

Cason said everyone involved made money except him – the scammer, the ATM company and even attorneys working on the case.

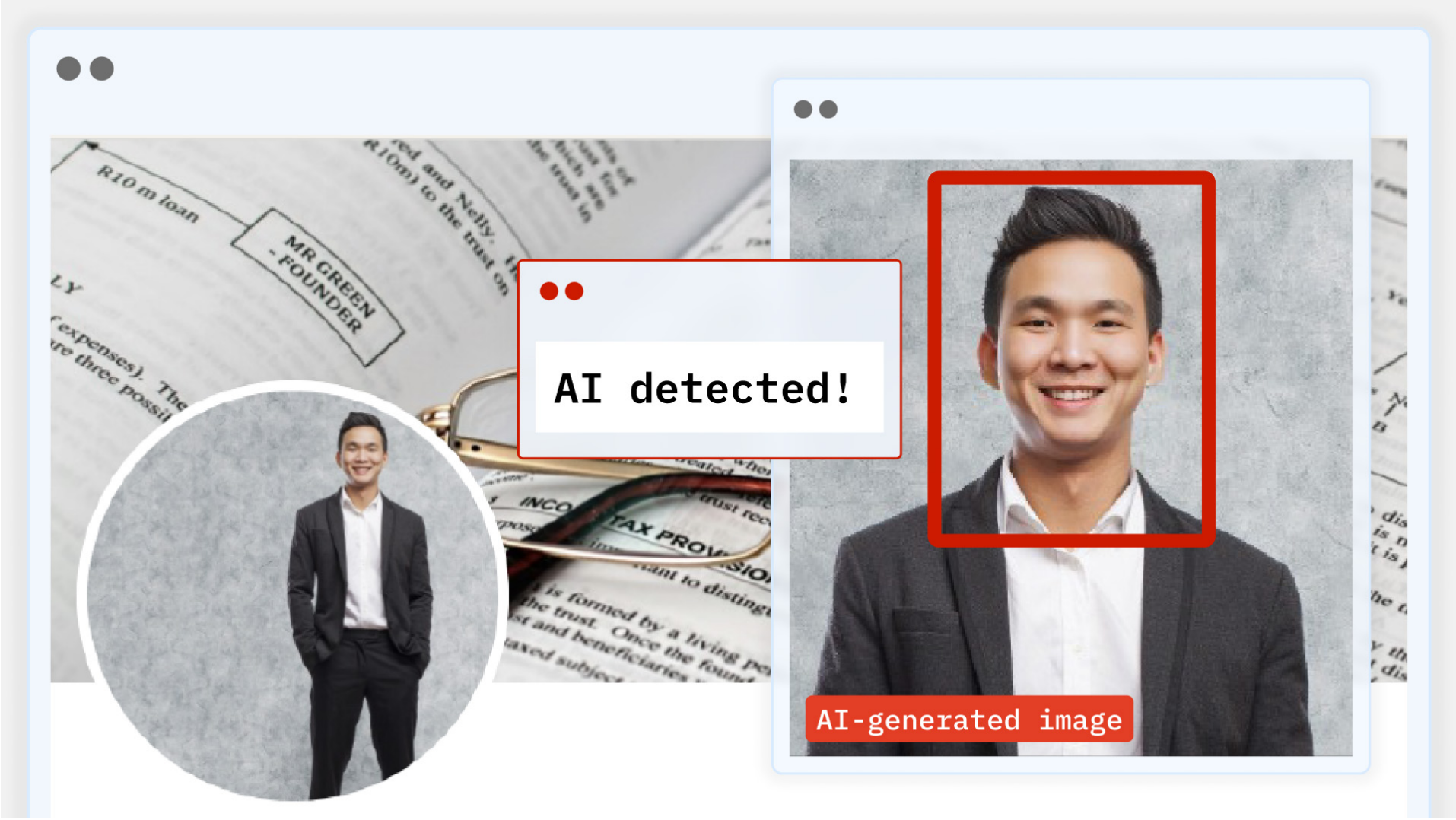
“I got screwed,” Cason said.

This story has been updated.

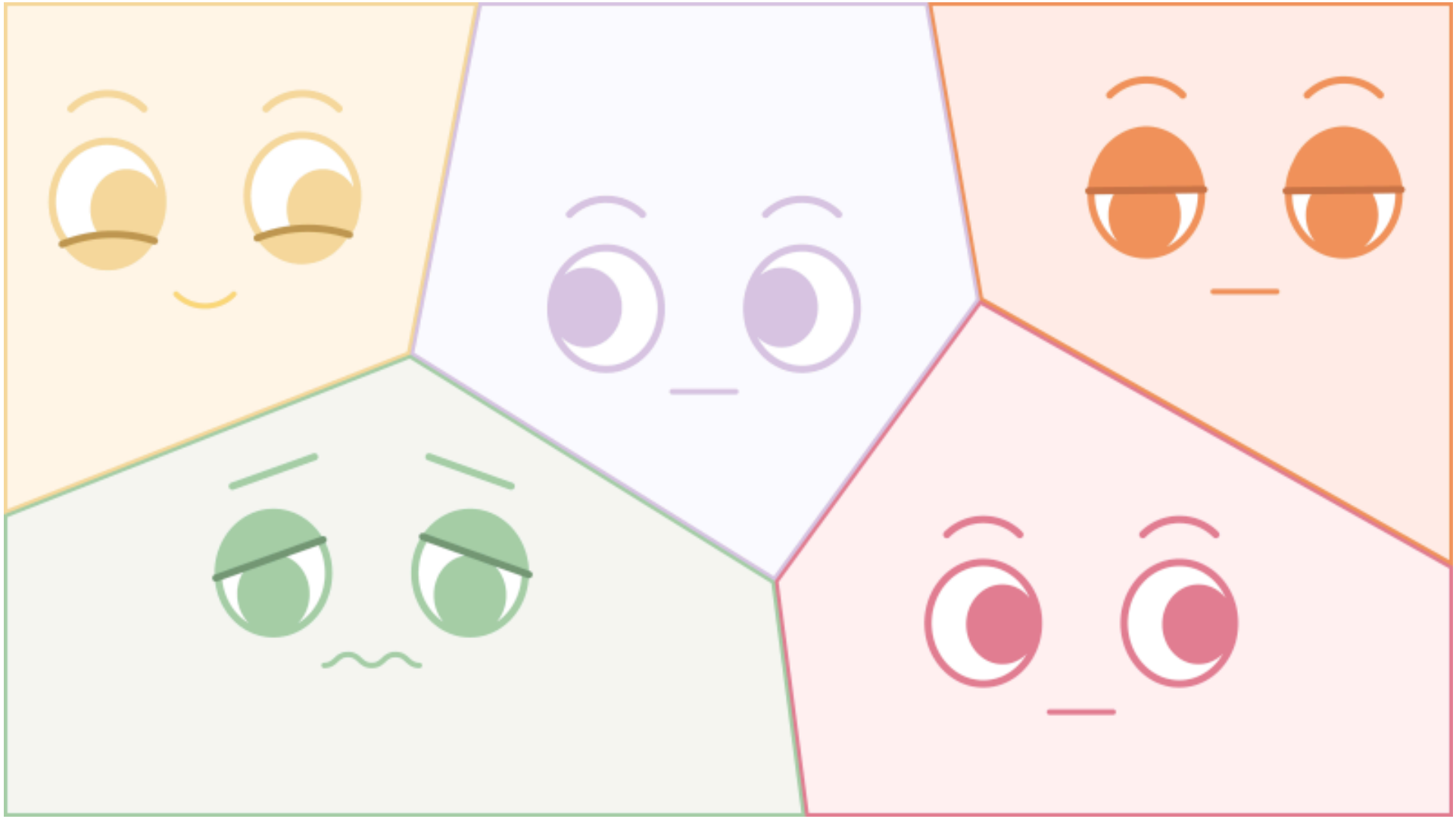
Related stories



How elderly dementia patients are unwittingly fueling political campaigns



Inside North Korea’s effort to infiltrate US companies



What does an independent mean in politics?

Credits

Reporters

Curt Devine, Majlie de Puy Kamp, Yahya Abou-Ghazala, Casey Tolan and Kyung Lah

Developer
Byron Manley

Illustrator
Amy O'Kruk

Designers
Eleanor Stubbs and Amy O'Kruk

Editors
Tim Elfrink, Patricia DiCarlo, Gillian Roberts and Matt Lait

Video editor
Ted Severson

Photojournalists
Rory Ward, Dave Ruff and McKenna Ewen

Additional animation
Duncan Senkumba

Summary

Cryptocurrency, Digital or Virtual Currency and Digital Assets 2025 Legislation

Updated September 11, 2025

Related Topic: Financial Services

Digital or virtual currencies are a medium of exchange but are not regular money.

Unlike paper bills and coins, cryptocurrencies are not issued or backed by the U.S. government or any other government or central bank. The lack of a physical token to count and hold may confuse some. Rather, Bitcoin and other cryptocurrencies are a form of digital currency used in electronic payment transactions—no coins, paper money or banks are involved; there are zero to minimal transaction fees; transactions are fast and not bound by geography; and, like using cash, transactions are anonymous.

Digital currencies are stored in digital wallets, which are software or apps installed by users on their computer or mobile device.

Each digital wallet contains encrypted information, called public and private keys, that is used to send and receive the digital currency. All digital currency transactions are recorded in a virtual public ledger called the "blockchain," which is maintained by digital currency "miners." These miners can be anyone, anywhere in the world, who is willing to invest in the specialized computer hardware needed to rapidly process complex computations. Miners are awarded digital currency, like Bitcoin, Ripple, Dogecoin and Litecoin, in exchange for verifying each transaction and adding it to the blockchain.

At least 40 states have introduced or pending legislation regarding cryptocurrency, digital or virtual currencies and other digital assets in the 2025 legislative session.

Examples of enacted legislation include:

- Arizona required cryptocurrency kiosk operators to disclose relevant terms and conditions and required that an operator use blockchain analytics and tracing software to help prevent fraud. In a second bill, the state established the Bitcoin and Digital Assets Reserve Fund.
- Arkansas amended the Uniform Commercial Code to provide that the term "money" does not include a central bank digital currency.
- Georgia created a Senate Study Committee on Artificial Intelligence and Digital Currency.
- Iowa defined charges associated with digital financial asset transaction kiosks.
- Michigan declared May 13, 2025, is Digital Asset Awareness Day.
- Montana prohibited the use of central bank digital currency by governing authorities.
- Nebraska adopted the Controllable Electronic Record Fraud Prevention Act.

- North Dakota required virtual currency kiosk operators to be licensed under the state money transmitter law.
- Oregon added an article regulating controllable electronic records to its Uniform Commercial Code.
- South Dakota updated its Uniform Unclaimed Property Act to include provisions related to virtual currency and notice requirements.
- Utah authorized the state treasurer to invest public funds in certain digital assets.
- Wyoming provided that no state agency shall use public funds to assist in any manner in the testing, adoption or implementation of a central bank digital currency.

Related Topic: Financial Services

Search:

Jurisdiction and Summary	Bill Number	Bill Title	Bill Status
Alabama	H 482	State Government	Pending
Alabama	H 483	Government Administration	Pending
Alabama	H 617	Consumer Protection	Pending
Alabama	S 17	Digital Assets	Pending
Alabama	S 282	Government Administration	Pending
Alabama	S 283	State Government	Pending
Alaska	H 99	Money Transmission	Pending
Alaska	S 86	Money Transmission	Pending
American Samoa	None		
Arizona	H 2324	Forfeiture of Digital Assets	Pending
Arizona	H 2387	Cryptocurrency Kiosks and Fraud Prevention	**Enacted**
Arizona	H 2654	Cryptocurrency and Blockchain Commission	Pending
Arizona	H 2749	Digital Assets	**Enacted**
Arizona	H 2906	Financial Technology and Digital Assets Program	Vetoed
Arizona	S 1024	State Agencies	Vetoed

Jurisdiction and Summary	Bill Number	Bill Title	Bill Status
Arizona	S 1025	Virtual Currency	Vetoed
Arizona	S 1026	Virtual Currency	Pending
Arizona	S 1062	Legal Tender and Cryptocurrency	Pending
Arizona	S 1095	Central Bank Digital Currency	Vetoed
Arizona	S 1373	Digital Assets Strategic Reserve Fund	Vetoed
Arizona	SCR 1001	Property Tax Exemptions	Pending
Arkansas	H 1467	Uniform Money Services Act	**Enacted**
Arkansas	H 1508	Public Finance	**Enacted**
Arkansas	H 1533	Decentralized Unincorporated Nonprofit Association	Failed - Adjourned
Arkansas	H 1746	Uniform Commercial Code	**Enacted**
Arkansas	S 10	States Data Centers	Failed
Arkansas	S 11	State Data Centers	Failed
Arkansas	S 47	Uniform Commercial Code	Failed - Adjourned
Arkansas	S 60	Digital Asset Mining Business	Failed
Arkansas	S 133	Uniform Commercial Code	**Enacted**
Arkansas	S 171	Business and Commercial Law	**Enacted**
California	A 236	Digital Financial Asset Businesses: Regulatory Fees	Pending
California	A 1029	Statements of Financial interest: Digital Financial	Pending
California	A 1052	Digital Financial Assets	Pending

Jurisdiction and Summary	Bill Number	Bill Title	Bill Status
California	A 1118	Criminal Procedure: Search Warrants	Pending
California	A 1180	Department of Financial Protection and Innovation	Pending
California	S 97	Digital Financial Assets: Stablecoins	Pending
California	S 822	Unclaimed Property: Digital Financial Assets	Pending
Colorado	H 1067	Criminal Asset Forfeiture	Failed - Adjourned
Colorado	H 1224	Revised Uniform Unclaimed Property Act Modifications	To governor
Colorado	S 79	Vending of Digital Assets Act	To governor
Colorado	S 81	Treasurer's Office	To governor
Connecticut	H 5237	Cryptocurrency Pig Butchering Scams	Failed
Connecticut	H 6651	Cryptocurrency Theft	Failed
Connecticut	H 6970	Adoption of Amendments to the Uniform Commercial Code	Enacted
Connecticut	H 6990	Seizure and Forfeiture of Digital Wallets	Pending
Connecticut	H 6991	Definitions Applicable to the Money Transmission	Pending
Connecticut	H 7082	Certain Requirements Applicable to Virtual Currency	Pending
Delaware	None		
District of Columbia	None		
Florida	H 319	Virtual Currency Kiosk Businesses	Failed

Jurisdiction and Summary	Bill Number	Bill Title	Bill Status
Florida	H 487	Investment of Public Funds in Bitcoin	Failed
Florida	H 515	Uniform Commercial Code	To governor
Florida	S 132	Legal Tender	Failed
Florida	S 292	Virtual Currency Kiosk Businesses	Failed
Florida	S 550	Investment of Public Funds in Bitcoin	Failed
Florida	S 1666	Uniform Commercial Code	Failed
Georgia	HR 905	Department of Education	Pending - Carryover
Georgia	S 178	State Depository Board	Pending - Carryover
Georgia	S 228	State Depositories	Pending - Carryover
Georgia	SR 391	Artificial Intelligence and Digital Currency	**Adopted**
Guam	None		
Hawaii	H 1277	Digital Financial Asset Transaction Kiosk	Pending - Carryover
Hawaii	S 362	Digital Currency	Pending - Carryover
Idaho	None		
Illinois	H 742	Digital Assets and Consumer Protection Act	Pending
Illinois	H 1844	Strategic Bitcoin Reserve Act	Pending
Illinois	H 4081	Digital Asset Control	Pending
Illinois	HR 446	Recognition Resolution	Pending

Jurisdiction and Summary	Bill Number	Bill Title	Bill Status
Illinois	S 1429	Environmental Protection Act	Pending
Illinois	S 1797	Digital Assets and Consumer Protection Act	Pending
Illinois	S 2319	Virtual Currency Kiosk Consumer Protection Act	Pending
Indiana	H 1156	Digital Asset Mining	Failed - Adjourned
Indiana	S 542	Electronic Payments	Failed - Adjourned
Iowa	H 246	Investment of Public Moneys in Digital Assets	Pending
Iowa	S 403	Investment of Public Moneys in Digital Assets	Pending
Iowa	S 449	Digital Financial Asset Transaction Kiosks	**Enacted**
Kansas	H 2235	Technology Enabled Fiduciary Financial Institutions Act	Failed - Adjourned
Kansas	S 34	Investing in Bitcoin Exchange Traded Products	Failed - Adjourned
Kentucky	H 376	State Financial Practices	Failed - Adjourned
Kentucky	H 377	Digital Assets	Failed - Adjourned
Kentucky	H 701	Blockchain Digital Assets	**Enacted**
Louisiana	H 37	Contracts	Pending
Louisiana	H 483	Banks and Banking	Pending
Louisiana	HR 317	Commercial Regulations	Adopted

Jurisdiction and Summary	Bill Number	Bill Title	Bill Status
Maine	S 494	Limits on Virtual Currency Kiosks	Pending - Carryover
Maine	H 967, Special Session	Commission to Study the Taxation of Digital Assets	Pending
Maine	H 1313, Special Session	State Revised Unclaimed Property Act	Pending
Maine	S 515, Special Session	Commission to Study Fostering a Positive Economic	Pending
Maine	S 553, Special Session	Virtual Currency Kiosks	Pending
Maryland	H 454	Digital Asset and Blockchain Technology Task Force	Failed - Adjourned
Maryland	H 761	Uniform Disposition of Abandoned Property Act	To governor
Maryland	H 900	Electric Company Data Centers	Failed - Adjourned
Maryland	H 1389	Strategic Bitcoin Reserve Act	Failed - Adjourned
Maryland	S 305	Virtual Currency Kiosk Operator	**Enacted**
Maryland	S 665	Uniform Disposition of Abandoned Property Act	To governor
Massachusetts	H 46	Financial Education in Schools	Pending
Massachusetts	H 88	Blockchain and Cryptocurrency	Pending
Massachusetts	H 89	Cryptocurrencies and Digital Assets	Pending
Massachusetts	H 1089	Virtual Currency Kiosk Operators	Pending
Massachusetts	H 1247	Regulations on Certain Virtual Currencies	Pending

Jurisdiction and Summary	Bill Number	Bill Title	Bill Status
Massachusetts	H 3279	Taxation and Investment in Digital Financial Assets	Pending
Massachusetts	S 38	Special Commission on Blockchain and Cryptocurrency	Pending
Massachusetts	S 40	Office of the State Treasurer	Pending
Massachusetts	S 707	Certain Virtual Currencies	Pending
Massachusetts	S 757	Certain Virtual Currencies	Pending
Massachusetts	S 804	Qualifying Virtual Currency Kiosk Operators	Pending
Massachusetts	S 1967	Bitcoin Strategic Reserve	Pending
Massachusetts	S 2008	Purchasing Power of State Funds	Pending
Michigan	H 4085	Cryptocurrency Mining	Pending
Michigan	H 4086	State Treasury	Pending
Michigan	H 4087	State Treasury	Pending
Michigan	H 4510	Retirement Fund	Pending
Michigan	H 4511	Digital Assets	Pending
Michigan	H 4512	Bitcoin Mining	Pending
Michigan	H 4513	Bitcoin Program	Pending
Michigan	HR 100	Date Designation	**Adopted**
Minnesota	H 2946	Minnesota Bitcoin Act	Pending
Minnesota	H 3253	Defines Central Bank Digital Currency	Pending
Minnesota	S 1879	Energy Savings Goals	Pending
Minnesota	S 2661	Minnesota Bitcoin Act	Pending

Jurisdiction and Summary	Bill Number	Bill Title	Bill Status
Minnesota	S 2768	Campaign Finance	Pending
Minnesota	S 3096	Elections	Pending
Mississippi	H 557	Central Bank Digital Currency Use	Failed
Mississippi	H 1042	Mississippi Bullion Depository	Failed
Mississippi	H 1043	Mississippi Bullion Depository	Failed
Mississippi	H 1590	Blockchain Basics Act	Failed
Missouri	H 433	Storage and Use of Gold and Silver	Pending
Missouri	H 630	Constitutional Money Act	Pending
Missouri	H 733	Storage and Treatment of Gold and Silver	Pending
Missouri	H 754	Standards for Certain Financial Organizations	Enacted
Missouri	H 754	Standards for Certain Financial Organizations	Pending
Missouri	H 970	Video Lottery Gaming Terminals	Pending
Missouri	H 1136	Digital Assets Authorization Act	Pending
Missouri	H 1217	Bitcoin Strategic Reserve Fund	Pending
Missouri	H 1428	Virtual Currency Kiosk Consumer Protection Act	Pending
Missouri	S 25	Modifies Provisions Relating to Gold and Silver	Pending
Missouri	S 98	Financial Institution Accounts Fraud	To governor
Missouri	S 194	Legal Tender	Pending
Missouri	S 309	Digital Assets	Pending

Jurisdiction and Summary	Bill Number	Bill Title	Bill Status
Missouri	S 614	New Provisions Relating to Digital Assets	Pending
Missouri	S 779	Virtual Currency	Pending
Montana	H 263	Digital Asset Mining and Data Center Ratemaking Laws	Failed
Montana	H 382	Specie Legal Tender Act	Failed
Montana	H 429	Precious Metals and Digital Assets Investment	Failed
Montana	H 453	Cryptocurrency Income Tax Payments	Failed
Montana	H 639	Gambling Laws	Failed
Montana	S 265	Financial Freedom and Innovation Act	**Enacted**
Montana	S 330	Blockchain and Digital Innovation Task Force	**Enacted**
Montana	S 426	Uniform Commercial Code	**Enacted**
Montana	S 535	Experimental Treatments	**Enacted**
N. Mariana Islands	None		
Nebraska	L 526	Cryptocurrency Mining Excise Tax	To governor
Nebraska	L 609	Controllable Electronic Record Fraud Prevention Act	**Enacted**
Nevada	S 258	Industrial Insurance	Enacted
New Hampshire	H 302	State Treasury Investments	**Enacted**
New Hampshire	H 310	Real World Assets	To governor
New Hampshire	H 639	Blockchain Basic Laws	Pending
New Jersey	A 449	Digital Payment Platform	Pending

Jurisdiction and Summary	Bill Number	Bill Title	Bill Status
New Jersey	A 1517	Financial Literacy Instruction	Pending
New Jersey	A 2249	Digital Asset and Blockchain Technology Act	Pending
New Jersey	A 2345	Virtual Currency and NFTs	Pending
New Jersey	A 4880	Cryptocurrency Automatic Teller Machines	Pending
New Jersey	A 5384	Virtual Currency Kiosk Consumer Protection	Pending
New Jersey	S 666	Virtual Currency and Blockchain Regulation Act	Pending
New Jersey	S 1304	Digital Asset and Blockchain Technology Act	Pending
New Jersey	S 1618	Digital Payment Platform	Pending
New Jersey	S 1634	Public Officials Gift Restrictions	Pending
New Jersey	S 3694	Cryptocurrency Automatic Teller Machines	Pending
New Jersey	S 4143	Artificial Intelligence Data Centers Energy Usage Plans	Pending
New Jersey	S 4288	Virtual Currency Kiosk Consumer Protection	Pending
New Mexico	H 363	Decentralized Unincorporated Nonprofit Act	Failed - Adjourned
New Mexico	S 275	Strategic Bitcoin Reserve Act	Failed - Adjourned
New York	A 213	State-Issued Cryptocurrency	Pending
New York	A 391	Virtual Tokens	Pending
New York	A 3279	State Cryptocurrency and Blockchain Study Task Force	Pending

Jurisdiction and Summary	Bill Number	Bill Title	Bill Status
New York	A 3307	2022 Uniform Law Commission Recommended Amendments	Pending
New York	A 5023	Election Contributions Made in Cash or Bitcoin	Pending
New York	A 5353	Electric Generating Facilities	Pending
New York	A 6266	Limited Purpose Trust Companies	Pending
New York	A 6515	Offenses of Virtual Token Fraud	Pending
New York	A 6549	New York Children's Online Safety Act	Pending
New York	A 7788	State Agencies Acceptance of Cryptocurrencies	Pending
New York	A 7807	Fiat-Collateralized Stablecoins As a Form of Bail	Pending
New York	A 8104	Study on Designation of Economic Empowerment Zones	Pending
New York	A 8718	Public Officials and Their Families	Pending
New York	A 8813	Regulation of Business Involving Virtual Currencies	Pending
New York	A 8966	Digital Asset Transactions	Pending
New York	A 9044	Person Offering Loot Boxes to Consumers	Pending
New York	S 1840	2022 Uniform Law Commission Recommended Amendments	Pending
New York	S 3262	Limited Purpose Trust Companies	Pending
New York	S 3347	State Energy Research and Development Authority	Pending
New York	S 3801	Digital Currency Task Force	Pending

Jurisdiction and Summary	Bill Number	Bill Title	Bill Status
New York	S 3985	Task Force to Study State Issued Cryptocurrency	Pending
New York	S 4728	State Cryptocurrency and Blockchain Study Task Force	Pending
New York	S 5473	Disclosures By a Developer of Virtual Tokens	Pending
New York	S 7672	Municipal Corporations Cybersecurity Incidents	Enacted
New York	S 7824	Offenses of Virtual Token Fraud and Illegal Rug Pulls	Pending
New York	S 8214	Public Officials and Their Families	Pending
North Carolina	H 40	General Statutes Commission Recommendations	Enacted
North Carolina	H 92	NC Digital Assets Investments Act	Pending
North Carolina	H 506	2025 State Investment Modernization Act	Pending
North Carolina	H 920	Digital Asset Freedom Act	Pending
North Carolina	S 117	Uniform Commercial Code	Pending
North Carolina	S 327	Bitcoin Reserve and Investment Act	Pending
North Carolina	S 709	State Investment Modernization Act	Pending
North Dakota	H 1149	Revised Uniform Unclaimed Property Act	**Enacted**
North Dakota	H 1184	Digital Asset and Precious Metal Investment	Failed
North Dakota	H 1239	Blockchain Technology Protection	Failed
North Dakota	H 1441	Specie Legal Tender	Failed

Jurisdiction and Summary	Bill Number	Bill Title	Bill Status
North Dakota	H 1447	Virtual Currency Kiosks	**Enacted**
North Dakota	HCR 3001	State Treasurer and State Investment Board	Failed
North Dakota	HCR 3022	Political Subdivisions	Failed
Ohio	H 18	Strategic Cryptocurrency Reserve Act	Pending
Ohio	H 116	Blockchain Basics Act	Pending
Ohio	H 426	Safekeeping and Management of Unclaimed Digital Assets	Pending
Ohio	S 57	Bitcoin Reserve Act	Pending
Oklahoma	H 1203	Strategic Bitcoin Reserve Act	Pending
Oklahoma	H 1871	Digital Currency	Pending
Oklahoma	H 1891	State Government	Pending
Oklahoma	S 325	Bitcoin	Pending
Oklahoma	S 611	State Government	Pending - Carryover
Oklahoma	S 785	Oklahoma Banking Code	Pending
Oklahoma	S 888	Digital Assets	Pending
Oklahoma	S 1083	Digital Assets	To governor
Oregon	H 2071	Blockchain Protocols and Digital Assets	Pending
Oregon	S 146	State Treasurer Study on Trust Property	Pending
Oregon	S 167	Uniform Commercial Code	**Enacted**
Pennsylvania	H 501	Alternative Energy Portfolio Standards Act	Pending

Jurisdiction and Summary	Bill Number	Bill Title	Bill Status
Pennsylvania	H 883	Virtual Currency Lenders	Pending
Pennsylvania	H 1210	Crypto Asset Mining Operations	Pending
Pennsylvania	H 1729	Online Safety for Children	Pending
Pennsylvania	H 1812	Ethics Standards and Financial Disclosure	Pending
Pennsylvania	S 66	Ethics Standards and Financial Disclosure	Pending
Pennsylvania	S 97	Code of Conduct	Pending
Pennsylvania	S 501	Alternative Energy Portfolio Standards Act	Pending
Puerto Rico	None		
Rhode Island	H 5121	Virtual Currency Kiosks Regulation	Pending
Rhode Island	H 5564	The State Economic Growth Blockchain Act	Pending
Rhode Island	H 5636	Financial Institutions Currency Transmissions	Pending
Rhode Island	H 5810	Proposal to Study Blockchain and Cryptocurrency	Pending
Rhode Island	H 5868	Prohibition of Production of Private Digital Asset Keys	Pending
Rhode Island	H 6007	The State Digital Asset Retention Act	Pending
Rhode Island	H 6290	Imposing a Wealth Tax on Individuals and Entities	Pending
Rhode Island	S 16	Financial Institutions Currency Transmissions	Pending

Jurisdiction and Summary	Bill Number	Bill Title	Bill Status
Rhode Island	S 373	To Study Blockchain and Cryptocurrency	Pending
Rhode Island	S 375	Prohibition of Production of Private Digital Asset Keys	Pending
Rhode Island	S 451	Personal Income Tax Exemptions	Pending
Rhode Island	S 779	Wealth Tax of Worldwide Wealth	Pending
South Carolina	H 3304	Central Bank Digital Currency	Pending
South Carolina	H 3442	Definition of Money	Pending
South Carolina	H 3454	Definition of Electronic	Pending - Carryover
South Carolina	H 3751	Modifications of Gross Income	Pending
South Carolina	H 4256	Digital Assets	Pending
South Carolina	S 163	Central Bank Digital Currency	Pending
South Carolina	S 444	Sports Wagering Act	Pending
South Dakota	H 1196	Uniform Unclaimed Property Act	**Enacted**
South Dakota	H 1202	State to Invest in Bitcoin	Failed - Adjourned
South Dakota	HCR 6006	State Investment Council Invest in Bitcoin	Failed - Adjourned
Tennessee	H 916	Campaigns and Campaign Finance	Pending
Tennessee	S 590	Campaigns and Campaign Finance	Pending
Texas	H 991	Abortion and Abortion Inducing Drugs	Pending
Texas	H 1598	Establishment of a Bitcoin Reserve	Pending

Jurisdiction and Summary	Bill Number	Bill Title	Bill Status
Texas	H 2767	Regulation of Online Global Marketplaces	Pending
Texas	H 2798	Virtual Currency Kiosk Transactions	Pending
Texas	H 3110	Civil Asset Forfeiture of Digital Currency	Pending
Texas	H 3301	Establishing the Permanent Public School Fund	Pending
Texas	H 4233	Requirements for Digital Asset Service Providers	Pending
Texas	H 4258	Authority of the Comptroller of Public Accounts	Pending
Texas	H 4853	Skimmers on Electronic Terminals	Pending
Texas	H 4908	Establishment of the Texas Prosperity Payout Fund	Pending
Texas	H 5510	Abortion Offenses	Pending
Texas	HJR 175	Right to Own Medium of Exchange	Pending
Texas	HJR 177	Constitutional Amendment	Pending
Texas	H 66, First Special Session	Women and Child Safety Act	Failed - Adjourned
Texas	H 80, Second Special Session	Abortion-Inducing Drug Distribution	Failed - Adjourned
Texas	S 1	General Appropriations Bill	Enacted
Texas	S 21	Strategic Bitcoin Reserve	Pending
Texas	S 665	Issuance of Gold and Silver Specie	Pending
Texas	S 778	Texas Strategic Bitcoin Reserve	Pending

Jurisdiction and Summary	Bill Number	Bill Title	Bill Status
Texas	S 1244	Unclaimed Securities and Virtual Currency	Pending
Texas	S 1498	Civil Asset Forfeiture of Digital Currency	Pending
Texas	S 1648	Regulation of Online Global Marketplaces	Pending
Texas	S 1705	Regulation of Virtual Currency Kiosks	Pending
Texas	S 1941	Digital Asset Service Provider Required Reports	Pending
Texas	S 2174	Requirements for Digital Asset Service Providers	Pending
Texas	S 2223	Amendments to the Uniform Commercial Code	Pending
Texas	S 2371	Skimmers on Electronic Terminals	To governor
Texas	S 2880	Abortion Civil Liabilities	Pending
Texas	S 2922	Issuance and Regulation of an Oil Backed Stablecoin	Pending
Texas	SCR 8	Creation of a Central Bank Digital Currency	Pending
Texas	SJR 55	Constitutional Amendment	Pending
U.S. Virgin Islands	None		
Utah	H 230	Blockchain and Digital Innovation Amendments	**Enacted**
Utah	H 306	Gold-backed Digital Payment System	Vetoed
Vermont	H 137	Regulation of Insurance Products and Services	Enacted

Jurisdiction and Summary	Bill Number	Bill Title	Bill Status
Vermont	H 206	Uniform Commercial Code	Enacted
Vermont	H 137	Regulation of Insurance Products and Services	**Enacted**
Vermont	H 370	Public Welfare	Pending
Vermont	S 129	Regulation of Virtual Currency Kiosk Operators	Pending
Virginia	H 1796	Decentralized Autonomous Organization	Vetoed
Virginia	H 2428	Classification of Tangible Personal Property	Failed
Virginia	S 1170	Disclosure of Digital Assets	Failed
Washington	H 1268	Virtual Currency Transaction Kiosks	Pending - Carryover
Washington	H 1319	Wealth Tax	Pending - Carryover
Washington	H 2046	Select Financial Intangible Assets Tax	Pending - Carryover
Washington	S 5280	Consumers of Virtual Currency Kiosks	Pending - Carryover
Washington	S 5316	Uniform Unclaimed Property Act	**Enacted**
Washington	S 5797	Tax on Stocks Bonds	Pending - Carryover
West Virginia	H 2383	Criminal Forfeiture Process Act	Failed - Adjourned
West Virginia	H 2463	Gold Silver and Crypto Currency Legal Tender	Failed - Adjourned
West Virginia	H 2673	Guilty Verdict	Failed - Adjourned

Jurisdiction and Summary	Bill Number	Bill Title	Bill Status
West Virginia	HCR 99	Preventing Financial Fraud and Scams	Failed - Adjourned
West Virginia	S 441	Digital Currency Backed by Gold	Failed - Adjourned
West Virginia	S 465	Precious Metals and Digital Currency Act	Failed - Adjourned
West Virginia	S 591	Criminal Forfeiture Process Act	Failed - Adjourned
Wisconsin	A 384	Virtual Currency Kiosks	Pending
Wisconsin	S 386	Virtual Currency Kiosks	Pending
Wisconsin	None		
Wyoming	H 137	Revision of Statutes and Other Legislative Enactments	**Enacted**
Wyoming	H 201	State Funds Investment in Bitcoin	Failed
Wyoming	H 264	Central Bank Digital Currencies	**Enacted**
Wyoming	H 308	Cryptographic Frontiers Act	Failed
Wyoming	S 95	Special Purpose Depository Institution Amendments	**Enacted**

Related Resources

Updated February 02, 2026

Housing and Homelessness Legislation Database

NCSL's Housing and Homelessness Legislation Database tracks filed bills in the 50 states, District of Columbia and U.S. territories.

Children and Families, Financial Services

Database

Updated February 02, 2026

Economic Mobility Enacted Legislation Database

Learn more about enacted legislation related to economic mobility while searching through our economic mobility database.

Children and Families, Financial Services

Database

Updated December 12, 2025

Housing and Homelessness Toolkit

State legislators seeking to tackle housing or homelessness issues have a variety of policy levers to consider. This collection of informational resources is a great starting point for understanding many aspects of housing and homelessness policy.

Children and Families, Financial Services

Stateline

Citing potential for fraud, blue and red states pass new crypto ATM laws

While the crypto machines can be used for legitimate reasons, they've become favored by scammers.

BY: **KEVIN HARDY** - JULY 28, 2025 10:00 AM

A cryptocurrency ATM is shown in a convenience store in 2022 in Miami. Several states have passed new laws regulating these machines, which officials say are increasingly being used to scam consumers. (Photo by Joe Raedle/Getty Images)

They may resemble other ATMs, but officials are increasingly warning about the potential for fraud with the expanding fleet of cryptocurrency ATMs popping up across the country.

The National Consumers League says the largely unregulated machines have become favored by scammers for their anonymity and irreversibility – once a user transfers or deposits funds, that money is essentially gone.

While officials say the machines can be used for legitimate purposes, red and blue states are increasingly imposing new regulations to protect consumers: AARP says 11 states have recently passed new laws or regulations of the machines.

"In state after state, AARP found lawmakers on both sides of the aisle and local law enforcement eager to work on commonsense rules that balance innovation and consumer safety," Nancy LeaMond, AARP's executive vice president and chief advocacy and engagement officer, said in a news release.

Last year, the FBI reported nearly 11,000 complaints of cryptocurrency ATM fraud. Those cases disproportionately affected older Americans and cost victims $246.7 million.

Cryptocurrencies are digital assets, including bitcoin, that offer an alternative payment or method without control of a central bank or government like other currencies. Crypto ATMs, sometimes called crypto kiosks, allow users to insert cash or use debit cards to convert currencies such as U.S. dollars into cryptocurrencies.

The Federal Trade Commission says crypto ATM scams often start with a call or text message warning of a supposed problem, such as unauthorized bank charges or suspicious activity on an Amazon account.

The FTC says consumers should contact banks or other institutions directly about any account issues. And it warns consumers not to believe anyone who says they must use a crypto ATM to address a financial problem.

"Real businesses and government agencies will never do that — anyone who does is a scammer," the agency said.

After signing a bill with new regulations, Nebraska Republican Gov. Jim Pillen was clear that the state would continue to welcome cryptocurrency businesses as it aims to become a hub for the industry.

The Nebraska law requires ATM operators to acquire state licensure, warn customers of the potential for criminal exploitation and take "reasonable steps to detect and prevent fraud." The law also limits transactions to $2,000 per day for new customers and $10,500 for existing customers, and requires operators to issue refunds for properly reported fraudulent transactions.

At least 40 states have introduced legislation regarding cryptocurrency, digital or virtual currencies and other digital assets in the 2025 legislative session, according to the National Conference of State Legislatures. Those measures include ATM regulations, prohibiting the use of digital currencies by governments and allowing state investment in digital assets.

Federal lawmakers are also taking action on the issue. The Republican-controlled U.S. House of Representatives declared the week of July 14 "Crypto Week," when lawmakers considered several pieces of legislation.

At the end of that week, President Donald Trump signed into law the GENIUS Act, the first major law governing digital currency. It establishes a regulatory framework for the industry.

Trump hopes the bill will instill confidence in the industry that spent heavily to strengthen its legitimacy and political might, The Associated Press reported.

"This signing is a massive validation of your hard work and your pioneering spirit," the president told crypto executives.

In state legislatures, new bills regulating crypto ATMS have enjoyed bipartisan support. AARP tracking shows new bills have been approved in Arkansas, Iowa and Oklahoma, as well as in more liberal states such as Maryland and Vermont.

In May, Arizona Democratic Gov. Katie Hobbs signed Republican-sponsored legislation that sets daily transaction limits and mandates crypto ATM operators provide customers certain disclosures and warnings.

The legislation followed local news coverage of at least two dozen crypto scams, including one that cost an Arizonan $28,000.

Stateline reporter Kevin Hardy can be reached at khardy@stateline.org.

AG Consumer Protection

Bitcoin ATMs – Frequent Source of Scams and Money Laundering

Bitcoin ATMs have become a preferred tool for scammers looking to defraud unsuspecting victims—especially seniors. These transactions are not like traditional financial transactions. The money sent through Bitcoin ATMs is nearly impossible to recover. This fact makes them an attractive option for criminals engaged in fraud and money laundering.

How Bitcoin ATM Scams Work

Scammers prey on the public's lack of familiarity with cryptocurrency. They exploit individual fears through sophisticated fraud schemes. A common scam targeting older adults involves a fraudulent message or phone call. The call might be from someone claiming to be with Apple, Google, or another well-known company, or even law enforcement. The scammer tells the victim that their financial accounts have been compromised. The call recipient is told they need to take immediate action to prevent unauthorized transactions on their account. If the scammer is pretending to be from a law enforcement agency, they may even threaten the victim with criminal prosecution or jail time if the victim doesn't pay a fine right away.

Victims are then instructed to withdraw large amounts of cash from their bank accounts. They are told to deposit the funds into a Bitcoin ATM. The cash is inserted and converted into Bitcoin. The victim is directed to scan and send a receipt or QR code to the scammer. The moment that transaction is completed, the money is gone — permanently. Traditional bank transfers, wire transfers, or credit card transactions have fraud prevention measures. These measures provide customer protection or financial institution safeguards to stop or reverse the transfer. That is not the case with Bitcoin ATM transactions.

Why Bitcoin ATMs Are a Major Risk

Bitcoin ATMs lack oversight and regulation. For this reason, they are widely used for scamming and money laundering. Some consumers may attempt to use them for legitimate transactions. However, they often come with very high fees. The fees make them an inefficient and costly way to buy cryptocurrency. It's safer and cheaper to convert cash to cryptocurrency through a licensed and regulated online exchange.

Without regulation, victims of Bitcoin ATM scams have no meaningful consumer protections. They also have little or no recourse for recovering their stolen funds. Financial institutions have fraud prevention departments that monitor transactions. Banks can file suspicious activity reports (SARs) to investigate potential fraud. Unfortunately, Bitcoin ATMs operate outside these safeguards. They allow scammers to steal money quickly and anonymously.

Real-Life Scams Cost Victims Thousands

Fraudsters employ Bitcoin ATMs for a well-known fraud scheme. They convince the victims that their Apple Pay or another account has been hacked. They urge the victim to withdraw their money and deposit it into a Bitcoin ATM. The scammers promise the money will be safe from hackers there in the ATM. The victim completes the transaction and sends a copy of the Bitcoin receipt to the scammers. The scammers then disappear with the money.

In another twist, the scammers may convince victims to download software onto their phones. This gives the criminals access to the victim's SIM card and phone data. The victims incur additional expenses when they discover they can only block the criminals' access to their information by purchasing another cell phone.

A Call for Stronger Consumer Protections

Bitcoin ATMs are an unchecked risk for consumers. Michigan is not alone in facing this growing problem. Some states have taken action by limiting Bitcoin ATM transactions to $1,000 per day. The amount scammers can steal from victims in a single transaction is significantly reduced in this way. A similar limit in Michigan could have prevented an elderly couple from losing their entire life savings.

How to Protect Yourself from Bitcoin ATM Scams

To avoid becoming a victim of a Bitcoin ATM scam, remember these key points:

- **No legitimate company or government agency will ever ask you to deposit money into a Bitcoin ATM**. If someone makes such a request, it's a scam
- **Beware of urgent requests**. Scammers create a sense of urgency to prevent victims from thinking critically about the request.
- **Do not trust caller ID**. Fraudsters can spoof phone numbers to make it appear as though they are calling from a trusted source
- **Never download unknown software or grant remote access to your devices**. This can allow scammers to take control of your personal information.
- **Talk to your bank before making large withdrawals**. If you're instructed to move money in an unusual way, seek advice first.
- **If you believe you have been targeted by a scam, report it immediately**. Scams can be reported to the Michigan Attorney General's Consumer Protection Team and local law enforcement.

Stay informed and help advocate for stronger regulations. In doing so, we can help protect consumers from the devastating impact of Bitcoin ATM scams. Urge your state legislators to support laws that limit these high-risk transactions if you are concerned about the lack of consumer protections surrounding Bitcoin ATMs.

Contact the Attorney General's Office:

For general consumer questions or to file a complaint, you may reach the Michigan Department of Attorney General's Consumer Protection Team at:

Consumer Protection Team
P.O. Box 30213
Lansing, MI 48909
517-335-7599
Fax: 517-241-3771
Toll-free: 877-765-8388
Online complaint form

Bitcoin ATMs – Frequent Source of Scams and Money Laundering

HB 324

“An Act relating to virtual currency kiosks; relating to transactions involving virtual currency; and relating to unfair trade or deceptive acts or practices."

Bitcoin ATMs increasingly used by scammers to target victims, critics say

Americans in 2024 lost nearly $250 million to scams that used Bitcoin ATMs

By Jay O'Brien and Lucien Bruggeman
October 9, 2025, 1:14 AM

"Yes, requesting crypto is now the No. 1 preferred method of criminals," Nofziger replied. "It is a huge problem."

Authorities have taken notice. Last month, the Washington, D.C., attorney general's office sued Athena Bitcoin, one of the largest bitcoin ATM machine purveyors in the country, accusing it of "pocketing hundreds of thousands of dollars in undisclosed fees on the backs of scam victims."

The lawsuit claims 93% of the transactions on Athena's devices in the District "are the product of outright fraud," and that "the median age of victims was 71 years."

https://abcnews.com/US/bitcoin-atms-increasingly-scammers-target-victims-critics/story?id=126305810

Crypto crime scene

How the companies behind crypto ATMs profit as Americans lose millions to scams

By Curt Devine, Majlie de Puy Kamp, Yahya Abou-Ghazala, Casey Tolan, Kyung Lah, Amy O'Kruk, Byron Manley and Eleanor Stubbs, CNN

Published October 14, 2025

TRANSACTION RECEIPT

Status: Pending coins

Market price: $67,000
Sales price: $83,400 +24%
Service fee: $3

Cash: $4,300
Bitcoin sent: 0.05155024 BTC

THANK YOU FOR USING BITCOIN DEPOT!

https://www.cnn.com/interactive/2025/10/us/crypto-atm-scams-companies-profit-invs-vis/

A CNN investigation, which included a review of more than 700 criminal cases and complaints, has found that crypto ATM companies make money by often marking up the price of cryptocurrency by 20% to 30% or more on transactions, including the illicit ones. Despite public claims, they often fail to refund money to victims and aggressively fight police to claw back scam money seized from machines.

The companies have also largely failed to adopt measures that could stifle scammers, such as strict transaction limits, and have heavily lobbied state legislatures to neuter laws that would force them to better protect victims. Some states have passed or proposed laws that closely match model legislation with fewer protections pushed by industry lobbyists.

In interviews with CNN, four former crypto ATM company employees said that companies are not doing enough to prevent fraud or help victims.

One former senior staffer at a crypto ATM company who spoke anonymously for fear of reprisal described the general philosophy at his former employer as, "it's not my problem if someone is stupid and gets scammed."

Another former staffer said, "If there was a way to prevent 100% of scams there is no way this industry would survive."

Multiple investigations from attorneys general and financial regulators have concluded many crypto ATM deposits involve scams, findings that came after interviewing hundreds of victims and reviewing thousands of transactions. Last month, the DC attorney general alleged that more than 90% of deposits in one company's ATMs came from fraud.

What's driving business

Crypto ATM companies have argued fraud is not a significant driver of business, with some highlighting a report by the analytics group TRM Labs, which found that 1.2% of cash-to-crypto transactions were illicit in 2023.

But even the analytics group behind that report acknowledged in a statement to CNN that "the reality is clear: a significant share of scams and fraud move through these machines."

Iowa's attorney general sued Bitcoin Depot this year, alleging that scams accounted for "more than half of all money taken in by Bitcoin Depot in Iowa" over a roughly three-year period ending in 2024, more than $7 million in scam transactions. The attorney general said in another suit that CoinFlip's top 20 users in the state were all scam victims. The companies have disputed the claims in court.

Documents show a regulator in Maine denied a license application from Bitcoin Depot in April on the grounds that its crypto ATMs "caused an unacceptably high number of Maine consumers to suffer financial loss." The state concluded that elderly consumers accounted for more than 70% of money transmitted on its machines in the state over about two years. The regulator also found the company's ATMs lack "necessary controls, warnings, and safeguards."

In June, Australian authorities said they contacted 90 people who were among the biggest crypto ATM users and found that around 85% were scam victims or "money mules" who had been coerced into moving suspected illicit funds through the ATMs, according to AUSTRAC, the country's financial intelligence unit.

https://www.cnn.com/interactive/2025/10/us/crypto-atm-scams-companies-profit-invs-vis/

A vector for money laundering

Those anecdotal findings are echoed by a CNN analysis of blockchain data over the last decade, which shows that the bulk of all cash deposited in ATMs operated by the biggest US companies has ended up on exchanges based overseas.

Some law enforcement officials said the prevalence of such overseas transfers raises questions about the companies' claims that a small minority of their users' transactions are illegitimate.

Most of the top 10 exchanges that received funds say their services aren't accessible to US users, and many are based in jurisdictions with historically weak anti-money laundering laws, such as the Cayman Islands and Nigeria, CNN's analysis found.

"It's a red flag to us, knowing that a large majority of financial crimes that are happening in the United States are run by overseas actors," said a Secret Service official who requested anonymity due to the sensitivity of their position. "It likely is a money laundering indicator if large fees are charged and people are willing to pay those when there are other options that are much cheaper and just as convenient."

https://www.cnn.com/interactive/2025/10/us/crypto-atm-scams-companies-profit-invs-vis/

Crypto kiosk companies claim no liability

Police try to assist when victims call for help – but often have little recourse. That's what happened to Cason, the Iowa victim.

When Cason contacted the sheriff's office in July 2023, investigators got a search warrant for the machine and seized the cash he had deposited, intending to return the money to him.

But Bitcoin Depot argued in court that Cason had authorized the transaction and had agreed to the company's terms of service when he used the machine. His cash had already been turned into cryptocurrency and transferred away, the company said.

The case went all the way to Iowa's state Supreme Court, which ruled in favor of Bitcoin Depot in the spring. Because scammers had convinced Cason to bypass company requirements that users only send funds to crypto wallets they control, the court found Bitcoin Depot wasn't liable.

Cason never saw the cash again.

https://www.cnn.com/interactive/2025/10/us/crypto-atm-scams-companies-profit-invs-vis/

- Scammers often have victims use established crypto wallets to bypass new account restrictions.
- Crypto kiosk companies have argued in court that because scammers convince victims to bypass the terms of service on the kiosk, the kiosk company is not liable or subject to offer refunds.

Non-Comprehensive List of States in Litigation with Crypto Kiosk Operators

- Massachusetts
- Pennsylvania
- Iowa
- Maine
- California
- Missouri
- Arizona
- Indiana

- Washington DC

Attorney General Schwalb Sues Crypto ATM Operator for Financially Exploiting District Residents

September 8, 2025

Lawsuit Alleges That 93% of Deposits to Athena Bitcoin, Inc. Are From Scams That Target Vulnerable Residents & Seniors & That Athena Profits from Illegal, Hidden Fees

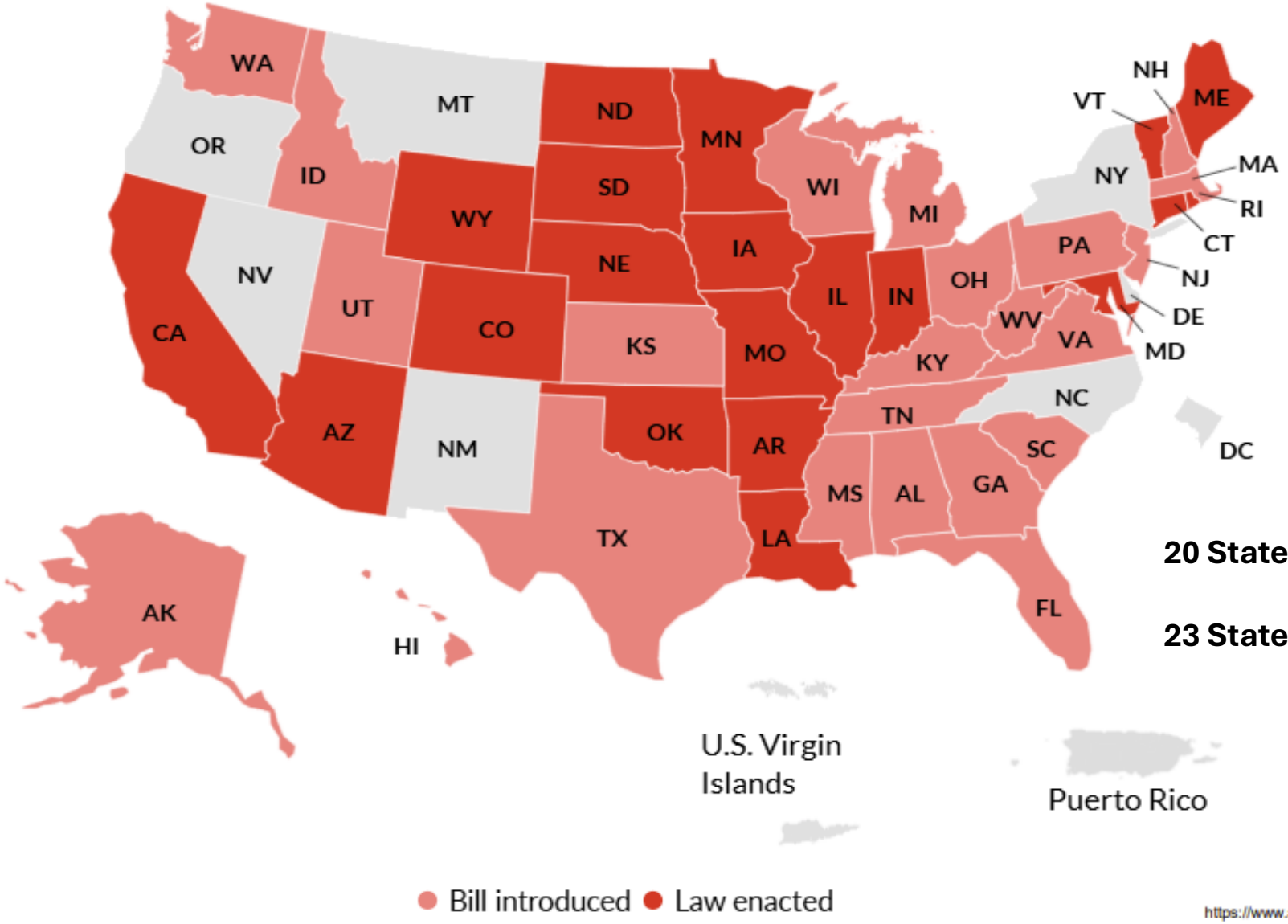
Attorney General Brian L. Schwalb today sued Athena Bitcoin, Inc. (Athena), one of the country's largest operators of Bitcoin Automated Teller Machines (BTMs), for charging undisclosed fees on deposits that it knows are often the result of scams, and for failing to implement adequate anti-fraud measures. When users discover they have been scammed and seek refunds, Athena imposes a strict "no refunds" policy on their entire transactions—even failing to return the significant undisclosed fees it collects from scam victims.

An investigation by the Office of the Attorney General (OAG) showed that Athena BTMs appeal to criminals because Athena fails to provide effective oversight, creating an unchecked opportunity for illicit international fraud. Athena BTMs are most frequently used by scammers targeting elderly users who are less familiar with cryptocurrency and less likely to report fraud. According to the company's own data from its first five months of operations in the District:

- 93% of all Athena BTM deposits were the direct result of scams;
- Nearly half of all deposits were flagged to Athena as the product of fraud;
- Victims' median age was 71; and
- The median amount lost per scam transaction was $8,000, with one victim losing a total of $98,000 in nineteen transactions over a period of several days.

https://oag.dc.gov/release/attorney-general-schwalb-sues-crypto-atm-operator

States With, or Considering, Cryptocurrency Kiosk Legislation



20 States w/ Law Enacted

23 States w/ Law Introduced

https://www.aarp.org/advocacy/crypto-atm-fraud-protections/

What Happens After Legislation?

THE BOTTOM LINE

The crypto ATM's days in America may be numbered

PUBLISHED SAT, JAN 10 2026-10:06 AM EST UPDATED SUN, JAN 11 2026-11:26 AM EST

Kevin Williams

WATCH LIVE

KEY POINTS

Cryptocurrency ATM machines are a magnet for scammers who dupe unwitting victims into sending large sums of money overseas.

Spokane, Washington, became the largest municipality in the United States to enact a ban on all crypto ATMs within the city limits.

80 percent of the world's bitcoin teller machines are located in the U.S.

https://www.cnbc.com/2026/01/10/bitcoin-crypto-atm-scam-fraud-regulation.html

The Spokane ban was one of the first in the nation, following a similar ordinance passed in Stillwater, Minnesota, after a resident was scammed there. "We've received no complaints about the removal," Dillon said. He is hopeful that the legislature will pass a statewide ban in the next session (which begins Monday) which would stop the crypto ATMs from simply being relocated to neighboring municipalities.

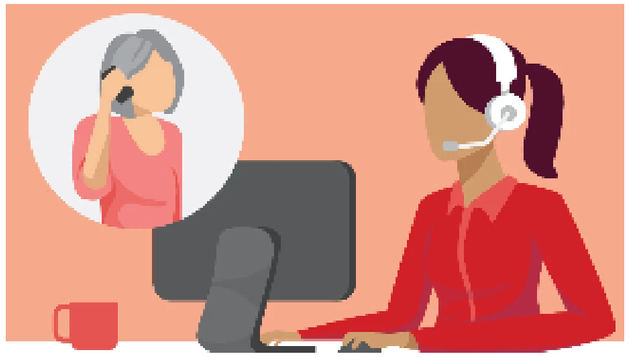
Questions?

AARP Alaska

Consumer Protections for Crypto Kiosks

Why is AARP focused on this?

Criminals are **using crypto kiosks to steal hundreds of millions of dollars from Americans** each year through scams. AARP, through our Fraud Watch Network, noticed **more and more older Americans being impacted** by this type of crime.



WORK & FINANCES

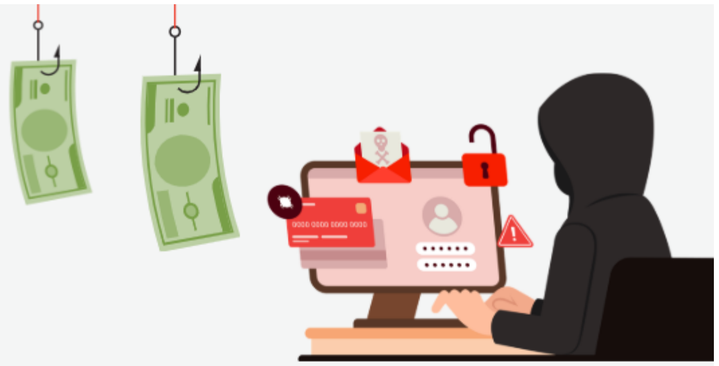
AARP Fraud Watch Network™ Helpline

AARP Alaska

Crypto ATMs: The Latest Tool in Scammers' Arsenal

By Teresa Holt, AARP Alaska

Published January 22, 2026



Mabel's Story

Mabel, a 79-year-old who contacted AARP's Fraud Watch Network Helpline, searched a number for Netflix online and instead of finding a legitimate Netflix number, found herself in touch with Netflix impersonators who scammed her.

Mabel sent over $250,000 via a crypto kiosk. She also purchased gold bars and cashier's checks to be picked up by what turned out to be a government impersonator.

What does the data show?

$246.7 million total theft from Americans via crypto kiosk reported to IC3 in 2024

Cryptocurrency ATMs/Kiosks

10,956 Complaints; $246.7 Million in Losses

99% Increase in Complaints from 2023
31% Increase in Losses from 2023

The FBI Warns of Fraudulent Schemes Leveraging Cryptocurrency ATMs and QR Codes to Facilitate Payment

REPORTS of CRYPTO ATM/KIOSK USE by AGE GROUP

Age Group	Count	Losses
Under 20	7	$51,913
20 - 29	280	$3,739,620
30 - 39	361	$4,241,387
40 - 49	319	$3,621,774
50 – 59	349	$5,523,230
Over 60	2,674	$107,206,251

CRIME TYPES MOST ASSOCIATED WITH CRYPTO ATM USE

	Count	Losses		Count	Losses
Extortion	4,189	$5,601,953	Government Impersonation	1,786	$44,587,335
Tech Support	3,037	$107,429,709	Investment	606	$38,090,269

Alaska

In **2023**:

- 2 complaints
- $36,779 losses

In **2024**:

- 48 complaints
- $917,758 losses

Source: FBI 2024 Annual IC3 Report: https://www.ic3.gov/AnnualReport/Reports/2024_IC3Report.pdf

What is a crypto kiosk and how does it work?

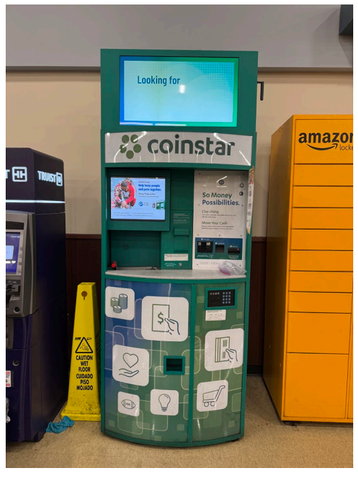
- Also called “crypto ATMs” or “virtual currency ATMs” or “Bitcoin ATMs” or “BTMs”
- Allow users to **insert cash** and have cryptocurrency **sent to a digital wallet**
- Some kiosks also allow you to sell your cryptocurrency to the kiosk in exchange for cash
- Crypto kiosks are regulated as Money Services Businesses at the federal level, **but lack state-level regulation in many states, including Alaska**.
- **Different from centralized cryptocurrency exchanges** like Coinbase, Gemini, or Kraken, which do not have physical locations
- **Charge high fees** to exchange funds (7-50%)

COINFLIP

ATHENA BITCOIN

BITCOIN DEPOT

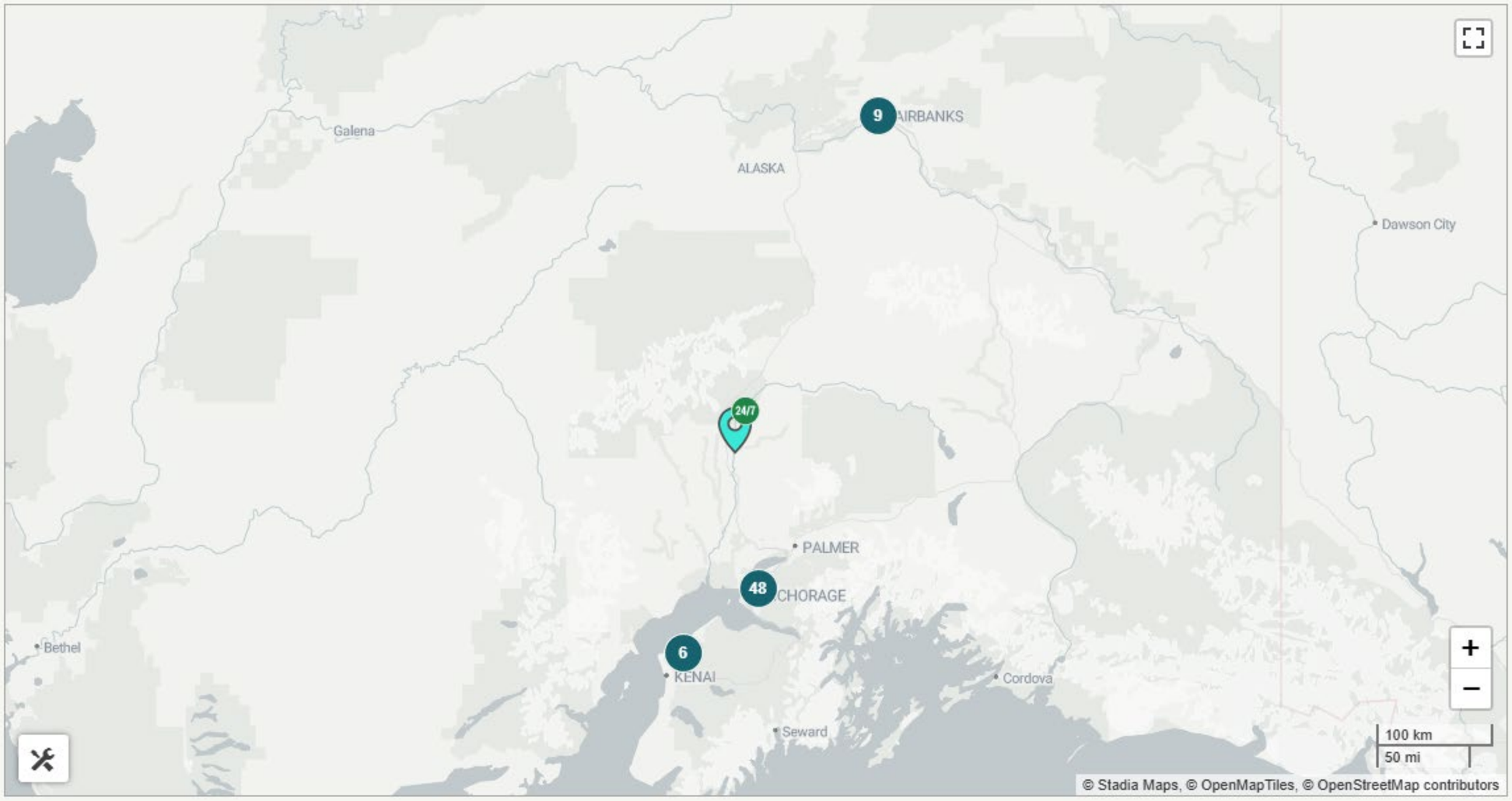
rockitcoin



AARP® Crypto Kiosks in Alaska

Bitcoin ATMs in Alaska, United States.

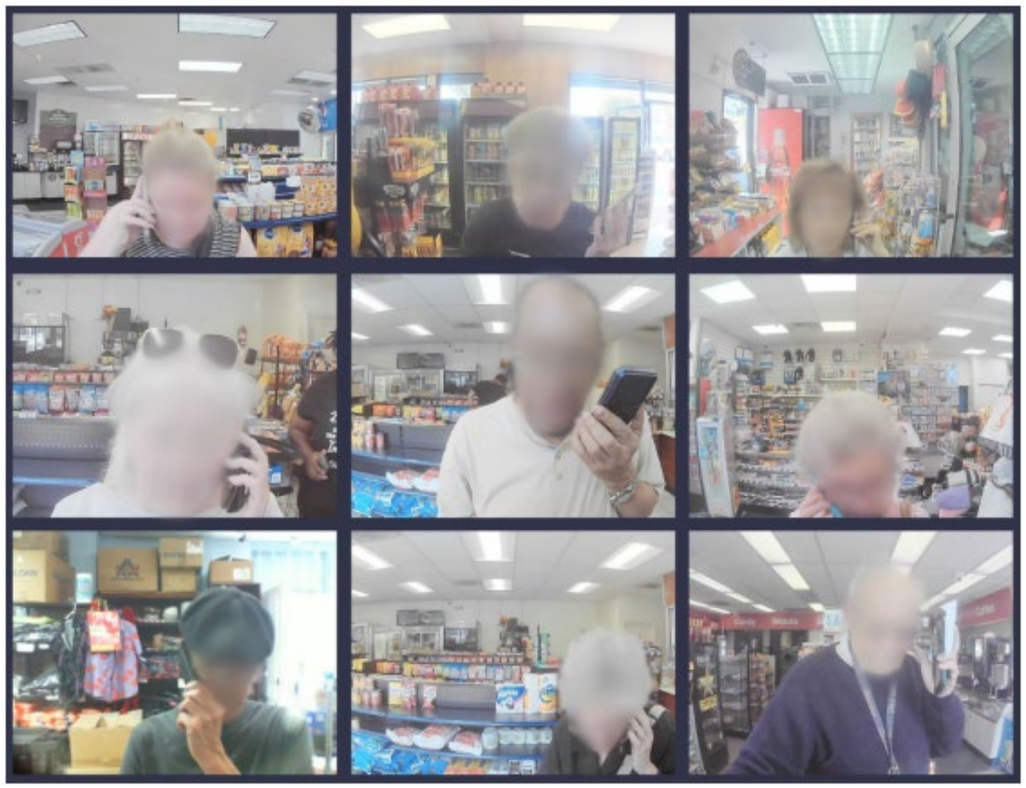
Total number of Bitcoin ATMs / Tellers in Alaska, AK: 64



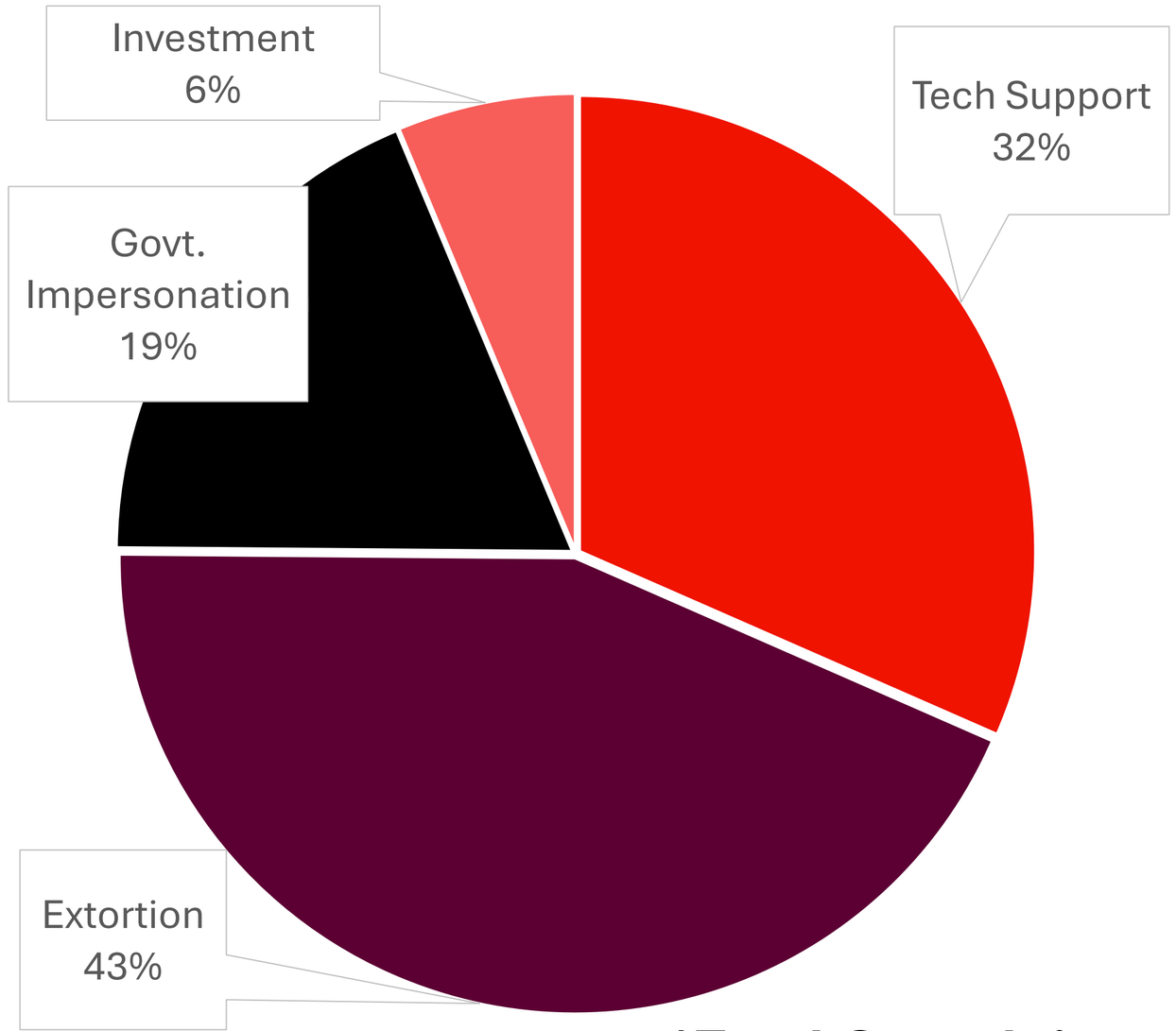
Source: Coin ATM Radar: https://coinatmradar.com/state/3/bitcoin-atm-alaska/

How do these scams work?

Victims being coached to send funds using a cryptocurrency kiosk.



Percent of Total Complaints*



***Total Complaints: 9,618 (2024)**

Source: FBI 2024 Annual IC3 Report:
https://www.ic3.gov/AnnualReport/Reports/2024_IC3Report.pdf

Questions?

Legislative Principles

AARP is advocating across the country for important consumer protections that will deter criminals from leveraging cryptocurrency kiosks in their schemes. This will prevent older Americans from losing hard-earned money to criminals.

We support legislative principles that will increase the safety of these kiosks by:

- **Requiring money transmitter licensing** of cryptocurrency kiosk operators in the state
- Implementing **daily transaction limits** to limit the appeal of these machines to criminals
- **Completing user identification verification** prior to transacting
- **Printing receipts** with relevant transactional information, which allow law enforcement to investigate immediately
- Requiring cryptocurrency operators to **refund** transactions related to fraud
- **Clearly displaying the fees** and exchange rate charged
- **Posting fraud warning notices** and clarifying steps people should take if they suspect fraudulent activity