IN THE CIRCUIT COURT OF JASPER COUNTY
29TH JUDICIAL CIRCUIT
STATE OF MISSOURI

THE STATE OF MISSOURI ex rel. CATHERINE L. HANAWAY, ATTORNEY GENERAL Plaintiff, v. GPD HOLDINGS LLC d/b/a COINFLIP, Defendant.	No. _____ **JURY TRIAL DEMANDED**

PETITION FOR RELIEF

INTRODUCTION

1. It's a story that's far too common: A foreign scammer targets vulnerable or unsophisticated people claiming that they must transfer large sums of money immediately. Sometimes the scammer offers an enticing investment opportunity or a reward to unlock by first sending a sum of money. Other times, it's the promise of a budding romance, where the faceless partner then claims to need financial help. And still others, it's flat-out extortion—with scammers saying that the target is in deep legal trouble and needs to make an immediate payment or that a target's loved one is stuck in a foreign country and requires a money transfer promptly. Unfortunately, scammers' imaginations know no bounds. But the stories all have the same ending—innocent people lose their hard-earned money. Even worse, the targets of these scams often are the elderly on fixed incomes. And because the scammers are

frequently in another country, the prospects of justice and financial recovery for the victims are next-to-zero.

2. Even as governments and technology companies have found ways to thwart scammers' efforts, the charlatans have adapted their practices. Cryptocurrency has sadly proven itself an effective means for scammers to hide their tracks and avoid the paper trails of standard financial transactions. Thus, scammers now routinely demand that victims pony up with cryptocurrency.

3. Disgustingly, private companies exist that facilitate and then handsomely profit off these financially devastating swindles. Defendant GPD Holdings LLC d/b/a CoinFlip is but one such company. CoinFlip operates "Bitcoin ATMs"—electronic terminals that convert regular currency into Bitcoin (the best-known cryptocurrency). Once the money is converted, the consumer can then send the cryptocurrency to accounts all over the world. As such, scam victims will use readily accessible Bitcoin ATMs—often found in gas stations, liquor stores, bars, vape shops, and other retail venues—to convert, send, and then forever lose their money.

4. Not only does CoinFlip knowingly facilitate fraudulent transactions—it profits from them with hidden and excessive fees. Specifically, when a victim uses a CoinFlip ATM to convert their cash into Bitcoin, CoinFlip imposes fees on the transaction. These fees can be upwards of 20% of the transaction's value. But CoinFlip has not routinely disclosed these transaction fees clearly and concisely. Instead, CoinFlip has compounded the injury to victims by making victims pay more and hiding how much of a cut CoinFlip gets from the fraud.

5. The victims of these scams describe the nightmares they suffered, aided and abetted by CoinFlip. In the fall of 2025, someone using the name Selina Lee contacted Victim #1—an 80-year-old veteran—by text message. Victim #1 did not know Lee. During their text conversation, Lee claimed to have made a lot of money through cryptocurrency and encouraged Victim #1 to invest in Bitcoin through an investment business called CoinFlip. He ultimately sent Lee a total of $180,000.00–$200,000.00 from September 2025 to March 2026. Lee continued to request more and more money until Victim #1 had nothing left. He sold his vehicle, pulled money out of his legitimate investment accounts, and almost lost his apartment. Luckily, a friend helped pay his rent and some other expenses. At one point, Lee told Victim #1 she wanted to combine her money with his money. But Victim #1 stopped talking with Lee in March 2026, before he could be bilked further.

6. When Victim #1 deposited cash into the CoinFlip ATM, he directed the transaction to a specific Bitcoin wallet number. The ATM itself never clearly stated a fee that Victim #1 would be charged for the transaction—only the unknown fraudster Lee told him that there would be a fee of $5,000 to $15,000. Sometimes he spoke with Lee on the phone, while other times he believed he was speaking with someone from CoinFlip, via text message, telling him what to do.

7. When Victim #1 tried to withdraw his funds from the ATM, he would receive a text message, from a person he believed was a CoinFlip representative. The withdrawal transaction would always fail due to him needing to verify his identity or some other nonsense excuse.

8. Victim #1 was never able to get any of his money back. He does not have anything left of his savings and subsists off Social Security. He has filed complaints with the FBI and with the St. Peters, Missouri Police Department. He never heard back from the FBI, and the St. Peters Police Department has said that they cannot help him.

9. In March of 2026, Victim #2 received a phone call from a female claiming to be a police officer with the Jefferson County Sheriff's Office. The scammer told her that she had two existing warrants for missing jury duty. Victim #2 told the caller that she was excused from jury duty the prior August and the court was supposed to send her a letter, but they never did. The caller told her that the jury pool session got moved from August 2025, to March 6, 2026 and since she missed jury duty on two occasions there were two warrants issued for her arrest. The female caller told Victim #2 that she would need to pay the fines to avoid arrest.

10. Victim #2 became upset and scared. She believed this phone call was legitimate because the caller knew about her jury duty and the exemption in Jefferson County from the previous August. The caller transferred Victim #2 to a second supposed police officer who told her she was sending three forms via text message that Victim #2 would need to fill out and pay the fees of $10,000 to deactivate the warrants. Victim #2 said she could not pay $10,000. The caller then changed the demand to $2,500 and said she would need to deposit the payment in a cryptocurrency ATM. Victim #2 packed up her infant daughter and drove to her bank where she withdrew $1,000 in cash.

11. After leaving her bank, the caller directed her to a vape shop with a CoinFlip ATM to deposit the cash. Two buttons appeared on the CoinFlip ATM screen asking Victim #2 if she wanted to deposit less than $1,000 or more than $1,000 and she selected the less-than-$1,000 button. The CoinFlip ATM then asked what currency she wanted to use. A male vape shop employee asked Victim #2 if she knew whom she was talking to and whether she was sending money to someone she knew. The employee told her to hang up the phone because she was being scammed. Victim #2 then called the phone number on the ATM and spoke with a CoinFlip employee who told her that he would text her a code and she would have to repeat it back to him, so he could send her the documents to file a complaint. Victim #2 thought this too was a scam and she hung up the phone, left the vape shop, and went home.

12. Victim #2 did not receive a receipt from the CoinFlip ATM and she had no idea where her $1,000 went until later that day when she corresponded with a CoinFlip representative. The CoinFlip representative said he was familiar with the scam and said he was not sure if she could get her money back. In the end, he told her that she could only get the fees on the transaction refunded—$182.38. Victim #2 does not recall any conspicuous disclosures about transaction fees.

13. In April 2025, Victim #3 received a call from someone purporting to be from the Boone County Sheriff's Office. The caller told her she had a warrant for her arrest and needed to go to the Sheriff's Office and pay $9,600 to cancel the warrants. Victim #3 advised she did not have that much money. The caller then told her to pay $1,000 by going to a "police monitored" CoinFlip ATM. There was a sign on the

machine that stated it was "FDIC Police Monitored." The caller stayed with her on the phone and walked her through how to deposit the cash. She deposited $900 and immediately tried to cancel as she suspected she was being scammed. She called CoinFlip and was told the money was already gone and they could not help her. She has not been able to get her money back.

14. CoinFlip knows that its machines are used to perpetrate devastating financial frauds. Yet the company is content to profit (handsomely) off each such transaction. And it has added insult to injury by not having fully disclosed to victims the actual transaction costs that they face in using these machines to convert their dollars into Bitcoin. Imposing these hidden costs qualifies as a straightforward violation of the Missouri Merchandising Practices Act (MMPA).

THE PARTIES

15. Plaintiff State of Missouri is a sovereign State of the United States of America.

16. Catherine L. Hanaway is the Attorney General of the State of Missouri. Attorney General Hanaway is authorized to "institute, in the name and on the behalf of the state, all civil suits and other proceedings at law or in equity requisite or necessary to protect the rights and interests of the state, and enforce any and all rights, interests or claims against any and all persons, firms or corporations in whatever court or jurisdiction such action may be necessary; and he may also appear and interplead, answer or defend, in any proceeding or tribunal in which the state's interests are involved." Mo. Rev. Stat. § 27.060.

17. The MMPA authorizes the Attorney General to file suit "[w]henever it appears to [her] that a person has engaged in, is engaging in, or is about to engage in any method, act, use, practice or solicitation, or any combination thereof, declared to be unlawful by" the MMPA. *Id.* § 407.100. She may seek civil penalties, restitution, and damages, among other relief. *Id.*

18. Defendant is GPD Holdings LLC d/b/a CoinFlip, a foreign business entity headquartered at 433 W. Van Buren Street, Suite 1050N, Chicago, IL 60607.

JURISDICTION AND VENUE

19. This Court has jurisdiction under Mo. Rev. Stat. §§ 407.020, .100, 526.010.1, .030–.050, and 527.010.

20. Venue is proper in this Court under the MMPA venue provisions (Section 407.100), as well as the venue provisions of Section 508.010.

21. Under the MMPA, venue is appropriate in any county "in which the violation alleged to have been committed occurred." *Id.* § 407.100. CoinFlip has engaged in deceptive or unfair trade practices in Carthage, Jasper County.

22. CoinFlip maintains two of its ATM machines in Carthage, Missouri. The first is located at the Wagon Liquor, 157 E. Central Avenue, Carthage, MO 64836. The second is at Vapor Maven, 2426 Grand Avenue, Carthage, MO 64836. According to CoinFlip's website, these machines operate seven days a week.

23. Because venue exists under the specialized venue provision of the MMPA, the State need not satisfy the general venue provision of Section 508.100. But in any event, that statute is satisfied as well. Because CoinFlip is a nonresident, "suit may be brought in any county in this state." *Id.* § 508.010.2(4).

FACTUAL ALLEGATIONS

24. CoinFlip makes representations on its website that it directs to individuals in Missouri, including in Carthage, Jasper County.

25. CoinFlip advertises itself as the "world's largest network of cryptocurrency ATMs by transaction volume." *Who We Are*, CoinFlip, available at https://coinflip.tech/about (last visited May 11, 2026). CoinFlip boasts of a network of more than 5,500 Bitcoin ATMs (BTMs) across the United States and several other countries. *Id.* As of September 26, 2025, CoinFlip operated 143 BTMs in Missouri.

26. CoinFlip uses retail-partnership contracts to place its BTMs in places like convenience stores, liquor stores, vape shops, and gas stations.

27. CoinFlip reports that it has processed over one million transactions for over 300,000 loyal customers. *Who We Are*, CoinFlip, available at https://coinflip.tech/about (last visited May 11, 2026).

28. A sizeable portion of those transactions have occurred in the State of Missouri—as evidenced by CoinFlip's maintaining over 140 BTMs within the State. Many of these transactions have been identifiable fraudulent transactions. The Attorney General has spoken to or received complaints from several users of CoinFlip's BTMs in Missouri—with three victims' experiences recounted above. The transactions of these users occurred because of a scam and represent hundreds of thousands of dollars in transactions.

29. The Attorney General reasonably believes the number of known scam transactions will grow as more consumers are contacted. On information and belief, the fraudulent losses of Missourians at CoinFlip BTMs total in the millions of dollars.

I. BTMs and scams go hand-in-hand.

30. Cryptocurrency has surged as swindlers' payment-method of choice in recent years because it is portable, difficult to trace, and transactions conducted through cryptocurrency are irreversible.

31. Widespread access to BTMs has made this possible. Reported losses using BTMs overwhelmingly come from fraudsters impersonating government officials, business representatives, and tech-support teams. Scammers often direct victims to BTMs and give step-by-step instructions on how to insert money and convert it to cryptocurrency. *What To Know About Cryptocurrency and Scams*, Fed. Trade Comm'n (May 2022), https://consumer.ftc.gov/articles/what-know-about-cryptocurrency-scams#scams.

32. When people use BTMs, their reported losses are exceptionally high—federally, the median reported loss is $10,000. Emma Fletcher, *Bitcoin ATMs: A Payment Portal for Scammers*, Fed. Trade Comm'n (Sept. 3, 2024), https://www.ftc.gov/news-events/data-visualizations/data-spotlight/2024/09/bitcoin-atms-payment-portal-scammers.

33. The Federal Trade Commission reports that fraud losses at BTMs are "skyrocketing"—increasing nearly tenfold from 2020 to 2023. *Id.* In just the first half of 2024, reported fraud losses were over $65 million. *Id.* This sum likely reflects only a fraction of the harm since the vast majority of frauds go unreported. *Id.*

34. Tragically, these frauds particularly affect older adults. Since 2020, reported fraud losses by seniors have increased over twentyfold on scams using cryptocurrency as the payment method (compared to an eightfold increase in scams

using bank transfer). Protecting Older Consumers 2024–2025, at 26–27, Fed. Trade Comm'n (Dec. 1, 2025), https://www.ftc.gov/system/files/ftc_gov/pdf/P144400-OlderAdultsReportDec2025.pdf.

35. These scams work by directing older adults to deposit cash into BTM machines. *Id.* at 24, 29.

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

Cryptocurrency ATMs/Kiosks

13,460 Complaints; $389 million in Losses

23% Increase in Complaints from 2024
58% Increase in Losses from 2024

The FBI Warns of Fraudulent Schemes Leveraging Cryptocurrency ATMs and QR Codes to Facilitate Payment

Crypto ATM/Kiosk Use Reported by Age Group

Age Group	Count	Losses
Under 20	58	$124,013
20 - 29	825	$6,474,240
30 - 39	1,275	$10,936,943
40 - 49	1,472	$20,826,227
50 – 59	1,524	$44,584,724
60+	6,188	$257,466,130

Internet Crime Complaint Ctr., *Federal Bureau of Investigation Internet Crime Report 2025*, at 53, https://www.ic3.gov/AnnualReport/Reports/2025_IC3Report.pdf. Americans over age sixty report more than quadruple the aggregate scam transactions, and more than 40% greater average losses per transaction than the next-oldest age cohort. *Id.*

37. On information and belief, Missourians' transaction volumes and amounts through CoinFlip's BTMs similarly increase by age.

II. CoinFlip advertises its BTMs as safe, but in practice, CoinFlip facilitates pervasive scam transactions.

38. Contrary to its stated focus on fraud prevention, CoinFlip's records show its inability to prevent scam transactions processed through its Missouri BTMs. CoinFlip is engaged in "deception, fraud, false pretense, false promise, misrepresentation, unfair practice or the concealment, suppression, or omission of any material fact in connection" with the continued operation of their BTMs in Missouri. Mo. Rev. Stat. § 407.020.1.

39. CoinFlip publicly states that its BTMs are safe and have fraud-prevention mechanisms. Yet, scam transactions at its Missouri BTMs continue to occur regularly.

40. In a blogpost entitled, "Are Bitcoin ATMs Safe?" published on CoinFlip's website, the post proclaims that a BTM "is a safe option" to buy Bitcoin. Scott Wilson, *Are Bitcoin ATMs Safe?* (Oct. 29, 2025), https://coinflip.tech/blog/are-bitcoin-atms-safe. According to the blogpost, BTMs provide "a safe and secure option to instantly buy and sell cryptocurrency." *Id.*

41. In another blogpost, CoinFlip writes that BTMs "are the safest way to buy bitcoin with cash and other cryptocurrencies using cash." CoinFlip, *What Is a Crypto ATM and How Does It Work?* (Nov. 3, 2021), https://coinflip.tech/blog/what-is-a-crypto-atm-and-how-does-it-work.

42. CoinFlip also asserts that it "work[s] hard with compliance teams and other parties to prevent scams." Wilson, *supra* ¶ 40.

43. CoinFlip advertises that it employs a process that "strengthen[s] the barriers against fraud, money laundering, and other illicit activities." CoinFlip, *Get to Know "KYC" in Crypto* (May 30, 2024), https://coinflip.tech/blog/getting-to-know-kyc-in-crypto. According to CoinFlip, this "Know Your Customer" process is a "roadblock from criminal activities" and "deter[s] fraudsters and money launderers from exploiting the anonymity of digital currencies." *Id.* It "provides CoinFlip the necessary information to discover bad actors and uphold the integrity of the crypto market." *Id.*

44. CoinFlip says that its BTMs provide scam protection. It advertises that it protects customers from fraud by: (1) "Blockchain analytics to detect and prevent suspicious activity"; (2) "A dedicated, internal Compliance team leading our regulatory efforts"; (3) "Educational resources to increase awareness of common scams"; and (4) "Live customer support ready to assist in real-time." CoinFlip's training and compliance documents also speak at length about the dangers of money transfers, the prevalence of scams, and the various ways to identify potential scams.

45. But CoinFlip knows that many of the transactions it processes are coerced or unwanted—initiated by or at the behest of scammers.

46. Hence, despite publically portraying itself as being concerned about fraud and scams and as protecting its customers from fraud, CoinFlip's reality tells a different story.

47. CoinFlip knows that suspicious activity is occurring based on the digital "wallets" into which converted Bitcoin gets deposited. Ordinarily, consumers should

have their own wallet where their newly converted cryptocurrency ends up. In other words, the wallet and the cryptocurrency in it should remain under the consumer's control. Yet, CoinFlip regularly processes transactions where an individual sends money to a different person's digital wallet. This is evident from transactions because *other consumers* have already sent cryptocurrency to that wallet. And this occurs despite CoinFlip's compliance training stating that the person converting the cryptocurrency must control the destination wallet.

48. CoinFlip knows that bad actors use its BTMs to collect proceeds. The company logs "blacklist reported criminal and terrorist wallet addresses."

49. CoinFlip's records include many other obvious warning signs of fraud being perpetrated through their machines.

a. CoinFlip's customer base is overwhelmingly older. CoinFlip acknowledges that "elder financial exploitation" is "one of the fastest-growing forms of fraud." CoinFlip's example is telling: "An elder can be drawn into a money mule scheme through coercion or deception and then be directed to transfer money between accounts on behalf of criminal third parties." CoinFlip established a "Financial Exploitation Reporting Policy" to educate its employees about "financial exploitation of vulnerable adults" and to establish procedures for when exploitation is suspected. Under this Financial Exploitation Reporting Policy, CoinFlip's "frontline" employees are supposedly "trained to identify elder abuse, along with scams and

fraud typologies common to cryptocurrency." Specifically, CoinFlip says its employees can identify and report suspicious behavior, transactions, and interactions of customers over sixty years old. But despite its employees' (supposed) awareness of elder financial exploitation, the company policy, and employee training, CoinFlip has failed to implement adequate policies that actually protect vulnerable people. The continued exploitation of elderly consumers via CoinFlip BTMs exemplifies this.

b. Multiple CoinFlip users sent money to the same Bitcoin address. CoinFlip requires users to enter their names, dates of birth, and mobile phone numbers. It also makes its users verify that they own and control the Bitcoin address to which they send money. CoinFlip's terms of service require every user to confirm that he will "[o]nly send cryptocurrency [himself] and not others[,] [o]nly send cryptocurrency to a digital wallet owned by [him, and] [n]ever send cryptocurrency to someone [he] do[es]n't know or ha[s]n't met in person." As CoinFlip states, "sending funds to another person is not permitted by our terms and conditions." This is because, unlike with a traditional bank account, once a cryptocurrency transaction occurs, it is virtually impossible to reverse. Despite requiring customers to make this attestation, CoinFlip routinely ignores potential red flags—namely multiple users sending cryptocurrency to the same wallet.

c. Another warning sign is when users have a large amount of Bitcoin addresses and are connected to multiple wallets. A Bitcoin address is 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.

d. On information and belief, individual Missouri consumers have sent funds to more than one Bitcoin address. One reason a person may have multiple wallets is to ensure that if a company actually performing consumer-protection duties flagged a wallet as belonging to a scammer, the scammer would have alternative wallets to skirt enforcement. CoinFlip is acutely aware of these risks. Indeed, CoinFlip targets financially unsophisticated people who are "underbanked and unbanked," so a consumer depositing money into multiple accounts should automatically trigger further investigation. Nonetheless, CoinFlip does nothing to prevent these transactions.

III. CoinFlip's policies and practices are insufficient to address scams.

50. CoinFlip's primary method of preventing victims from using a BTM to send funds is to place "highly visible fraud warnings at [their] kiosks and display the most updated information regarding scams." Kevin Lolli, *Safe in Six – Six Questions Designed to Keep You Safe from Scams*, CoinFlip (May 5, 2025), https://coinflip.tech//blog/safe_in_six?utm_source=li&utm_medium=post&utm_campaign=weekly10.

51. These warnings insufficiently protect Missouri consumers, and CoinFlip knows it. CoinFlip profits off every transaction—including fraudulent transactions—so CoinFlip has no financial incentive to protect fraud victims.

52. CoinFlip's internal documents show that, in 2021, 99.64% of its transactions were for customers purchasing cryptocurrency. This lopsided amount of purchasing transactions shows that victims use CoinFlip's BTMs for fraudulent transfers and CoinFlip's methods of fraud prevention remain woefully insufficient.

53. Moreover, the majority of CoinFlip's BTMs are one-way machines, meaning consumers can only use them to buy cryptocurrency. Hence, sophisticated cryptocurrency investors looking to manage their portfolio would have little-to-no use for most CoinFlip BTMs. Rather, CoinFlip does not usually provide two-way machines because it knows its consumers are often scammed and only need to deposit

cash into the machines. Indeed, in Missouri, the State is aware of only *one* out of approximately 140 CoinFlip BTMs where users can withdraw cash from the BTM.

54. CoinFlip competes with online cryptocurrency exchanges, which sell cryptocurrency at a significantly lower cost than CoinFlip BTMs. CoinFlip targets less sophisticated consumers—the unbanked or underbanked—who seek to buy cryptocurrency with cash to satisfy quick demands for payment.

55. Who CoinFlip targets could not be more obvious: CoinFlip advertises that its BTMs "don't require any extensive expertise, making them an excellent choice for first-time crypto buyers." CoinFlip, *What Is a Bitcoin ATM and How Does It Work?* (Sept. 4, 2024), https://coinflip.tech/blog/how-does-a-bitcoin-atm-work.

56. CoinFlip's "incredibly convenient locations like corner shops, grocery stores, gas stations, restaurants, and more" make them "an excellent choice for those making their first crypto purchase." CoinFlip, *What Is a Crypto ATM and How Does It Work?* (Nov. 3, 2021), https://coinflip.tech/blog/what-is-a-crypto-atm-and-how-does-it-work.

57. As CoinFlip's current CEO and cofounder, Ben Weiss, put it, "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.

58. Continuing, Weiss explained, "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." *Id.*

59. On information and belief, former CEO and cofounder Daniel Polotsky similarly 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."

60. However, CoinFlip is markedly different in operation. Its primary customer base is older individuals with large sums of assets in traditional bank accounts. Frequently, its individual customers direct funds to dozens of Bitcoin address and wallets—a major red flag.

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

a. CoinFlip underutilizes cryptocurrency's tracking capabilities. Cryptocurrencies, like Bitcoin, use blockchain, which records every transaction. CoinFlip has access to Elliptic software, which traces cryptocurrency transactions. As CoinFlip's internal documents state, Elliptic "[a]utomates the ability to look into specific crypto addresses, transactions, entities, and link them to real world actors"; "[a]utomates compliance checks by using wallet risk scores"; "[m]onitors addresses and transactions associated with specific entities, ranging from crypto exchanges to darknet markets"; and "[a]llows the Company to explore

transactional relationships and uncover suspicious activity." CoinFlip even advertises this capability—saying it uses "blockchain analytics to detect and prevent suspicious activity." CoinFlip therefore has the capacity to monitor and halt inherently suspicious transactions—such as transactions sending Bitcoin to foreign-owned wallets or attempts by several different consumers to send Bitcoin to a single wallet. But rather than stopping suspicious transactions, employing blockchain analytics software to analyze transaction patterns, and questioning users, CoinFlip just collects fees off these fraudulent transactions.

b. CoinFlip also fails to use its BTM's machine-surveillance capabilities. Each BTM has an internet-connected video camera accessible to CoinFlip remotely. CoinFlip's policies allow its compliance teams to monitor transactions and prevent people from making transactions as someone else. Many fraudsters maintain continuous phone contact with their victims—directing them how to deposit the proceeds. CoinFlip understands this is a risk. *See* Scott Wilson, *Are Bitcoin ATMs Safe?* (Oct. 29, 2025) https://coinflip.tech/blog/are-bitcoin-atms-safe ("If anyone tries to force you to make an urgent Bitcoin ATM payment, it is likely a scam."). Comparatively, few willing BTM (or ATM) users operate a BTM while on the phone—entering information into the machine and placing bills into the machine generally requires two hands. CoinFlip could monitor Missouri consumers to identify clear red

flags—such as older people being on the phone while attempting to use a BTM. Instead, CoinFlip prefers to continue profiting off fraud.

IV. CoinFlip profits from Missouri scam victims.

62. CoinFlip retains a significant percentage of all money processed via its BTMs in Missouri through its transaction fees.

63. While CoinFlip charges these exorbitant transaction fees, it has never been easier to buy cryptocurrency. Cryptocurrency can be purchased through other BTM providers (e.g., Bitcoin Depot, Athena), online cryptocurrency exchanges (e.g., Coinbase, Kraken, Binance), traditional investment platforms (e.g., Fidelity, Charles Schwab, Robinhood), and payment apps (e.g., Venmo, CashApp, PayPal).

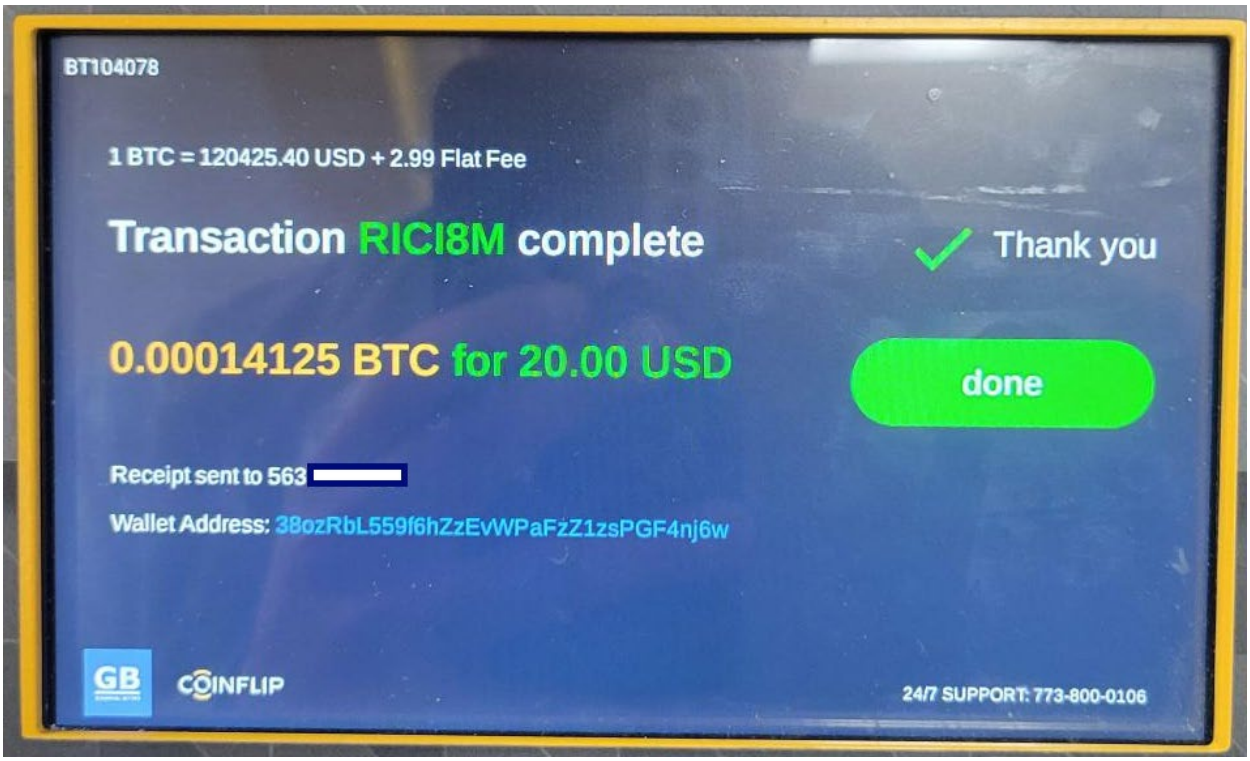
64. CoinFlip's own internal data makes clear that CoinFlip profits based on its symbiotic relationship with scammers. Charlatans manipulate unwitting and vulnerable Missourians into using CoinFlip's BTMs: The scammers retain the bulk of the victims' money but CoinFlip takes a large cut based on its transaction fees.

65. CoinFlip has engaged in deceptive practices to conceal what it really charges Missouri consumers buying cryptocurrency through its BTMs.

66. CoinFlip charges a Network Fee of $2.99. CoinFlip has consistently displayed this $2.99 fee during transactions.

67. But the total fees are much higher. CoinFlip charges a Transaction Fee ranging up to 21.90% of the transaction value. The details of this Transaction Fee are buried in its Terms of Service. On information and belief, CoinFlip has further concealed this fee during the transactions by not clearly showing the amount taken

out for the Transaction Fee during the transaction—like in the image below, which displays the Network Fee (as the "$2.99 Flat Fee"), but not the Transaction Fee.



68. Moreover, CoinFlip has made it difficult for users to determine which fees apply by having a combined Terms of Service for online, app, and kiosk services.

69. These gimmicks have kept unsophisticated purchasers from understanding how much of their money was converted into Bitcoin versus how much money went to CoinFlip in fees. Hence, CoinFlip has led Missourians into thinking they were *only* paying $2.99 for fees.

70. In reality, these fees mean that if a Missourian put $100 cash into the machine, that consumer may only receive back about $75.76 worth of Bitcoin.

71. Many Missourians who used CoinFlip's BTMs were unaware of the amount of money CoinFlip extracted in transaction fees. These consumers believed

that they paid a small service fee (the $2.99 Network Fee) similar to a traditional bank ATM. CoinFlip has encouraged this belief by hiding the fees in an ambiguous "Transaction Fee" that is buried in its complex Terms of Service and not clearly disclosed to consumers.

72. CoinFlip's having hidden its true transaction fees matches the experience of Victims #1, #2, and #3. None of them recall a conspicuous disclosure of transactions fees. *See supra* ¶¶ 6, 12, 13.

73. The cost of a product or service is a material term to the transaction. *See Hutchens v. Burrell, Inc.*, 342 S.W.3d 399, 404 (Mo. App. W.D. 2011) ("[A]s in all contracts, price is a material term."). CoinFlip hid that material term in fine print that it intended to go unnoticed by Missouri consumers.

74. CoinFlip had the ability to display clearly its Transaction Fee. For example, in addition to telling the user how many (fractions of) Bitcoins he is buying, CoinFlip could have displayed this amount in dollars at the current market rate. The user could have then seen how much money was diverted to the Transaction Fee. CoinFlip did not do this because it wanted customers to assume its fee structure was like a traditional bank ATM—and hence overlook how CoinFlip charged them up to nearly 22% in fees for transactions.

75. In failing to prevent obvious and repeated uses of its machines for fraud and misleading consumers about the fees charged for use of its ATM machines, CoinFlip has committed unfair and deceptive practices and engaged in misrepresentation. All are actionable under the MMPA.

CLAIMS FOR RELIEF

COUNT I
VIOLATION OF THE MISSOURI MERCHANISING PRACTICES ACT
FAILURE TO PROTECT CONSUMERS

76. The State incorporates all of the allegations contained in the preceding paragraphs above as if set forth herein.

77. CoinFlip's failing to take adequate measures to prevent fraudulent transactions on its BTMs is an unfair practice.

78. The MMPA deems "an unlawful practice" actionable by the Attorney General "[t]he act, use, or employment by any person of any deception, fraud, false pretense, false promise, misrepresentation, unfair practice or the concealment, suppression, or omission of any material fact in connection with the sale or advertisement of any merchandise in trade or commerce." Mo. Rev. Stat. § 407.020.

79. CoinFlip sells merchandise as defined by the MMPA. "Merchandise" includes "any objects, wares, goods, commodities, intangibles, real estate or services." Mo. Rev. Stat. § 407.010(4). The terms of the MMPA are "unrestricted, all-encompassing and exceedingly broad," and "the literal words cover every practice imaginable and every unfairness to whatever degree." *Conway v. CitiMortgage, Inc.*, 438 S.W.3d 410, 416 (Mo. banc 2014).

80. CoinFlip's practice of selling cryptocurrency through its BTMs in a manner that allows prevalent scam transactions to be processed constitutes an "unfair practice." An "unfair practice" is "any practice" which "presents a risk of, or causes, substantial injury to consumers" by "either (1) [o]ffend[ing] any public policy as it has been established by the Constitution, statutes or common law of this state,

or by the Federal Trade Commission, or its interpretive decisions; or (2) [being] unethical, oppressive or unscrupulous." 15 C.S.R. § 60-8.020. Likewise, for "harm resulting to a third person from the tortious conduct of another, one is subject to liability if he . . . knows that the other's conduct constitutes a breach of duty and gives substantial assistance or encouragement to the other." Restatement (Second) of Torts § 876 (Am. Law Inst. 1979); *accord Shelter Mut. Ins. Co. v. White*, 930 S.W.2d 1, 3–4 (Mo. App. W.D. 1996) (describing how Missouri law recognizes such liability).

81. The losses to Victims #1, #2, and #3 from transactions processed through CoinFlip's Missouri BTMs totals approximately $200,000. This amount is only expected to grow as the Attorney General continues to contact victims and confirm data related to transactions in this State.

82. CoinFlip's BTMs are causing "substantial injury to consumers." Missourians are losing their life savings, going bankrupt, and suffering myriad other injuries because of CoinFlip's BTMs.

83. CoinFlip manages its BTMs in an "unethical" or "unscrupulous" manner. CoinFlip's BTMs operate primarily as a means for scammers to exploit victims in Missouri. CoinFlip's BTMs create a path to financial ruin for Missourians, especially older, uninformed, and more vulnerable Missourians. CoinFlip knows this. Yet CoinFlip has failed to take timely, appropriate, and effective action to detect and prevent fraud-induced money transfers through its BTMs. Rather, CoinFlip operates its BTMs without safeguards in an effort to profit from defrauded Missourians.

84. By managing its BTMs in an unethical or unscrupulous manner, and thereby causing substantial injury to consumers, CoinFlip violates the MMPA.

COUNT II
VIOLATION OF THE MISSOURI MERCHANISING PRACTICES ACT
MISREPRESENTATION OF FEES

85. The State incorporates all of the allegations contained in paragraphs 1 through 75 above as if set forth herein.

86. CoinFlip has deceived Missourians about the price of cryptocurrency purchased through its BTMs.

87. CoinFlip's history of failing to present to Missourians conspicuously the price of cryptocurrency and the fees paid, hiding the fees in lengthy and complex Terms of Service, and only displaying the Network Fee are deceptive acts and practices under the MMPA.

88. This failure to have a transparent fee structure is a deceptive practice. *See Soertaert v. Novania Flips, LLC*, 631 S.W.3d 580, 587 (Mo. App. W.D. 2021).

89. Fees associated with buying cryptocurrency are "a material term." *Hutchens*, 342 S.W.3d at 404.

90. CoinFlip has only consistently advertised the $2.99 Network Fee associated with using its BTMs in a clear and conspicuous manner. This has misled users into believing that it was the sole fee for using CoinFlip BTMs.

91. CoinFlip buried the extra charge known as the Transaction Fee in the Terms of Service—instead of displaying it with the Network Fee. Consumers would

have had to undertake considerable math to determine the total fees associated with the purchase of cryptocurrency from a CoinFlip BTM.

92. CoinFlip's deceptions regarding the pricing and fees associated with cryptocurrency through its BTMs violate the MMPA.

PRAYER FOR RELIEF AND DEMAND FOR JUDGMENT

Plaintiff prays this Court:

a. Award penalties of up to $1,000 for each MMPA violation by CoinFlip over the past five years: up to $1,826,000.

b. Award restitution of ascertainable losses for each person in Jasper County to whom CoinFlip provided cryptocurrency for its undisclosed fees in the last five years.

c. Award restitution of ascertainable losses for each person in Missouri to whom CoinFlip provided cryptocurrency for its undisclosed fees in the last five years.

d. Award restitution for all ascertainable losses incurred by Victims #1, #2, and #3.

e. Award punitive damages.

f. Preliminarily and permanently enjoin CoinFlip from continuing to operate its machines in Missouri until CoinFlip implements fraud-prevention measures.

g. Preliminarily and permanently enjoin CoinFlip from continuing to make illegal, false statements misrepresenting its transaction fees in Missouri.

h. Plaintiff demands a trial by jury on all issues so triable.

Dated: May 20, 2026

Respectfully submitted,

CATHERINE L. HANAWAY
Missouri Attorney General

LOUIS J. CAPOZZI, III
Solicitor General

/s/ William James Seidleck
William James Seidleck, #77794
Principal Deputy Solicitor General
Graham D. Miller, #77656
Deputy Solicitor General
Attorney General's Office
815 Olive Street, Suite #200
St. Louis, Missouri 63101
Telephone: (573) 301-5359
Fax: (573) 751-0774
William.Seidleck@ago.mo.gov
Graham.Miller@ago.mo.gov

Attorneys for Plaintiff