COMMONWEALTH OF MASSACHUSETTS

SUFFOLK, ss.

SUPERIOR COURT
CIVIL ACTION NO.

COMMONWEALTH OF MASSACHUSETTS,

Plaintiff,

v.

BITCOIN DEPOT OPERATING LLC,
BITCOIN DEPOT INC.

Defendants.

COMPLAINT

(CONTAINS REDACTIONS)

I. INTRODUCTION

1. Bitcoin Depot Operating LLC ("Bitcoin Depot") owns and operates hundreds of Bitcoin kiosks in Massachusetts. It advertises that it is bringing "Crypto to the Masses," touts itself as a way for the unbanked and underbanked to purchase crypto and participate in the digital economy, and tells consumers that they can use its kiosks to buy Bitcoin for remittances.
2. In carrying out this purported mission, Bitcoin Depot uses deceptive tactics to sell its Bitcoin. It advertised Bitcoin prices that it would not honor and adds hidden fees to purchases that exceed the maximum fees listed in its disclosures to consumers.
3. Further, the primary impact of Bitcoin Depot's kiosks in Massachusetts is to facilitate the transfer of large amounts of money from consumers to crypto scammers. The Attorney General's Office contacted hundreds of Bitcoin Depot's largest customers in Massachusetts, each of whom had spent $10,000 or more at the kiosks between August 2023 and January

2025 and, based on these contacts along with crypto tracing and Bitcoin Depot's blacklist, found that more than 80% of these customers had utilized Bitcoin Depot's kiosks as a result of scams. The $10.6 million in revenue related to these scam customers' transactions was almost 60% of the total revenue that Bitcoin Depot took in from its kiosks in Massachusetts during this period. Further, the Attorney General's Office found fewer than ten customers who may have been using Bitcoin Depot's kiosks for legitimate transactions.

4. These numbers are not a surprise to Bitcoin Depot. Bitcoin Depot's employees had warned the company years ago that almost all of its large transactions were related to scams. Instead of fixing the issue, Bitcoin Depot reduced the questions that it asked customers, so it found out about fewer scams. Bitcoin Depot also heightened the bar for designating transactions as scams, which allowed unknowing scam victims to continue using Bitcoin Depot's kiosks to keep sending money to the scammers.

5. Notwithstanding its knowledge that many of its largest transactions were perpetrated by scammers separating customers from their savings, Bitcoin Depot raised its daily transaction limit from $15,000 to $25,000 and increased its markup on the Bitcoin it sold to more than 40% by the end of 2024 (markup on Bitcoin from online sellers often is between .5% and 3%). The increased transaction limit and markup allowed scammers to more efficiently procure money from scam victims (because they could get more money in fewer victim trips to the kiosks) and allowed Bitcoin Depot to keep a bigger cut.

6. Further, when customers informed Bitcoin Depot that they had been scammed, Bitcoin Depot often said that there was nothing it could do and did not provide refunds of its fees, even though it had kept up to 30% of the money that the customer put into the kiosks. Bitcoin Depot provided other scammed customers with partial fee refunds, often limited to $1,000,

even if the fees that customers paid Bitcoin Depot totaled much more. These refund decisions allowed Bitcoin Depot to keep the money of scam victims even though it had taken their money knowing that most of their large customers were scam victims.

7. Bitcoin Depot Inc., Bitcoin Depot's owner, also withheld critical information from investors about how much of Bitcoin Depot's revenue came from scams. In its 10-K, Bitcoin Depot Inc. warned investors that Bitcoin Depot's machines were at risk of being used in fraud scams. What Bitcoin Depot Inc. didn't tell investors was that Bitcoin Depot's employees in 2021 and 2022 were estimating that 90% of its biggest customers were scam victims. Bitcoin Depot Inc. also didn't reveal that Bitcoin Depot's own conservative internal metrics, based on its limited Know Your Customer program and [redacted], in 2023 had identified between 13%-16% of the overall money volume coming through its kiosks was scam-related. These scam transactions were directly tied to Bitcoin Depot's revenue through the markup it charged on all the Bitcoin that it sold. In 2024, more than 99% of Bitcoin Depot Inc.'s revenue came from kiosk transactions. Scammers utilizing Bitcoin Depot kiosks to move money was not just a "risk," it was a reality, and scam-based transactions were a major revenue center of the company. This is material information that investors needed to know when they were choosing to purchase stock in Bitcoin Depot Inc. as opposed to other investment alternatives.

II. JURISDICTION AND VENUE

8. The Attorney General is authorized to bring this action pursuant to G.L. c. 93A, § 4.
9. The Court has jurisdiction over the defendants pursuant G.L. c. 223A, § 3.
10. The Court has jurisdiction over the subject matter of this action pursuant to G.L. c. 93A, § 4.

11. Venue is proper in Suffolk County pursuant to G.L. c. 223, § 5, and G.L. c. 93A, § 4.

12. On January 8, 2026, the Attorney General's Office sent each Defendant a letter in accordance with the provisions of G.L. c. 93A, § 4, paragraph 2.

III. THE PARTIES

13. Pursuant to G.L. c. 93A, section 4, the Attorney General brings this action in the name of the Commonwealth.

14. Defendant Bitcoin Depot Operating LLC is a Delaware Limited Liability Company headquartered in Atlanta, Georgia.

15. Defendant Bitcoin Depot Inc. is a Delaware corporation headquartered in Atlanta, Georgia.

16. Whenever this Complaint references an act, deed, or transaction of any corporation, the reference means that the corporation engaged in such act, deed, or transaction by or through its officers, directors, agents, employees, or other representatives while they were actively engaged in the management, direction, control, or transaction of its business affairs.

IV. BACKGROUND

A. Bitcoin Depot

a. Corporate Structure and Kiosks

17. Bitcoin Depot was formed in 2016, as Lux Vending, LLC ("Lux Vending"). It was solely owned by BT Assets, Inc. ("BT Assets"). In 2022, Lux Vending and BT Assets entered into a reverse recapitalization transaction with GSR II Meteora Acquisition Corp ("GSMA"), a publicly-traded blank check corporation. The transaction closed in 2023.

18. After the transaction, Lux Vending became Bitcoin Depot Operating LLC. Bitcoin Depot Operating LLC is a limited liability company that operates kiosks selling Bitcoin. It is wholly owned by Bitcoin Depot Inc., which is the successor to GSMA. Bitcoin Depot Inc. is

a publicly traded corporation. Massachusetts investors have held stock in Bitcoin Depot Inc. during the times relevant for the allegations in this Complaint.

19. Bitcoin Depot Inc. officers have historically served as members of Bitcoin Depot. Bitcoin Depot's employees participate in Bitcoin Depot Inc.'s Omnibus Incentive Plan. Bitcoin Depot is Bitcoin Depot Inc.'s principal operating company in the United States. Bitcoin Depot has no independent business outside of its business as Bitcoin Depot Inc.'s subsidiary.

20. Bitcoin Depot owns more than 8,000 crypto kiosks throughout the country, including hundreds in Massachusetts. The kiosks, otherwise known as Bitcoin ATMs, are often located in minimarts, gas stations or other businesses with long hours. Bitcoin Depot sells customers Bitcoin through its kiosks.

b. Bitcoin Depot's Advertising and Operations

21. Bitcoin Depot advertises its crypto kiosks as a way for people to buy crypto without the hassle of opening accounts or revealing much personal information. On its website, Bitcoin Depot says that its kiosks "meet or exceed regulatory requirements while maximizing privacy—keeping users like you safe." Bitcoin Depot describes its kiosks as a way to get coins into the user's crypto wallet as quickly and easily as possible. Bitcoin Depot also markets its services as useful to almost anybody, enumerating the people who could utilize its kiosks as: "Investment-minded individuals; tech-savvy youth; International and cross-border users; First-time crypto buyers; [and] busy professionals." [https://bitcoindepot.com/bitcoin-atm-info/what-makes-btc-atms-so-special/, Last Visited 10-17-2025]

22. The mechanics of using a Bitcoin Depot crypto kiosk to purchase Bitcoin work as follows: a customer approaches a kiosk, sees a price for Bitcoin posted on the kiosk display, provides their phone number and an identification card, and identifies a crypto wallet into which the

customer would like Bitcoin Depot to send the newly purchased cryptocurrency. The customer certifies that they control the wallet, agrees to Bitcoin Depot's terms and conditions, and puts the required currency (to pay for the requested Bitcoin) into the machine. After the customer completes inserting the required currency, Bitcoin Depot transmits the purchased Bitcoin to the identified wallet.

23. At the time of purchase, Bitcoin Depot informs customers of a $3 transaction fee. Customers may spend between $20 and $25,000 at a time at the machine.[1] Bitcoin Depot represents that all transactions are final once completed.

24. In the middle of its lengthy terms of service, which customers must accept the first time they visit the machine, Bitcoin Depot discloses that it would add a "spread" to the price of the Bitcoin. Bitcoin Depot indicates that this additional fee can be as much as 23% of the transaction price. In other words, Bitcoin Depot can mark up the price of Bitcoin that it sells to its customers. In Massachusetts, neither the existence of the spread, nor the amount of the spread, is identified on the Bitcoin Depot kiosk screens that customers click through to purchase Bitcoin. The spread is only mentioned in section 9.1 of Bitcoin Depot's terms of service, which a customer would need to scroll through to find. Customers who spent more than $10,000 at Bitcoin Depot's kiosks were often not aware that Bitcoin Depot applied a spread to the transaction or were subject to any fees beyond the $3 transaction fee.

25. In addition to gathering phone information and identification from customers, Bitcoin Depot conducts what it calls Know Your Customer ("KYC") and Anti-Money Laundering ("AML") compliance measures. The company's KYC and AML apply more stringently to some transactions than to others. [redacted] Customers purchasing crypto need to provide a name

[1] Subject, in many instances, to a $25,000 daily limit.

and identification card, along with basic purchase information.[2] [redacted] Bitcoin Depot, with commercial software, can also trace which wallet(s) received the Bitcoin purchased by customers and to where the Bitcoin is transmitted from the initial wallet.

26. Additionally, Bitcoin Depot monitors transactions for a series of red flag warnings, which alert Bitcoin Depot if a customer engages in risky behavior. This behavior includes visiting Bitcoin Depot machines more than once a day and/or transmitting Bitcoin to the same wallet as other customers.[3]

B. Bitcoin Depot Deceives Customers with Drip Pricing Tactics and Excessive Hidden Fees

a. Bitcoin Depot Misled Customers When Selling Bitcoin

27. As noted in paragraph 23, supra, when customers approach a Bitcoin Depot kiosk and begin a transaction, the kiosk informs them that there is a $3 transaction fee for conducting the transaction, similar to the fee charged for use of an out-of-network ATM.[4] In the upper corner of the screen, the kiosk gives a price for Bitcoin.

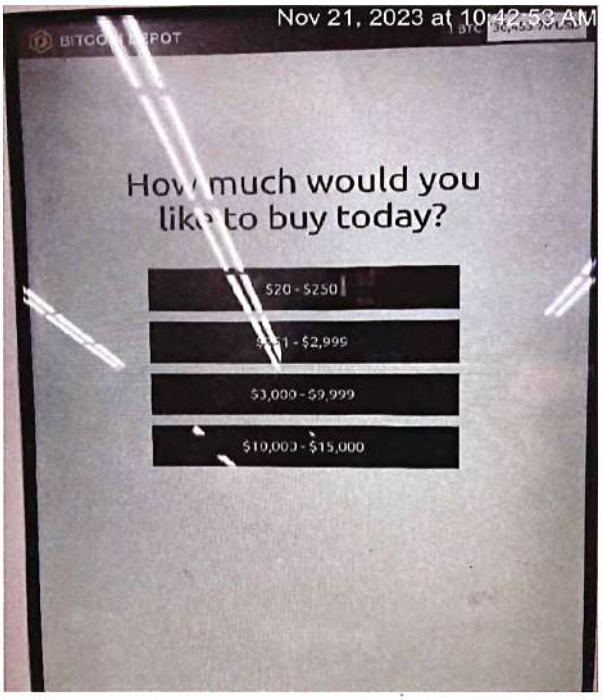
28. In some transactions, Bitcoin Depot started the transaction displaying a price for Bitcoin that was close to the trading price of Bitcoin on major exchanges. For example, in one transaction conducted by the Attorney General's Office in November of 2023, the price of one Bitcoin was initially listed as $36,453.70 on Bitcoin Depot's kiosk. This was approximately the trading price of Bitcoin on the spot market as of November 21, 2023.

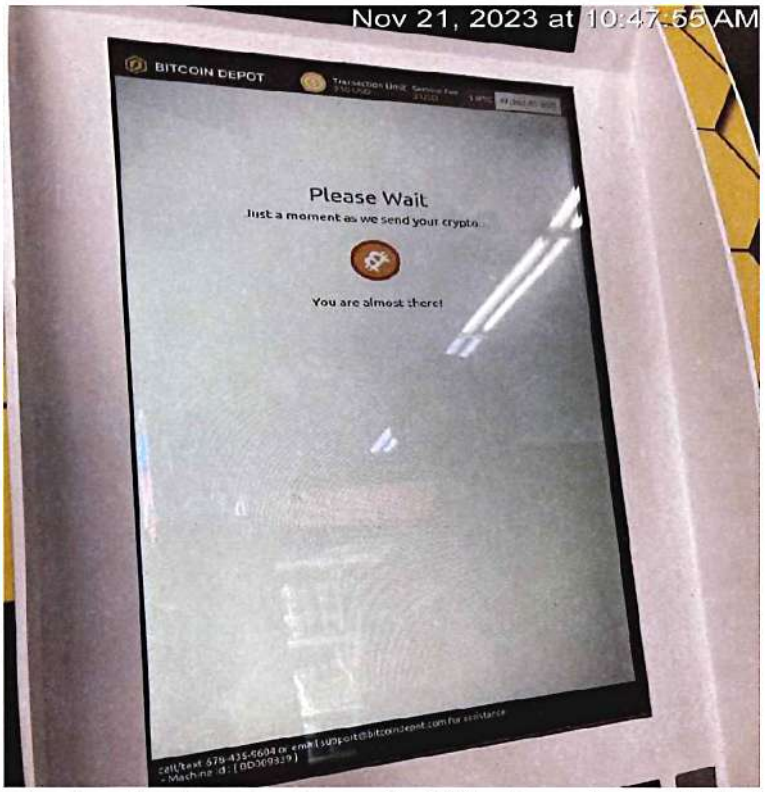
---

[2] Bitcoin Depot put out an October 2025 press release stating that all customers must now provide identification to purchase crypto. Prior to that, customers purchasing small amounts of Bitcoin would only need to provide a telephone number.

[3] A customer visiting multiple kiosks in a day and multiple customers sending to the same wallet are common indicators of scams. See eg FinCEN Notice, FIN-2025-NTC1, August 4, 2025, p.7.

[4] Bitcoin Depot's website even has a page comparing its kiosks to ATMs. (https://bitcoindepot.com/bitcoin-atm-info/bitcoin-atms-vs-traditional-atms/, Last Visited 10/17/25).





29. However, by the time the Attorney General's Office investigator clicked through the screens and put money into the machine five minutes later, the displayed price of Bitcoin had changed and was listed on the kiosk display screen as $47,562.61 for one Bitcoin.

30. This drastic change in the displayed price was not the result of a sudden increase in the price of Bitcoin, but instead was the result of Bitcoin Depot's pre-planned and misleading marketing tactics. Bitcoin Depot had applied the spread buried in its terms and conditions and had put that figure on the screen after already luring in the customer with a much more reasonable and competitive price. Bitcoin Depot applies a markup between 15% and 50% to all of the transactions at the kiosks.[5] On large transactions, Bitcoin Depot's hidden spread can generate thousands of dollars for Bitcoin Depot. Bitcoin Depot was never going to sell the Bitcoin at the original price of $36,453.70 that it displayed on its kiosks.

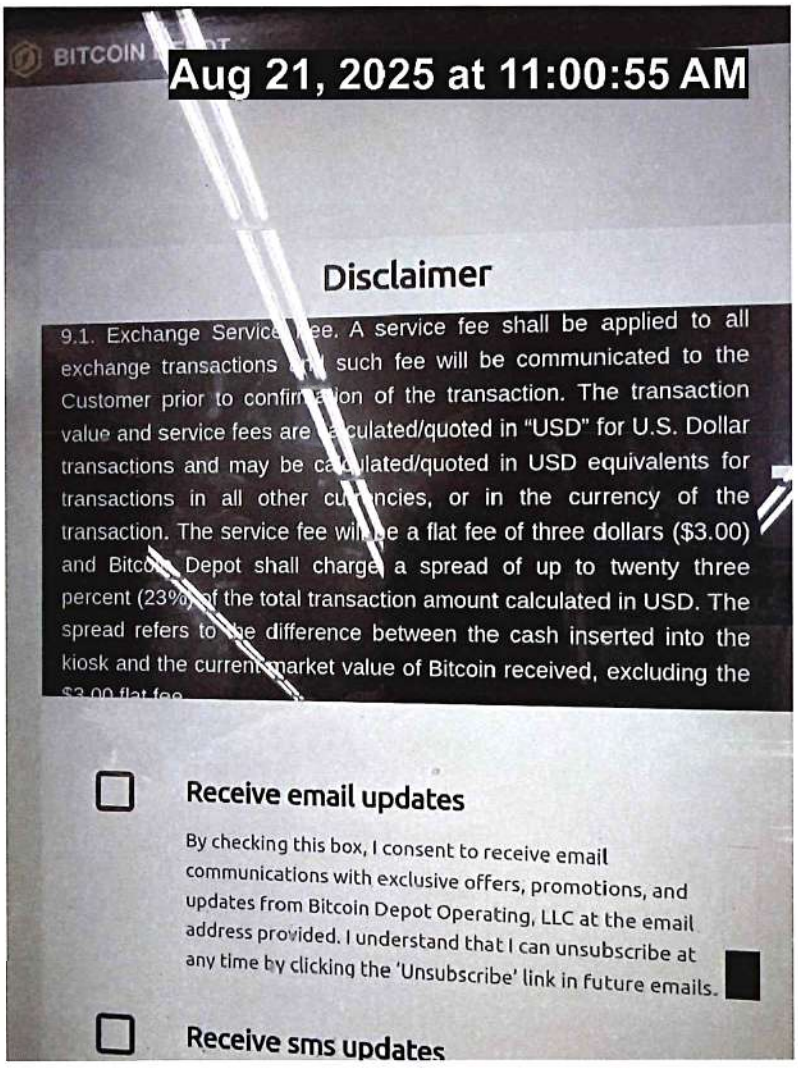
b. Bitcoin Depot Charged Customers Hidden Fees in Excess of the Fee Limits Set Forth in Bitcoin Depot's Terms and Conditions

31. While Bitcoin Depot has changed its practices regarding the time and manner of disclosing its spread-pricing, the company's tactics remain unfair and deceptive. In more recent transactions, conducted in 2025, Bitcoin Depot initially disclosed a price of Bitcoin that included its spread for the price of Bitcoin. However, even in these transactions, Bitcoin Depot did not break out the spread amount from the total price nor identify the percentage of its inflated markup. This lack of transparency left customers practically unable to determine if Bitcoin Depot was complying with Section 9.1 of its terms and conditions,[6] which limited the spread to 23% of the purchase price, not including the $3 transaction fee.

---

[5] Bitcoin Depot's markup is much larger than the markup applied by online sellers. The markup in online transactions is often between .5% and 3%, rather than Bitcoin Depot's much larger spreads.

[6] The terms and conditions available at the kiosks in Massachusetts are different than the terms and conditions available on Bitcoin Depot's website.



32. In fact, in many of these transactions, Bitcoin Depot had not complied with the cap in its terms and conditions. Instead, the company regularly charged a spread in excess of 23% of the transaction price. A review of the spread on the transactions between August of 2023 and January of 2025 shows that Bitcoin Depot charged spreads exceeding 23% in more than 7,000 of the 12,700 transactions reviewed. In more than 2,300 transactions, the spread

exceeded 29% of the purchase price. Because Bitcoin Depot did not disclose the amount of spread it applied to each transaction, customers had no way to know that Bitcoin Depot was violating its own terms and conditions. As a result of Bitcoin Depot's spread pricing practices, customers paid significant amounts to Bitcoin Depot beyond the amounts that Bitcoin Depot had agreed was the maximum fee/spread it would charge. In many instances, this amounted to thousands of dollars.

C. Bitcoin Depot Knowingly Facilitated Crypto Scams

a. Crypto Scams are Common, Varied, and Devastating

33. Crypto scams are a known problem. The scammers use all sorts of stories and tools to convince victims to turn their money into crypto and send it to the scammers. Scammers pretend to be romantic partners who need money for their family or to flee a war-torn country. Scammers mislead consumers into believing that the scammers have placed or found child pornography on the consumers' computers and will have the consumer victims arrested unless the victims pay the scammers. Scammers gain access to people's computers and then pretend to be the victim's bank trying to help the victim keep their money safe or pose as government agents trying to help the victim.

34. While the permutations used by scammers are endless, the results of the crypto scams are often very similar. Victims are left devastated. They will have their assets drained and can be left with nothing. Some victims do not even have enough money after being scammed to make monthly car loan payments or pay their monthly heating bills. Other victims are left with empty 401(k) or similar accounts, large tax bills, and no prospects for a safe and secure retirement. For example, a Bitcoin Depot compliance analyst spoke with a woman who had

been so devastated by a crypto scam that she planned to end her own life. The scams often depend on the existence of Bitcoin Depot's crypto kiosks.

35. The crypto kiosks are critical to the scams because they allow the victims to immediately convert their money into cryptocurrency and transfer it to the scammers. The existence of the kiosks makes an entire additional class of consumers vulnerable to these scams. Absent the kiosks, only consumers who already had or could be persuaded to utilize online crypto accounts would be at risk. The kiosks allow victims who are unfamiliar with crypto to feel more comfortable with the process perpetrated by the scammers. The kiosk machine is much like an ATM and is both familiar and simple for victims to operate. The victims are resultingly less hesitant, and scammers can readily steer them into immediately changing their money into crypto, which scammers can quickly move beyond the reach of the victims.[7] Due to the nature of crypto kiosk machines, the money is in the scammers' crypto wallets, often overseas, before victims realize that the whole thing is a fraud.

b. Bitcoin Depot Knows that its Machines are Used for Fraud

36. Bitcoin Depot is well aware that scammers may seek to use Bitcoin Depot kiosks to perpetrate fraud against victims. Bitcoin Depot Inc. warns its investors that its kiosks can be utilized in scams, and it puts scam warnings on its kiosks' screens. Bitcoin Depot, however, also knows that the screen warnings, along with its KYC/AML program, are ineffective at stopping scams.

37. The kiosk screen disclosures are ineffective because scammers are often talking live on the phone with consumers as the consumers go to the kiosks. The scammers can talk the victims

[7] Some scam victims do not even realize that they are purchasing crypto. The scammers convince the victims that they are going to a special ATM to transfer money.

through the scam warnings, convincing the victims that the warnings do not apply to them. Bitcoin Depot, based on consumer complaints and its own analysis, knows this to be the case.

38. Bitcoin Depot's KYC/AML program is also ineffective. While a KYC/AML program should provide a kiosk company with sufficient information on its users and their situations to determine, in many instances, if fraud is afoot (and then put it in a position to warn the consumer or stop the transaction), Bitcoin Depot's system does not, and its system will not help prevent fraud. [redacted] Further, as detailed below, Bitcoin Depot is now less likely than ever to identify fraud, as it has chosen to limit the questions that it asks its customers.

39. In 2021, members of Bitcoin Depot's Enhanced Due Diligence Team ("EDD Team"),[9] who conducted the KYC/AML contacts with customers and traced transactions, determined that more than 90% of the people that they were contacting were scam victims. [redacted] The EDD Team employees informed Bitcoin Depot's Chief Compliance Officer (CCO), Mark Smalley, of Bitcoin Depot's kiosks being used in scams victimizing Bitcoin Depot's largest customers. One Bitcoin Depot compliance analyst advised the CCO and his supervisor that he believed that the company was facilitating money laundering at an "extreme volume."

---

[8] Bitcoin Depot, as of October 2025, represents that it now takes an identification card for each customer.

[9] Many of these EDD Team employees were experienced compliance analysts who had worked in compliance before they joined Bitcoin Depot.

[10] Because Bitcoin transactions occur on a blockchain, it is possible to follow the Bitcoin as it moves from wallet to wallet. Over time, certain wallets are identified as being used as part of scams. Other wallets can be classified as high-risk based on the entity hosting the wallet being associated with known scams or illegal transactions.

40. Later in 2021, Bitcoin Depot changed its KYC/AML process for contacting customers, making the KYC/AML process less effective. [redacted] This change facilitated more fraud. [redacted]

41. As an example of this new policy, in November 2021, a customer was sending hundreds of thousands of dollars overseas. The customer believed that she was sending the money for an "investment." Although a Bitcoin Depot employee initially stopped further transactions, that employee's decision was reversed by the company. Specifically, the [redacted] Unfreezing the account allowed both the customer to keep sending their money into a likely scam and Bitcoin Depot to collect the markup on the Bitcoin that the likely victim bought through Bitcoin Depot's kiosks. In another instance, a Massachusetts customer, who was unknowingly being scammed, found that Bitcoin Depot froze her account but then reinstated it, without ever providing her any specific evidence or explicit warning that she had been the victim of a scam. Bitcoin Depot allowed her to continue losing money to the scammers while continuing to profit from those transactions.

42. Bitcoin Depot's documents from 2023 showed that crypto scams continued to plague Bitcoin Depot's kiosks, particularly with respect to high value transactions. Bitcoin Depot's metrics from March through September of 2023 showed that even with its new narrower classification metrics, Bitcoin Depot continued to report that between 13% and 16% of the volume of money that went through its kiosks was scam-related. The metrics also showed that the designated scam transactions, on average, were larger than Bitcoin Depot's other transactions, with an average scam transaction exceeding $8,500 while the average Bitcoin Depot transaction was approximately $1,100. Thus, scam transactions were disproportionately the largest transactions, which involved the largest and most lucrative

fees. Bitcoin Depot, Inc. did not include any of this information in its disclosures to investors.

c. Scam Transactions Predominated Bitcoin Depot's Business in Massachusetts

43. Scams dominate Bitcoin Depot's transactions in Massachusetts, particularly its largest transactions. Between August of 2023 and January of 2025 (the "Massachusetts Survey Period"), 552 customers spent $10,000 or more at Bitcoin Depot's kiosks ("Large Customers"). Collectively, these 552 Large Customers spent more than $13.2 million during the Massachusetts Survey Period. Based on surveys, phone calls, and police reports, the Attorney General's Office was able to establish that the transactions of 250 Large Customers were scam-related. These 250 Large Customers spent approximately $5.4 million at Bitcoin Depot's kiosks during the Massachusetts Survey Period. Through wallet tracing, blockchain analysis, and Bitcoin Depot's own blacklist, the Attorney General's Office found approximately 200 additional customers whose transactions were scam-related. In total, the Attorney General's Office found that the transactions of 458 of the Large Customers were scam-related (the "Scam Customers").[11] Thus 83% of the 552 Large Customers during the Massachusetts Survey Period, were Scam Customers. The money spent by the Scam Customers at Bitcoin Depot's kiosks totaled $10.6 million or about 80% of the $13.2 million spent by the Large Customers during the Massachusetts Survey Period. After successfully

[11] Many other transactions of the Large Customers had some indicia that they may have been scam-related. However, where the indicia was weaker and the Attorney General's Office was not able to confirm the scam with the customer or through other documents such as police reports, the Attorney General's Office did not include the customer in the group of Scam Customers.

contacting hundreds of the Large Customers, the Attorney General's Office found fewer than ten customers who may have been using Bitcoin Depot's kiosks for legitimate purposes.[12]

44. This $10.6 million spent by the Scam Customers is also almost 60% of the total $18.1 million that all customers spent at Bitcoin Depot's Massachusetts kiosks during the Massachusetts Survey Period. Thus, more than half of the money flowing through the kiosks during the review period was scam-related.[13]

45. The prevalence of scams at its kiosks in Massachusetts is not and should not be a surprise to Bitcoin Depot. Bitcoin Depot's employees had warned the company about the extremely high prevalence of fraud transactions going through its kiosks all over the country. In addition, Massachusetts law enforcement officers had served multiple search warrants on Bitcoin Depot's kiosks to seize money from the machines after receiving consumer complaints that Bitcoin Depot kiosks had been used to facilitate fraud. Other Massachusetts police officers report that they have directly contacted Bitcoin Depot regarding fraudulent transactions. Dozens of customers also reported that they have contacted Bitcoin Depot indicating that they were fraud victims.

46. Despite the high scam rates, particularly in larger transactions, Bitcoin Depot between 2023 and 2025 increased its maximum purchase amount to $25,000 per day from $15,000 per day.

---

[12] Even this small number of customers may be an overstatement. A couple of customers appeared to be using the kiosks to purchase and invest in Bitcoin. Another customer may have been investing in Bitcoin but was not aware of the fees associated with the kiosk. A few other customers claimed to be using the kiosks legitimately, but traces of the transaction showed that they were transmitting money to wallets that were tied to other wallets identified as part of known scams and/or addresses, such as Bitcoin mixers, which are often used to defeat crypto traces.

[13] The proportion of scam-related transactions during the Massachusetts Survey Period is likely even higher, as the Attorney General's Office did not receive responses back from all survey recipients.

Bitcoin Depot also increased its spread on the transactions. In early 2022, Bitcoin Depot's average spread on transactions was under 20%. In the last quarter of 2024, Bitcoin Depot's average spread had increased to more than 29%. With the increased transaction limit and the increased spread, Bitcoin Depot was taking a larger percentage of bigger transactions, including a multitude of scam transactions.

d. Many of Bitcoin Depot's Transactions Should Have Raised Red Flags

47. The elderly are well-recognized as a group vulnerable to scams. The Scam Customers, who all purchased at least $10,000 in Bitcoin during the Massachusetts Survey Period, had a median age of 67. Thus, more than half of the 458 Scam Customers were 67 years old or older. More than 340 of the 458 Scam Customers or more than 70% of the Scam Customers, were 60 years old or older. Further, many of the Scam Customers were well older than the median. More than 40 Scam Customers were 80 years old or older, and they collectively spent more than $700,000 at the Bitcoin Depot kiosks during the Massachusetts Survey Period. On average, each of these "over 80" Scam Customers put more than $17,500 in cash into Bitcoin Depot machines during the Massachusetts Survey Period.

48. In at least 400 instances between 2019 and January of 2025, Bitcoin Depot approved transactions where customers used more than one Bitcoin Depot kiosk on the same day. Bitcoin Depot approved these transactions despite being informed by its compliance analysts that customers going to multiple machines in one day is often a sign that the customer is being directed to the machines by scammers.[14]

[14] It is a common warning that going to multiple kiosks in a single day can be a sign of scams involving structuring or "smurfing." See eg FinCEN Notice, FIN-2025-NTC1, August 4, 2025, 7.

49. Many transactions approved by Bitcoin Depot had blatant discrepancies. Some of the customers used fake names like "John Wick" and the "Chosen One." In another case, a customer using a Texas address and a Michigan phone number put, over the course of four days, more than $29,000 into Bitcoin Depot kiosks located in Massachusetts towns of Sharon and Walpole in October of 2024. The individual whose identity was used in these transactions, however, had never been to Massachusetts. Instead, his identity had been stolen the month before and had been fraudulently used at Bitcoin Depot's kiosks.

50. Many customers also transmitted newly purchased Bitcoin to wallets on foreign exchanges such as Binance,[15] Bybit, OKX, HTX, MEXC, and Gate.io, as well as peer-to-peer trading platforms. These foreign exchanges and peer-to-peer platforms do not allow U.S. residents to hold wallets or accounts on their exchanges and/or platforms, or in many cases, even access the exchange with a U.S. based IP address. Despite this, the Attorney General's Office found that during the Massachusetts Survey Period, Bitcoin Depot's customers in Massachusetts transmitted more than $1.8 million from Massachusetts Bitcoin Depot kiosks to wallets on overseas exchanges or peer-to-peer trading platforms.

51. In short, many of the transactions via Bitcoin Depot's kiosks appeared questionable on their face, violated Bitcoin Depot's transaction rules, or were identified as fraudulent by Bitcoin Depot's own employees.

D. <u>Bitcoin Depot Often Did Not Provide Refunds to Scam Victims</u>

52. Through its inflated margins and other fees, Bitcoin Depot kept a large portion of the cash customers put into its machines. When scam victims contacted Bitcoin Depot to seek the

[15] Binance is distinct from Binance US. Binance US does allow for the transfer of assets from U.S. residents' wallets.

return of their stolen money, Bitcoin Depot often misled them into believing that all of their money had been sent to the scammers. Bitcoin Depot representatives in many cases told them that there was nothing Bitcoin Depot could do to help and did not offer them a process for getting or seeking any refund amounts (even though Bitcoin Depot had such a process, to provide at least a fractional return of funds). Bitcoin Depot representatives simply told customers that Bitcoin Depot was sorry for their loss of funds or that they were on their own. Bitcoin Depot made these statements despite having kept up to 30% of the money, through its fees and spread, that customers put into its kiosks. Bitcoin Depot had the ability to return the fees collected from Massachusetts victims. Further, Bitcoin Depot had taken the money from the customers knowing that almost all of its large transactions were scam-related and not legitimate arms-length purchases.

53. Bitcoin Depot did refund a portion of its fees to some customers, but often capped that refund at $1,000, much less than the several thousands of dollars in fees that Bitcoin Depot had collected from its large transaction customers. Again, Bitcoin Depot's actions and misleading statements allowed Bitcoin Depot to keep much of the markup that Bitcoin Depot had taken from customers who were scammed.

E. Bitcoin Depot Inc. Deceived Investors

54. In its 2023 S-1, Bitcoin Depot Inc. warned investors: "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." [2023 S-1, p.12]. (emphasis added)

55. In its 2025 10-K, Bitcoin Depot Inc. again warned investors: "Our products and services may be exploited to facilitate illegal activity such as fraud, money laundering, gambling, tax evasion, and scams. If any users use our business to further such activities, our business could be adversely affected." [2025 10-k, p.18]. (emphasis added)

56. In its 2023 S-1 and the 2025 10-K, Bitcoin Depot Inc. projected a future possibility that scams could impact the business, but the company did not disclose that this was in fact happening right then to an alarming degree. Bitcoin Depot Inc. did not provide information to investors about the scope of fraud and money laundering that was already taking place on Bitcoin Depot's kiosks and noted in its internal reports. Bitcoin Depot Inc. also did not inform investors that its former employees had advised the company that almost all of its large kiosk transactions were the result of fraud or violations of its terms of service. While Bitcoin Depot Inc. told potential investors and its current securities holders there was an unspecified risk that services "***may*** be exploited" and that "business ***could*** be adversely affected" (emphasis added), Bitcoin Depot Inc. withheld the more pertinent information that services ***were*** being exploited at a material level and that business ***was*** being adversely affected already.

57. Bitcoin Depot Inc. had been advised years earlier that almost all of Bitcoin Depot's largest customers were victims of scams. In response to these warnings, Bitcoin Depot limited the questions that the EDD Team would ask affected customers. Even after taking such willful steps to remain ignorant, including reducing the type and number of scams that Bitcoin

Depot would verify, Bitcoin Depot's internal metrics repeatedly showed that scams permeated its largest transactions and made up at least 13% of its volume.

58. Bitcoin Depot Inc. knew definitively that there was not simply a risk of fraud occurring via its subsidiary's kiosks, but that fraud was occurring on a large scale. The company affirmatively failed to provide this information to investors. Indeed, Bitcoin Dept Inc.'s misleading disclosures put investors at ease, letting them believe the risk of fraud was only a potential one, when in fact scams via Bitcoin Depot kiosks had already been widespread and rampant for some time.

V. CAUSES OF ACTION

Count I

(Misleading Pricing to Sell Bitcoin in Violation of G.L. c. 93A, 940 C.M.R. 3.05, 3.13, 3.16, 6.01(g) and 6.04(2))

59. The Commonwealth repeats and realleges the preceding paragraphs of this Complaint.

60. Bitcoin Depot and Bitcoin Depot Inc.[16] are, and at all relevant times were, persons engaged in "trade or commerce" in Massachusetts as defined and used in Chapter 93A, G.L. c. 93A, §§ 1(a)-(b), 2, including through the sale of Bitcoin to consumers.

61. Bitcoin Depot engaged in unfair or deceptive acts or practices in violation of G.L. c. 93A, § 2 by displaying lower Bitcoin prices at the beginning of a transaction that it would not honor and then adding hidden fees, as the transaction went on, until the final Bitcoin price was much higher than the original displayed price (also known as drip pricing).

[16] Bitcoin Depot Inc. acted through its subsidiary Bitcoin Depot, except as to Count V, which it acted itself.

62. At least through 2023, when customers approached Bitcoin Depot's kiosks, Bitcoin Depot provided the trading price of Bitcoin on the upper right-hand corner of the screen to customers as the price of the Bitcoin that it was selling. To a customer approaching Bitcoin Depot's kiosk, this price appeared to be the price at which they could purchase Bitcoin at the kiosk, along with the $3 transaction fee that Bitcoin Depot told customers it would charge them.

63. This lower price, which Bitcoin Depot displayed on its kiosk screens, was represented by Bitcoin Depot to customers in the course of soliciting customer business and encouraging the customers to purchase Bitcoin from its kiosks.

64. Bitcoin Depot did not and would not sell Bitcoin to customers at this lower price.

65. Instead, as the customers went through additional steps to use Bitcoin Depot kiosks and proceed with the transaction, the price of Bitcoin in the upper right-hand corner of kiosk screens jumped higher. This jump in price reflected a hidden spread between the trading price of Bitcoin and the price at which Bitcoin Depot would sell it to customers.

66. Bitcoin Depot did not itemize this spread nor display the spread on its kiosk transaction screens. Bitcoin Depot did not disclose that the first Bitcoin price represented to the customer did not include the spread, instead implying that the initially displayed price was the sales price.

67. The existence of Bitcoin Depot's spread was only mentioned in the middle of the long terms and conditions presented to customers the first time they used Bitcoin Depot's kiosks.

68. Bitcoin Depot's actions constitute violations of Chapter 93A, § 2 and 940 C.M.R. 3.05, 3.13, 3.16, 6.01(g) and 6.04(2).

69. Bitcoin Depot acts as an agent or instrumentality of Bitcoin Depot Inc., making Bitcoin Depot Inc. vicariously liable for Bitcoin Depot's actions.

Count II

(Charging Excessive Fees in Violation of G.L. c. 93A, 940 C.M.R. 3.05, 3.13, 3.16 and 6.04(1))

70. The Commonwealth repeats and realleges the preceding paragraphs of this Complaint.

71. Aside from its practice of drip pricing as discussed in Count I, Bitcoin Depot also violated G.L. c. 93A, § 2 because of the size of its hidden fees. Specifically, Bitcoin Depot's hidden fees charged to customers exceeded the cap that Bitcoin Depot agreed in its terms and conditions would be the maximum charge for any transaction.

72. In its terms and conditions, which Bitcoin Depot proffered and which kiosk users click through the first time they use Bitcoin Depot's kiosks, Bitcoin Depot promised that the spread between the market and sale price would be capped at 23% of the purchase price, not including the $3 service fee.

73. During a purchase at its kiosks, Bitcoin Depot did not disclose how much its spread was to the customer, making it practically impossible for customers to determine if Bitcoin Depot was complying with the limit contained in its terms and conditions.

74. Bitcoin Depot, in fact, in more than 7,000 transactions, charged customers a spread in excess of 23% of the purchase price. In more than 2,000 transactions, Bitcoin Depot's spread exceeded more than 29% of the purchase price. These transactions, where Bitcoin Depot exceeded the cap, made up more than half of the transactions that occurred during the Massachusetts Survey Period.

75. Because Bitcoin Depot did not disclose its markup to customers, the customers had no idea that Bitcoin Depot was violating the terms and conditions set out at the time of purchase.

76. Bitcoin Depot unfairly and deceptively misled customers and overcharged them in violation of the promises and agreement that it made with the customers when they utilized its kiosks. Bitcoin Depot knew at the time it entered into the agreement with the customers at the kiosks that it would violate the agreement and overcharge them.

77. Bitcoin Depot's actions constitute violations of Chapter 93A, § 2 and 940 C.M.R. 3.05, 3.13, 3.16 and 6.04(1).

78. Bitcoin Depot acts as an agent or instrumentality of Bitcoin Depot Inc., making Bitcoin Depot Inc. vicariously liable for Bitcoin Depot's actions.

Count III

(Facilitation of Fraud in Violation of G.L. c. 93A and 940 C.M.R. 3.16)

79. The Commonwealth repeats and realleges the preceding paragraphs of this Complaint.

80. Bitcoin Depot engaged in unfair or deceptive acts or practices in violation of G.L. c. 93A, § 2 by facilitating fraud.

81. More than 80% of the buyers spending more than $10,000 at Bitcoin Depot's kiosks in Massachusetts during the Massachusetts Survey Period were Scam Customers.[17] The purchases related to these buyers made up $10.6 million of the $18.1 million spent at Bitcoin Depot's kiosks in Massachusetts between August of 2023 and January of 2025. The Attorney General's Office, in interviewing many of Bitcoin Depot's largest Bitcoin customers in Massachusetts, found fewer than ten who may have been using Bitcoin Depot's kiosks to legitimately purchase Bitcoin.

[17] See ¶ 43, supra.

82. In dozens of cases, customers self-identified to Bitcoin Depot that they had been defrauded. Police and other enforcers repeatedly contacted the company with other evidence of fraud, and the company's own employees repeatedly reported extreme levels of fraud to Bitcoin Depot.

83. Bitcoin Depot knew, based on the large numbers of frauds, that its process was fraud-ridden and that high-dollar value customers were subjected to the grave risks of fraud when using its kiosks.

84. In other instances, Bitcoin Depot knew that customers were victims of ongoing fraudulent schemes, which repeatedly used the kiosks to extract money from specific customers. Indeed, supervisors overruled Bitcoin Depot employees who acted to block scams from continuing. Specifically, [redacted]

85. The victim customers, unaware of the fraud scheme, used Bitcoin Depot's kiosks to transmit crypto to the scammers' crypto wallets at the behest of those scammers. Bitcoin Depot usually kept 13%-30% of the money that the victims put into its kiosks.

86. Once a portion of the victims' money was converted into Bitcoin and transmitted to the wallet specified by the scammers, it was difficult if not impossible for the victims to get their money transmitted to the scammers back.

87. Bitcoin Depot's former employees, trained in anti-money laundering and fraud detection, warned Bitcoin Depot that its kiosks were primarily used to transfer money from scam victims to scammers and estimated that 90% of the customers spending the most money at the kiosks were fraud victims.

88. After receiving these warnings from its experienced staff, Bitcoin Depot changed its procedures to reduce the amount of fraud its analysts found: [redacted]

89. If contacted by customers seeking to recover the funds lost to a scam via its kiosks, Bitcoin Depot often would not assist customers in attempting to recover the funds customers had sent to the scammers nor return the "fees" (the portion of the customers' cash that Bitcoin Depot had kept) that it charged customers.

90. Bitcoin Depot facilitated this fraud by providing the essential element—its crypto kiosk—in the scam, structuring its oversight so as to not only allow but also understate fraudulent activity, and ignoring violations of its rules (its kiosk terms and conditions) to allow multiple transactions and large transfers that it knew were fraudulent. Bitcoin Depot knew of the fraud and knew that for each fraudulent transfer it stood to make significant profits through its fees and markups. Bitcoin Depot, by not taking steps to stop the fraud occurring via its kiosks, took advantage of the fraud which was obstructing the consumers' decision making.

91. There is no countervailing benefit that offsets the injuries that customers suffered using Bitcoin Depot's kiosks as part of fraudulent schemes.

92. Bitcoin Depot is liable for each of these fraudulent transactions, as it knew of the risks, provided the means for the fraud, and directly benefitted from the completion of fraudulent transactions.

93. Bitcoin Depot's actions constitute violations of Chapter 93A, § 2 and 940 C.M.R. 3.16.

94. Bitcoin Depot acts as an agent or instrumentality of Bitcoin Depot Inc., making Bitcoin Depot Inc. vicariously liable for Bitcoin Depot's actions.

Count IV

(Deceptive Refund Policy in Violation of G.L. c. 93A and 940 C.M.R. 3.16)

95. The Commonwealth repeats and realleges the preceding paragraphs of this Complaint.

96. Bitcoin Depot engaged in unfair or deceptive acts or practices in violation of G.L. c. 93A, § 2 through deceiving customers about its ability to assist scam victims.

97. Bitcoin Depot's employees had warned Bitcoin Depot that in almost all of Bitcoin Depot's large transactions customers were being scammed out of their money using Bitcoin Depot's crypto kiosks.

98. Bitcoin Depot, in spite of these warnings, reduced the questions that its analysts asked of customers to whom they spoke [redacted] Bitcoin Depot later also raised its transaction limits so that customers could put more money into its machines at one time. The company also kept practices in place despite knowing the current modus operandi created large risks of fraud. For instance, [redacted]

99. Bitcoin Depot took these actions even though it knew, from its analysts, that asking more questions of its largest customers would reveal that the transactions were scams and that Bitcoin Depot's kiosks were facilitating fraud and money laundering.

100. In short, with its knowledge of the overwhelming number of scams occurring at its kiosks, its choice to reduce the questions that it asked customers, [redacted] Bitcoin Depot did not take customers' money in good faith.

101. Yet in many cases, when the scammed customers called Bitcoin Depot to tell Bitcoin Depot that they had been scammed and that their money had been stolen, Bitcoin Depot told them that there was nothing that the company could do and did not offer them or tell them about any potential refund process, even for the significant fees that Bitcoin Depot had collected and kept from the scammed customers. In other cases, it gave customers a process for a refund but only returned some of the fees that Bitcoin Depot had received from the customers.

102. Bitcoin Depot's statements were inaccurate. Bitcoin Depot had kept a large portion of the customers' money and had the ability to return it. Further, because Bitcoin Depot had not acted in good faith in taking the money from the customers; customers who had been scammed had a right to get the money back from Bitcoin Depot.

103. By not returning the money and telling customers that there was nothing that Bitcoin Depot could do to help the customers, Bitcoin Depot committed unfair and deceptive practices. Similarly, in the instances where Bitcoin Depot did offer a process or pathway to seek a refund, and Bitcoin Depot provided only a partial fee refund, Bitcoin Depot also committed unfair and deceptive practices. Bitcoin Depot was able to keep the money that it knew was derived from its customers being defrauded, even though it had reason to know of the fraud when it had taken the money from the customers.

104. Bitcoin Depot's deception about its ability to return money and assist customers violated Chapter 93A, § 2 and 940 C.M.R. 3.16.

105. Bitcoin Depot acts as agent or instrumentality of Bitcoin Depot Inc., making Bitcoin Depot Inc. vicariously liable for Bitcoin Depot's actions.

Count V

(Bitcoin Depot Inc. Withheld Material Information from Investors in Violation of G.L. c. 93A and 940 C.M.R. 3.16)

106. The Commonwealth repeats and realleges the preceding paragraphs of this Complaint.

107. Bitcoin Depot Inc. has engaged in unfair or deceptive acts or practices in connection with the sale of securities to Massachusetts investors in violation of G. L. c. 93A, § 2 and 940 C.M.R. 3.16.

108. Such unfair or deceptive acts or practices include, without limitation, selling, facilitating, or causing the sale of securities to Massachusetts investors by means of materially false or misleading statements in the offering documents for such securities concerning Bitcoin Depot's knowledge of the extreme amounts of fraudulent transactions that utilized its kiosks.

109. Bitcoin Depot Inc. knew or should have known that its acts or practices were in violation of G. L.c. 93A, § 2 and 940 C.M.R. 3.16.

110. Bitcoin Depot Inc. willfully violated G. L. c. 93A, § 2 and 940 C.M.R. 3.16 with respect to its securities sales to Massachusetts investors.

111. Bitcoin Depot Inc. acquired payments from Massachusetts investors by means of its unfair or deceptive acts or practices, causing them to suffer an ascertainable loss by purchasing securities (i) that were riskier than Bitcoin Depot Inc. represented them to be, and/or (ii) they would not have purchased but for Bitcoin Depot Inc.'s misrepresentations and nondisclosures.

112. Bitcoin Depot Inc.'s unfair or deceptive acts or practices resulted in harm to consumers.

VI. RELIEF REQUESTED

WHEREFORE, the Commonwealth requests that this Court:

A. Enjoin Bitcoin Depot from accepting transactions larger than $10,000 per day at kiosks located in Massachusetts without taking additional steps to prevent fraud, including but not limited to (i) speaking with any new customers seeking to buy more than $10,000 in Bitcoin and asking a series of questions to identify fraud risks, and (ii) agreeing to provide a full refund of any fees and spread taken by Bitcoin Depot if a customer reports that the

transaction was the result of fraud, files a police report, and presents that police report to Bitcoin Depot within thirty days of the transaction.

B. Order Bitcoin Depot to refund to customers all money that Bitcoin Depot collected related to transactions determined to be the result of fraud against the customers.

C. Order Bitcoin Depot to refund to customers all spread collected in excess of 23% of the transaction amount.

D. Order Bitcoin Depot to refund all spread to customers where Bitcoin Depot began the transaction at the kiosk with a displayed Bitcoin price that did not include the spread that Bitcoin Depot eventually charged to the customers as part of the transaction.

E. Order Bitcoin Depot to refund all spread and fees to customers whom Bitcoin Depot told it could not help when they reported fraud.

F. Order Bitcoin Depot Inc. to offer to Massachusetts purchasers of Bitcoin Depot's securities the option to tender their securities in exchange for payment or to receive damages payments in the amount that would be provided under G.L. c. 110A, § 410(a)(2).

G. Order Bitcoin Depot and Bitcoin Depot Inc. to pay the Commonwealth civil penalties of $5,000 for each violation of G.L. c. 93A, § 2, and to pay the reasonable costs of investigation and litigation of such violation, including reasonable attorneys' fees, pursuant to G.L. c. 93A, § 4.

H. Grant such and further relief as this Court deems just and proper.

COMMONWEALTH OF MASSACHUSETTS
ANDREA CAMPBELL
ATTORNEY GENERAL

Michael Sugar BBO #683901
Assistant Attorney General
Office of the Attorney General

One Ashburton Place, 18th Floor
Boston, MA 02108
617-963-2595
Michael.Sugar@Mass.Gov