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.

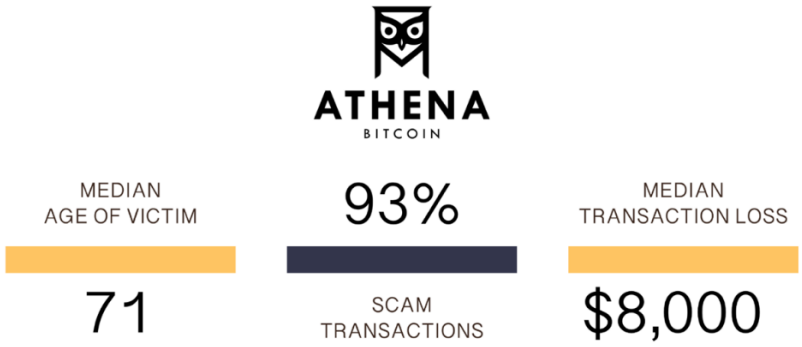
6. The scammer in control of the wallet may then transfer the money to another wallet controlled by the scammer or convert the Bitcoin to cash via offshore Bitcoin exchanges, such as Binance, Bybit, or KuCoin. Once the money has been deposited into the scammer's wallet, the transaction cannot be reversed.

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.

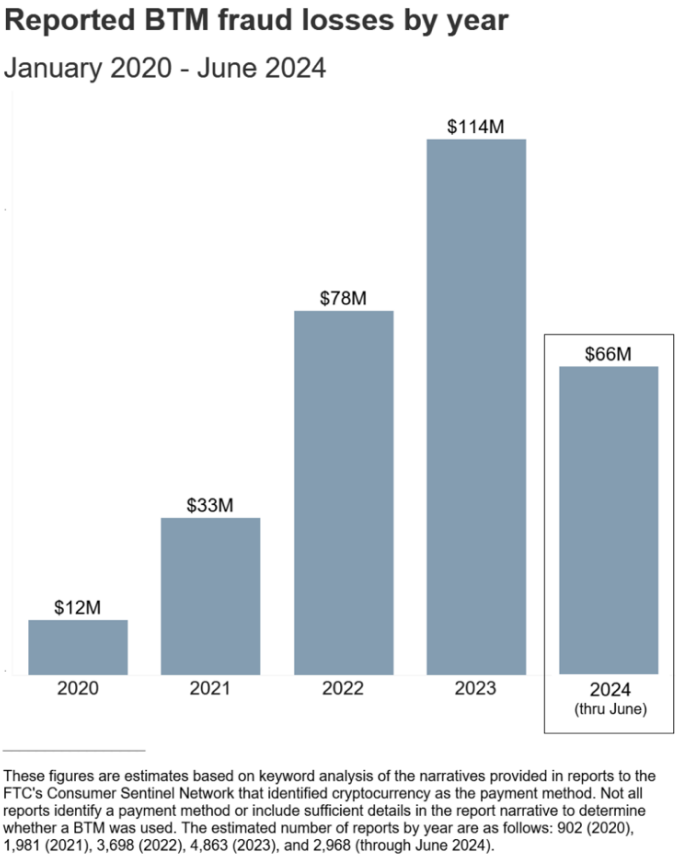
16. This Court has personal jurisdiction over the Defendant under D.C. Code §§ 13-422 and 13-423.

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.

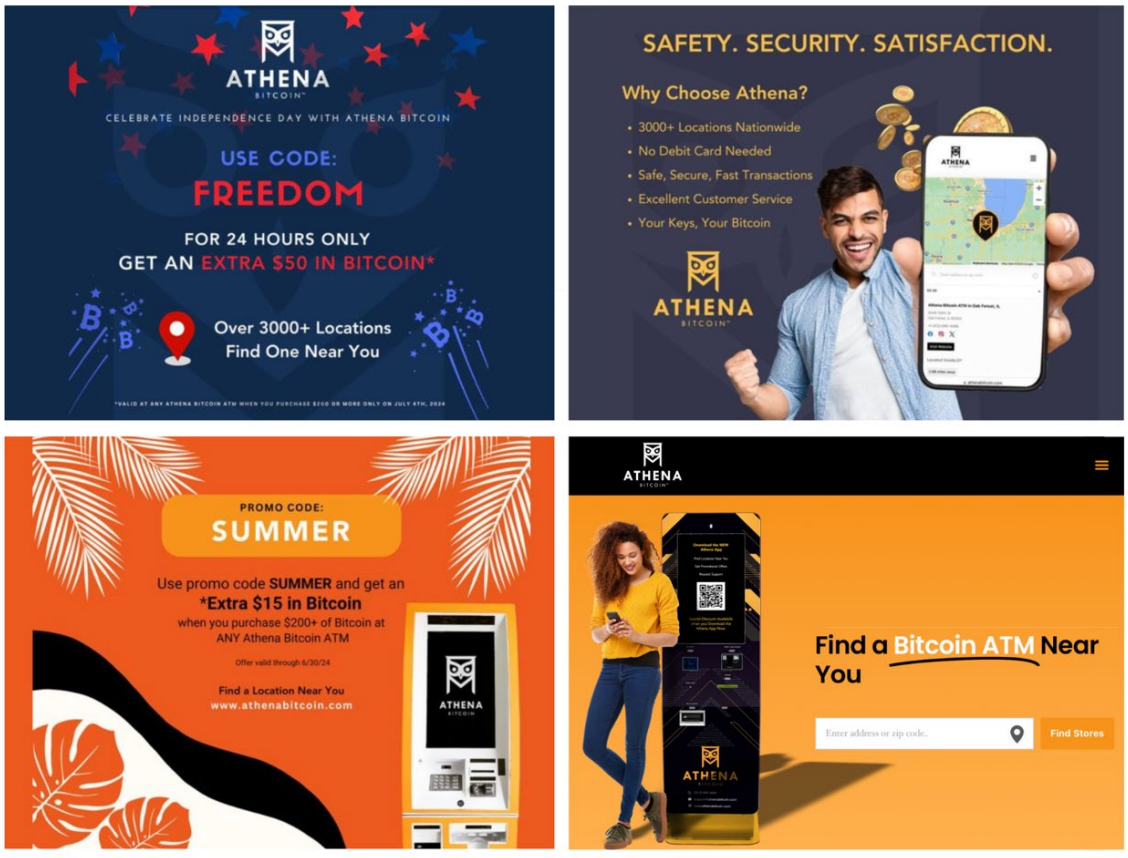
23. Scammers do not select these BTMs randomly. They direct victims to specific operators, favoring those with lax security measures and weak fraud prevention protocols—providing victims precise instructions on where to find BTMs in each city.

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.

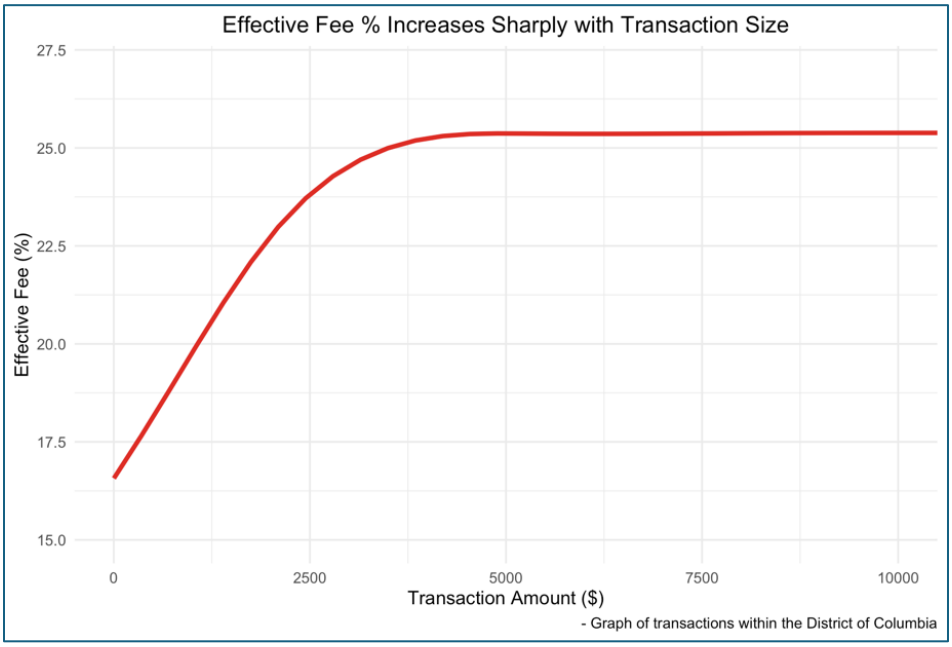
33. In SEC filings, Athena describes the primary source of its revenue much more plainly:

> 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.

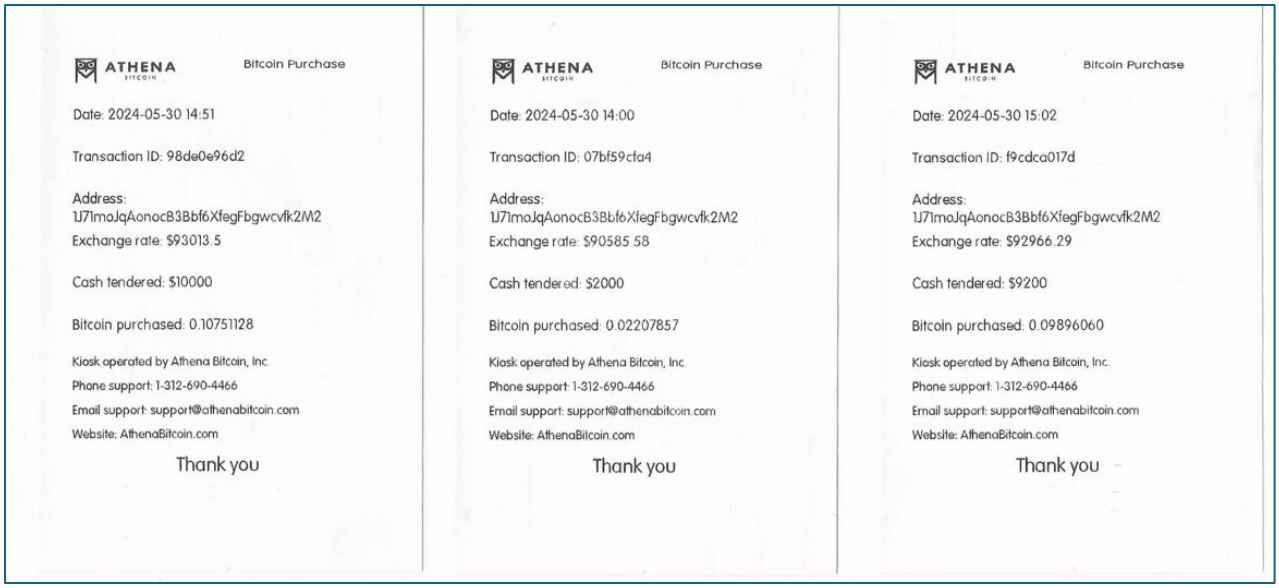
34. Part of the "secret" of Athena's fee method is that the more Bitcoin a user buys, the higher the fee percentage. In the District, small transactions are assessed a fee as low as 13%,

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.

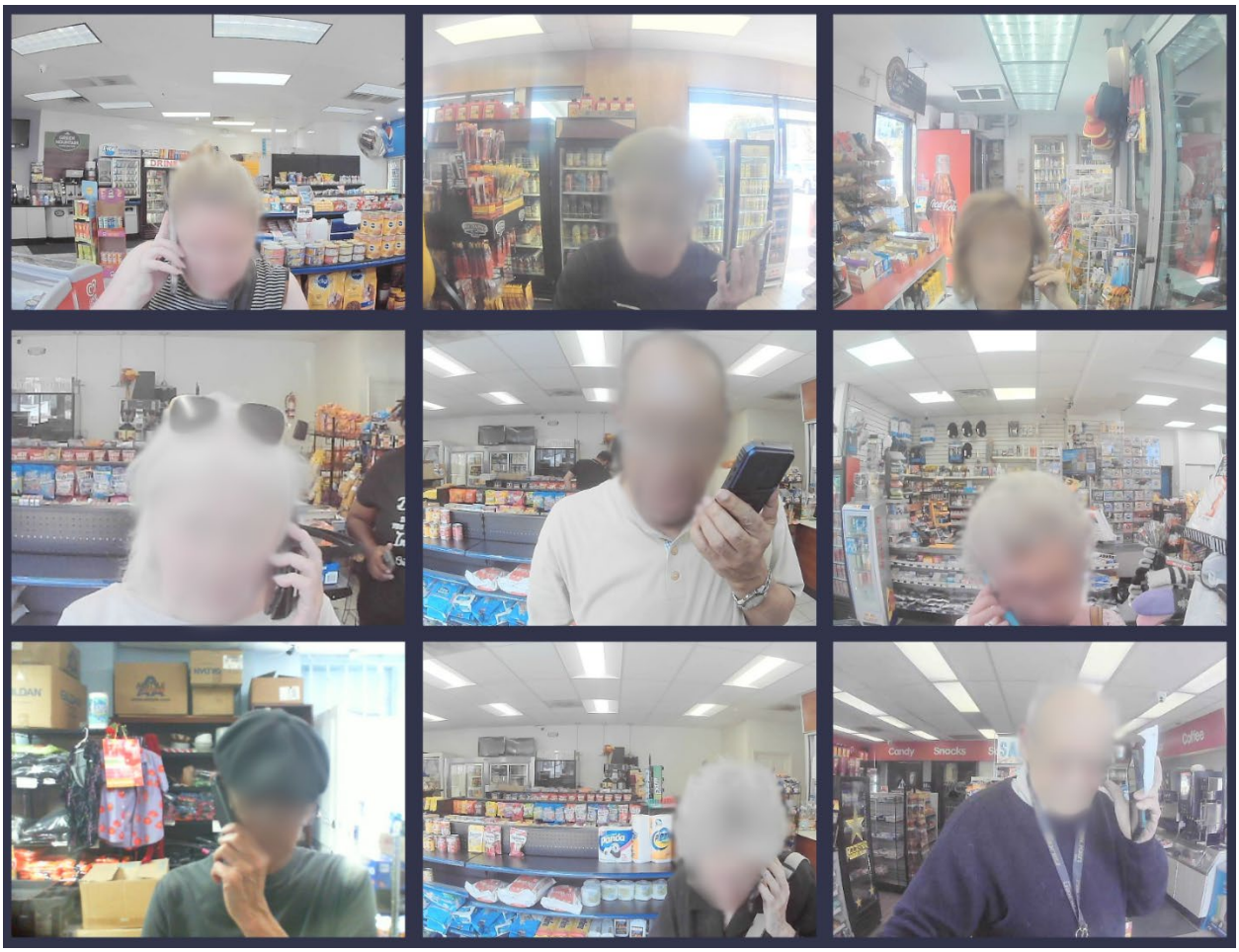
47. The release attempts to free Athena of all future liability while requiring the victim to blame themselves "under penalty of perjury" for not sufficiently heeding the onscreen warnings.

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]

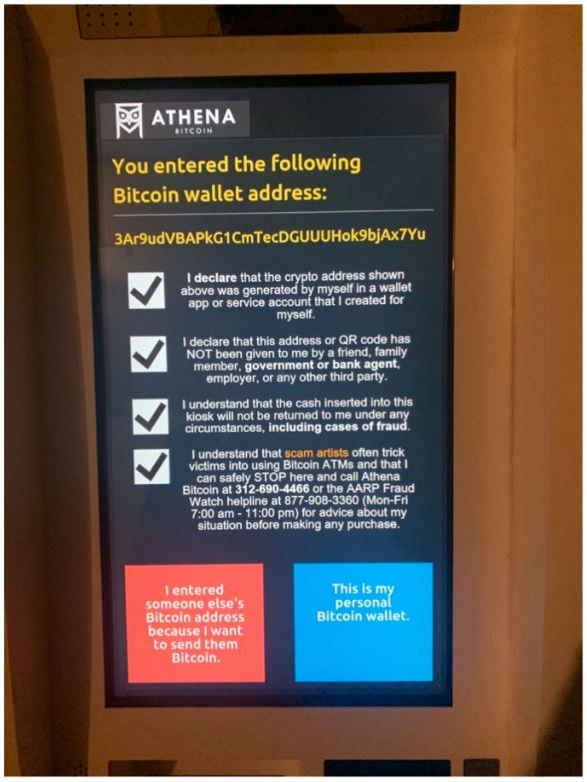
55. Despite clear data showing that its warnings do nothing to stop the imposter scams driving most of its revenue, Athena has continued operating unchanged—attempting to insulate itself behind ineffectual warnings and allowing its network of machines to grow into a pipeline for large-scale elder financial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

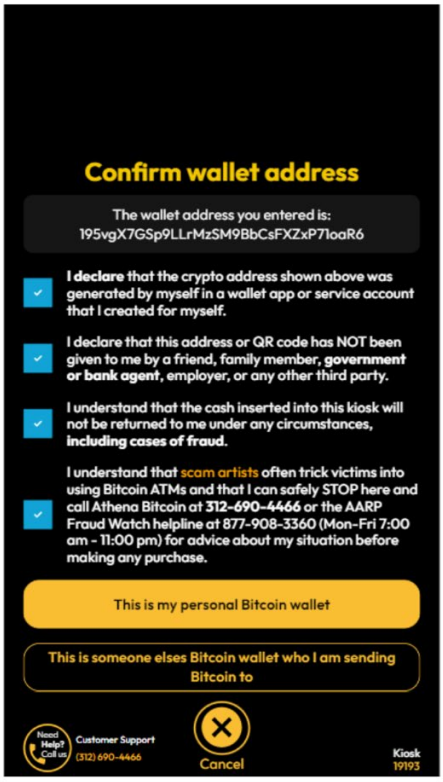
57. For example, on July 10, 2024, a 75-year-old District resident lost $27,600 in a single BTM transaction; on July 15, 2024, a 79-year-old District resident lost $18,500 in a single BTM transaction; and on August 30, 2024, a 73-year-old District resident lost $24,500 in a single BTM transaction. Athena 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