IN THE UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF INDIANA
INDIANAPOLIS DIVISION

STEVE BECKETT, individually and on behalf of all others similarly situated,
% DannLaw
15000 Madison Avenue
Lakewood, OH 44107

Plaintiffs,

v.

BITCOIN DEPOT, INC.
% Corporation Service Company Registered Agent
135 North Pennsylvania Street, Suite 1610
Indianapolis, IN 46204

AND

BITCOIN DEPOT OPERATING, LLC (D/B/A BITCOIN DEPOT),
% Corporation Service Company Registered Agent
135 North Pennsylvania Street, Suite 1610
Indianapolis, IN 46204

Defendants.

Case No.

Judge

COMPLAINT FOR DAMAGES

JURY DEMAND ENDORSED HEREON

Plaintiff Steve Beckett, individually and on behalf of all others similarly situated, brings this Complaint for Damages against Defendants Bitcoin Depot, Inc. and Bitcoin Depot Operating, LLC. Plaintiff makes these allegations with personal knowledge with respect to himself and on information and belief derived from, among other things, investigation of counsel and review of public documents as to all other matters, as follows:

SUMMARY OF CASE

1. This action seeks to hold Bitcoin Depot accountable for systematically facilitating cryptocurrency scams through its Bitcoin ATM network, particularly targeting elderly and vulnerable consumers who lose thousands of dollars to fraudsters using Bitcoin Depot's machines.

2. Plaintiff Steve Beckett, a 66-year-old retiree, lost $7,000 when scammers impersonating Microsoft and law enforcement coerced him into depositing cash at a Bitcoin Depot ATM. Despite obvious red flags—an elderly first-time user making three large transactions totaling $7,000 within 24 hours—Bitcoin Depot's ATM processed each transaction without intervention, taking its substantial cut before transferring the remainder to the scammers' wallet.

3. Impersonation scams using Bitcoin ATMs have become a nationwide epidemic. Fraudsters routinely impersonate government agencies, tech companies, and law enforcement to convince victims—particularly seniors—that they must urgently deposit cash into Bitcoin ATMs to resolve fabricated emergencies. Federal Trade Commission data shows fraud losses at Bitcoin ATMs increased nearly tenfold from 2020 to 2023, with older adults losing more than two-thirds of all dollars reported stolen through these machines.[1]

4. As one of the largest Bitcoin ATM operators in North America, Bitcoin Depot has actual knowledge that its ATMs are routinely used for these impersonation scams. The company's own SEC filings admit its services "may be exploited to facilitate illegal activity such as fraud" and that its "risk management policies may not be sufficient."[2] Bitcoin Depot has even published

[1] Federal Trade Commission, September 3, 2024, "FTC Data Spotlight. Bitcoin ATMs: a payment portal for scammers," www.ftc.gov/news-events/data-visualizations/data-spotlight/2024/09/bitcoin-atms-payment-portal-scammers (last visited July 11, 2025)

[2] Bitcoin Depot, Inc., Form 10-Q, United States Securities and Exchange Commission, pp. 63, 67 (Sept. 30, 2023)

articles acknowledging that "seniors are particularly vulnerable" to cryptocurrency scams and that "elder theft and scams are at an all-time high."[3]

5. Despite this knowledge—and despite publicly claiming to provide "safe and secure" Bitcoin ATM services—Bitcoin Depot prioritizes profits over protection.[4] The company charges fees up to 50% of transaction amounts, deriving substantial revenue from fraudulent transactions while implementing only ineffective on-screen warnings that demonstrably fail to prevent scams.[5]

6. This lawsuit alleges Bitcoin Depot's conduct violates Indiana's Deceptive Consumer Sales Act through misrepresenting the security of its services and failing to implement adequate safeguards. The complaint also brings claims for Replevin, Negligence, and Voluntary Assumption of Duty for Bitcoin Depot's breach of its self-proclaimed commitment to customer protection.

7. Plaintiff seeks to certify a class of similarly situated victims and requests treble damages under Indiana's senior consumer protection law, immediate return of wrongfully detained funds, injunctive relief requiring effective protective measures, and attorney fees.

PARTIES

8. Plaintiff Steve Beckett ("Plaintiff Beckett") is a 66-year-old Indiana resident and retired professional with a background in management at major corporations including Xerox and

[3] Bitcoin Depot, What Crypto Scams Seniors Should Watch For (May 23, 2023), https://bitcoindepot.com/bitcoin-atm-info/what-crypto-scams-seniors-should-watch-for/ (last visited July 11, 2025)
[4] Bitcoin Depot, Protecting Yourself from Bitcoin ATM Scams and Fraud, https://bitcoindepot.com/scam-fraud/ (last visited July 11, 2025)
[5] Bitcoin Depot, Terms and Conditions, https://bitcoindepot.com/terms-and-conditions/ (last visited July 11, 2025)

Amazon. Despite his professional experience, Plaintiff Beckett had limited familiarity with cryptocurrency when he was victimized by scammers using Bitcoin Depot's ATM network.

9. Defendant Bitcoin Depot, Inc. is a Delaware corporation with its principal place of business in Georgia that operates the largest cryptocurrency kiosk network in North America, claiming to operate more than 8,400 Bitcoin ATMs across the United States, Canada, and Puerto Rico.

10. Defendant Bitcoin Depot Operating, LLC, is a foreign LLC registered to do business in Indiana. As an LLC, Bitcoin Depot is considered a resident of the state of each of its members. According to public filings by Bitcoin Depot, Inc., Bitcoin Depot Operating, LLC, is a wholly owned subsidiary of BT HoldCo, LLC, of which Bitcoin Depot, Inc. is the sole managing member. Accordingly, Bitcoin Depot Operating, LLC, is considered a resident of the states of Delaware and Georgia.

11. Bitcoin Depot, Inc., and Bitcoin Depot Operating, LLC, are referred to collectively hereinafter as the "Bitcoin Depot."

JURISDICTION AND VENUE

12. This Court has subject matter jurisdiction over this action pursuant to the Class Action Fairness Act, 28 U.S.C. § 1332(d), because this is a class action in which the number of members of all proposed plaintiff classes in the aggregate is 100 or more, the amount in controversy exceeds the sum or value of $5,000,000, exclusive of interest and costs, minimal diversity exists because at least one member of the plaintiff class is a citizen of a state different from at least one defendant, and none of the exceptions under 28 U.S.C. § 1332(d)(4) apply to this action.

13. This Court has personal jurisdiction over Bitcoin Depot because it conducts substantial business in Indiana, including:

a. Operating and maintaining 418 Bitcoin ATMs throughout Indiana, generating substantial revenue from Indiana residents;

b. Advertising its services to Indiana consumers; and

c. Conducting the specific transactions at issue in this lawsuit with Indiana resident Steve Beckett.

14. Venue is proper in this Court pursuant to 28 U.S.C. § 1391 because the events giving rise to these claims occurred in Dearborn County, Indiana, where Bitcoin Depot operates ATMs and conducts regular business with Indiana consumers, and because a substantial part of the events or omissions giving rise to the claims occurred within this judicial district.

15. Bitcoin Depot purposefully availed itself of Indiana's market and legal protections by establishing a comprehensive network of ATMs throughout the state, making it subject to Indiana's jurisdiction and consumer protection laws.

16. This Court has supplemental jurisdiction over any state law claims that do not independently satisfy CAFA's requirements pursuant to 28 U.S.C. § 1367(a) because such claims are so related to the claims within this Court's original jurisdiction that they form part of the same case or controversy under Article III of the United States Constitution.

ALLEGATIONS

A. Bitcoin Depot's Business Model and Services

17. Bitcoin Depot operates one of the largest cryptocurrency kiosk networks in North America, claiming to operate more than 8,400 Bitcoin ATMs across the United States, Canada, and Puerto Rico. In Indiana alone, Bitcoin Depot operates over 418 ATMs.

18. Bitcoin Depot strategically places its ATMs in high-traffic retail locations through partnership contracts with national, regional, and independent convenience stores, grocery stores, liquor stores, and gas stations, maximizing accessibility to cash-carrying consumers.

19. Bitcoin ATMs are self-service kiosks that convert cash directly into Bitcoin cryptocurrency. The machines resemble traditional ATMs with a touchscreen display, keypad, bill acceptor slot for cash insertion, and camera to scan QR codes linked to Bitcoin wallets where funds are transferred.

20. Bitcoin Depot's business model differs significantly from traditional online cryptocurrency exchanges in ways that make the ATMs particularly attractive to scammers:

a. **Immediate cash-to-Bitcoin conversion** without requiring bank accounts or credit cards;

b. **Instant transfers** with little or no delay after payment, unlike traditional exchanges that impose waiting periods;

c. **Anonymous "non-custodial" wallets** brought by users or generated by the ATM, giving Bitcoin Depot no control over or knowledge of who accesses the wallet's private keys, unlike traditional exchanges that maintain control and comply with anti-money laundering regulations.

21. Bitcoin Depot markets these features—speed, convenience, and anonymity—as advantages while charging substantially higher fees than traditional exchanges. For transactions involving Plaintiff, Bitcoin Depot retained approximately 25-30% of the cash deposited as fees before converting the remainder to Bitcoin.

22. Under Bitcoin Depot's current terms of service published in January 2025, the company can charge fees up to 50% of the total transaction amount.[6]

23. Bitcoin Depot's high-fee, high-volume business model generates substantial revenue from each transaction. The company announced a 25% revenue reduction in Q3 2024 compared to 2023 specifically because California legislation limited daily transactions to $1,000, demonstrating the company's dependence on high-value transactions.[7]

24. Bitcoin Depot derives revenue not only from legitimate cryptocurrency purchases but also from fraudulent transactions, as the company retains its substantial fees regardless of whether the underlying transaction is legitimate or part of a scam targeting vulnerable consumers.

B. The Cryptocurrency ATM Scam Epidemic

25. Cryptocurrency ATM scams have reached epidemic proportions nationwide, with Bitcoin ATMs serving as the primary payment method for fraudsters targeting vulnerable consumers. Federal Trade Commission data shows fraud losses at Bitcoin ATMs increased nearly tenfold from $12 million in 2020 to $114 million in 2023.[8]

26. The median reported loss when using cryptocurrency kiosks was $10,000 in the first six months of 2024, compared to $447 in general fraud cases—demonstrating that Bitcoin ATM scams result in disproportionately devastating financial losses.[9]

---

[6] Bitcoin Depot, Terms and Conditions, https://bitcoindepot.com/terms-and-conditions/ (last visited July 11, 2025)

[7] Bitcoin Depot Reports Third Quarter 2024 Financial Results, https://ir.bitcoindepot.com/news-events/press-releases/detail/87/bitcoin-depot-reports-third-quarter-2024-financial-results (last visited July 11, 2025)

[8] Federal Trade Commission, September 3, 2024, "FTC Data Spotlight. Bitcoin ATMs: a payment portal for scammers," www.ftc.gov/news-events/data-visualizations/data-spotlight/2024/09/bitcoin-atms-payment-portal-scammers (last visited July 11, 2025)

[9] Fed. Trade Comm'n, Protecting Older Consumers 2023-2024: A Report of the Federal Trade Commission, at 17 (Oct. 18, 2024)

27. Elderly adults are the primary targets of Bitcoin ATM scams. People aged 60 and over were more than three times as likely as younger adults to report losses using Bitcoin ATMs, with older adults accounting for more than two-thirds of all dollars reported lost through these machines.[10]

28. "Cryptocurrency ATM Scams" follow a predictable pattern that exploits Bitcoin ATMs' speed and anonymity features:

a. Scammers contact victims by telephone, impersonating trusted entities including government agencies (IRS, Social Security Administration, Federal Reserve), technology companies (Microsoft, Apple), law enforcement, banks, or utility companies;

b. Scammers create artificial urgency by claiming the victim's accounts are compromised, they face legal trouble, or immediate action is required to prevent financial loss;

c. Scammers direct victims to withdraw cash and deposit it into Bitcoin ATMs while providing QR codes containing the scammer's wallet address;

d. Scammers remain on the phone throughout the process, using psychological manipulation and threats to prevent victims from recognizing the fraud.

29. Common cryptocurrency scam variations specifically targeting seniors include:

a. Government impersonation scams claiming victims owe taxes, face arrest, or need to "protect" their Social Security benefits;

b. Tech support scams claiming victims' computers are hacked or infected with viruses;

[10] *Id*.

c. Grandparent scams claiming relatives are in legal trouble and need bail money;

d. Romance scams targeting lonely seniors through dating websites and social media.

30. Bitcoin ATMs are the scammers' preferred payment method because they offer immediate, irreversible transfers to anonymous wallets with minimal verification requirements. Traditional wire transfer services and money order systems have implemented safeguards that make Bitcoin ATMs more attractive for fraudulent schemes.

31. The Federal Trade Commission has specifically recognized Bitcoin ATMs as "a payment portal for scammers," warning that these machines present unique risks due to their combination of cash acceptance, immediate transfers, and anonymity.[11]

32. The cryptocurrency ATM scam epidemic represents a foreseeable and well-documented threat to consumer welfare, particularly affecting vulnerable elderly populations who are less familiar with cryptocurrency technology and more susceptible to authority-based manipulation tactics.

C. Bitcoin Depot's Actual Knowledge of Scam Exploitation

33. Bitcoin Depot has actual knowledge that its ATMs are routinely exploited for cryptocurrency scams targeting elderly and vulnerable consumers. This knowledge comes from multiple sources, including government reports, industry data, direct consumer complaints, and the company's own internal admissions.

34. In September 2023, Bitcoin Depot publicly admitted in its SEC filing that it was aware "[o]ur products and services may be exploited to facilitate illegal activity such as fraud, money laundering, gambling, tax evasion, and scams."[12]

[11] Federal Trade Commission, September 3, 2024, "FTC Data Spotlight. Bitcoin ATMs: a payment portal for scammers"

[12] Bitcoin Depot, Inc., Form 10-Q, United States Securities and Exchange Commission, p. 67 (Sept. 30, 2023)

35. Bitcoin Depot further acknowledged in the same SEC filing that its risk management systems are inadequate: "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."[13]

36. Bitcoin Depot has published articles on its own website acknowledging the vulnerability of seniors to cryptocurrency scams. In an article titled "What Crypto Scams Seniors Should Watch For," Bitcoin Depot explicitly recognized that "Seniors are particularly vulnerable to these [cryptocurrency] scams, as they may be more trusting of strangers and less familiar with how cryptocurrency works."[14]

37. In the same publication, Bitcoin Depot acknowledged that "Elder theft and scams are at an all-time high" and specifically identified common cryptocurrency scams targeting elderly consumers, including grandparent scams, tech support scams, and romance scams.[15]

38. Bitcoin Depot receives direct consumer complaints documenting scam victimization through its ATM network. Recent complaints posted to Bitcoin Depot's Better Business Bureau profile include multiple reports of victims losing substantial sums to scammers:

a. A complaint about a victim who deposited $9,900 into a Bitcoin Depot ATM after being scammed, with Bitcoin Depot refusing to provide a refund and stating "it was a legit deposit";[16]

---

[13] *Id*. at pp. 63, 67

[14] Bitcoin Depot, What Crypto Scams Seniors Should Watch For (May 23, 2023), https://bitcoindepot.com/bitcoin-atm-info/what-crypto-scams-seniors-should-watch-for/ (last visited July 11, 2025)

[15] *Id*.

[16] Better Business Bureau Complaint, Bitcoin Depot Operating LLC, April 16, 2025, https://www.bbb.org/us/ga/atlanta/profile/virtual-currency/bitcoin-depot-operating-llc-0443-28143445/complaints (last visited July 11, 2025)

b. A complaint about an elderly father who lost significant funds to scammers, with the complainant noting that Bitcoin Depot "allow[s] criminals to continue their fraudulent activities" and lacks adequate security measures;[17]

c. Multiple complaints describing elderly victims depositing tens of thousands of dollars while following telephone instructions from scammers impersonating government agencies and tech support.[18]

39. Bitcoin Depot's customer demographics demonstrate actual knowledge that elderly adults comprise its primary user base, despite the company's public claims about serving the "unbanked" and facilitating international remittances. Federal data confirms that older adults are more likely to be targeted for scams and less likely to report losses, making them attractive targets for exploitation.[19]

40. Bitcoin Depot is aware that multiple users regularly send Bitcoin to identical wallet addresses, indicating that funds are being sent to third parties rather than to wallets owned by the users themselves—a clear violation of Bitcoin Depot's stated policies requiring users to send Bitcoin only to their own wallets.[20]

41. Despite claiming to employ "various measures to protect [its] customers from scams and fraud" and asserting that "by taking these measures, we are able to provide our customers with a safe and secure Bitcoin ATM experience," Bitcoin Depot's own data

---

[17] Better Business Bureau Complaint, Bitcoin Depot Operating LLC, January 22, 2025, https://www.bbb.org/us/ga/atlanta/profile/virtual-currency/bitcoin-depot-operating-llc-0443-28143445/complaints (last visited July 11, 2025)

[18] Better Business Bureau Complaints, Bitcoin Depot Operating LLC, August 22, 2024 and September 5, 2024, https://www.bbb.org/us/ga/atlanta/profile/virtual-currency/bitcoin-depot-operating-llc-0443-28143445/complaints (last visited July 11, 2025)

[19] Fed. Trade Comm'n, Protecting Older Consumers 2023-2024: A Report of the Federal Trade Commission, at 17 (Oct. 18, 2024)

[20] Bitcoin Depot FAQ, https://bitcoindepot.com/faq/ (last visited July 11, 2025)

demonstrates that its safeguards fail to prevent scam transactions, as evidenced by the continued stream of consumer complaints and the company's own admission that its risk management "may not be sufficient."[21]

42. Bitcoin Depot CEO Brandon Mintz has stated that the company's objective is to "safely, securely, bring Bitcoin to the masses," yet the company's internal data and external reports confirm that Bitcoin Depot's ATMs are causing consumers "substantial, unavoidable injury" that far outweighs any purported consumer benefits.[22]

D. Bitcoin Depot's Inadequate Response and Failures

43. Despite its actual knowledge of widespread scam exploitation, Bitcoin Depot has deliberately chosen to implement only minimal, demonstrably ineffective safeguards that prioritize transaction volume and profits over consumer protection.

44. Bitcoin Depot's primary anti-fraud measure consists of displaying on-screen warnings and placing stickers on ATMs with messages such as "ARE YOU BEING SCAMMED?" and "Do not buy bitcoin for IRS payments, utility bills, or if someone says you have been hacked or are being investigated. These are scams!"[23]

45. These warning-based measures are fundamentally inadequate and Bitcoin Depot knows it. Federal Trade Commission research on scam prevention messaging demonstrates that

---

[21] Bitcoin Depot, Protecting Yourself from Bitcoin ATM Scams and Fraud, https://bitcoindepot.com/scam-fraud/ (last visited July 11, 2025)

[22] Crypto ATM Provider Bitcoin Depot Announces Nasdaq Listing for July 3, CRYPTOSLATE (July 2, 2023)

[23] USA Today, "Bitcoin ATM scams targeting seniors surge. Here's how consumer advocates want to stop them" (April 21, 2025), https://www.usatoday.com/story/money/2025/04/21/bitcoin-atm-scams-consumer-protection/83201725007/ (last visited July 11, 2025)

warnings often fail because scammers disrupt victims' ability to reason, creating psychological states where victims cannot process warning information effectively.[24]

46. Bitcoin Depot's own transaction data proves the ineffectiveness of its warnings. The continued high volume of scam transactions reported through consumer complaints and the company's own admission that it "cannot ensure" detection of illegal activity confirm that warning messages fail to prevent fraud.[25]

47. Bitcoin Depot deliberately fails to implement meaningful transaction monitoring despite having the technological capability to do so. The company allows transactions that should trigger automatic intervention, including:

a. **Large cash deposits by first-time users**, particularly elderly customers exhibiting signs of distress;

b. **Multiple maximum-value transactions** by the same individual within short time periods;

c. **Sequential deposits to identical Bitcoin wallet addresses** from different users, indicating third-party control;

d. **Customers visibly following telephone instructions** while struggling to complete transactions.

48. Bitcoin Depot has no policies specifically designed to protect consumers aged 60 or older from fraud, despite acknowledging that seniors comprise its primary user base and are

[24] Federal Trade Commission, "A Review of Scam Prevention Messaging Research," https://consumer.ftc.gov/system/files/consumer_ftc_gov/pdf/A%20Review%20of%20Scam%20Prevention%20Messaging%20Research.pdf (last visited July 11, 2025)

[25] Bitcoin Depot, Inc., Form 10-Q, United States Securities and Exchange Commission, pp. 63, 67 (Sept. 30, 2023)

"particularly vulnerable" to cryptocurrency scams. Other cryptocurrency kiosk companies have implemented elderly-specific protections that Bitcoin Depot deliberately chooses not to adopt.[26]

49. Bitcoin Depot fails to utilize available blockchain tracking capabilities that could identify and prevent scam patterns. While every Bitcoin transaction is permanently recorded on the blockchain, Bitcoin Depot does not use this technology to detect when multiple victims send funds to the same scammer-controlled wallets.

50. When obvious red flags occur, Bitcoin Depot's ATMs provide superficial warnings but allow customers to bypass them and complete transactions without meaningful intervention. Even when warnings are triggered, the company does not:

a. Contact customers to verify their intentions;

b. Implement cooling-off periods for large or suspicious transactions;

c. Require enhanced verification for elderly or distressed users;

d. Temporarily hold funds pending verification of transaction legitimacy.

51. Bitcoin Depot could implement but deliberately chooses not to adopt effective protective measures that would reduce scam victimization, including:

a. Mandatory identity verification for large transactions, particularly by elderly users;

b. Transaction limits and waiting periods for first-time users making substantial deposits;

c. Real-time customer service calls for transactions exhibiting multiple risk factors;

d. Enhanced monitoring systems that detect patterns consistent with scam activity.

[26] Bitcoin Depot, What Crypto Scams Seniors Should Watch For (May 23, 2023), https://bitcoindepot.com/bitcoin-atm-info/what-crypto-scams-seniors-should-watch-for/ (last visited July 11, 2025)

52. Bitcoin Depot's refusal to implement adequate safeguards is driven by economic considerations. The company understands that effective protective measures would reduce transaction volume and the substantial fees it derives from each completed transaction, regardless of legitimacy.

53. When consumers report scam victimization and request assistance, Bitcoin Depot's customer service routinely denies relief and retains its share of the fraudulent proceeds. The company's standard response claims that Bitcoin transactions are "irreversible," while maintaining possession of the original cash deposits and refusing to return even the fees it collected.

54. Bitcoin Depot's inadequate response creates substantial public policy harms, including: (a) enabling a business model that profits from criminal activity; (b) facilitating systematic elder financial abuse; (c) undermining consumer confidence in legitimate cryptocurrency services; and (d) imposing social costs through increased victimization of vulnerable populations.

55. The harm to consumers from Bitcoin Depot's inadequate safeguards is entirely foreseeable and substantially outweighs any purported benefits of the company's service model. Bitcoin Depot operates in conscious disregard of known risks to prioritize profits over the financial security of vulnerable elderly consumers.

E. Bitcoin Depot's Voluntary Assumption of Protective Duties

56. Bitcoin Depot has voluntarily and publicly assumed a duty to protect its customers from cryptocurrency scams and fraud through extensive marketing representations, educational materials, and explicit commitments to consumer safety that go beyond mere legal compliance.

57. Bitcoin Depot prominently represents on its website that it employs "various measures to protect [its] customers from scams and fraud," explicitly stating that "by taking these measures, we are able to provide our customers with a safe and secure Bitcoin ATM experience."[27]

58. Bitcoin Depot CEO Brandon Mintz has publicly stated that the company's central objective is to "safely, securely, bring Bitcoin to the masses," creating reasonable consumer expectations that the company prioritizes customer protection in its operations.[28]

59. Bitcoin Depot has published extensive educational content specifically addressing cryptocurrency scams, including a dedicated webpage titled "Protecting Yourself from Bitcoin ATM Scams and Fraud" where the company acknowledges that "these [Bitcoin] ATMs can be a target for scammers and fraudsters" and commits that "it is important to educate our customers on potential scams and fraud."[29]

60. Through its marketing materials and website content, Bitcoin Depot represents that it provides:

a. Comprehensive scam warnings on all kiosks with information about common fraud schemes;

b. Educational resources to help customers identify and avoid cryptocurrency scams;

c. Readily available customer support to address questions about potential transactions;

d. Security measures to protect Bitcoin ATMs from fraudulent use and tampering.[30]

---

[27] Bitcoin Depot, Protecting Yourself from Bitcoin ATM Scams and Fraud, https://bitcoindepot.com/scam-fraud/ (last visited July 11, 2025)
[28] Crypto ATM Provider Bitcoin Depot Announces Nasdaq Listing for July 3, CRYPTOSLATE (July 2, 2023)
[29] Bitcoin Depot, Protecting Yourself from Bitcoin ATM Scams and Fraud, https://bitcoindepot.com/scam-fraud/ (last visited July 11, 2025)
[30] *Id*.

61. Bitcoin Depot's assumption of protective duties is particularly significant given the company's actual knowledge that seniors comprise its primary user base and are "particularly vulnerable" to cryptocurrency scams. By marketing to this vulnerable population while simultaneously acknowledging their susceptibility to fraud, Bitcoin Depot voluntarily undertook enhanced responsibilities for their protection.

62. Bitcoin Depot's public commitments created reasonable expectations among consumers—including Plaintiff and class members—that the company would exercise reasonable care to detect and prevent obvious scam scenarios, particularly those involving elderly customers making large, unusual transactions.

63. Bitcoin Depot's voluntary assumption of protective duties distinguishes its legal obligations from those of passive service providers. By actively marketing safety and security as service features, the company transformed consumer protection from a regulatory requirement into a contractual commitment and competitive advantage.

64. Bitcoin Depot's assumed duties extend beyond general legal compliance to include reasonable steps to prevent the specific types of fraud the company acknowledges are prevalent in its industry and disproportionately affect its customer base.

65. Having voluntarily assumed these protective duties, Bitcoin Depot became legally obligated to perform them with reasonable care. The company's failure to implement adequate safeguards despite its public commitments constitutes a breach of its voluntarily assumed duties to Plaintiff and class members.

66. Bitcoin Depot's breach of its assumed duties is particularly egregious because the company continues to market safety and security as service features while internally

acknowledging that its risk management systems "may not be sufficient" to prevent the very harms it promises to address.[31]

67. Consumers, including Plaintiff, reasonably relied on Bitcoin Depot's representations about safety and security when choosing to use the company's ATMs rather than alternative cryptocurrency services or declining to engage in cryptocurrency transactions altogether.

68. Bitcoin Depot's voluntary assumption of protective duties created a special relationship with its customers that imposed heightened obligations to act reasonably to prevent foreseeable harm, particularly to vulnerable elderly consumers who are the primary targets of cryptocurrency ATM scams.

F. The Specific Harm to Steve Beckett

69. Plaintiff Beckett is a 66-year-old retired professional with a successful management career at major corporations including Xerox and Amazon. Despite his business experience, Plaintiff Beckett had limited familiarity with cryptocurrency technology when he became a victim of the sophisticated fraud scheme that exploits Bitcoin Depot's inadequate safeguards.

70. On December 16, 2024, Plaintiff Beckett received a fraudulent computer message claiming his screen was locked and directing him to call Microsoft for assistance. Following the instructions, he contacted the provided number and spoke with an individual claiming to be Microsoft representative "Josh Butler" with badge number MS2252.

71. The scammer employed classic impersonation fraud tactics, gaining Plaintiff Beckett's trust by assuming a position of authority and technological expertise. Plaintiff Beckett

[31] Bitcoin Depot, Inc., Form 10-Q, United States Securities and Exchange Commission, pp. 63, 67 (Sept. 30, 2023)

granted remote access to his computer, believing he was receiving legitimate technical support from Microsoft.

72. The scammer escalated the fraud by claiming Plaintiff Beckett's computer and accounts had been compromised to purchase illegal pornography, including child pornography, and to make unauthorized purchases with multiple credit and debit cards. This fabricated crisis was designed to create panic and urgency that would override Plaintiff Beckett's normal reasoning abilities.

73. Using psychological manipulation and threats of legal consequences, the scammer convinced Plaintiff Beckett that law enforcement was involved and that his financial accounts were at risk. The scammer instructed Plaintiff Beckett to withdraw cash and deposit it into Bitcoin ATMs to "secure" his funds and resolve the alleged criminal activity.

74. On December 16, 2024, under continuing duress and fearing fabricated legal consequences, Plaintiff Beckett withdrew $4,000 from his checking account at Fifth Third Bank. He then proceeded to the Circle K gas station at 1202 E Eads Pkwy, Lawrenceburg, Indiana, where he made his first encounter with Bitcoin Depot's ATM.

75. At 2:20 PM EST on December 16, 2024, Plaintiff Beckett deposited $1,000 into the Bitcoin Depot ATM. Despite being an elderly first-time user clearly acting under telephone instructions from an unknown party, Bitcoin Depot's ATM processed the transaction without intervention, converting the cash to 0.00662458 Bitcoin and transferring it to the scammer’s wallet address, while retaining a substantial fee.

76. Fifteen minutes later, at 2:35 PM EST, Plaintiff Beckett deposited an additional $3,000 into the same Bitcoin Depot ATM. This second large transaction by the same elderly user within minutes should have triggered immediate intervention, yet Bitcoin Depot's systems again

processed the transaction without meaningful safeguards, transferring 0.01981750 Bitcoin to the identical scammer-controlled wallet.

77. The following day, December 17, 2024, Plaintiff Beckett withdrew an additional $3,100 from his bank account and returned to the same Bitcoin Depot ATM at 2:35 PM EST, depositing $3,000 in his third large transaction within 24 hours. This pattern—an elderly customer making repeated maximum-value deposits to the same wallet address while following telephone instructions—presented obvious red flags that Bitcoin Depot's systems ignored.

78. After completing his third transaction, Plaintiff Beckett began to notice fraud warnings associated with Bitcoin ATM usage and started to question whether something might be wrong with the situation. When the scammer then instructed him that he now needed to empty out his IRA accounts for additional deposits, Plaintiff Beckett's suspicions were further heightened.

79. Recognizing the gravity of the situation, Plaintiff Beckett went home and discussed the matter with his wife. Together, they returned to the Circle K where the Bitcoin Depot ATM was located so she could examine the machine and assess the situation firsthand. While in the Circle K parking lot, they called Bitcoin Depot's customer service to report the suspected fraud.

80. The Bitcoin Depot representative confirmed that it was likely a fraudulent account to which Plaintiff Beckett had sent his money. When Plaintiff Beckett asked whether he could obtain a refund of his losses, the representative told him that there was no way for him to get his money back and that the money was now lost. Significantly, the representative failed to mention anything about the substantial fees—approximately $2,000—that Bitcoin Depot had retained from his transactions.

81. Across all three transactions, Bitcoin Depot retained approximately 25-30% of each of Plaintiff Beckett's $7,000 in cash as fees—roughly $2,000—before transferring the

remainder as Bitcoin to the scammer's wallet. Bitcoin Depot profited substantially from Plaintiff Beckett's victimization while implementing no protective measures.

82. The blockchain record for the scammer's wallet address shows that the scammers immediately withdrew all Bitcoin from the wallet, leaving a zero balance and confirming that Plaintiff Beckett's funds were irretrievably stolen through Bitcoin Depot's facilitation.

83. After realizing he had been defrauded, Plaintiff Beckett promptly filed a police report with the Lawrenceburg Police Department (Incident # L24-11763) and contacted Bitcoin Depot seeking assistance and recovery of his stolen funds.

84. Bitcoin Depot refused to provide meaningful assistance, declined to reverse the transactions, and retained Plaintiff Beckett's stolen cash. The company's response exemplified its standard practice of denying relief to scam victims while keeping the substantial fees derived from fraudulent transactions.

85. Plaintiff Beckett's experience represents a textbook case of Bitcoin Depot's systemic failures: (a) an elderly, vulnerable customer; (b) obvious signs of distress and telephone manipulation; (c) multiple large transactions in rapid succession; (d) deposits to a third-party wallet; (e) clear red flags ignored by inadequate safeguards; and (f) refusal to provide relief after notification of fraud.

86. As a direct result of Bitcoin Depot's failures and the underlying fraud, Plaintiff Beckett suffered immediate financial losses of $7,000—representing a substantial portion of his retirement savings. He also experienced significant emotional distress, anxiety about his financial security, and the practical consequences of losing funds needed for living expenses and medical care.

87. Plaintiff Beckett's harm was entirely preventable through reasonable safeguards that Bitcoin Depot deliberately chose not to implement. Simple protective measures—such as transaction limits for first-time elderly users, mandatory verification for large sequential deposits, or customer service intervention for obvious red flag scenarios—would have detected and prevented this fraud.

88. Plaintiff Beckett's experience is representative of a systematic pattern affecting similarly situated victims who have suffered financial losses due to Bitcoin Depot's inadequate safeguards, deceptive practices, and prioritization of profits over consumer protection. The common legal and factual issues make this case appropriate for class treatment to address the widespread harm caused by Bitcoin Depot's conduct.

G. Bitcoin Depot's Retention of Stolen Funds

89. After processing fraudulent transactions through its ATM network, Bitcoin Depot systematically retains possession of victims' stolen cash and converts it to its own use rather than returning it to victims or cooperating with law enforcement to facilitate recovery.

90. When victims deposit cash into Bitcoin Depot ATMs under fraudulent circumstances, the physical currency remains in Bitcoin Depot's possession and control within the machine's cash storage compartments. Bitcoin Depot then transfers this cash to its own accounts as part of its regular collection and deposit procedures.

91. Bitcoin Depot maintains a deliberate policy and practice of retaining cash deposited by scam victims even after being notified that the transactions were fraudulent. The company refuses to return stolen funds to victims based on its position that Bitcoin transactions are "irreversible," while simultaneously maintaining possession and control of the original cash deposits.

92. Bitcoin Depot's "irreversibility" representations are misleading and false as applied to the substantial fees it retains from each transaction. While Bitcoin cryptocurrency transfers may be irreversible, the cash fees collected by Bitcoin Depot—typically 25-50% of the total transaction amount—remain in the company's possession and are entirely reversible through simple refund procedures.

93. Bitcoin Depot's retention of stolen cash constitutes wrongful possession and unlawful detention of property belonging to scam victims. The company has no lawful right to possess funds obtained through fraud, regardless of whether those funds were voluntarily deposited by victims acting under duress and deception.

94. Upon receiving notice that deposited funds were obtained through fraud—whether through direct victim complaints, police reports, or obvious transactional red flags—Bitcoin Depot becomes a knowing possessor of stolen property with actual notice of the rightful owners' superior claims to possession.

95. Bitcoin Depot's standard practice when confronted with scam reports is to deny liability, refuse refunds, and retain the stolen funds for its own benefit. Consumer complaints document the company's consistent pattern of responses claiming "there is nothing they can do" while keeping substantial fees from fraudulent transactions.[32]

96. Bitcoin Depot's retention of stolen funds violates fundamental principles of restitution and unjust enrichment. The company derives substantial financial benefit from criminal activity while victims suffer devastating losses, creating an unconscionable disparity that the law does not permit.

---

[32] Better Business Bureau Complaints, Bitcoin Depot Operating LLC, https://www.bbb.org/us/ga/atlanta/profile/virtual-currency/bitcoin-depot-operating-llc-0443-28143445/complaints (last visited July 11, 2025)

97. Bitcoin Depot has the practical ability to return stolen funds to victims, particularly the substantial fees it retains from each transaction. The company's claims of helplessness are pretextual justifications for retaining the proceeds of criminal activity.

98. Bitcoin Depot's policy of retaining stolen cash creates perverse incentives that encourage continued criminal exploitation of its ATM network. By profiting from fraudulent transactions without consequence, the company becomes a financial beneficiary of ongoing criminal enterprise targeting vulnerable elderly consumers.

99. Bitcoin Depot's wrongful retention of stolen property causes ongoing harm to victims who are deprived of funds needed for living expenses, medical care, and other essential needs. The company's refusal to return easily recoverable funds compounds the original harm inflicted by the underlying fraud.

100. The cash deposits at issue belong rightfully to the victims who were defrauded, not to Bitcoin Depot or the scammers who orchestrated the theft. Bitcoin Depot's continued possession of these funds is wrongful and without legal justification.

101. Bitcoin Depot's retention of stolen funds violates public policy by incentivizing the company to facilitate rather than prevent cryptocurrency fraud. The company's ability to profit from criminal activity without returning stolen proceeds creates a business model that depends on continued exploitation of vulnerable consumers.

CLASS ALLEGATIONS

102. This action is brought and may properly proceed as a class action pursuant to Civ.R. 23.

103. Plaintiff seeks certification of the following class:

> All persons who, during the Class Period, completed a cash-to-Bitcoin transaction at a Bitcoin Depot ATM located in Indiana as part of an impersonation scam, and who (a)

reported the fraudulent transaction to Bitcoin Depot, law enforcement, or any government agency, or (b) made such transaction under circumstances that provided Bitcoin Depot with actual or constructive notice of the fraudulent nature of the transaction.

104. As used in the class definition:

a. "Class Period" means the period beginning six (5) years prior to the filing of this Complaint through the date a class certification order is entered;

b. "Bitcoin Depot ATM located in Indiana" means any Bitcoin ATM owned, operated, maintained, or controlled by Bitcoin Depot that is physically located within the state of Indiana;

c. "Impersonation scam" means any fraudulent scheme where perpetrators impersonate or falsely represent themselves as government agencies (including IRS, Social Security Administration, Federal Reserve, or law enforcement), technology companies (including Microsoft, Apple, or other tech support), financial institutions, utility companies, family members in distress, romantic interests, or other trusted entities to deceive victims into depositing cash into Bitcoin ATMs, including all scam types that Bitcoin Depot has acknowledged or described in its publications, SEC filings, or other communications;

d. "Actual or constructive notice" includes circumstances where Bitcoin Depot knew or reasonably should have known of the fraudulent nature of the transaction based on obvious red flags such as: elderly customers making large deposits while following telephone instructions; multiple large transactions in rapid succession by the same user; deposits to wallet addresses known to be associated with fraudulent activity; or transaction patterns consistent with known scam methodologies that Bitcoin Depot has acknowledged in its publications or SEC filings.

105. Excluded from the Class are: (a) Bitcoin Depot and its officers, directors, employees, subsidiaries, and affiliates; (b) governmental entities; (c) any judge presiding over this action and members of their immediate families; and (d) any person who, according to Bitcoin Depot's records, executed a release of claims against Bitcoin Depot prior to the filing of this Complaint.

106. **Numerosity** (Civ.R. 23(a)(1)): The Class is so numerous that joinder of all members is impracticable. Based on the Federal Trade Commission's findings that Bitcoin ATM fraud losses increased from $12 million in 2020 to $114 million in 2023, and that Bitcoin Depot operates over 418 ATMs in Indiana alone as one of the largest operators in North America, the Class likely includes hundreds or thousands of impersonation scam victims. The widespread nature of these scams, Bitcoin Depot's extensive Indiana ATM network, and the company's own admissions about exploitation of its services demonstrate that the Class is sufficiently numerous. The exact number of Class members is known to Bitcoin Depot through its transaction records and complaint history but is not readily ascertainable by Plaintiff. Joinder of all Class members would be impracticable due to the large number of potential members, their geographic dispersion throughout Indiana, and the likelihood that many victims may be unaware of this litigation or reluctant to pursue individual legal action.

107. **Commonality** (Civ.R. 23(a)(2)): There are questions of law and fact common to all Class members, including:

a. Whether Bitcoin Depot's business practices and safeguards constitute deceptive acts under the Indiana Deceptive Consumer Sales Act;

b. Whether Bitcoin Depot failed to implement reasonable measures to detect and prevent cryptocurrency ATM scams despite actual knowledge of their prevalence;

c. Whether Bitcoin Depot's representations about providing "safe and secure" Bitcoin ATM services were false or misleading;

d. Whether Bitcoin Depot voluntarily assumed a duty to protect customers from scams and breached that duty;

e. Whether Bitcoin Depot's conduct was negligent, grossly negligent, or reckless;

f. Whether Bitcoin Depot wrongfully retains cash deposited by scam victims;

g. The appropriateness of injunctive relief requiring Bitcoin Depot to implement effective protective measures.

108. **Typicality** (Rule 23(a)(3)): Plaintiff's claims are typical of the claims of other Class members. Like other Class members, Plaintiff: (a) was victimized by an impersonation scam involving fraudulent representations by criminals posing as trusted entities; (b) deposited cash into a Bitcoin Depot ATM located in Indiana as a direct result of the scam; (c) exhibited obvious red flags that provided Bitcoin Depot with constructive notice of the fraudulent transaction; (d) suffered financial losses when Bitcoin Depot processed the fraudulent transaction despite these warning signs; (e) reported the fraud to law enforcement, providing Bitcoin Depot with additional notice when contacted; and (f) remains harmed by Bitcoin Depot's wrongful retention of stolen funds. Plaintiff's claims arise from the same course of conduct, legal theories, and systematic failures that affect all Class members who were victims of impersonation scams using Bitcoin Depot ATMs.

109. **Adequacy of Representation** (Rule 23(a)(4)): Plaintiff will fairly and adequately protect the interests of the Class. Plaintiff has no interests antagonistic to or in conflict with other Class members. Plaintiff has retained experienced counsel with substantial expertise in class action litigation, consumer protection law, and cases involving elder financial abuse. Plaintiff is

committed to prosecuting this action vigorously and has the financial resources necessary to adequately represent the Class. Proposed Class Counsel have extensive experience in complex litigation and class actions, and have successfully represented consumers in similar cases.

110. This class action satisfies the requirements of Civ.R. 23(b)(2) because Bitcoin Depot has acted or refused to act on grounds that apply generally to the Class, so that final injunctive relief or corresponding declaratory relief is appropriate respecting the Class as a whole. Bitcoin Depot's inadequate safeguards, deceptive practices, and systematic retention of stolen funds affect all Class members uniformly, making injunctive relief requiring implementation of effective protective measures appropriate for the entire Class.

111. This class action also satisfies the requirements of Civ.R. 23(b)(3) because:

a. Predominance: Questions of law and fact common to Class members predominate over any questions affecting only individual members. While individual damages may vary, the core legal and factual issues regarding Bitcoin Depot's conduct, policies, and liability are common to all Class members and can be resolved on a class-wide basis.

b. Superiority: A class action is superior to other available methods for fairly and efficiently adjudicating the controversy. The matters pertinent to this finding include:

i. Class members' interests in individually controlling the prosecution of separate actions: Class members have minimal interest in individually controlling the prosecution of separate actions because: (i) individual claims are relatively small compared to litigation costs; (ii) the legal issues are identical across all claims; (iii) many Class members are elderly and may

lack the resources or sophistication to pursue individual litigation; and (iv) the primary goal is industry-wide reform that benefits all consumers.

ii. Extent and nature of any litigation concerning the controversy already begun by or against class members: Plaintiff is not aware of any other litigation concerning the same controversy that has been commenced by or against other Class members.

iii. Desirability or undesirability of concentrating the litigation in the particular forum: It is desirable to concentrate this litigation in this forum because the harmful conduct occurred in Indiana, Plaintiff is an Indiana resident, Bitcoin Depot conducts substantial business in Indiana through its extensive ATM network, and Indiana has a strong interest in protecting its residents from deceptive practices and elder financial abuse.

iv. Likely difficulties in managing a class action: This case presents no unusual management difficulties. The Class is readily identifiable through Bitcoin Depot's transaction records, the claims arise from a common course of conduct, and the legal theories are straightforward applications of established consumer protection principles.

112. For all the foregoing reasons, this action satisfies all requirements of Federal Rule of Civil Procedure 23 and should be certified as a class action for both injunctive relief under Rule 23(b)(2) and monetary damages under Rule 23(b)(3).

CAUSES OF ACTION

COUNT ONE
VIOLATION OF INDIANA DECEPTIVE CONSUMER SALES ACT
I.C. § 24-5-0.5-4(a) and I.C. § 24-5-0.5-4(i)
(on behalf of the Plaintiff and the Class)

113. Plaintiff incorporates by reference all previous allegations as if fully set forth herein.

114. This action is brought under Indiana Code § 24-5-0.5-4(a) for incurable deceptive acts and Indiana Code § 24-5-0.5-4(i) for enhanced remedies available to senior consumers.

115. Bitcoin Depot's provision of Bitcoin ATM services to Plaintiff constitutes a "consumer transaction" under I.C. § 24-5-0.5-2(a)(1) as it involved the sale of services and intangibles to Plaintiff for purposes that were primarily personal and household.

116. Bitcoin Depot qualifies as a "supplier" under I.C. § 24-5-0.5-2(a)(3)(A) as it regularly engages in consumer transactions through its extensive network of over 8,400 Bitcoin ATMs, including more than 418 ATMs in Indiana.

117. Plaintiff Steve Beckett is a "senior consumer" under I.C. § 24-5-0.5-2(a)(9) as he is 66 years old, entitling him to enhanced remedies under I.C. § 24-5-0.5-4(i).

118. Bitcoin Depot committed multiple deceptive acts in connection with its consumer transactions with Plaintiff and the Class, including but not limited to:

a. Misrepresenting the characteristics and benefits of its services in violation of I.C. § 24-5-0.5-3(a) by claiming to provide "safe and secure Bitcoin ATM services" and employing "various measures to protect customers from scams and fraud" when Bitcoin Depot knew its safeguards were demonstrably ineffective;

b. Representing that its services have characteristics they do not have in violation of I.C. § 24-5-0.5-3(a) by marketing enhanced security and customer protection features that Bitcoin Depot admits in its SEC filings "may not be sufficient" to prevent fraud;

c. Engaging in unfair or deceptive conduct in violation of I.C. § 24-5-0.5-3(b)(27) by:

i. Failing to implement adequate transaction monitoring despite actual knowledge of widespread scam exploitation;

ii. Processing obvious fraudulent transactions without meaningful intervention;

iii. Retaining substantial fees from transactions Bitcoin Depot knew or should have known were fraudulent;

iv. Refusing to provide meaningful assistance or relief to known scam victims.

119. Bitcoin Depot's conduct constitutes "incurable deceptive acts" under I.C. § 24-5-0.5-2(a)(8) because Bitcoin Depot's deceptive practices were committed as part of a systematic scheme, artifice, or device with intent to defraud or mislead vulnerable consumers by:

a. Deliberately targeting elderly consumers while knowing they are "particularly vulnerable" to cryptocurrency scams, as evidenced by Bitcoin Depot's own admissions and industry knowledge;

b. Intentionally implementing only superficial safeguards designed to provide plausible deniability while allowing profitable fraudulent transactions to proceed unimpeded;

c. Systematically retaining substantial profits from transactions Bitcoin Depot knew or should have known were fraudulent, including approximately $2,000 in fees from Plaintiff's $7,000 in fraudulent transactions;

d. Operating a systematic business model that Bitcoin Depot admits depends on high-volume transactions, including those resulting from criminal exploitation of vulnerable consumers;

e. Engaging in a pattern of false representations about safety and security across its extensive network of over 8,400 ATMs while having actual knowledge that such representations were materially false and misleading;

f. Systematically failing to warn consumers about the high risk of scams despite having actual knowledge of widespread exploitation of its systems by fraudsters targeting elderly victims.

120. Bitcoin Depot's systematic scheme demonstrates intent to defraud or mislead vulnerable consumers because:

a. Bitcoin Depot had actual knowledge that its ATMs were routinely exploited for scams targeting elderly consumers, as evidenced by its SEC filings, published industry reports, consumer complaints, and law enforcement advisories;

b. Bitcoin Depot deliberately chose not to implement adequate safeguards because doing so would reduce its transaction volume and profits, demonstrating conscious prioritization of revenue over consumer protection;

c. Bitcoin Depot continued to market false representations about safety and security despite knowing its systems were inadequate to protect vulnerable consumers;

d. Bitcoin Depot's conduct demonstrates conscious disregard for consumer welfare in favor of corporate profits, including the systematic retention of fees from transactions it knew or should have known were fraudulent.

121. The systematic nature of Bitcoin Depot's deceptive scheme is further evidenced by the scale of operations across over 8,400 locations nationwide with standardized inadequate safeguards, uniform marketing representations about safety and security that Bitcoin Depot knew

were false, systematic profit retention from fraudulent transactions across its network, and a pattern of denying relief to scam victims while retaining fees derived from their victimization.

122. As a direct and proximate result of Bitcoin Depot's incurable deceptive acts, Plaintiff suffered actual damages of $7,000 representing the total amount stolen from him through Bitcoin Depot's systematic facilitation of the fraudulent scheme.

123. Bitcoin Depot's systematic deceptive acts were the proximate cause of Plaintiff's losses, as the fraudulent transactions would not have been completed without Bitcoin Depot's systematically inadequate safeguards and intentional failure to detect and prevent obvious scam activity.

124. Bitcoin Depot's deceptive acts were "willful" within the meaning of I.C. § 24-5-0.5-4(a) because Bitcoin Depot's systematic scheme demonstrates conscious disregard for the rights and welfare of vulnerable consumers in favor of corporate profits.

125. Because Bitcoin Depot's deceptive acts were willful, Plaintiff is entitled to enhanced damages under I.C. § 24-5-0.5-4(a).

126. As a senior consumer who suffered harm from Bitcoin Depot's incurable deceptive acts, Plaintiff is entitled to treble damages under I.C. § 24-5-0.5-4(i), which provides enhanced protection for consumers aged 60 and over.

127. The enhanced remedies for senior consumers under I.C. § 24-5-0.5-4(i) are particularly appropriate given that Bitcoin Depot's systematic scheme specifically targeted elderly consumers while knowing they are particularly vulnerable to the type of scams facilitated by Bitcoin Depot's intentionally inadequate systems.

128. This action is timely filed within two years of the occurrence of the deceptive acts as required by I.C. § 24-5-0.5-5(b), as the fraudulent transactions occurred on December 16-17, 2024, and this Complaint is filed in 2025.

COUNT TWO
REPLEVIN
I.C. § 32-35-2-1
(on behalf of the Plaintiff and the Class)

129. Plaintiff incorporates by reference all previous allegations as if fully set forth herein.

130. This action is brought under Indiana Code § 32-35-2-1 for the wrongful taking and unlawful detention of Plaintiff's personal property by Bitcoin Depot.

131. Plaintiff Steve Beckett is the rightful owner of and has superior title to approximately $2,100 in United States currency representing the fees and charges that Bitcoin Depot retained from his $7,000 in deposits made into Bitcoin Depot's ATM on December 16-17, 2024.

132. Bitcoin Depot has no valid right to retain the fees charged on fraudulent transactions because the underlying transactions were induced by fraud and performed under duress, Bitcoin Depot processed transactions that it knew or should have known were fraudulent, and Bitcoin Depot cannot lawfully profit from facilitating criminal fraud against vulnerable consumers.

133. Bitcoin Depot's retention of the fees is unlawful because it received actual notice that the underlying transactions were the product of criminal fraud through Plaintiff's direct contact with Bitcoin Depot reporting the fraudulent nature of the transactions, the police report filed by Plaintiff (Lawrenceburg Police Department Incident # L24-11763) documenting the fraud, and the obvious red flags present during the transactions that provided constructive notice of fraudulent activity.

134. Bitcoin Depot lacks any legal justification or authority to retain fees charged on fraudulent transactions because Bitcoin Depot's terms of service do not authorize retention of fees from transactions it knows are fraudulent, Bitcoin Depot's claims that transactions are "irreversible" are false and misleading as applied to the fees it retained, Bitcoin Depot has the practical ability to return the fees it collected, and no valid contract exists that would authorize Bitcoin Depot to retain proceeds from criminal fraud.

135. Plaintiff made a demand upon Bitcoin Depot for return of the fees it wrongfully retained, but Bitcoin Depot refused to return the fees despite having actual knowledge that they were derived from fraudulent transactions.

136. Bitcoin Depot's possession of the approximately $2,100 in fees is wrongful because Bitcoin Depot is holding these funds contrary to Plaintiff's superior rights and without legal authority to retain proceeds from fraudulent transactions.

137. As a direct result of Bitcoin Depot's wrongful retention of the fees, Plaintiff has suffered damages including loss of approximately $2,100 in funds, emotional distress and anxiety, and economic harm from being deprived of the use of funds that were improperly retained from fraudulent transactions.

COUNT THREE
NEGLIGENCE / GROSS NEGLIGENCE / RECKLESSNESS
(on behalf of the Plaintiff and the Class)

138. Plaintiff incorporates by reference all previous allegations as if fully set forth herein.

139. Defendant Bitcoin Depot owed a duty of reasonable care to Plaintiff and other similarly situated consumers arising from multiple sources:

140. As a commercial operator of financial service kiosks that facilitate cash-to-cryptocurrency transactions, Defendant owed a duty to exercise reasonable care in the design, operation, monitoring, and maintenance of its ATMs to prevent foreseeable harm to users.

141. Defendant's provision of financial services through self-service kiosks created a special relationship with its customers, particularly vulnerable elderly consumers, requiring Defendant to exercise reasonable care to protect them from foreseeable risks associated with cryptocurrency transactions.

142. Defendant voluntarily assumed a heightened duty of care by:

a. Publicly representing that it employs "various measures to protect customers from scams and fraud" and provides "safe and secure Bitcoin ATM services";

b. Publishing educational materials specifically acknowledging the vulnerability of seniors to cryptocurrency scams;

c. Marketing security features and customer protection as competitive advantages;

d. Explicitly undertaking to warn customers about common scam patterns and provide customer support.

143. Defendant's actual knowledge of widespread scam exploitation of its ATM network, as evidenced by its SEC filings, published articles, and consumer complaints, created a duty to implement reasonable safeguards to prevent foreseeable harm to vulnerable users.

144. As one of the largest cryptocurrency ATM operators in North America, Defendant owed a duty to conform its conduct to industry standards and reasonable practices for preventing cryptocurrency fraud, particularly given the well-documented epidemic of Bitcoin ATM scams targeting elderly consumers.

145. The existence and scope of Defendant's duty is established as a matter of law based on the relationship between the parties, Defendant's voluntary undertakings, actual knowledge of risks, and the foreseeability of harm to vulnerable consumers using cryptocurrency ATMs.

146. Defendant breached its duty of reasonable care by failing to conform its conduct to the standard expected of a reasonable cryptocurrency ATM operator under similar circumstances. Specifically, Defendant failed to implement adequate transaction monitoring despite knowing that elderly customers are particularly vulnerable to scams and that large sequential transactions by first-time users are indicative of fraud. Defendant failed to intervene when obvious warning signs of scam activity were present, despite clear indications that Plaintiff was following telephone instructions and exhibiting signs of distress typical of scam victims. Defendant failed to implement effective safeguards, relying solely on ineffective on-screen warnings while refusing to adopt protective measures used by other cryptocurrency operators. Defendant maintained policies and procedures that it admitted "may not be sufficient" to prevent fraud, and refused to investigate or assist in recovery after being notified of the fraudulent nature of Plaintiff's transactions.

147. Plaintiff suffered actual injury in the form of financial losses totaling $7,000, emotional distress, and consequential damages as a direct and proximate result of Defendant's breach of its duty of reasonable care.

148. But for Defendant's breaches of duty, Plaintiff's losses would not have occurred because reasonable transaction monitoring, meaningful intervention during obvious distress, cooling-off periods for large sequential transactions, or adoption of reasonable safeguards used by other operators would have detected and prevented the fraudulent scheme that victimized Plaintiff.

149. Plaintiff's injuries were reasonably foreseeable to Defendant because Defendant acknowledged that seniors are "particularly vulnerable" to cryptocurrency scams, admitted

awareness that its services "may be exploited to facilitate illegal activity such as fraud," was aware of Federal Trade Commission data documenting the epidemic of Bitcoin ATM fraud targeting elderly consumers, and the specific pattern of Plaintiff's victimization matched scam methodologies that Defendant had identified in its educational materials.

150. There were no intervening causes that would break the causal chain between Defendant's negligent conduct and Plaintiff's injuries, as Defendant's failure to implement reasonable safeguards was a proximate cause of Plaintiff's ability to complete the fraudulent transactions despite the underlying fraud being perpetrated by third-party scammers.

151. As a direct and proximate result of Defendant's negligence, Plaintiff suffered actual damages of $7,000 representing the total amount lost through the fraudulent transactions, loss of use of funds needed for living expenses and medical care, emotional distress, anxiety, and mental anguish from the financial exploitation, and incidental damages including time and expense attempting to recover the stolen funds.

152. Defendant's conduct constituted gross negligence and recklessness because Defendant acted with conscious disregard for the safety and financial well-being of its customers despite actual knowledge of substantial risks.

153. Defendant's gross negligence is evidenced by continuing to process transactions from vulnerable populations despite knowing its safeguards were inadequate, admitting in SEC filings that its risk management "may not be sufficient" while refusing to implement reasonable improvements, profiting from transactions it knew or should have known were fraudulent, and prioritizing corporate profits over the protection of vulnerable elderly consumers.

154. Defendant's reckless conduct demonstrates a conscious disregard for the rights and safety of others, warranting enhanced damages and other appropriate relief.

COUNT FOUR
VOLUNTARY ASSUMPTION OF A DUTY

155. Plaintiff incorporates by reference all previous allegations as if fully set forth herein.

156. Defendant Bitcoin Depot voluntarily and gratuitously assumed a duty of care to protect its customers, including Plaintiff, from cryptocurrency scams and fraud through affirmative conduct that created a special relationship and imposed a corresponding duty to act reasonably.

157. Defendant specifically undertook customer protection responsibilities through deliberate actions, not legal mandates, including:

a. Representing that it employs "various measures to protect customers from scams and fraud" and provides "safe and secure Bitcoin ATM services";

b. Creating and publishing extensive educational materials, including a dedicated webpage titled "Protecting Yourself from Bitcoin ATM Scams and Fraud";

c. Implementing scam detection and warning systems by posting "scam warnings on all kiosks" and prompting customers about common scams;

d. Representing that "customer support staff [are] readily available to address questions or concerns about potential transactions";

e. Employing "security measures to protect its Bitcoin ATMs from tampering and other types of fraud";

f. Acknowledging that "seniors are particularly vulnerable" to cryptocurrency scams and publishing targeted educational content for elderly customers.

158. These undertakings were voluntary competitive advantages and marketing features, not mere legal compliance.

159. Defendant's failure to exercise reasonable care in performing its voluntarily assumed duties increased the risk of harm to Plaintiff beyond what would have existed without the undertaking. By creating false marketplace security that made Bitcoin ATMs appear safer than they actually were, Defendant contributed to industry perceptions of meaningful fraud protections while failing to implement adequate safeguards. Defendant implemented demonstrably ineffective warnings that provided justification for processing obviously fraudulent transactions and held itself out as knowledgeable about fraud patterns while failing to utilize such expertise to protect vulnerable customers.

160. Defendant breached its voluntarily assumed duty by failing to exercise reasonable care in performing its specific protective undertakings. Despite undertaking to provide effective scam warnings, Defendant implemented only superficial warnings that it knew were ineffective. Despite representing readily available customer support, Defendant failed to intervene when Plaintiff exhibited obvious signs of distress and fraudulent manipulation. Despite undertaking security measures against fraud, Defendant failed to implement transaction monitoring for obvious patterns like elderly customers making large sequential deposits while following telephone instructions. Despite assuming duties to educate customers about scam patterns, Defendant failed to provide effective education that would have prevented Plaintiff's victimization. Despite acknowledging seniors' particular vulnerability, Defendant failed to implement age-specific protections for elderly customers like Plaintiff.

161. Defendant's breach was systematic, as evidenced by ongoing consumer complaints documenting similar failures with other vulnerable customers.

162. Defendant's breach of its voluntarily assumed protective duties was the proximate cause of Plaintiff's injuries. But for Defendant's breach, Plaintiff's losses would not have occurred,

as reasonable performance of assumed warning, monitoring, and customer support duties would have detected and prevented the fraudulent scheme.

163. The harm suffered by Plaintiff was precisely the foreseeable consequence that Defendant's assumed protective duties were intended to prevent, as evidenced by Defendant's own publications identifying the exact scam pattern that victimized Plaintiff.

164. As a direct and proximate result of Defendant's breach of its voluntarily assumed duties, Plaintiff suffered compensable injuries including actual financial losses of $7,000, loss of use of funds needed for essential expenses, emotional distress from financial exploitation, and incidental damages from attempting to recover stolen funds.

PRAYER FOR RELIEF

WHEREFORE Plaintiff Steve Beckett, on behalf of himself and all others similarly situated, requests judgment in their favor against Defendants Bitcoin Depot, Inc. and Bitcoin Depot Operating, LLC as follows:

A. Certifying this action as a Class Action on behalf of the Class as defined herein, appointing Plaintiff as Class Representative, and appointing Plaintiff's Counsel as counsel for the Class;

B. Awarding Plaintiff and Class members all nominal, statutory, actual, compensatory, consequential, incidental, and enhanced damages, as well as restitution and disgorgement as allowed by law or equity;

C. Awarding Plaintiff and Class members all pre- and post-judgment interest;

D. Awarding Plaintiff and Class members all reasonable attorneys' fees, expenses, and costs; and

E. Granting such other relief as the Court deems just and appropriate.

JURY DEMAND

Plaintiff Steven Beckett respectfully demands a trial by jury on all issues so triable.

Respectfully submitted,

/s/ Brian D. Flick
Brian D. Flick (OH #0081605)
Marita I. Ramirez (OH #0110882) *
**Pro Hac Vice Application Anticipated*
DannLaw
15000 Madison Avenue
Lakewood, OH 44107
Phone: 216-373-0539
Fax: 216-373-0536
notices@dannlaw.com
Attorneys for Plaintiff Steven Beckett and the putative class