Barkley B. Smith, ISBN 9193
Barkley Smith Law, PLLC
999 W Main St., STE 100
Boise, ID 83702
P: 208-481-4812
Email: barkley@barkleysmithlaw.com

Brian D. Flick (OH #0081605)*
Marita I. Ramirez (OH #0110882)*
DannLaw
15000 Madison Avenue
Lakewood, OH 44107
Phone: 216-373-0539
Fax: 216-373-0536
Email: msmith@dannlaw.com
Email: notices@dannlaw.com
**Pro Hac Vice Application Anticipated*

Attorneys for Plaintiffs

UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF IDAHO

KAREN LACEY and ROBERT LACEY, individually and on behalf of all others similarly situated, Plaintiff, v. BITCOIN DEPOT, INC. and BITCOIN DEPOT OPERATING, LLC (D/B/A BITCOIN DEPOT), Defendant.	Case No.: 1:26-cv-288 **CLASS ACTION COMPLAINT** **DEMAND FOR JURY TRIAL**

Plaintiffs Karen Lacey and Robert Lacey, individually and on behalf of all others similarly situated, bring this Class Action Complaint for Damages against Defendants Bitcoin Depot, Inc. and Bitcoin Depot Operating, LLC (d/b/a Bitcoin Depot). Plaintiffs make these allegations with personal knowledge with respect to themselves 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 vulnerable consumers who, when manipulated into states of panic and urgency by fraudsters claiming identity theft or other emergencies, lose thousands of dollars through Bitcoin Depot's machines.

2. Plaintiffs Karen and Robert Lacey were targeted by a sophisticated impersonation scam in which fraudsters, posing as Norton customer service representatives and FBI agents, convinced them that their identities had been used in connection with serious criminal activity, including child pornography and illegal gambling, and that all of their financial accounts were in immediate danger of being compromised. Under this fabricated crisis, Plaintiffs were coerced into withdrawing funds from their accounts and depositing cash at a Bitcoin Depot ATM, with the scammers maintaining constant surveillance and psychological control to prevent Plaintiffs from seeking outside help.

3. Despite obvious red flags—including first-time users making large cash deposits while visibly acting under telephone instructions from unknown parties—Bitcoin Depot's ATM processed each transaction without meaningful intervention, taking its substantial cut before transferring the remainder to the scammer's wallet.

4. Impersonation scams using Bitcoin ATMs have become a nationwide epidemic. Fraudsters routinely impersonate government agencies, tech companies, and law enforcement to convince victims that they must urgently deposit cash into Bitcoin ATMs to resolve fabricated emergencies involving suspicious account activity, identity theft, or money laundering. Federal Trade Commission data shows fraud losses at Bitcoin ATMs increased nearly tenfold from 2020 to 2023, topping $65 million in just the first half of 2024, with a median loss of $10,000 per victim—reflecting how these scams systematically target consumers in moments of panic and distress.[1]

5. 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 articles acknowledging the widespread nature of cryptocurrency scams, describing how fraudsters use "fabricated sense of urgency, tricking you into making hasty decisions" and warning that these scams "play on your best and worst impulses" to target vulnerable consumers across all demographics.[3]

6. Despite this knowledge—and despite publicly claiming to provide "safe and secure" Bitcoin ATM services—Bitcoin Depot prioritizes profits over protection.[4] The company

[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 September 5, 2025).
[2] Bitcoin Depot, Inc., Form 10-Q, United States Securities and Exchange Commission, pp. 63, 67 (Sept. 30, 2023) .
[3] Bitcoin Depot, Common Crypto Scams, https://bitcoindepot.com/bitcoin-atm-info/common-crypto-scams/ (last visited September 5, 2025).
[4] Bitcoin Depot, Protecting Yourself from Bitcoin ATM Scams and Fraud, https://bitcoindepot.com/scam-fraud/ (last visited July 11, 2025).

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]

7. This lawsuit alleges Bitcoin Depot's conduct violates the Idaho Consumer Protection Act, Idaho Code §§ 48-601 through 48-619, through misrepresenting the security of its services and failing to implement adequate safeguards. The complaint also brings claims for Negligence, Voluntary Assumption of Duty for Bitcoin Depot's breach of its self-proclaimed commitment to customer protection, and Unjust Enrichment.

8. Plaintiffs seek injunctive relief requiring effective protective measures, immediate return of wrongfully detained funds, compensatory damages, and attorney fees.

PARTIES

9. Plaintiff Karen Lacey ("Plaintiff Karen Lacey") is a resident of the State of Oregon. Plaintiff Karen Lacey had limited familiarity with cryptocurrency when she and her husband were victimized by scammers using Bitcoin Depot's ATM network. The vulnerability created by the scammers' psychological manipulation—impersonating Norton customer service representatives and FBI agents, fabricating allegations of criminal activity including child pornography and illegal gambling, claiming Plaintiffs' accounts were in imminent danger, and maintaining constant surveillance to prevent Plaintiffs from seeking outside assistance—demonstrates how these schemes exploit victims regardless of their background.

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

10. Plaintiff Robert Lacey ("Plaintiff Robert Lacey") is the husband of Plaintiff Karen Lacey and is a resident of the State of Oregon. Plaintiff Robert Lacey was similarly victimized by the same scam and suffered financial losses as a result of Bitcoin Depot's inadequate safeguards.

11. 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.

12. Defendant Bitcoin Depot Operating, LLC, is a Delaware limited liability company registered to do business in Idaho. 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 Florida.

13. Bitcoin Depot, Inc., and Bitcoin Depot Operating, LLC, are referred to collectively hereinafter as the “Bitcoin Depot.”

JURISDICTION AND VENUE

14. 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.

15. This Court has personal jurisdiction over Bitcoin Depot because it conducts substantial business in Idaho, including: (a) operating and maintaining Bitcoin ATMs throughout Idaho, generating substantial revenue from Idaho residents; (b) maintaining a registered agent in Boise, Idaho; (c) advertising its services to Idaho consumers; and (d) conducting the specific transactions at issue in this lawsuit with Karen and Robert Lacey in Idaho.

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

17. Bitcoin Depot purposefully availed itself of Idaho's market and legal protections by establishing a network of ATMs throughout the state, maintaining a registered agent in Idaho, and conducting business with Idaho consumers, making it subject to Idaho's jurisdiction and consumer protection laws.

18. 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

19. Bitcoin Depot operates one of the largest cryptocurrency kiosk networks in North America, with more than 8,400 Bitcoin ATMs across the United States, Canada, and Puerto Rico — including approximately 60 locations embedded in Idaho communities, reflecting the company's push to bring crypto access to every corner of the country.

20. 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.

21. 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.

22. 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.

23. Bitcoin Depot markets these features—speed, convenience, and anonymity—as advantages while charging substantially higher fees than traditional exchanges.

24. Under Bitcoin Depot's terms of service published in January 2025, the company charged fees up to 50% of the total transaction amount. Bitcoin Depot revised its terms of service

in March 2026, swapping the explicit 50% cap for a $3.00 flat fee and an open-ended markup — one the company warns customers could be 'significantly greater' than competing services.[6]

25. Bitcoin Depot's high-fee, high-volume business model generates substantial revenue from each transaction, and the company's own financial filings reveal just how exposed that model is when regulators intervene. When California legislation capping daily Bitcoin ATM transactions took effect in January 2024, Bitcoin Depot's full-year revenue fell roughly 17%, dropping from $689 million in 2023 to $573.7 million in 2024.[7] The company's earnings report cited that California law directly as a primary driver of the decline. When a new wave of state transaction caps took effect in late 2025, quarterly revenue fell another 15% — from $136.8 million in Q4 2024 to $116 million in Q4 2025.[8] Bitcoin Depot's CEO again pointed to the regulations as the main cause. Looking ahead, the company has warned investors to expect its core business revenue to fall an additional 30% to 40% in 2026 as that regulatory pressure continues to build. *Id*. Taken together, the pattern is difficult to ignore: each time regulators have restricted how much customers can transact at a Bitcoin ATM, Bitcoin Depot's revenue has followed.

26. Because Bitcoin Depot collects its fees the moment a transaction is completed, the legitimacy of that transaction is, financially speaking, irrelevant to the company. A scam victim feeding cash into a Bitcoin Depot kiosk generates the same revenue as any other customer. And while the company does offer a refund process, it is entirely on its own terms: Bitcoin Depot can deny any refund request for any reason, at its sole discretion. Should it choose to grant one, it

[6] https://bitcoindepot.com/terms-and-conditions/ (last visited April 6, 2026)
[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 April 6, 2026).
[8] https://ir.bitcoindepot.com/news-events/press-releases/detail/124/bitcoin-depot-reports-fourth-quarter-and-full-year-2025 (last visited April 6, 2026)

reserves the right to charge the victim an additional fee of up to 10% of the transaction amount — and to keep any market gains on the refunded funds.[9]

B. The Cryptocurrency ATM Scam Epidemic

27. 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.[10] The FTC reported that 2024 was on track to be even worse, with more than $65 million in losses recorded in just the first six months of the year. *Id*.

28. The median reported loss when using cryptocurrency kiosks was $10,000 compared to $447 in general fraud cases—demonstrating that Bitcoin ATM scams result in disproportionately devastating financial losses.[11]

29. 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.[12]

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

---

[9] https://bitcoindepot.com/refund-policy/ (last visited April 6, 2026)
[10] 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).
[11] Fed. Trade Comm'n, Protecting Older Consumers 2023-2024: A Report of the Federal Trade Commission, at 17 (Oct. 18, 2024).
[12] *Id*.

a. Scammers contact victims by telephone, impersonating trusted entities including government agencies (IRS, Social Security Administration, Federal Reserve), technology companies (Microsoft, Apple), financial technology companies (PayPal), 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.

31. 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.

32. 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.[13]

33. The cryptocurrency ATM scam epidemic represents a foreseeable and well-documented threat to consumer welfare, particularly affecting vulnerable elderly populations who

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

are less familiar with cryptocurrency technology and more susceptible to authority-based manipulation tactics.

C. Bitcoin Depot's Actual Knowledge of Scam Exploitation

34. 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.

35. 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."[14]

36. 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."[15]

37. Bitcoin Depot has published extensive content on its own website demonstrating comprehensive knowledge of cryptocurrency scams and their methodologies. In multiple detailed articles, Bitcoin Depot describes the precise tactics scammers use, including how they create 'fabricated sense of urgency, tricking you into making hasty decisions,'[16] how they 'play on your

[14] Bitcoin Depot, Inc., Form 10-Q, United States Securities and Exchange Commission, p. 67 (Sept. 30, 2023).
[15] *Id*. at pp. 63, 67.
[16] Bitcoin Depot, Common Crypto Scams (March 10, 2025), https://bitcoindepot.com/bitcoin-atm-info/common-crypto-scams/ (last visited September 5, 2025).

best and worst impulses,'[17] and how they employ 'imposter scams' where fraudsters 'pose as Bitcoin ATM operators or support personnel.'[18] The company has catalogued eight different types of Bitcoin ATM scams, including 'Federal Agency Scams' where 'scammers pretend to be federal agencies, claiming that the victim has broken certain laws or regulations while using the Bitcoin ATM.'[19] Bitcoin Depot acknowledges that while seniors may be particularly vulnerable to these scams, the psychological manipulation techniques are designed to exploit any consumer placed in a state of distress, regardless of age or background.[20]

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";[21]

[17] *Id.*
[18] Bitcoin Depot,12 Days of Bitcoin #8 - Eight Bitcoin ATM Scams (December 19, 2023), https://bitcoindepot.com/bitcoin-atm-info/12-days-of-bitcoin-8-eight-bitcoin-atm-scams/ (last visited September 8, 2025).
[19] *Id.*
[20] 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 September 8, 2025).
[21] 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;[22]

c. Multiple complaints describing elderly victims depositing tens of thousands of dollars while following telephone instructions from scammers impersonating government agencies and tech support.[23]

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.[24]

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.[25]

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

[22] 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).
[23] 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).
[24] Fed. Trade Comm'n, Protecting Older Consumers 2023-2024: A Report of the Federal Trade Commission, at 17 (Oct. 18, 2024).
[25] 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."[26]

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.[27]

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!"[28]

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

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

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.[30]

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. Moreover, 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 "particularly vulnerable" to cryptocurrency scams. Other cryptocurrency kiosk companies

[29] 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).
[30] Bitcoin Depot, Inc., Form 10-Q, United States Securities and Exchange Commission, pp. 63, 67 (Sept. 30, 2023).

have implemented elderly-specific protections that Bitcoin Depot deliberately chooses not to adopt.[31]

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.

[31] 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 financial abuse targeting vulnerable populations, including elderly adults, individuals with limited English proficiency, those unfamiliar with technology, and people in financial distress; (c) undermining consumer confidence in legitimate cryptocurrency services; and (d) imposing social costs through increased victimization of consumers who may be more susceptible to high-pressure tactics and psychological manipulation.

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."[32]

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.[33]

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."[34]

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.[35]

---

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

61. Bitcoin Depot's assumption of protective duties is particularly significant given the company's actual knowledge that vulnerable populations—including seniors and those experiencing financial distress—comprise a substantial portion of its user base and are susceptible to cryptocurrency scams. By marketing to these vulnerable populations while simultaneously acknowledging through its own publications that consumers can be exploited through psychological manipulation tactics, 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 vulnerable 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.[36]

67. Consumers, including Plaintiff, reasonably relied on Bitcoin Depot's representations about safety and security when they were directed by scammers to use the company's ATMs. Even though victims do not typically choose which specific ATM to visit—as scammers direct them to particular locations—consumers can still reasonably expect that any ATM operator advertising robust security measures would implement basic protections against obvious fraud scenarios.

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 consumers who are the primary targets of cryptocurrency ATM scams.

F. The Specific Harm to Karen Lacey and Robert Lacey

69. Plaintiff Karen Lacey is a resident of the State of Idaho. Plaintiff Karen Lacey had limited familiarity with cryptocurrency technology when she became a victim of the sophisticated fraud scheme that exploits Bitcoin Depot's inadequate safeguards.

70. In or around mid-2025, Plaintiff Karen Lacey received an email indicating that a Norton 360 product had been renewed and charged to her credit card. As a former Norton subscriber who knew she had not renewed her subscription, Plaintiff Karen Lacey recognized the

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

discrepancy and decided to investigate further. Critically, however, she knew better than to click any links contained in an unsolicited and suspicious email. Instead, she independently conducted her own Google search to locate what she thought was a legitimate customer service number for Norton, and called that number to inquire about the alleged charge.

71. When Plaintiff Karen Lacey's call was answered, the individual on the other end identified themselves as a Norton customer service representative and informed her that she would need to be transferred to the fraud department. Once transferred, a second individual told her the matter was connected to cybercrime and that she would need to be connected with the FBI.

72. The call was then transferred to a purported FBI agent, who told Plaintiff Karen Lacey and her husband, Plaintiff Robert Lacey, that their accounts had been hacked and used to purchase child pornography and facilitate illegal gambling. The agent warned them that their accounts were now compromised and that they needed to withdraw their funds immediately to protect their savings.

73. To further the deception, the purported FBI agent directed Plaintiffs to a .gov website where they were shown what appeared to be official government documents implicating them in these crimes. The agent then warned Plaintiffs that an active investigation was underway and that they were not to tell anyone — not family, not friends, no one. Doing so, they were told, would jeopardize the investigation and cause the FBI to abandon their case entirely. To ensure compliance, the agent claimed that Plaintiffs were being actively watched and monitored.

74. Plaintiffs were not without skepticism. Before a single dollar was deposited, Plaintiff Robert Lacey told his wife he intended to call the FBI directly to verify that what they were being told was real. But before he could act on it, the voice on the phone told Plaintiff Karen Lacey to instruct her husband to get back in the car. The scammers knew what he was about to do.

They were being watched. The scammers' apparent awareness of Mr. Lacey's movements in real time was so disorienting and so frightening that it didn't read as a manipulation tactic; it read as proof that everything they had been told was true. Whatever instinct toward caution Plaintiffs had carried into that moment was overwhelmed by fear, and they did what they believed they had to do.

75. The scammers reinforced that illusion at every turn. At some point during the ordeal, Plaintiffs noticed that wireless networks labeled 'FBI' had appeared among the available connections on their phones. To Plaintiffs, this was visible confirmation that federal agents were indeed monitoring their every move. These networks were not a fleeting anomaly. They remained visible on Plaintiffs' devices for months after the deposits were made, sometimes disappearing over weekends before reappearing again, as late as February 2026.

76. Under continuing psychological duress and believing they were protecting their finances from a genuine criminal threat, Plaintiffs did not make a single panicked withdrawal — they endured days of sustained manipulation, each day returning to a Bitcoin Depot ATM as instructed. On August 9, they deposited $25,000. On August 11, another $25,000. On August 13, they made two separate deposits of $13,000 each — $26,000 in a single day. In total, Plaintiffs deposited $76,000 into Bitcoin Depot ATMs over the course of five days, each transaction executed under the same crushing psychological duress, and each one processed by Bitcoin Depot without meaningful intervention. The pattern was unmistakable: first-time users, large deposits, multiple days in a row, visibly acting under telephone direction at the machine. At each step, Bitcoin Depot's ATMs collected their fees and transferred the remainder to the scammer's wallet address without pause.

77. The fraud's damage extended far beyond the financial. For months, Plaintiffs told no one what had happened, not out of indifference, but out of shame and fear. It wasn't until December 2025, when Plaintiff Karen Lacey visited her son, that she finally disclosed what she and her husband had endured. By that point, Plaintiffs had come to realize they had been scammed — they had never received any instructions to retrieve the funds they believed they were depositing for safekeeping — but they had felt too ashamed, and honestly still too frightened, to do anything about it

78. Her son moved quickly. He retained an attorney, contacted Bitcoin Depot to notify them of the fraud, and filed an IC3 complaint with the FBI. Following that intervention, Bitcoin Depot issued Plaintiff Karen Lacey two refund checks, each in the amount of $1,000.00, characterized as 'Customer Refunds.' The gesture was as inadequate as it was telling: the two checks combined did not even cover the fees Bitcoin Depot had collected from Plaintiffs' transactions. Of the $76,000 Plaintiffs lost, Bitcoin Depot's response was to return $2,000.

79. Plaintiffs' experience represents a textbook case of Bitcoin Depot's systemic failures: Vulnerable customers acting under extreme psychological distress. Unmistakable signs of telephone manipulation playing out in real time at the machine. Large cash deposits directed to a third-party wallet. The same customers returning day after day. Every meaningful red flag was present, and none of them triggered any intervention.

80. The consequences for Plaintiffs were devastating and life-altering. Plaintiff Karen Lacey was retired when the fraud occurred. She is no longer retired. The $76,000 she and her husband lost represented their entire savings, and when it was gone, so was the retirement she had earned. She was forced back into the workforce and now works rotating day/night shifts at a hospital which has taken a physical and emotional toll on her at this stage in her life. Beyond the

financial ruin and the exhausting grind of starting over, Plaintiffs spent months living in fear and shame before they could bring themselves to tell anyone what had happened. That silence, and the suffering behind it, is part of what Bitcoin Depot's indifference cost them.

81. None of it needed to happen. Transaction limits for first-time users, mandatory verification for large deposits, or basic customer service intervention when obvious red flags presented themselves — any one of these reasonable safeguards could have stopped this fraud before it started. Bitcoin Depot simply lacked the will to implement them.

G. Bitcoin Depot's Retention of Stolen Funds

82. 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.

83. 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.

84. 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.

85. 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.

86. 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.

87. 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.

88. 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.[37]

89. 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.

90. 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.

[37] 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).

91. 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.

92. 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.

93. 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.

94. 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

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

96. 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 Idaho 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.

97. As used in the class definition:

a. "Class Period" means the period beginning six (6) years prior to the filing of this Complaint through the date a class certification order is entered;

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

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: 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.

98. 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.

99. **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 topped $65 million in just the first six months of 2024 alone — and that Bitcoin Depot operates approximately 60 ATMs throughout Idaho as one of the largest operators in North America, the Class likely includes hundreds of impersonation scam victims in Idaho alone. The widespread and well-documented nature of these scams, Bitcoin Depot's Idaho ATM network, and the company's own admissions about the 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 Plaintiffs. Joinder of all Class members would be impracticable due to the number of potential members, their geographic dispersion throughout Idaho, and the likelihood that many victims, like Plaintiffs themselves, may be unaware of their legal rights or too ashamed and frightened to pursue individual legal action.

100. **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 unfair or deceptive acts under the Idaho Consumer Protection Act, Idaho Code §§ 48-601 through 48-619;

b. Whether Bitcoin Depot failed to implement reasonable measures to detect and prevent cryptocurrency ATM scams despite actual knowledge of their prevalence and the specific tactics used against its customers;

c. Whether Bitcoin Depot's representations that it provided "safe and secure" Bitcoin ATM services and employed "various measures to protect customers from scams and fraud" were false or misleading;

d. Whether Bitcoin Depot voluntarily assumed a duty to protect customers from scams and breached that duty by failing to deliver the protections it publicly promised;

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

f. Whether Bitcoin Depot wrongfully retains cash deposited by scam victims after receiving notice of the fraudulent nature of the transactions; and

g. The appropriateness of injunctive relief requiring Bitcoin Depot to implement effective protective measures, including transaction limits for first-time users, mandatory verification for large deposits, and real-time customer service intervention for transactions exhibiting obvious fraud indicators.

101. **Typicality** (Rule 23(a)(3)): Plaintiffs' claims are typical of the claims of other Class members. Like other Class members, Plaintiffs: (a) were victimized by an impersonation scam in which criminals posing as trusted entities — specifically Norton customer service representatives and FBI agents — coerced them into depositing cash into Bitcoin Depot ATMs; (b) deposited cash into Bitcoin Depot ATMs located in Idaho as a direct result of that scam; (c) exhibited obvious red flags that provided Bitcoin Depot with constructive notice of the fraudulent nature of their transactions, including first-time use, large deposits made over multiple consecutive days, and visible telephone direction at the machine; (d) suffered substantial financial losses when Bitcoin Depot processed those transactions without meaningful intervention; (e) reported the fraud to law enforcement and directly notified Bitcoin Depot, providing actual notice; and (f) received only token, inadequate relief from Bitcoin Depot despite that notice. Plaintiffs' claims arise from the

same course of conduct, the same legal theories, and the same systemic failures that affect all Class members victimized through Bitcoin Depot's ATM network.

102. **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.

103. 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.

104. 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 the amount of individual damages will vary, the core legal and factual issues — Bitcoin Depot's knowledge of scam exploitation, the adequacy of its safeguards, the deceptiveness of its representations, and its liability for the systemic failures documented throughout this Complaint — are common to all Class members and capable of resolution on a class-wide basis.

b. Superiority: A class action is superior to other available methods for the fair and efficient adjudication of this controversy. Relevant considerations include:

i. Individual control: Class members have minimal interest in individually controlling separate actions. Individual claims, while devastating to each victim, are likely modest relative to the cost of individual litigation. Many Class members are elderly Idaho residents who lack the resources, sophistication, or awareness to pursue claims on their own, as Plaintiffs' own experience illustrates. The primary objective of this litigation is systemic reform that benefits all Idaho consumers, not merely individual recovery.

ii. Existing litigation: Plaintiffs are not aware of any other litigation concerning the same controversy that has been commenced by or against other Class members in Idaho.

iii. Concentration of litigation: It is desirable to concentrate this litigation in this Court. The harmful conduct at issue occurred in Idaho, Plaintiffs are Idaho residents, Bitcoin Depot operates ATMs throughout Idaho and maintains a registered agent in Boise, and Idaho has a compelling interest in protecting its residents, particularly its elderly residents, from deceptive practices and financial exploitation through consumer protection laws specifically designed for that purpose.

iv. Manageability: This case presents no unusual management difficulties. The Class is readily identifiable through Bitcoin Depot's own transaction records and complaint history. The claims arise from a common course of conduct

and uniform business practices. The legal theories are straightforward applications of established Idaho consumer protection, negligence, and equity principles.

105. 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 injunctive relief under Rule 23(b)(2) and monetary damages under Rule 23(b)(3).

CAUSES OF ACTION

COUNT ONE
VIOLATION OF THE IDAHO CONSUMER PROTECTION ACT
Idaho Code §§ 48-601 through 48-619
(on behalf of the Plaintiff and the Class)

106. Plaintiffs incorporate by reference all previous allegations as if fully set forth herein.

107. The Idaho Consumer Protection Act ("ICPA") prohibits unfair methods of competition and unfair or deceptive acts or practices in the conduct of trade or commerce within the State of Idaho, including any act or practice that is misleading, false, or deceptive to consumers. Idaho Code §§ 48-618, 48-603(17). The Idaho Rules of Consumer Protection further define such conduct, providing that a seller violates the ICPA when it makes a promise "with the capacity or tendency to mislead a consumer acting reasonably under the circumstances." IDAPA 04.02.01.030.

108. At all relevant times, Bitcoin Depot was engaged in "trade" or "commerce" within the meaning of the ICPA by operating Bitcoin ATM kiosks throughout the State of Idaho, offering cryptocurrency conversion services to Idaho consumers, and collecting substantial fees from those transactions. Plaintiffs purchased those services by depositing cash into Bitcoin Depot's ATMs in exchange for Bitcoin, paying substantial transaction fees in the process.

109. Bitcoin Depot's unfair and deceptive acts and practices in violation of the ICPA include, but are not limited to:

a. representing to consumers — through its website and marketing materials — that its Bitcoin ATM services were "safe and secure" and that Bitcoin Depot employs "various measures to protect customers from scams and fraud," when Bitcoin Depot knew, or in the exercise of due care should have known, that its ATMs were regularly exploited by scammers and its safeguards were demonstrably inadequate, in violation of Idaho Code § 48-603(17) and IDAPA 04.02.01.030;

b. making representations regarding customer safety and security that are directly contradicted by Bitcoin Depot's own SEC filings, in which the company admits its services "may be exploited to facilitate illegal activity such as fraud" and that its "risk management policies may not be sufficient," in violation of IDAPA 04.02.01.032;

c. misrepresenting the irreversibility of Bitcoin transactions by characterizing them as "irreversible" while simultaneously retaining substantial cash fees that are entirely reversible through straightforward refund procedures; and

d. continuing to process and profit from transactions exhibiting obvious indicators of fraud, including large cash deposits by first-time users acting visibly under telephone direction, without meaningful intervention, despite actual knowledge that its ATMs were routinely used as instruments of fraud targeting vulnerable consumers.

110. Bitcoin Depot's deceptive and unfair conduct directly and proximately caused Plaintiffs' losses. Plaintiffs deposited funds, and paid substantial transaction fees, based on Bitcoin

Depot's misleading representations about the safety and security of its services and its failure to implement the protections it promised. The funds deposited by Plaintiffs constitute an ascertainable loss of money that is concrete, discoverable, and readily capable of being established.

111. Bitcoin Depot's violations are not isolated lapses. They are repeated and flagrant. Bitcoin Depot has actual knowledge, drawn from its own SEC filings, consumer complaints, government reports, and the content of its own website, that its ATMs are routinely exploited to defraud vulnerable consumers. Despite that knowledge, it has deliberately failed to implement adequate safeguards while continuing to collect fees from the very transactions its inaction enables.

112. As a result of Bitcoin Depot's violations of the ICPA, Plaintiffs are entitled to actual damages, restitution, injunctive relief, punitive damages, attorney's fees pursuant to Idaho Code § 48-608(5), costs, and such other relief as the Court deems just and appropriate.

COUNT TWO
NEGLIGENCE
(on behalf of the Plaintiff and the Class)

113. Plaintiffs incorporate by reference all previous allegations as if fully set forth herein.

114. At all relevant times, Bitcoin Depot operated a network of Bitcoin ATM kiosks accessible to the general public, including vulnerable consumers such as Plaintiffs, at locations throughout the State of Idaho. By placing and operating these kiosks in public locations and inviting consumers to use them for substantial financial transactions, Bitcoin Depot owed a legal duty to exercise reasonable care in the design, operation, and monitoring of its ATMs to prevent foreseeable harm to its users.

115. Bitcoin Depot had actual knowledge, drawn from its own SEC filings, consumer complaints, FTC data, and the content of its own published website, that its ATMs were routinely

exploited by scammers targeting vulnerable consumers. Bitcoin Depot's own website catalogued the precise scam pattern used against Plaintiffs, including "Federal Agency Scams" in which scammers impersonate government officials to coerce victims into depositing cash at Bitcoin ATMs. Bitcoin Depot's own SEC filings acknowledge that its services "may be exploited to facilitate illegal activity such as fraud" and that its "risk management policies may not be sufficient." The harm suffered by Plaintiffs was not merely foreseeable, it was, by Bitcoin Depot's own account, a known and recurring risk.

116. The foreseeability of harm to Plaintiffs was exceptionally high. Bitcoin Depot knew that elderly and vulnerable consumers were being targeted through its machines with increasing frequency. Bitcoin Depot knew that impersonation scams were among the most common tactics used against its customers. And Bitcoin Depot knew that its existing safeguards were inadequate to address that risk. That knowledge gave rise to a legal duty to act.

117. The burden of implementing reasonable protective measures was minimal. Transaction limits for first-time users, mandatory verification for large or unusual deposits, holding periods for suspicious transactions, and real-time customer service intervention for obvious red flag patterns are technologically feasible measures already implemented by other operators in the same industry. The cost of these measures is trivial compared to the financial devastation their absence enables.

118. Bitcoin Depot breached its duty of care. Despite actual knowledge that its ATMs were routinely used as instruments of fraud against vulnerable consumers, Bitcoin Depot failed to implement reasonable and effective safeguards to prevent that foreseeable harm. Specifically, Bitcoin Depot failed to:

a. implement transaction limits for new or first-time users;

b. require meaningful identity verification or additional authentication for large or unusual transactions;

c. institute holding periods or review protocols for suspicious transactions;

d. employ effective real-time transaction monitoring or fraud detection systems capable of identifying obvious patterns of fraudulent activity; and

e. provide meaningful customer service intervention when customers exhibited obvious signs of distress or fraudulent manipulation at its machines.

119. In place of these measures, Bitcoin Depot relied solely on passive on-screen warnings that it knew, or should have known, were wholly ineffective in the context of impersonation scams. Its own published materials acknowledged that victims of these scams act under extreme psychological duress and are unable to recognize or respond to generic warnings. Relying on those warnings as its primary safeguard, while declining to implement measures that would have actually worked, constitutes a clear breach of Bitcoin Depot's duty of reasonable care.

120. That breach is further evidenced by what happened to Plaintiffs specifically. Between August 9 and August 13, 2025, Plaintiffs — first-time users — made four separate large cash deposits into Bitcoin Depot ATMs over the course of five days, each time visibly acting under telephone direction. The deposits totaled $76,000. Not one of those transactions triggered any intervention by Bitcoin Depot. Each was processed without pause, with Bitcoin Depot collecting its fees before transferring the remainder to the scammer's wallet address.

121. Bitcoin Depot's breach was the direct and proximate cause of Plaintiffs' losses. Without Bitcoin Depot's ATMs processing the transactions, Plaintiffs' funds could not have been converted from cash to cryptocurrency and transferred to the scammer's wallet in the manner they

were. Bitcoin Depot's failure to implement reasonable safeguards was a substantial factor in enabling the fraud to succeed.

122. Had Bitcoin Depot adopted any of the reasonable protective measures described above, transaction limits, verification requirements, a hold on suspicious transactions, or customer service intervention, the fraud would have been detected and Plaintiffs' losses would have been prevented or significantly mitigated. A first-time customer making five large cash deposits over five consecutive days while visibly on the phone is not an ambiguous situation. It is precisely the pattern that Bitcoin Depot's own published materials identified as a hallmark of fraud. Reasonable safeguards would have caught it.

123. Bitcoin Depot cannot claim that Plaintiffs' losses were unforeseeable or unusual. Plaintiffs' experience is the most predictable and well-documented category of harm arising from Bitcoin Depot's failure to act — the exact scam pattern Bitcoin Depot described in its own publications, targeting exactly the population of consumers Bitcoin Depot acknowledged was most at risk. The causal chain is direct and unbroken.

124. As a direct and proximate result of Bitcoin Depot's negligence, Plaintiffs suffered actual damages including the total loss of $76,000 in savings, the substantial transaction fees and markups retained by Bitcoin Depot from each fraudulent transaction, severe emotional distress, the loss of Plaintiff Karen Lacey's retirement, and the ongoing practical consequences of losing funds needed for essential living expenses. These damages are concrete, documented, and directly caused by Bitcoin Depot's failure to exercise the reasonable care it owed.

COUNT THREE
VOLUNTARY ASSUMPTION OF A DUTY
(on behalf of the Plaintiff and the Class)

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

126. Under Idaho law, when a person voluntarily undertakes to assist or protect another, they are required to exercise reasonable care in doing so. Bitcoin Depot did not merely acknowledge the risk of fraud in passing, it affirmatively and repeatedly held itself out as a protector of its customers against that very risk, making specific, concrete commitments that went well beyond legal compliance and that it used as deliberate competitive advantages in the marketplace.

127. Those commitments included:

a. representing on its website and in marketing materials that Bitcoin Depot employs "various measures to protect customers from scams and fraud" and provides "safe and secure Bitcoin ATM services";

b. creating and publishing extensive educational content, including dedicated webpages titled "Common Crypto Scams" and "12 Days of Bitcoin #8 - Eight Bitcoin ATM Scams," specifically designed to warn consumers about the fraud tactics its ATMs were being used to facilitate;

c. implementing scam detection and warning systems, including posting "scam warnings on all kiosks" and prompting customers about common scams at the point of transaction;

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"; and

f. acknowledging that vulnerable consumers are susceptible to cryptocurrency scams and publishing targeted educational content about specific scam tactics — including "Federal Agency Scams" involving impersonation of government officials, the precise tactic used against Plaintiffs.

128. Each of these undertakings constitutes an affirmative act taken with the intent of protecting consumers from fraud. Together, they created a duty — voluntarily assumed — that required Bitcoin Depot to exercise reasonable care in actually delivering the protections it promised.

129. Bitcoin Depot failed to exercise that care. The warnings it posted were superficial and demonstrably ineffective. The customer support it advertised as readily available did not intervene when Plaintiffs exhibited obvious signs of distress and fraudulent manipulation at its machines. The security measures it promoted did not include basic transaction monitoring capable of detecting the patterns playing out in plain sight, the same patterns Bitcoin Depot's own published materials identified and described.

130. The consequences of that failure were precisely what Bitcoin Depot's own assumed duties were designed to prevent. By holding itself out as a company that actively protected consumers from fraud, Bitcoin Depot created a false sense of marketplace security, making its ATMs appear safer than they were and contributing to the conditions under which Plaintiffs, and others like them, were victimized. Plaintiffs reasonably relied on Bitcoin Depot's representations that its services were safe and that protections were in place. That reliance worsened their position: they used Bitcoin Depot's ATMs believing the safeguards advertised were real, when in fact those safeguards were hollow.

131. Bitcoin Depot's breach was not an isolated failure. It is systematic, as evidenced by a consistent pattern of consumer complaints documenting the same failures with the same categories of vulnerable customers.

132. As a direct and proximate result of Bitcoin Depot's breach of its voluntarily assumed duties, Plaintiffs suffered actual financial losses representing the entirety of their savings, loss of use of funds needed for essential living expenses, severe emotional distress, and the incidental costs of attempting to recover what was taken from them. But for Bitcoin Depot's breach, reasonable performance of the warning, monitoring, and customer support duties it voluntarily assumed would have detected and prevented the fraud before a single dollar was lost.

COUNT FOUR
UNJUST ENRICHMENT
(on behalf of the Plaintiff and the Class)

133. Plaintiffs incorporate by reference all previous allegations as if fully set forth herein.

134. Between August 9 and August 13, 2025, Plaintiffs personally deposited $76,000 in cash directly into Bitcoin Depot's ATM kiosks. Bitcoin Depot retained a substantial portion of those funds as transaction fees and markups — money that never reached the scammer's wallet but went directly into Bitcoin Depot's own accounts. The benefit was conferred directly, personally, and without any intermediary: Plaintiffs placed cash into Bitcoin Depot's machines, and Bitcoin Depot kept a portion of it.

135. Bitcoin Depot had actual knowledge of the benefit it received. Bitcoin Depot's entire business model is built on collecting transaction fees and markups from users of its ATMs, and its own records reflect the receipt and retention of the specific funds Plaintiffs deposited. Bitcoin Depot knew that Plaintiffs' cash was used to purchase Bitcoin at a significant markup, and

that a substantial, calculable portion of those funds was retained by Bitcoin Depot as profit. The amounts retained are not speculative — they are ascertainable from Bitcoin Depot's own transaction records and capable of precise mathematical computation.

136. Bitcoin Depot voluntarily accepted and retained the fees and markups from Plaintiffs' transactions. After being notified that those transactions were the product of a sophisticated fraud scheme and that Plaintiffs were victims, Bitcoin Depot did not return what it had taken. It issued two checks of $1,000 each — a total of $2,000 against $76,000 in losses, and an amount that did not even cover the fees Bitcoin Depot collected from Plaintiffs' deposits. The rest it kept.

137. That retention is inequitable under any fair assessment of the circumstances. Bitcoin Depot had actual and constructive knowledge, drawn from its own SEC filings, consumer complaints, regulatory warnings, and published website content, that its ATMs were routinely used as instruments of fraud targeting vulnerable consumers. Bitcoin Depot published guides on its own website describing the precise scam pattern used against Plaintiffs, including impersonation of federal law enforcement agents. It knew this was happening. It chose to address it with on-screen warnings it knew were ineffective, while continuing to process and profit from every transaction, fraudulent or not.

138. Retaining the fees collected from Plaintiffs under these circumstances, after actual notice of the fraud, after receiving police reports and federal crime complaints from Plaintiffs, and after issuing a token refund that did not come close to making Plaintiffs whole, is exactly the kind of conduct that unjust enrichment is designed to remedy. It would be inequitable to allow Bitcoin Depot to keep what it took from Plaintiffs under these conditions. The measure of Bitcoin Depot's

unjust enrichment is the full amount of fees and markups it retained from Plaintiffs' transactions — sums that are liquidated, documented, and have not been returned.

139. Bitcoin Depot's routine operating expenses would have been incurred regardless of whether Plaintiffs deposited a single dollar into its machines. There is no causal relationship between the fees Bitcoin Depot retained from Plaintiffs' fraudulent transactions and any particular expenditure, and accordingly Bitcoin Depot has no basis to offset its unjust enrichment against its general costs of doing business.

140. As a direct result of Bitcoin Depot's unjust enrichment, Plaintiffs suffered actual damages including the loss of their deposited funds and the deprivation of the use and benefit of their property. Plaintiffs are also entitled to prejudgment interest on the amounts wrongfully retained by Bitcoin Depot. The funds Bitcoin Depot collected from Plaintiffs' transactions are liquidated and capable of mathematical computation from Bitcoin Depot's own records. Bitcoin Depot has retained those funds beyond any reasonable time and without Plaintiffs' consent, and full compensation requires that prejudgment interest be awarded to make Plaintiffs whole.

PRAYER FOR RELIEF

WHEREFORE Plaintiffs Karen Lacey and Robert Lacey, individually and on behalf of all others similarly situated, respectfully request that the Court enter judgment in their favor against Defendants Bitcoin Depot, Inc. and Bitcoin Depot Operating, LLC, and grant the following relief:

A. Certifying this action as a class action on behalf of the Class as defined herein, appointing Plaintiffs as Class Representatives, and appointing Plaintiffs' Counsel as counsel for the Class;

B. Awarding Plaintiffs and Class members actual, compensatory, consequential, and incidental damages for all losses suffered as a result of Bitcoin Depot's conduct, including the return of all funds wrongfully retained by Bitcoin Depot;

C. Awarding restitution and disgorgement of all fees, markups, and other benefits Bitcoin Depot unjustly retained from fraudulent transactions processed through its ATM network;

D. Granting injunctive relief requiring Bitcoin Depot to implement effective protective measures to detect and prevent cryptocurrency ATM scams, including transaction limits for first-time users, mandatory verification for large deposits, real-time transaction monitoring, and meaningful customer service intervention for transactions exhibiting obvious fraud indicators;

E. Awarding punitive damages for Bitcoin Depot's repeated and flagrant violations of the Idaho Consumer Protection Act;

F. Awarding prejudgment and post-judgment interest on all amounts wrongfully retained;

G. Awarding Plaintiffs and Class members their reasonable attorney's fees, litigation expenses, and costs pursuant to Idaho Code § 48-608(5) and any other applicable provision; and

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

Respectfully submitted,

/s/ *Barkley Smith*
Barkley B. Smith
Attorney for Plaintiff