UNITED STATES DISTRICT COURT
DISTRICT OF MASSACHUSETTS

JOSHUA MCCOLLUM, OAKFORD CRAWSON LLC, JEFFREY MAGOVENY, NG BOON MIN, LIM TECK YEOW, ALEXEJ KRAVETSKER, and MICHAEL MEDOVOJ on behalf of themselves and all others similarly situated,

Plaintiffs,

v.

CIRCLE INTERNET GROUP, INC., and CIRCLE INTERNET FINANCIAL, LLC,

Defendants.

Case No. 1:26-cv-11733

AMENDED CLASS ACTION COMPLAINT

Jury Trial Demanded

Plaintiffs Joshua McCollum, Oakford Crawson LLC, Jeffrey Magoveny, Ng Boon Min, Lim Teck Yeow, Alexej Kravetsker, and Michael Medovoj, on behalf of themselves and all others similarly situated, allege the following against Defendants Circle Internet Group, Inc., a Delaware Corporation, and Circle Internet Financial, LLC, a Delaware limited liability company (collectively "Circle").

INTRODUCTION

1. On April 1, 2026, unidentified bad actors (hereinafter "Attackers") drained hundreds of millions of dollars in cryptocurrency assets from Drift Protocol, a decentralized perpetuals exchange on the Solana blockchain.

2. At the time, the attack was the largest cryptocurrency exploit of 2026, and the second largest in Solana's history. It is widely believed to have been orchestrated and executed by groups linked to the Democratic People's Republic of Korea ("North

Korea").

3. In just 12 minutes, the Attackers seized control of Drift's asset transfer mechanisms and stole an estimated $280 million in various crypto assets.

4. Though the taking was swift, the getaway was not. The Attackers' exit plan involved transferring the stolen assets to the Ethereum blockchain, and ultimately into the Ether crypto token. Once in Ether, the Attackers could more effectively mask the identity of the assets through various third-party applications. This offloading process, which relied on Circle's stablecoin USDC and its blockchain bridge CCTP, took approximately eight hours.

5. But within just one hour, the Internet took notice of the heist. Posting on X.com, major crypto commentators and actors rang alarm bells and called out Circle by name to intervene. Drift warned its users of the massive exploit and froze all transactions on its Protocol, stating: "This is not an April Fools' joke." And multiple, smaller crypto players froze some of the stolen assets and shut down bridging capabilities, so the assets might be recovered.

6. Circle, however, knowingly gave the Attackers use of its technology and services for several hours, despite its ability to freeze the assets and stop the exodus into Ether.

7. Two weeks later, Circle CEO Jeremy Allaire defended its decision to provide its bridging service to Attackers. He argued that asking a private company like Circle to cut off services to criminals would present a "moral quandary" and suggested that victims should instead obtain court orders to stop illicit transfers.

8. By law, however, Circle was not free to look the other way while knowing it was enabling this misappropriation. Even though Circle saw what was happening and could have easily protected investors, its chosen course of action benefited the Attackers — and itself. Drift depositors have lost hundreds of millions of dollars, which they are unlikely to recover unless Circle is held accountable for its, at best, reckless indifference to the exploit enabled by its technology and services.

9. Plaintiffs are among the many investors harmed by Circle's conduct. Through this lawsuit, Plaintiffs seek to hold Circle responsible. They bring this suit on behalf of themselves and all other similarly situated investors and seek full recovery of their losses and all other relief provided for by law or equity.

PARTIES

Plaintiffs

10. Plaintiff Joshua McCollum is a citizen and resident of Missouri.

11. Oakford Crawson LLC is a limited liability company formed in Arizona, with its principal place of business in Arizona.

12. Jeffrey Magoveny is a citizen and resident of Connecticut.

13. Ng Boon Min is a citizen and resident of Singapore.

14. Lim Teck Yeow is a citizen and resident of Singapore.

15. Alexej Kravetsker is a citizen and resident of Germany.

16. Michael Medovoj is a citizen and resident of Germany.

Defendants

17. Defendant Circle Internet Group, Inc. is a publicly traded Delaware

Corporation with its principal place of business in New York, New York.

18. Defendant Circle Internet Financial, LLC, is a limited liability company formed in Delaware, with its principal place of business in Boston, Massachusetts. Circle Internet Financial's sole member is Circle Internet Holdings, Inc., a wholly owned subsidiary of Circle Internet Group, Inc.

JURISDICTION AND VENUE

19. This Court has jurisdiction over this action pursuant to the Class Action Fairness Act of 2005 (codified at 28 U.S.C. § 1332(d)(2)). At least one member of the proposed class is a citizen of a different state than Defendants, there are more than one hundred members of the proposed class, and the aggregate amount in controversy exceeds five million dollars ($5,000,000.00), exclusive of interest and costs.

20. This Court has specific personal jurisdiction over Defendants because Plaintiffs' claims arise out of and relate to Defendants' unlawful conduct in Massachusetts. Specifically, upon information and belief, Circle's actions and decision-making giving rise to liability took place at the Boston headquarters of Circle Internet Financial.

21. Venue is proper in this District under 28 U.S.C. § 1391(b) because Defendants' unlawful course of conduct occurred in large part in this District.

BACKGROUND

22. Cryptocurrencies are forms of digital assets that exist on a blockchain. Individual cryptocurrencies, like Bitcoin or Ether, are called "tokens." These tokens are held in, and transferred between, digital "wallets" with individualized addresses.

Cryptocurrency (or "crypto") can be traded, used to make purchases, loaned, or simply held as an investment.

23. A blockchain is a digital ledger that records transactions across a network of computers rather than through a single bank, company, or government. Transactions are verified by participants located throughout the world and then added to the ledger. Because no single central authority maintains the ledger, blockchain networks are often described as decentralized. It functions like a shared ledger that is maintained and verified by many computers around the world rather than a single, central authority.

24. A stablecoin is a type of cryptocurrency that is designed to maintain a steady value, unlike cryptocurrencies like Bitcoin or XRP that can swing wildly in value. Stablecoins are considered "real world asset" tokens because they represent some off-chain asset, such as a U.S. dollar, treasury bill, or other traditional asset. Circle's stablecoin USDC, for example, is pegged to the U.S. dollar, and each USDC is backed by $1 in actual reserves.

25. Traditional cryptocurrency assets, by contrast, are not backed by specific off-chain assets. Their values are instead derived from factors such as the technical capabilities of the relevant blockchain, the number of users on the network, the amount of value stored on or transferred through the network, and the businesses, developers, and applications built on top of it.

26. Solana is a high-speed blockchain designed for very fast, low-cost transactions using a more centralized architecture. Many Solana-based tokens are created with built-in "freeze authority" functions under the network's token standard,

allowing issuers to freeze wallets or tokens if they retain that authority.

27. Ethereum is a more decentralized and widely adopted blockchain. Its native asset, Ether, is the underlying currency of the network itself — not a token issued under a separate "smart contract" — and therefore cannot be frozen or blacklisted by a private issuer, unlike some independently created tokens on Solana or Ethereum that include administrative control functions in their code.

28. A crypto "bridge" is a system that allows digital assets to move between different blockchains — such as between Solana and Ethereum — by locking, transferring, minting, or otherwise representing assets across networks. Bridges are often used because most blockchains cannot natively communicate with one another.

STATEMENT OF FACTS

Circle's Business and Services

29. Circle is a cryptocurrency business that bills itself as a "full-stack platform for the new internet financial system."[1] Circle's platform "combines blockchain infrastructure, digital assets, [and] applications into a single, integrated foundation for modern finance" that allows users to "[m]ove money around the world any time, near instantly."[2] Circle touts the fast and seamless nature of its products, advertising the technology as: "Borderless by design. Near-instant by default."[3]

30. Central to Circle's capabilities is its flagship crypto product USDC, the most widely adopted stablecoin in the United States. USDC's stability and wide

[1] https://bit.ly/3PUjtF1
[2] *Id.*
[3] https://bit.ly/41vxtaQ

adoption permit users to move in and out of crypto positions quickly without having to convert assets to "bank" money.

31. Another of Circle's core features is its Cross-Chain Transfer Protocol (CCTP), a bridge for moving USDC between blockchains. Bridging through CCTP is not a passive process. If a user wants to move USDC from the Solana blockchain to the Ethereum blockchain vita CCTP, Circle must "burn" each Solana-based USDC and mint a new Ethereum-based USDC.

32. In addition, unlike decentralized validators or smart contracts, Circle's CCTP system requires an affirmative, centralized attestation before the newly minted USDC can be released onto a destination chain. Without this attestation, which Circle generates through its "Iris" system, the transfer will fail before the bridging is finalized.[4]

33. Because the resulting, bridged token is native USDC that is issued by Circle and subject to its control, the CCTP strengthens USDC as a crypto infrastructure and locks developers into Circle's ecosystem. This bolsters USDC's market position against competitors like Tether, whose stablecoin is the world's largest by market capitalization.

34. The more widely used and adopted that Circle's USDC and CCTP are, the more valuable the company becomes. Accordingly, Circle seeks to burnish its image as an ecosystem that is frictionless and open to all.

[4] https://developers.circle.com/cctp

35. Circle maintains control over USDC, including the ability to "freeze" its transfer or bridging. Circle can also block specific crypto wallet addresses from using its CCTP bridge.

36. For example, on March 23, 2026, Circle froze USDC held in 16 wallets tied to a sealed civil lawsuit in federal court. This rendered the funds nontransferable and unusable on chain. At least one of those wallets has since been unfrozen.

37. Instances of Circle's intervention, however, are an exception. Circle repeatedly has allowed unfettered use of its stablecoin and bridge services during large breaches involving millions of dollars in misappropriated funds.[5]

38. Just months before the attack on Drift, Circle refused to freeze USDC stolen in a $13 million SwapNet exploit, despite pleas from law enforcement and private sector experts.[6] In 2025, Circle permitted $61 million in stolen USDC to be bridged through its CCTP, then waited a month before blacklisting the attackers' wallet.[7] Over the past four years, Circle has amassed over $420 million in alleged compliance failures.[8] This pattern has caused respected crypto commentator @ZachXBT to label Circle a "bad actor" that "never take[s] care of [its] users as a centralized stablecoin issuer" of USDC.[9]

39. By contrast, Circle's competitor Tether has taken a proactive approach in freezing its stablecoin USDT to halt illegal acts. In 2025, Tether's founder stated,

---

[5] https://bit.ly/3PRnHNG
[6] *Id.*
[7] *Id.*
[8] *Id.*
[9] https://bit.ly/4vlARmm

"Tether's strength lies in the transparency of blockchain technology and our ability to act decisively when abuse is detected."[10] In 2026, the co-founder of the Tether-based USDT0 bridge said, "TradFi catches fraud after the money moves. USDT0 can stop it before."[11]

The Drift Protocol

40. Drift Protocol is primarily known as a decentralized exchange where users, both natural persons and institutions, can trade digital assets, including leveraged positions on the directional movement of cryptocurrencies.

41. For example, users can place bets whether the price of Bitcoin will rise or fall over any interval of their choosing. To place these bets, users must deposit crypto assets as collateral onto Drift's platform. Users may also make deposits to earn interest from Drift's lending features.

42. Drift accepts only select cryptocurrency tokens on the Solana blockchain. Drift is built on the Solana blockchain and relies on its infrastructure to execute trades, track balances, and manage user accounts. Transactions on Solana are processed and recorded publicly and transparently, allowing users to send, receive, and store digital assets.

43. Circle mints its stablecoin USDC on multiple blockchains, including Solana. Accordingly, USDC can be deposited, traded, or transferred on Drift Protocol. Because Circle issues USDC, Circle has unique control over transactions involving its

[10] https://bit.ly/3Q93FOL
[11] https://bit.ly/4tUZ0z5

stablecoin, regardless of the blockchain.

The Drift Exploit

44. On April 1, 2026, Drift Protocol was infiltrated by a cybercrime group believed to be affiliated with the government of North Korea. This group commonly uses social engineering and technical exploitation to gain access to cryptocurrency platforms and rapidly launder stolen funds through on-chain transactions.

45. The Attackers' plot against Drift Protocol began in fall 2025, months before the exploit. Posing as a legitimate, high-frequency trading firm, the Attackers induced Drift's Security Council members, who have ultimate control over the Protocol, to pre-sign transactions using a Solana feature called durable nonce. This allowed those transactions to be executed seamlessly at a later date.

46. By March 2026, the Attackers had secured the necessary approvals to conduct the heist. Then, on April 1, the Attackers executed the pre-signed transactions within minutes of one another, enabling a rapid takeover of Drift Protocol's administrative control. They introduced a fictitious asset, manipulated its price through controlled liquidity and oracle inputs, and altered protocol parameters to facilitate the removal of user funds.

47. Within minutes, the Attackers drained more than $285 million in assets, both in USDC and other Solana-based tokens that they quickly swapped for USDC. They then began transferring the USDC across blockchain networks.

48. The Attackers employed Circle's CCTP to bridge the Solana-based USDC to Ethereum-based USDC. This plan was not assured to succeed, given that the

transactions were publicly observable and traceable. At any point during the multi-hour getaway operation, Circle had the power to freeze the assets on a smart-contract level or blacklist the Attackers' wallet address from CCTP. Instead, Circle burned and minted over $230 million in USDC, in more than 100 separate transactions, through its CCTP bridging service.

49. With the USDC now on the Ethereum blockchain, the Attackers swapped it for Ether, another cryptocurrency that cannot be frozen or seized and may be concealed with the use of third-party applications, like TornadoCash.

50. The value of Drift users' stolen cryptocurrency currently sits in over one hundred Ethereum-based wallets, unreachable from law enforcement and unrecoverable.

Circle Knew of the Exodus of Drift Assets Through Its CCTP

51. Upon information and belief, the exploit of Drift Protocol and drain of deposited cryptocurrency began at approximately 11:15 a.m. Eastern Daylight Time (EDT) on April 1, 2026.

52. In the hours that followed, commentators, crypto investigators, and victims flocked to X, the platform formerly known as Twitter, to discuss the Drift exploit. For years, X has been the preeminent media platform for cryptocurrency news and discussions.

53. At 12:15 p.m., one hour after the exploit began, major crypto investor and influencer Mert Mumtaz (@mert) began alerting his 447,000+ followers in the crypto community—and explicitly Circle—that large amounts of Drift deposits had been

drained.[12] He posted: "hello someone from circle reach out asap, seeing high likelihood of a potentially large exploit."

54. At 12:45 p.m., Oleg Petrov (@ol3gpetrov), CTO of the bridge toolkit company SwapKit, made the call to disable their Solana bridge functionality in light of the signs of a massive Drift hack.[13] During this period, countless mentions of the exploit flooded the X platform. Circle maintains an X account (@circle) on which it posts and monitors others' posts about itself.

55. At 2:10 p.m., Drift (@DriftProtocol) first acknowledged to its 135,000 X followers that it observed unusual activity on its protocol.[14] Drift implored users not to deposit funds on the protocol. "This is not an April Fools joke," it warned. Discussions of the exploit continued to proliferate across X.

56. At 2:58 p.m., Drift followed up in an X post:[15]

> Drift Protocol is experiencing an active attack. Deposits and withdrawals have been suspended. We are coordinating with multiple security firms, bridges, and exchanges to contain the incident. This is not an April Fools' joke. We'll provide additional updates from this account as more information is available to share.

57. Through continuing updates and discussion on X, and direct contact from Drift and other crypto players, Circle learned of the exploit and the Attackers' use of USDC to offload the funds onto the Ethereum blockchain.

58. Further, Circle itself had a duty to monitor suspicious activity on its

[12] https://bit.ly/4slDu4O
[13] https://bit.ly/4mfl3xo
[14] https://bit.ly/3OoyNcz
[15] https://bit.ly/4mfZHzS

CCTP, whose sole purpose is money transmission, under the Bank Secrecy Act, 31 U.S.C. 5311 *et seq.* Most retail CCTP transfers range from $10,000 to $500,000 in value and involve wallets with previous CCTP transactions. What Circle saw here was a brand-new wallet making multimillion-dollar transmissions in rapid succession—an anomaly that Circle is required to monitor and report under law. *See* 31 C.F.R. § 1022.320 (a money services business shall report any suspicious transaction relevant to a possible violation of law).

59. Circle has acknowledged its monitoring capabilities and responsibilities on a video[16] posted on its website:

> We use AI and advanced tools to stay ahead of financial crime risk. Why so much investment in risk management? Because it's essential to building financial infrastructure that scales globally. And it's the right thing to do. Fighting money laundering and terrorist financing is job #1. … We conduct blockchain and transaction monitoring …. We aim not just to comply, but to exceed the expectations of those who depend on us.

Circle Allowed the Attackers Free Use of Its USDC Token and CCTP Bridge

60. Given Circle's history of permitting criminal use of its technology and services, it is likely the Attackers had high confidence that Circle would again supply the tools instrumental to their heist. This assumption proved to be correct. Circle allowed them use of its cryptocurrency and bridge services over the approximately eight-hour getaway period.

61. In total, the Attackers escaped with around $230 million in assets belonging to Drift depositors. These losses would not have occurred, or would have

[16] https://bit.ly/4dopRO2 at 11:30 mark.

been substantially reduced, had Circle withdrawn its services.

62. The only reason the Attackers failed to make out with the full $285 million they had exploited was the timely intervention of other crypto players. For example, Ondo Finance successfully froze $537,000 in USDY, a tokenized yield-bearing asset on the Solana blockchain.[17] USDT0, the Tether-based competitor to Circle's CCTP, froze its stablecoin bridge within 29 minutes of the exploit, later confirming that "not a single compromised dollar moved through our rails."[18] And two transfers attempted "via Wormhole have been delayed by the Wormhole Governor until late July, effectively locking funds in transit."[19]

63. But despite Circle's ability to block the transfer of the stolen assets, Circle gave the Attackers use of its technology and services.

Circle Doubles Down on Its Drift Decision

64. Approximately two weeks after the Drift exploit, Circle CEO Jeremy Allaire gave the keynote address at a Circle-focused conference in Seoul, South Korea.[20] Allaire defended Circle's decision not to pull assistance from the Attackers, claiming that allowing a private company to make such decisions would pose a "moral quandary." Allaire underscored Circle's stated policy to restrict its services only pursuant to court orders.

65. Shortly after, Drift Protocol announced it was cutting ties with Circle and

[17] https://bit.ly/3OcpVqe
[18] https://bit.ly/42fjsOU
[19] https://bit.ly/42fJXnu
[20] https://bit.ly/3OJHrmj

instead partnering with Circle competitor Tether to make USDT its primary stablecoin.

Plaintiffs' Facts

Joshua McCollum

66. Plaintiff Joshua McCollum deposited cryptocurrency into Drift Protocol. On April 1, 2026, these assets had a value of approximately $23,500.

67. Plaintiff's funds were among the crypto assets that Attackers drained from Drift Protocol. These funds were then offboarded from the Solana blockchain via Circle's USDC stablecoin and CCTP bridging service.

68. Plaintiff remains deprived of the cryptocurrency he invested.

Oakford Crawson LLC

69. Plaintiff Oakford Crawson LLC deposited cryptocurrency into Drift Protocol. On April 1, 2026, these assets had a value of approximately $6,500.

70. Plaintiff's funds were among the crypto assets that Attackers drained from Drift Protocol. These funds were then offboarded from the Solana blockchain via Circle's USDC stablecoin and CCTP bridging service.

71. Plaintiff remains deprived of the cryptocurrency it invested.

Jeffrey Magoveny

72. Plaintiff Jeffrey Magoveny deposited cryptocurrency into Drift Protocol. On April 1, 2026, these assets had a value of approximately $350,000.

73. Plaintiff's funds were among the crypto assets that Attackers drained from Drift Protocol. These funds were then offboarded from the Solana blockchain via Circle's USDC stablecoin and CCTP bridging service.

74. Plaintiff remains deprived of the cryptocurrency he invested.

Ng Boon Min

75. Plaintiff Ng Boon Min deposited cryptocurrency into Drift Protocol. On April 1, 2026, these assets had a value of approximately $28,000.

76. Plaintiff's funds were among the crypto assets that Attackers drained from Drift Protocol. These funds were then offboarded from the Solana blockchain via Circle's USDC stablecoin and CCTP bridging service.

77. Plaintiff remains deprived of the cryptocurrency she invested.

Lim Teck Yeow

78. Plaintiff Lim Teck Yeow deposited cryptocurrency into Drift Protocol. On April 1, 2026, these assets had a value of approximately $1,000,000.

79. Plaintiff's funds were among the crypto assets that Attackers drained from Drift Protocol. These funds were then offboarded from the Solana blockchain via Circle's USDC stablecoin and CCTP bridging service.

80. Plaintiff remains deprived of the cryptocurrency he invested.

Alexej Kravetsker

81. Plaintiff Alexej Kravetsker deposited cryptocurrency into Drift Protocol. On April 1, 2026, these assets had a value of approximately $30,000.

82. Plaintiff's funds were among the crypto assets that Attackers drained from Drift Protocol. These funds were then offboarded from the Solana blockchain via Circle's USDC stablecoin and CCTP bridging service.

83. Plaintiff remains deprived of the cryptocurrency he invested.

Michael Medovoj

84. Plaintiff Michael Medovoj deposited cryptocurrency into Drift Protocol. On April 1, 2026, these assets had a value of approximately $20,000.

85. Plaintiff's funds were among the crypto assets that Attackers drained from Drift Protocol. These funds were then offboarded from the Solana blockchain via Circle's USDC stablecoin and CCTP bridging service.

86. Plaintiff remains deprived of the cryptocurrency he invested.

CLASS ACTION ALLEGATIONS

87. Pursuant to Rule 23 of the Federal Rules of Civil Procedure, Plaintiffs seek to pursue their claims on behalf of similarly situated persons. The parameters of the class may be refined through discovery and will be subject to Court approval and modification, but for purposes of this complaint, Plaintiffs propose the following class definition:

> All persons and entities who owned cryptocurrency that was stolen in the April 1, 2026, Drift exploit and transferred through Circle's stablecoin USDC and its blockchain bridge CCTP to the Ethereum blockchain.

88. Plaintiffs propose that the following persons be excluded from any certified class: Defendants; their current or former officers, directors, legal representatives, and employees; any and all parent companies, subsidiaries, affiliates, predecessors, successors, or assigns of Defendants; and any judge to whom this case is assigned, his or her spouse, and all persons within the third degree of relationship to either of them, as well as the spouses of such persons.

89. Plaintiffs reserve the right to re-define the class definition after conducting

discovery.

90. The proposed class satisfies the requirements of Rule 23(a), as well as 23(b)(1) and 23(b)(3), and is otherwise appropriate under 23(c)(4).

91. Numerosity. The members of the class are so numerous that joinder of all members is impracticable. The size of the class, which is estimated to consist of thousands of individuals and business entities, can only be ascertained through discovery.

92. Typicality. Plaintiffs' claims against Circle are typical of the claims of the members of the class. Plaintiffs and class members were all victims of the Drift exploit, each has claims against Circle for its role in that scheme, and each claim will depend on common proof that Circle knew about the exploit and substantially assisted, or of Circle's negligence in bridging or failing to freeze the stolen assets.

93. Adequacy. Plaintiffs will fairly and adequately protect the interests of the members of the class and have retained counsel competent and experienced in class action and financial crimes litigation.

94. Commonality and Predominance. Common questions of law and fact exist as to all members of the proposed class and predominate over any questions solely affecting individual members of the proposed class. The questions of law and fact common to the class include:

a. Whether the Attackers converted the property of Plaintiffs and the proposed class;

b. When Circle learned of the Attackers' actions;

c. Whether Circle made its technologies and services available to the Attackers;

d. Whether Circle's actions constitute substantial assistance to the Drift exploit;

e. Whether Circle owed a duty to Plaintiffs and the proposed class;

f. Whether Circle breached its duty to Plaintiffs and the proposed class; and

g. Whether class members lost money or property as a result of Circle's actions and inaction.

95. Superiority. A class action is superior to other available means for the fair and efficient adjudication of this dispute. The injury suffered by each class member, while meaningful on an individual basis, is not of such magnitude as to make the prosecution of individual actions economically feasible. Even if class members themselves could afford such individualized litigation, the court system could not. In addition to the burden and expense of managing many actions arising from the same criminal scheme, individualized litigation presents a potential for inconsistent or contradictory judgments. Individualized litigation increases the delay and expense to all parties and the court system presented by the legal and factual issues of the case. By contrast, a class action presents far fewer management difficulties and provides the benefits of single adjudication, economy of scale, and comprehensive supervision by a single court.

96. In the alternative, the proposed class may be certified because: (a) the prosecution of separate actions by the individual members of the proposed class would

create a risk of inconsistent adjudications; (b) the prosecution of individual actions could result in adjudications, which as a practical matter, would be dispositive of the interests of non-party class members or which would impair their ability to protect their interests; and (c) Defendants have acted or refused to act on grounds generally applicable to the proposed class, thereby making appropriate final and injunctive relief with respect to the members of the proposed class as a whole.

97. In the alternative, the common questions of fact and law, set forth in Paragraph 94, are appropriate for issue certification on behalf of the proposed class pursuant to Fed. R. Civ. P. 23(c)(4).

CAUSES OF ACTION

Count I
Aiding and Abetting Conversion

98. Plaintiffs allege this cause of action on behalf of themselves and the proposed class, and, in doing so, incorporate all preceding allegations.

99. The Attackers exercised dominion and control over Plaintiffs' and other class members' personal property, namely their crypto assets on the Solana blockchain, by converting the same to their own use.

100. The Attackers were not and are not the rightful owners of that property.

101. Circle did not freeze the converted assets (in USDC at the time) such that they could be recovered. Instead, Circle continued to provide the Attackers the means to transmute the entire value of the converted crypto into assets not subject to seizure.

102. Circle had knowledge that the Attackers did not own the property and

that Attackers were acting without the property owners' authorization in taking possession of their crypto assets.

103. Circle substantially assisted the Attackers in converting Plaintiffs' crypto assets by bridging their assets from the Solana blockchain to the Ethereum blockchain. Circle, through its CCTP, authenticated each bridge transaction and minted hundreds of millions of dollars in Ethereum-based USDC for the Attackers. The Attackers required the cooperation of Circle to abscond successfully with these assets and could not have done so without that assistance.

104. As a direct and proximate result of the above-described conduct of Circle, Plaintiffs and the members of the class sustained damages in an amount to be determined at trial. Plaintiffs and the class seek to recover all available remuneration, including damages and restitution, from Circle plus accrued and accruing interest, prejudgment interest, costs, and all other relief deemed fair and just.

Count II
Negligence

105. Plaintiffs allege, in the alternative, this cause of action on behalf of themselves and the proposed class, and, in doing so, re-allege and incorporate by reference all preceding allegations.

106. Circle knew or reasonably should have known that the Attackers stole assets belonging to Plaintiffs and other members of the class and were using Circle's USDC and CCTP to bridge those assets to the Ethereum blockchain, where tools existed to make them untraceable.

107. Circle owed a duty to Plaintiffs and other members of the class with respect to the use of CCTP. Circle's duty arises from the reasonable foreseeability of the harm to Plaintiff from failing to freeze the USDC in the Attackers' control and allowing Attackers' use of Circle's CCTP to bridge hundreds of millions of dollars of funds from the Solana blockchain to the Ethereum blockchain. Circle was in a unique position to prevent the harm suffered by Plaintiffs and the class.

108. Circle has acknowledged that "stay[ing] ahead of financial crime risk" is "the right thing to do." It has called "fighting money laundering and terrorist financing" "job number one," and professed its "aim not just to comply, but to exceed the expectations of those who depend on us."

109. Circle breached its duty to Plaintiffs and other members of the class when, among other things, it did not freeze the assets (in USDC at the time) and bridged hundreds of millions of dollars in stolen cryptocurrency from the Solana blockchain to the Ethereum blockchain, where those funds could not be recovered and the Attackers' identity could more easily evade detection.

110. As a direct and proximate cause of Circle's negligence, Plaintiffs and the members of the class have sustained damages in an amount to be determined at trial.

REQUEST FOR RELIEF

WHEREFORE, Plaintiffs, on behalf of themselves and all others similarly situated, request that the Court enter a judgment awarding the following relief:

a. An order certifying the proposed class and appointing the Plaintiffs as the Class Representatives and undersigned counsel as class counsel;

b. An award of damages and all other available monetary relief, including pre-judgment interest, on each claim in an amount to be established at trial;

c. An award of punitive damages in an amount to be established at trial;

d. An award of Plaintiffs' reasonable attorneys' fees and litigation costs;

e. Such other and further relief as this Court may deem just and proper.

DEMAND FOR JURY TRIAL

Plaintiffs demand a trial by jury as to all issues so triable.

Dated: May 11, 2026

Respectfully submitted,

/s/ John Roddy

John Roddy (BBO #424240)
BAILEY & GLASSER LLP
101 Arch Street, 8th Floor
Boston, MA 02110
Telephone: (617) 439-6730
Facsimile: (617) 951-3954
jroddy@baileyglasser.com

Rosemary M. Rivas (*pro hac vice forthcoming*)
Parker Hutchinson (*pro hac vice forthcoming*)
Yusuf Al-Bazian (*pro hac vice forthcoming*)
GIBBS MURA LLP
1111 Broadway, Suite 2100
Oakland, CA 94607
Telephone: (510) 350-9700
Facsimile: (510) 350-9701
rmr@classlawgroup.com
pnh@classlawgroup.com
yab@classlawgroup.com

Counsel for Plaintiffs Joshua McCollum, Oakford Crawson LLC, Jeffrey Magoveny, Ng Boon Min, Lim Teck Yeow, Alexej Kravetsker, and Michael Medovoj