UNITED STATES DISTRICT COURT
DISTRICT OF MASSACHUSETTS

JOSHUA MCCOLLUM, on behalf of himself and all others similarly situated,

Plaintiff,

v.

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

Defendants.

Case No. 1:26-cv-11733

CLASS ACTION COMPLAINT

Jury Trial Demanded

Plaintiff Joshua McCollum, on behalf of himself and all others similarly situated, alleges 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. 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 North Korea's government.

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 it might be recovered.

6. Circle, however, did nothing as the Attackers worked to offload their spoils. For hours, Circle knowingly permitted the Attackers use of its technology and services, despite its ability to freeze the assets and stop the exodus into Ether. As one prominent crypto commentator put it, "Circle was asleep while many millions of USDC was swapped . . . for hours, from the 9-figure Drift hack during U.S. hours."[1]

7. By law, Circle was not free to look the other way while knowing it was enabling this misappropriation. But even though Circle saw what was happening and could have taken action to protect investors, it chose to do nothing. Drift depositors have lost hundreds of millions of dollars, which they are unlikely to recover unless

[1] http://bit.ly/4t1yjZ8

Circle is held accountable for its – at best – reckless indifference to the exploit made possible by its technology and services.

8. Plaintiff is among the many investors harmed by Circle's conduct. Through this lawsuit, Plaintiff seeks to hold Circle responsible. He brings this suit on behalf of himself and all other similarly situated investors and seeks full recovery of his losses and all other relief provided for by law or equity.

PARTIES

Plaintiff

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

Defendants

10. Defendant Circle Internet Group, Inc. is a publicly traded Delaware Corporation with its principal place of business in New York, New York.

11. 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

12. 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.

13. This Court has specific personal jurisdiction over Defendants because Plaintiff's 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.

14. 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.

STATEMENT OF FACTS

Circle's Business and Services

15. Circle is a cryptocurrency company that bills itself as a "full-stack platform for the new internet financial system."[2] The 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."[3] Circle touts the fast and seamless nature of its products, advertising the technology as: "Borderless by design. Near-instant by default."[4]

16. Central to Circle's capabilities is its flagship crypto product USDC, the most widely adopted stablecoin in the United States. Unlike cryptocurrencies like Bitcoin or XRP that can swing wildly in value, stablecoins are designed to maintain a steady value. USDC, for example, is pegged to the U.S. dollar, and each USDC is backed by $1 in actual reserves. USDC's stability and wide adoption permit users to move in

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

and out of crypto positions quickly without having to convert assets to "bank" money.

17. Another of Circle's core features is its Cross-Chain Transfer Protocol (CCTP), a native system for moving USDC between blockchains. Because blockchains are not interoperable, users wishing to move assets across blockchains require "bridging" services like Circle's CCTP. To illustrate: if a user wants to move USDC from the Solana blockchain to the Ethereum blockchain, Circle's CCTP will "burn" each Solana-based USDC and mint a new Ethereum-based USDC.

18. Because the bridged token remains 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.

19. The more widely used and adopted 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.

20. Circle maintains control over USDC, including the ability to "freeze" its transfer or bridging. According to Circle's agreement with users minting new USDC, "Circle may suspend accounts in its sole and absolute discretion …."[5]

21. 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.

[5] https://www.circle.com/legal/user-agreement

22. 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.[6]

23. Just months before, Circle refused to freeze USDC stolen in a $13 million SwapNet exploit, despite pleas from law enforcement and private sector experts.[7] In 2025, Circle permitted $61 million in USDC to be bridged through its CCTP, then waited a month before blacklisting the attackers' wallet.[8] Over the past four years, Circle has amassed over $420 million in alleged compliance failures.[9] 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.[10]

24. 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, "Tether's strength lies in the transparency of blockchain technology and our ability to act decisively when abuse is detected."[11]

The Drift Exploit

25. Drift Protocol is primarily known as a decentralized exchange where users—both natural persons and institutions—can place leverage bets on the directional movement of cryptocurrency assets. For example, users can place bets whether the price

[6] https://bit.ly/3PRnHNG
[7] *Id.*
[8] *Id.*
[9] *Id.*
[10] https://bit.ly/4vlARmm
[11] https://bit.ly/3Q93FOL

of Bitcoin will rise or fall over any interval of their choosing.

26. 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. Drift accepts only select cryptocurrency tokens on the Solana blockchain.

27. On April 1, 2026, Attackers executed a heist of over half of the cryptocurrency deposited with Drift. In under 12 minutes, Attackers transferred approximately $280 million in assets from the Drift Protocol to two Solana wallets under their exclusive control.

28. These assets would be easily identifiable as those stolen from Drift and quickly frozen from transacting unless the Attackers took additional steps to offload them. Accordingly, the Attackers worked to move them into tokens on a separate blockchain that could not be frozen or easily identified.

29. First, the Attackers immediately swapped the various stolen assets to USDC, the stablecoin controlled by Circle. These swaps permitted freer movement of the assets and also protected them during that process because the token maintains a stable value.

30. Second, over approximately eight hours, the Attackers utilized Circle's CCTP to "bridge" that Solana-based USDC to Ethereum-based USDC. The Attackers' use of Circle's services to bridge these assets was not assured to succeed, given that Circle could have frozen the assets on a smart-contract level or blacklisted their wallet address for CCTP use during their hours-long getaway operation.

31. Finally, with the USDC now on the Ethereum blockchain, the Attackers

swapped it for Ether, another cryptocurrency that cannot be frozen and may be concealed with the use of third-party applications, like TornadoCash.

32. 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

33. 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).

34. 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.

35. 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."

36. 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

[12] https://bit.ly/4slDu4O

the signs of a massive Drift hack.[13] During this period, countless mentions of the exploit flooded the X platform.

37. At 2:10 p.m., Drift (@DriftProtocol) first acknowledged to its 135,000 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.

38. 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.

39. Through continuing updates and discussion on X, and direct contact from Drift, Circle learned of the exploit and the Attackers' use of USDC to offload the funds onto the Ethereum blockchain. Further, Circle itself had a duty to monitor suspicious activity on its CCTP, whose sole purpose is money transmission, under the Bank Secrecy Act, 31 U.S.C. 5311 *et seq.*

40. Approximately four hours after Drift's suspension of services—and eight hours after the exploit began—the Attackers had completed bridging the stolen assets through CCTP without any intervention by Circle.

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

41. Given Circle's history of inaction, it is likely the Attackers had high

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

confidence Circle would not freeze the USDC or the bridge transactions that were instrumental to their heist. This assumption proved to be correct. Circle allowed them free use of its cryptocurrency and bridge services over the approximately eight-hour getaway period.

42. In total, the Attackers escaped with around $230 million in assets belonging to Drift depositors. These losses would not have occurred, or would have been substantially reduced, had Circle taken timely action.

43. The only reason the Attackers failed to make out with the full $280 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.[16]

44. But despite Circle's ability to freeze transfer of the stolen assets, Circle permitted this criminal use of its technology and services.

Plaintiff's Facts

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

46. Plaintiff's funds were among the crypto assets that Attackers drained from Drift Protocol. The identity and location of these funds were then obfuscated via the use of Circle's USDC stablecoin and CCTP bridging service.

47. Plaintiff remains deprived of the cryptocurrency he invested.

[16] https://bit.ly/3OcpVqe

CLASS ACTION ALLEGATIONS

48. Pursuant to Rule 23 of the Federal Rules of Civil Procedure, Plaintiff seeks to pursue his 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, Plaintiff proposes the following class definition:

> All persons and entities who owned cryptocurrency that was stolen in the April 1, 2026, Drift exploit.

49. Plaintiff proposes that the following persons be excluded from any certified class: Defendant; its current or former officers, directors, legal representatives, and employees; any and all parent companies, subsidiaries, affiliates, predecessors, successors, or assigns of Defendant, 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.

50. 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).

51. 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.

52. Typicality. Plaintiff's claims against Circle are typical of the claims of the members of the class. Plaintiff 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.

53. Adequacy. Plaintiff will fairly and adequately protect the interests of the members of the class and has retained counsel competent and experienced in class action and financial crimes litigation.

54. 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 Attackers converted the property of Plaintiff and the proposed class;

b. When Circle learned of the Attackers' actions;

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

d. Whether Circle acted culpably in providing those technologies and services;

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

f. Whether Circle owed a duty to Plaintiff and the proposed class;

g. Whether Circle breached its duty to Plaintiff and the proposed class; and

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

55. 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.

56. 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.

CAUSES OF ACTION

Count I
Aiding and Abetting Conversion

57. Plaintiff alleges this cause of action on behalf of himself and the proposed class, and, in doing so, incorporates all preceding allegations.

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

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

60. Circle did not stop the Attackers from bridging and converting the USDC to Ether, either by freezing the converted assets (in USDC at the time) or preventing Attackers from using CCTP. Instead, Circle continued to provide Attackers the means to transmute the entire value of the converted crypto into crypto assets not subject to seizure.

61. 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.

62. Circle substantially assisted the Attackers in converting Plaintiff's crypto assets by providing the Attackers means to bridge their assets from the Solana blockchain to the Ethereum blockchain. Attackers required the cooperation of Circle to successfully abscond with these assets and could not have done so without that assistance.

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

Count II
Negligence

64. In the alternative, Plaintiff alleges this cause of action on behalf of himself and the proposed class, and, in doing so, incorporates all preceding allegations.

65. Circle knew or reasonably should have known that the Attackers stole assets belonging to Plaintiff 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.

66. Circle owed a duty to Plaintiff 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 the funds from the Solana blockchain to the Ethereum blockchain. Circle was in a position to prevent the harm suffered by Plaintiff and the class.

67. Circle breached its duty to Plaintiff and other members of the class when, among other things, it did not freeze the assets (in USDC at the time) and permitted the Attackers' use of CCTP to bridge hundreds of millions of dollars in stolen

cryptocurrency from the Solana blockchain to the Ethereum blockchain, where those funds and Attackers' identity could more easily evade detection.

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

REQUEST FOR RELIEF

WHEREFORE, Plaintiff, on behalf of himself and all others similarly situated, requests that the Court enter a judgment awarding the following relief:

a. An order certifying the proposed class and appointing the 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 Plaintiff's reasonable attorneys' fees and litigation costs;

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

DEMAND FOR JURY TRIAL

Plaintiff demands a trial by jury as to all issues so triable.

Dated: April 14, 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 Plaintiff Joshua McCollum and the Proposed Class