IN THE UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF NEW YORK

HAN KIM, YONG SEOK KIM, YONG HWA CHUNG KIM, CHUNG KOOK KIM, and DANI BUTLER, Plaintiffs, v. CIRCLE INTERNET GROUP, INC., and CIRCLE INTERNET FINANCIAL, LLC, Defendants.	Case No. 26-CV-5445 JURY TRIAL DEMANDED

COMPLAINT

Introduction

1. In 2000, Reverend Dong Shik Kim, who had moved to China from the U.S. seven years earlier to minister to refugees and people with disabilities, was kidnapped by a North Korean agent and taken into North Korea, where he was tortured and murdered by the state. In 2015, the Reverend's brother, Yong Seok Kim, and the Reverend's son, Han Kim, won a $330,000,000 money judgment against North Korea; and in 2025 the Reverend's widow, Yong Hwa Chung Kim, and two of his children, Dani Butler and Chun Kook Kim (collectively "the Kims"), won a $366,000,000 money judgment against North Korea. North Korea is a designated state sponsor of terrorism and has not paid anything towards the judgment against it. North Korea is also the world's most prolific hacker of crypto assets. It funds its nuclear program and ballistic missile program using crypto assets acquired through large and sophisticated hacks.

2. Defendant Circle Internet Financial LLC is a New York–headquartered company that issues a crypto asset called U.S. Dollar Coin (USDC) on many blockchains. Circle calls USDC a "stablecoin" because, according to Circle's terms of service, Circle "backs [every USDC with] an equivalent amount of U.S. Dollar-denominated assets held by Circle . . . on behalf of, and for the benefit of, [the coin-holders]." Circle has the power to freeze any USDC at any time.

3. On November 26, 2025, the Kims served a restraining notice on Circle Internet Group, Inc., and Circle Internet Financial, LLC (collectively, "Defendants" or "Circle"). The notice restrained all North Korean assets in Circle's control. The

restraining notice also explicitly applied to North Korean property that later comes into Circle's control.

4. On April 1, 2026, North Korea drained approximately $285 million in crypto assets from the Drift Protocol, a platform that offers crypto derivative trading. North Korean hackers sold some of those assets on the open market in exchange for roughly 232 million USDC.

5. But even though the Drift exploit bore many of the markers of an attack perpetrated by North Korean state actors, such that other non-affected entities were able to quickly attribute the exploit to North Korea, and despite the fact that the world watched North Korean agents use USDC to launder the wrongly taken assets over the course of a full day, Circle did not freeze the USDC held by North Korea. That is because Circle's *stated* policy is to ignore criminal, sanctioned use of USDC in *all* circumstances other than a specific request from the Government or a court: Circle's Chief Strategy Officer insisted that Circle freezes USDC only when "the law requires us to act," which Circle interprets to be only in response to a Government request.

6. But the law required Circle to act on April 1. After being served with a restraining notice by the family of someone who was kidnapped, tortured, and murdered by North Korea, Circle had "no discretion to ignore" the notice. *Sykes v. Bank of Am.*, 723 F.3d 399, 406 (2d Cir. 2013). Instead, it was obligated to "use reasonable care to abide by" that restraining notice, *Doubet, LLC v. Trs. of Columbia Univ.*, 2011 NY Slip Op 51219(U), 934 N.Y.S.2d 33 (N.Y. Sup. Ct. 2011).

7. Circle failed to do so. On a day when North Korea—the world's foremost crypto hacker—wrongly obtained hundreds of millions in dollars of crypto assets, exchanged those assets for USDC in a manner typical of previous North Korean laundering operations, and used a Circle service to bridge its USDC to another blockchain, Circle did nothing. This despite a public outcry and ample warning signs that North Korea was holding USDC.

8. Circle had the power and duty to freeze those crypto assets. Instead, Circle disregarded the law and, citing what its CEO called a "moral quandary," permitted North Korea to come out hundreds of millions of dollars richer while the Kims' judgment against North Korea remains completely unsatisfied. This lawsuit is an effort to collect the damages that the Kims suffered because of Circle's violation of the Kims' restraining notice.

Parties

9. Plaintiff Yong Seok Kim is the brother of the late Reverend Dong Shik Kim. Plaintiff Han Kim is the son of Reverend Kim. Plaintiff Yong Hwa Chung Kim is the widow of Reverend Kim. And Plaintiffs Chung Kook Kim and Dani Butler are the children of Reverend Kim. No Plaintiff is a resident of New York.

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

11. Defendant Circle Internet Financial, LLC is a Delaware limited liability company with its principal place of business in New York, New York. Circle Internet Financial, LLC's sole member is Circle Internet Holdings, Inc., a wholly owned subsidiary of Circle Internet Group, Inc., which is incorporated in Delaware.

Jurisdiction and Venue

12. This Court has subject-matter jurisdiction under 28 U.S.C. § 1332 because neither Plaintiff is a resident of the same state as either Defendant and the amount in controversy exceeds $75,000. No Plaintiffs is a citizen of New York; Defendant Circle Internet Group, Inc., is a Delaware corporation with its principal place of business in New York and is therefore a citizen of Delaware and New York; and Defendant Circle Internet Financial, LLC, is a limited liability company whose sole member is Circle Internet Holdings, Inc., a Delaware corporation with its principal place of business in New York, which makes Circle Internet Financial, LLC, a citizen of Delaware and New York.

13. This Court also has subject-matter jurisdiction under 28 U.S.C. § 1331 because this Action arises from the violation of an order of this Court.

14. This Court may exercise general personal jurisdiction over Defendants because they are headquartered here.

15. This Court may exercise specific personal jurisdiction over Defendants because they violated a restraining notice issued in aid of a judgment-enforcement proceeding in which they consented to the jurisdiction of this Court, and in which jurisdiction is proper regardless.

16. Venue is appropriate in this Court because Defendants are headquartered here and because Defendants violated a restraining notice issued by this Court.

The Kidnapping and Murder of Reverend Dong Shik Kim

17. In 1993, Reverend Dong Shik Kim moved from the U.S., where he was a lawful permanent resident, to China to work as a missionary providing humanitarian and religious services to North Korean families who had fled across the Sino–Korean border. *Kim v. Democratic People's Republic of Korea* ["DPRK"], 950 F. Supp. 2d 29, 36 (D.D.C. 2013).

18. In 2000, Reverend Kim was abducted by a member of the North Korean security services and secreted across the border into North Korea. *Kim v. DPRK*, 774 F.3d 1044, 1049 (D.C. Cir. 2014). No one outside North Korea has heard from Reverend Kim since. *Id.* He is presumed dead. *Id.*

19. Experts in North Korea's human-rights violations testified that North Korea sends those whom it deems to be "opponents of the . . . regime" to torture camps called *kwan-li-sos*. *Id.* at 1050. Experts further testified that Reverend Kim "suffered an untimely death" resulting "from torture and malnutrition . . . deliberately caused by his North Korean captors." *Id.* at 1050–51.

The Kims Obtain Judgments Against North Korea and Attempt to Enforce Them

20. In 2009, the Kim family sued North Korea for the abduction and murder of Reverend Kim. *Kim v. DPRK*, No. 09-CV-648, Dkt. 1 (D.D.C. April 8, 2009).

21. North Korea, after being properly served, did not appear to defend. *Id.* Dkt. No. 12 (entry of default). And so Plaintiffs sought a default judgment. *Id.* Dkt. No. 46. The district court denied that request, reasoning that Plaintiffs had not

presented evidence sufficient to meet the Foreign Sovereign Immunity Act's special provision for proof when a defendant defaults. *Kim*, 950 F. Supp. 2d at 34.

22. Plaintiffs appealed and the D.C. Circuit reversed, holding that "[t]he Kims . . . make a compelling case that North Korea" tortured Reverend Kim and murdered him outside of the normal legal process. 774 F.3d at 1050.

23. On remand, the district court entered a default money judgment of $15,000,000 in compensatory damages for each of Plaintiffs and $300,000,000 in punitive damages to be divided between them. *Kim v. DPRK*, 87 F. Supp. 3d 286, 291 (D.D.C. April 9, 2015).

24. Plaintiffs served the default judgment on North Korea, and on July 23, 2019, the court granted Plaintiffs permission to enforce the judgment under 28 U.S.C. § 1610(c).

25. In 2020, the Kim and Butler families sued and won a similar default judgment, *Butler v. DRPK*, Dkt. No. 31, 20-cv-2514 (D.D.C. Nov. 04, 2025), and their request for leave to enforce that judgment is currently pending, *id.*

26. In 2025, Plaintiffs registered the judgment in the United States District Court for the Southern District of New York, *Kim v. DPRK*, No. 25-mc-527 (S.D.N.Y. 2025), and served writs of execution on Defendants, as they possess North Korean assets in that district, *id.*

27. On November 26, 2025, the Kims served a restraining notice on Circle Internet Group, Inc., and Circle Internet Financial, LLC, through the registered agents for those entities, under New York C.P.L.R. § 5222.

28. The Kims' counsel, Charles Gerstein, also emailed a copy of the restraining notice to Josh Baskin, attorney for Circle in the Kims' judgment-collection action before this Court, on November 26, 2025. Baskin received and opened Gerstein's email. Baskin discussed the email's contents by phone with Gerstein on December 9, 2025.

29. The restraining notice notified Circle that the Kims hold a $330,000,000 judgment against North Korea, that judgment has been registered in the United States District Court for the Southern District of New York, and the entirety of the judgment is due and owing with interest accruing from the date of the judgment.

30. The Kims' restraining notice informed Circle that "you are in possession or custody of property in which the Judgment Debtor has an interest, specifically: assets, funds, and property interests of the Democratic People's Republic of Korea, including but not limited to United States Dollar Coins ("USDC"), digital or custodial wallet balances, any interest in Circle Internet Group, Inc. or its affiliates' United States cash reserves, and any other assets or interests owned by the Democratic People's Republic of Korea and its instrumentalities and agents, including, but not limited to, the Lazarus Group and the holdings at Ethereum blockchain wallet addresses 0x36f2D3871edd59d5C06DB8F0b12bE928d5922A70, 0xDa2e12E94060720581994eEc870F83d9C7200c2c, and 0x12ED7f6ed0491678764c2b222A58452926E44DB6."

31. The restraining notice further stated that "this Restraining Notice also covers all property in which the above-named Judgment Debtor has an interest

hereafter coming into your possession or custody, and all debts hereafter coming due from you to the Judgment Debtor."

32. The Kims' restraining notice contained the entirety of C.P.L.R. § 5222(b), which states in relevant part that "[a] judgment debtor or obligor served with a restraining notice is forbidden to make or suffer any sale, assignment, transfer or interference with any property in which he or she has an interest. . . . All property in which the judgment debtor or obligor is known or believed to have an interest then in and thereafter coming into the possession or custody of such a person, including any specified in the notice, and all debts of such a person, including any specified in the notice, then due and thereafter coming due to the judgment debtor or obligor, shall be subject to the notice . . ."

Background on Blockchains, Solana, and Bridges

33. A blockchain is a system for a distributed network of machines to keep a ledger of transactions publicly and securely. To maintain a blockchain, a distributed network of machines uses a cryptographic function called a "hash" to validate a series of transactions (a "block") and connect it (using another hash) to all prior series of transactions (hence "chain") in a way that is verifiable and immutable.

34. The term "blockchain" usually refers to exclusively electronic systems like Bitcoin and Ethereum used for trading crypto assets. The blockchain at issue in this case is called Solana.

35. Solana permits users to conduct transactions using "programs," which are otherwise known as "smart contracts." A Solana program automatically executes transactions when certain conditions are triggered.

36. Most Solana transactions include a "recent blockhash," which functions as a timestamp for the transaction. Solana can use a recent blockhash in that way because its system requires hashes to be produced sequentially. As a result, by default, a Solana transaction must be submitted and committed to a block before its recent blockhash is no longer recent enough. Otherwise, the transaction expires and cannot be executed.

37. But Solana also permits what it calls "durable nonce" transactions, which permit users to verify a transaction that can be submitted at any point in the future. Durable-nonce transactions differ from the typical Solana transaction because they use something called Durable Transaction Nonces to make every such transaction unique. Thus, durable-nonce transactions do not expire in the short window that applies to ordinary recent-blockhash transactions. Instead, they remain executable for any time once all parties to the transaction sign it, so long as the transaction remains otherwise valid.

38. To create a durable-nonce transaction, a user must first create a nonce account on Solana. Then the user must send the transaction to all counterparties to the transaction for authorization. The durable-nonce submission contains all relevant information about the transaction, thus enabling signers to evaluate the transaction before authorizing it. Once signers authorize the transaction by providing their signature, the transaction data cannot be materially altered without invalidating the signature. Anyone holding the fully signed transaction can submit it to the Solana network at any time in the future, so long as the transaction remains valid.

39. Blockchains vary from each other in many different ways. For example, unlike Solana, transactions on Bitcoin do not rely on a short-lived recent blockhash. As a further example, although Ethereum and Solana allow users to conduct transactions using smart contracts, Bitcoin has very limited smart contract functionality. Moreover, Solana processes transactions faster and cheaper than Ethereum does.

40. Many crypto assets are traded on each blockchain. For example, Bitcoin, Ethereum, and Solana have eponymously named assets that are "native" to their chains—Bitcoin ("BTC"), Ether ("ETH"), and Solana ("SOL"), respectively. But Ethereum and Solana also have many other (thousands, at least) crypto assets that are issued, held, transferred, and traded through applications built on those blockchains.

41. One category of crypto asset that has grown in popularity is "stablecoins." Stablecoins are a type of digital asset whose value is pegged to a currency or commodity. The largest stablecoins are pegged one-to-one to the United States dollar. Most stablecoins are available on some blockchains, but not others.

42. As the market for crypto assets and infrastructure has grown over the past decade, so has the number of public blockchains. For example, because the Ethereum blockchain is comparatively slow and expensive, some users began conducting their transactions on other chains that are similar to but faster than Ethereum. Meanwhile, Bitcoin, the most popular and generally most valuable digital

asset, cannot be traded on Ethereum, the most popular smart contract–capable blockchain.

43. Cross-chain bridge services arose to solve the problem of blockchain interoperability. The bridge operator locks or destroys assets on the origin chain, then reissues equivalent assets on the destination chain, thus effectively allowing users to send assets from one chain to another.

Background on Circle, USDC, and its Cross-Chain Transfer Protocol

44. Circle Internet Financial, LLC, issues USDC, a stablecoin pegged to the United States dollar. Circle Internet Financial, LLC's parent company is Circle Internet Group, Inc.

45. Circle's terms provide that "USDC is fully backed by an equivalent amount of U.S. Dollar-denominated assets held by Circle . . . on behalf of, and for the benefit of" those who hold USDC. Circle further explains that "for every USDC issued by Circle and remaining in circulation, Circle will hold on behalf of Users either one U.S. Dollar ("USD") or an equivalent amount of USD-denominated assets in its Segregated Accounts (the 'USDC Reserves')."

46. Circle Internet Financial, LLC, backs USDC with reserves that are managed by BlackRock and held in custody at BNY Mellon. Both BlackRock and BNY Mellon are headquartered in New York City.

47. As of June 15, 2026, Circle holds $75.1 billion in reserves and there are 74.9 billion USDC in circulation.

48. Circle Internet Financial, LLC, issues USDC on 34 blockchain networks, including Ethereum and Solana.

49. Circle issues USDC through a process called "minting" that permits businesses and institutions (individuals cannot mint USDC, per Circle's terms) to buy USDC from Circle in exchange for an equivalent number of dollars. For a business or institution to receive USDC via minting, that business or institution must link a bank account to Circle. After Circle receives the fiat deposit, it credits the business or institution with an account balance, at which time the business or institution receives USDC in its blockchain address.

50. Circle redeems USDC through a process called "redemption" or "offramp." Redemption is the reverse of minting. When a business or institution redeems USDC, Circle exchanges that business or institution's USDC at a one-to-one ratio for United States dollars. The redemption process begins when the business or institution creates a payout request that specifies the amount and destination bank account. After such a request is made, Circle debits the USDC amount from that business or institution's account, and Circle then sends United States dollars to that business or institution's bank account.

51. Because USDC is redeemable for $1, USDC trades for $1 on crypto exchanges and platforms where crypto assets are sold.

52. Circle mints and redeems USDC only to businesses or institutions with a Circle Mint account. Individuals are not currently eligible for Circle Mint accounts, although Circle permitted individuals to mint and redeem USDC until November 2023.

53. As part of the Circle Mint application process, each business and institution must provide Circle with accurate information about itself, its operations, beneficial owners, and the intended use of the Circle Mint account it is seeking.

54. Circle requires all businesses who wish to open a Circle Mint account to provide the following information: (1) registered business name; (2) country of incorporation or formation; (3) legal entity type; (4) expected monthly minting volume; (5) active platform users; (6) identification number; (7) date of incorporation or formation; (8) country of incorporation or formation; (9) business type; (10) business telephone number; (11) physical proof of business details; (12) physical proof of registered business address; (13) business website; (14) business model; (15) description of products/services; and (16) customer base description.

55. Depending on the business or institution's industry, Circle will require slightly different levels of information. As an example, Circle asks crypto exchanges who apply for a Circle Mint account to describe the products or services offered, but Circle does not ask the same of a personal-investment company or a trust that applies for a Circle Mint account. Circle requires crypto exchanges to provide, among other things, documentation of their cybersecurity measures; anti-money laundering policies; transaction monitoring procedures; and an independent audit of that entity's anti-money laundering program.

56. Circle requires documentation from Circle Mint applicants. Circle generally requires that all Circle Mint applicants provide government-issued identification of an applicant's beneficial owners and directors. Moreover, Circle

expects all institutions to provide an organizational chart or capitalization table that shows any shareholders in the company. Circle requires proof of a physical address, and does not accept PO boxes, registered agents, mail forwarding, or virtual addresses for this purpose.

57. Circle explains that it requires these documents "to ensure regulatory adherence and a secure onboarding process." As Circle has explained, its requirement that an applicant provide documentation of its ownership structure "[e]nsures compliance with Know Your Customer (KYC) policies." Circle has further explained that it demands documentation of an applicant's anti-money laundering compliance and an independent audit of the applicant's anti-money laundering program to "[e]nsure adherence to international financial regulations and sound [anti-money laundering] program."

58. Circle permits businesses and institutions from only certain countries to open a Circle Mint account. For example, Circle does not permit Circle Mint accounts to be opened by businesses or institutions from North Korea, Russia, Belarus, or the Islamic Republic of Iran.

59. Circle requires applicants to provide current, complete, and accurate information. It also requires applicants to provide "any additional information" that Circle "request[s] for the purposes of identity verification and the detection of money laundering, terrorist financing, fraud, or any other financial crime," both "when registering and on an ongoing basis." Circle further reserves the right to require

Circle Mint account holders to submit additional records and complete other verification steps.

60. When Circle created USDC, it gave itself the power to freeze the USDC balance of any wallet address, a power Circle calls "access denial" and which, when implemented, causes the USDC balance of a wallet address to equal whatever it equals at the time access denial is implemented until access denial is lifted.

61. Circle treats frozen USDC as removed from circulation.

62. Circle has the power to change the smart contracts that issue and control USDC at any time and in any way. Circle could, therefore, make the USDC balance of any wallet address equal whatever Circle wishes it to equal at any time.

63. Circle has exercised its power to freeze USDC on multiple occasions. For example, in August 2022, after the U.S. Treasury Department sanctioned Tornado Cash, Circle implemented access denial on Tornado Cash–related addresses, which froze addresses containing more than $75,000 USDC. And in July 2023, Circle implemented access denial on three wallet addresses containing $63 million USDC linked to the exploit of a cross-chain bridge.

64. Circle claims to freeze USDC only in response to court orders and government requests. Circle asserted in a hearing in this Court that "it is beyond our capacity or remit" to identify who owns USDC outside of Circle Mint accounts, and that Circle freezes funds only for certain delineated reasons and "*not* in response to suspicion, unverified social media posts, or requests from non-government actors," however reasonable or compelling that suspicion or other evidence may be.

65. Someone who holds USDC may send USDC to any wallet address they please. But if someone who holds USDC on a wallet address on the Solana blockchain wishes to transact with an entity who wants USDC on the Ethereum blockchain, it becomes necessary to use a bridge to transfer the USDC on the Solana blockchain to the Ethereum blockchain.

66. Circle Technology Services, LLC ("CTS"), a wholly owned subsidiary of Circle Internet Group, Inc., operates a bridge that it calls the Cross-Chain Transfer Protocol, or "CCTP." On information and belief, CTS has no distinct officers, employees, or independent management and is run entirely by Circle Internet Group, Inc., personnel and for the benefit of Circle Internet Group, Inc.

67. CCTP facilitates USDC transfers on blockchains by burning USDC (permanently removing it from the circulating supply) on the source blockchain (the blockchain on which the USDC is presently held) and minting it on the destination blockchain (the blockchain on which the user wishes to hold USDC).

68. Although the technical details differ based on the blockchains involved, CCTP operates as follows on all blockchains. First, a user initiates a transfer by calling the CCTP program on the source blockchain and prompting it to burn a specific amount of USDC. Once that happens, the source blockchain CCTP sends a message that says a specific amount of USDC was burned on that specific blockchain. Circle maintains an off-chain attestation service called "Iris," which observes the burn message and then signs an attestation that can be submitted on the destination

blockchain. Once that attestation message is submitted, CCTP on the destination chain will mint USDC for the user.

69. Circle claims that CCTP is "non-custodial." This is not true: according to a security audit published on Circle's website, an address called "owner" controls all smart contracts involved in CCTP's process and can burn tokens, mint tokens, and send "arbitrary cross-chain messages" without restriction. In other words, the whole system is controlled by the "owner," which is Circle, who therefore has custody of all assets in transit.

70. Circle's terms of service for using CCTP (which, per its terms, apply between the user, CTS, and other Circle affiliates "to the extent relevant") make clear that Circle may "suspend or terminate [the user's] use of [CCTP] at any time for any reason." And Circle's terms bar sanctioned parties from using CCTP.

71. CCTP calls itself a "permissionless" software resource, which means third-party companies and software developers may access, build on, and integrate it into their products for no charge and without specific authorization from any Circle entity.

The Drift Protocol

72. Drift Labs is a New York company founded by Cindy Leow and David Lu in 2021.

73. Drift Labs developed the Drift protocol ("Drift").

74. A protocol is a collection of programs, or "smart contracts," that together are the rough equivalent of software on a personal computer.

75. Some protocols allow for machine-executed borrowing, lending, and asset exchanges. And together these protocols created something called "DeFi," or "decentralized finance," which uses blockchains ostensibly to remove third parties, like traditional banking institutions and regulators, from financial transactions.

76. In the place of those traditional institutions, DeFi entrepreneurs created "DAOs" (pronounced "dows"), or "decentralized autonomous organizations." In a DAO, there is no formal corporate structure, no explicit liability protection, and no formalized distinction between, say, managers and directors. Instead, holders of specific tokens have governance rights that allow them to suggest actions that the associated DAO will take. Those suggestions are then voted on and implemented if the required number of tokenholders support the actions. Actions include many of those typically done by corporate officers, boards, or employees, such as spending treasury funds to hire people; changing organizational goals and policies; and even distributing treasury assets to tokenholders, like how corporations can authorize distributions to owners. Holders of governance tokens thus may participate in the governance of a protocol and have a potential claim on its profits.

77. Drift is a protocol built on the Solana blockchain that, among other things, permits users to deposit crypto assets as collateral to borrow other assets. Drift allows users to deposit crypto assets into lending pools and earn variable yield when other users borrow those assets. Drift permits borrowers to withdraw assets from Drift only by maintaining collateral whose protocol-recognized value exceeds the value of their borrow positions, as measured by the Drift protocol's risk parameters.

Drift's protocol determines variable yield and interest rates based in large part on the relevant asset in the relevant lending pool.

78. Drift does not allow fixed-term loans. Rather, Drift borrowers can maintain borrowed positions indefinitely so long as their accounts continue to satisfy Drift's collateral and margin requirements. If a borrower's position does not meet Drift's maintenance requirements, the borrower's collateral will be automatically liquidated by the Drift protocol, but the borrower gets to keep the borrowed assets without any other consequence.

79. Drift warns lenders of "the risk of borrower default." Drift maintains an Insurance Fund to protect lenders, but Drift acknowledges that "[w]hen there is not enough insurance available, the losses will be socialised across depositors."

80. Drift Labs launched Drift in 2021. The protocol hit $1 billion in volume in just 39 days. At first, Drift was formally run by Drift Labs and its administrative team, but on April 16, 2024, Drift Labs launched the Drift DAO foundation and the DRIFT governance token. Holders of DRIFT governance token control the Drift DAO—One token equals one vote over any proposal submitted to the DAO. In April 2024, Drift had a cumulative volume of over $20 billion and over 175,000 individuals or entities using the protocol.

81. Drift Labs announced that there would be a total of 1 billion DRIFT governance tokens, to be distributed over five years, with 53% to be distributed to the "community" ("encompassing a diverse range of stakeholders from stakers to algorithmic traders"), 25% to be allocated to "protocol development" ("current and

future contributors dedicated to developing Drift Protocol tooling"), and 22% to be distributed to "strategic participants" ("key partners in the space"). According to Drift's announcement, the Drift DAO Foundation "facilitate[s] the coordination of decisions and initiatives from the token holders and the DAO. The Foundation's DAO administration [is] Webslinger, an advisory firm."

82. Drift explained that the Drift DAO is a "multi-branch DAO" that consists of three arms: "Realms DAO for general protocol development, a Security Council for governing protocol upgrades, and a Futarchy DAO for funding technical grants."

83. The Realms DAO is "responsible for the overall development of the protocol" and "elects a Security Council comprised of the most knowledgeable contributors and developers within the Drift ecosystem."

84. As is most relevant here, the Security Council is responsible for "monitoring and updating risk parameters," such as "max deposit and open interest caps, asset/liability weights, [and] leverage."

85. The Futarchy DAO is "[r]esponsible for funding ecosystem projects and grants aimed at launching products adjacent to or directly related to Drift."

86. Drift's shift to be governed by a DAO was, in Drift Labs' view, "the first step towards the decentralization of Drift."

87. Today, Drift touts itself as a "decentralised exchange." In Drift's view, its "decentralization offers many benefits, including anonymity, transparency, fairness, [and] trustlessness."

88. "Trustlessness," in the world of blockchain and crypto assets, refers to a quality of a decentralized blockchain that allows users to not have to rely on trust in a third party. A trustless system has a neutral, algorithmic mechanism in place that permits participants to reach a consensus on a single truth without any one sentient authority figure and without needing to know or trust each other.

89. In calling itself a decentralized exchange, Drift explained that "execution of all trades is facilitated by smart contract technology with no human or third-party input to execute or fill trades."

90. But, in practice, it takes very few users to alter Drift's protocol. That is because Drift's Security Council has the power "to bypass ordinary tokenholder voting . . . to implement emergency proposals and actions necessary to preserve the safety or security of the Foundation, the DAO and/or Drift Protocol, its users, or the Foundation's assets. Examples of emergencies include but are not limited to security breaches, violations of core principles, network attacks, etc."

91. In addition, the Security Council has authority over protocol-level parameters and controls that affect Drift's borrow-and-lend markets including but not limited to max-deposit caps, withdrawal limits, collateral requirements, asset and liability weights, borrowing limits, and liquidation thresholds.

92. On or around March and April 2026, the Security Council was composed of five individuals.

93. To effect a change to protocol-level parameters and controls, the Security Council members had to authorize the change using what is called a "multisig," for

"multisignature." On the Solana blockchain, a multisig is an arrangement in which authority over an asset, account, or program is not controlled by a single private key, but instead requires approval from multiple designated signers before a transaction or administrative action can be executed. Drift uses the Squads multisig framework, in which actions are packaged as transactions under a proposal.

94. On or around March and April 2026, Drift required only two Security Council members to authorize a proposal containing a protocol-level administrative change in order for that change to be made. In essence, that meant that, despite Drift's decentralization claims, a grand total of two people had the power to control the Drift protocol.

The Drift Exploit

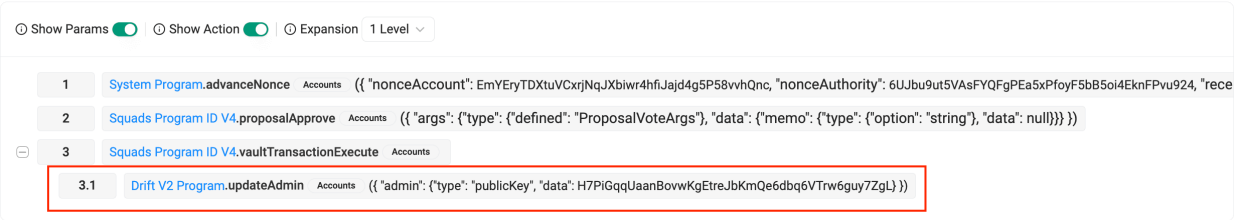
95. In or about Fall 2025, Drift contributors were approached by representatives of a quantitative-trading firm. These representatives said that they were looking to integrate their work with the Drift protocol. The individuals who interacted with Drift contributors were technically fluent, had verifiable professional backgrounds, and were familiar with how Drift operated.

96. These people created a Telegram group with Drift personnel, where the two sides had months of substantive conversations about trading strategies and potential integrations.

97. In the following months, the investor representatives worked with Drift contributors to "buil[d] a functioning operational presence inside the Drift ecosystem." The investor representatives worked with Drift contributors for several months.

98. On March 26, 2026, Drift migrated to a new system for its Security Council that required two of five Security Council members to authorize a transaction for it to go through. Moreover, Drift eliminated any "timelock" for the transactions, which meant that transactions would become effective upon being signed or entered.

99. By March 30, 2026, the investor representatives sent two durable-nonce transactions to at least two Drift Security Council members and obtained two Security Council members' signatures for each. The first transaction, committed at 2HvMSgDEfKhNryYZKhjowrBY55rUx5MWtcWkG9hqxZCFBaTiahPwfynP1dxBSR k9s5UTVc8LFeS4Btvkm9pc2C4H, created and approved the ability for the investors to have all the administrative privileges that Security Council members have for the Drift protocol.



100. The second transaction, committed at 4BKBmAJn6TdsENij7CsVbyMVLJU1tX27nfrMM1zgKv1bs2KJy6Am2NqdA3nJm4 g9C6eC64UAf5sNs974ygB9RsN1, executed the first transaction.

101. The Security Council members who signed the transactions had the ability to review the transactions before signing them. For whatever reason, the Security Council members who received the durable-nonce transactions signed them even though the durable-nonce transactions gave the investor representatives full administrative privileges on Drift.

102. Meanwhile, the investor representatives, unbeknownst to Drift or anyone else, created a crypto asset that they called Carbon Vote Token (CVT). The investor representatives then traded CVT with themselves many, many times at a consistent price of one dollar.

103. On April 1, 2026, at approximately 16:05 UTC, the investor representatives submitted the two pre-signed durable-nonce transactions, which gave them administrative control over Drift. After gaining administrative control, the individuals began altering the Drift protocol's parameters.

104. The investor representatives altered Drift to permit CVT to be used as collateral for borrowing on Drift and caused Drift to rely on CVT's trading history for its value—which the investor representatives had caused to be one dollar by trading with themselves over the preceding months.

105. The investor representatives then set CVT's borrowing limits to be extremely high and altered Drift's risk parameters to the point where the protocol would not question CVT's value.

106. After reconfiguring the protocol, the investor representatives deposited at least 500 million CVT into Drift. The protocol recognized the CVT deposit to be worth roughly $500 million.

107. By approximately 16:07 UTC on April 1, just minutes after depositing CVT on Drift, the investors withdrew at least eighteen different token types worth collectively $285 million.

108. The investors withdrew $71,415,648.66 in USDC.

109. In addition, the investors withdrew:

a. 42,721,062.00 Jupiter Perps LP (JLP) tokens, with a value of $159,329,898.68.

b. 164.35 Coinbase Wrapped Bitcoin (cbBTC) tokens, with a value of $11,321,165.24.

c. 125,000.00 Solana (SOL) tokens, with a value of $10,426,959.98.

d. 5,648,410.15 Tether USD (USDT) tokens, with a value of $5,648,410.13.

e. 5,254,016.98 USDS tokens, with a value of $5,254,126.13.

f. 2,200.59 Wrapped Ether (WETH) tokens, with a value of $4,684,896.11.

g. 45,292.21 dSOL tokens, with a value of $4,466,805.96.

h. 63.47 Wrapped Bitcoin (WBTC) tokens, with a value of $4,359,399.64.

i. 23,365,802.90 Fartcoin tokens, with a value of $4,145,112.56.

j. 33,976.51 Jito Staked SOL (jitoSOL) tokens, with a value of $3,598,696.98.

k. 2,865,380.80 syrupUSDC tokens, with a value of $3,318,311.45.

l. 21,241.62 Sanctum Infinity (INF) tokens, with a value of $2,496,178.85.

m. 17,418.92 Marinade Staked SOL (mSOL) tokens, with a value of $1,989,219.36.

n. 9,474.33 bSOL tokens, with a value of $1,015,762.26.

o. 583,980.69 Euro Coin (EURC) tokens, with a value of $678,093.68.

p. 8.61 zBTC tokens, with a value of $591,147.51.

q. 477,375.42 USDY tokens, with a value of $536,721.64.

r. 2,622,068.02 Jupiter (JUP) tokens, with a value of $429,820.12.

110. After withdrawing the non-USDC tokens, the investors used Solana-based DEX (decentralized exchange) aggregators to exchange the non-USDC crypto assets for USDC.

111. A DEX aggregator is a protocol that permits a user to swap one crypto asset for another by searching across multiple decentralized exchanges and liquidity pools for available trading routes, and then routing a token swap through one or more of those venues to complete the trade for the user. For example, JupiterSwap, a popular DEX aggregator, explains that its product "allow[s] users to exchange one token for another instantly on Solana," and that it does so by "scan[ning] liquidity pools in real time (Meteora, Raydium, Humidifi and >100 other liquidity sources), split[ting] the transaction if necessary, and optimiz[ing] the route to achieve the best overall execution."

112. As an example of how the investors used DEX aggregators, at 17:23:58 UTC on April 1, 2026, they used JupiterSwap to exchange 33,976.51 jitoSOL tokens—the exact amount they withdrew from Drift—for WSOL. JupiterSwap routed that swap through four channels: Jupiter Aggregator v6, Meteora DLMM program, Raydium Concentrated Liquidity, and Whirlpools Program. This transaction has

5RedmgHro2oPdReRx3Ht3PkzGLGeKNq7cYciz6f4vErN6KBSJd5QbPf5M89VF19Z RECcZU5kTSuqAxzPofNGFi3N as its hash signature. Then, at 17:29:19 UTC on April 1, 2026, the individuals sold that WSOL for USDC, using the JupiterSwap aggregator, at the hash signature xndcnqC8rxFCnRJx3VxyuChcho1MsSrUgx3wPe18pjqaoX2yetZtHY2CA3FQSyWii6 CHjPHr5nJ74xX8SwudC1T.

113. As illustrated in part by the above example, the investors sold the assets they withdrew from Drift for USDC on the open market in many small batches of transactions.

114. In total, the investors used DEX aggregators to sell the assets withdrawn from Drift for a total of approximately 232 million USDC, which the investors held on the Solana blockchain.

115. The investors then used Circle's CCTP to bridge the 232 million USDC from Solana to Ethereum. They did this in small batches too, beginning on April 1, 2026, at 16:27:59 UTC, and finishing at April 1, 2026, at 23:03:59 UTC. All told, the individuals moved the funds in more than one hundred discrete CCTP transactions.

116. Once the investors had bridged the full 232 million USDC to Ethereum, they used the USDC to purchase ETH on decentralized exchanges. The last such transaction occurred no earlier than 10:20 PM UTC on April 2, 2026.

Circle Fails to Freeze the USDC

117. It turned out that the "investor representatives" were not really investor representatives; they were North Korean state agents.

118. Within minutes of the investors' withdrawals of crypto assets from Drift, the broader crypto world understood that Drift had suffered an exploit and that Circle could stop it, and within hours it was clear to prudent observers that North Korea was behind the exploit.

119. At 18:15 UTC on April 1, the CEO of Helius, a prominent infrastructure platform on the Solana blockchain, tweeted "hello someone from circle reach out asap, seeing high likelihood of a potentially large exploit." He added three minutes later that "it seems drift might be getting exploited."

120. As the investors bridged their USDC from Solana to Ethereum, users on X were watching and commenting in real time. At 18:49 UTC on April 1, 2026, @lookonchain commented that "[t]he Drift Protocol exploiter is swapping the $270M+ stolen assets into $USDC, then bridging to #Ethereum to buy $ETH. So far, they have bought 19,913 $ETH ($42.6M)." At 20:14 UTC on April 1, @Cetipo commented that the "drift hacker is bridging to ETH through @circle right now."

121. On April 1, 2026, at 19:10 UTC, Drift posted on X that "We are observing unusual activity on the protocol. We are currently investigating. Please do not deposit funds into the protocol while we investigate." Then, 48 minutes later, Drift again took to X to announce that "Drift Protocol is experiencing an active attack. . . . We are coordinating with multiple security firms, bridges, and exchanges to contain the incident."

122. Upon information and belief, one of the entities that Drift tried working with on April 1 was Circle.

123. Circle had the ability to freeze, block, or otherwise restrict the movement of the USDC taken from Drift or acquired in exchange for assets taken from Drift via DEX aggregators.

124. Circle had the ability to freeze, block, or otherwise restrict the movement of all USDC bridged from Solana to Ethereum using Circle's CCTP.

125. Circle did nothing to stop the transfers.

126. Because of Circle's inaction, the North Korean agents had ample time to swap their USDC for Ether. Five hours after their exploit began (21:06 UTC), the investors still had roughly $50 million USDC that they had not exchanged for Ether. It was not until 10:20 PM UTC on April 2, 2026—more than 24 hours after the exploit began—that the investors finished swapping their USDC for Ether.

North Korea Perpetrated The Exploit, Which Circle Knew or Would Have Known Had it Exercised Due Care

127. On June 3, Drift announced that it had already engaged "Mandiant, a best-in-class cybersecurity and threat intelligence consultancy, to conduct an independent forensic analysis of the exploit," and that "Mandiant's investigation [already] conclusively attributed the attack to UNC6862, a North Korean threat group with direct ties to other state-sponsored actors involved in similar attacks on other platforms."

128. Independent blockchain-intelligence firms also attributed the exploit to North Korea. On April 2, 2026, Elliptic, a blockchain analytics and crypto asset risk-intelligence firm, announced that it had "identified multiple indicators suggesting

that the exploit of Drift Protocol is linked to the Democratic People's Republic of Korea."

129. On April 2, 2026, TRM Labs, another blockchain intelligence firm, investigated the exploit and concluded that it was "likely perpetrated by North Korean hackers."

130. Journalists from various outlets, like The Block, SecurityWeek, and CoinDesk, have also reported that North Korea was responsible for the Drift scheme.

131. North Korea is by far the most successful and prolific hacker of crypto assets in the world.

132. As the United States Department of Treasury explained in November 2025, "[t]he Government of the DPRK relies on a broad range of illicit activity, including cybercrime, to generate revenue for its WMD and ballistic missile programs and explicitly tasks its hackers to raise revenue using illicit methods. DPRK cyber actors are responsible for conducting high-level cyber-enabled espionage, disruptive cyberattacks, and financial theft at a scale unmatched by any other country. Over the past three years, North Korea–affiliated cybercriminals have stolen over $3 billion, primarily in cryptocurrency, often using sophisticated techniques such as advanced malware and social engineering."

133. In 2022, the Federal Bureau of Investigation, Cybersecurity and Infrastructure Security Agency, and the U.S. Department of the Treasury issued a joint Cybersecurity Advisory "to highlight the cyber threat associated with cryptocurrency thefts and tactics used by a North Korean state-sponsored advanced

persistent threat (APT) group since at least 2020." The Advisory explained that North Korean threat groups perform malicious activities "to generate and launder funds to support the North Korean regime."

134. According to the United States Department of Justice, "[f]or years, North Korea has exploited . . . cryptocurrency ecosystems to evade U.S. sanctions and bankroll its weapons program."

135. North Korea has long been responsible the majority of crypto hack losses. In 2025 alone, North Korea obtained $2 billion in crypto assets, or 59% of all crypto hack losses that year. In 2024, North Korea wrongfully obtained $1.3 billion in crypto assets, roughly 61% of all losses experienced that year.

136. In other words, if a crypto asset is taken in a hack or exploit, there is at least a 50% chance that the person who took it was North Korea.

137. As early as April 2022, the Federal Bureau of Investigation, the Cybersecurity and Infrastructure Security Agency, and the U.S. Treasury Department warned that "[t]he U.S. government has observed North Korean cyber actors targeting a variety of organizations in the blockchain technology and cryptocurrency industry, including cryptocurrency exchanges [and] decentralized finance (DeFi) protocols." The FBI, CISA, and Department of Treasury's joint advisory further detailed how North Korean schemes often employ "social engineering of victims" to "download trojanized cryptocurrency applications," which "enable[s] follow-on activities that initiate fraudulent blockchain transactions."

138. On September 3, 2024, the Federal Bureau of Investigation put out a public service announcement to alert the public that North Korea "is conducting highly tailored, difficult-to-detect social engineering campaigns against employees of decentralized finance ('DeFi'), cryptocurrency, and similar businesses to deploy malware and steal company cryptocurrency."

139. On February 26, 2025, the Federal Bureau of Investigation put out another public service announcement that pinned responsibility for a $1.5 billion ByBit hack on North Korea. The FBI's alert detailed that the North Korean actors "are proceeding rapidly and have converted some of the stolen assets to Bitcoin and other virtual assets dispersed across thousands of addresses on multiple blockchains." To launder the proceeds of the ByBit hack, North Korean actors used DeFi aggregators to discreetly exchange $386 million worth of assets using DeFi protocols.

140. TRM Labs reported in 2025 that, among North Korea–attributed crypto incidents causing nine-figure losses between 2023 and 2025, "multi-sig operator compromise" cases "dominate."

141. North Korean laundering patterns are distinctive. North Korean actors tend to prefer small, batched transactions concentrated below a $500,000 transfer value, whereas other bad actors tend to launder their funds in tranches above $1 million.

142. The Drift exploit and its aftermath are not the first time that North Korea–affiliated individuals have used USDC to launder crypto assets. In 2023,

North Korean operatives hacked the Atomic Wallet, withdrew approximately $100 million worth of crypto assets, swapped those assets into USDC and other stablecoins, and then swapped that USDC into other assets. As TRM Labs put it, "[t]his type of activity is a hallmark of recent" exploits by Lazarus Group, which was sanctioned for being an agency or instrumentality of North Korea.

143. Given North Korea's responsibility for a lion's share of the world's crypto heists, any reasonable participant in the crypto industry would have understood that a nine-figure exploit of a crypto protocol was probably committed by North Korea. That risk was especially apparent where, as here, the stolen assets were rapidly swapped through decentralized-exchange infrastructure, converted into USDC, and bridged across chains in a high-volume sequence of transactions—bearing a stark resemblance to other exploits perpetrated by North Korea.

144. Accordingly, when Circle did not exercise its power to freeze funds, it failed to seize assets that it knew or should have known belonged to North Korea.

Circle Explains That it Does Not Know Who Uses Its Service and Explains That Freezing Funds Would Put it in a "Moral Quandary"

145. To recap, on November 26, 2025, Circle received a restraining notice from the Kims who held a judgment against North Korea because that country kidnapped, tortured, and murdered their loved one; on April 1, 2026, North Korea obtained millions of USDC and laundered millions more using Circle's cross-chain transfer protocol; and, meanwhile, despite having the power to freeze the North Korean USDC, Circle did nothing.

146. Circle has not been shy in defending its inaction. On April 10, 2026, Dante Disparte, Circle's Chief Strategy Officer and Head of Global Policy & Operations, penned a blog post in which he stated that "when Circle freezes USDC, it is not because we have decided, unilaterally or arbitrarily, that someone's assets should be taken from them. It is because the law requires us to act." Similarly, he stated that Circle's "ability to freeze funds is a compliance obligation – exercised only when we are legally compelled by an appropriate authority, through lawful process." Disparte explained that Circle does not itself evaluate whether it is appropriate to freeze funds.

147. On April 13, 2026, Circle's founder and Chief Executive Officer, Jeremy Allaire, echoed Disparte's position. Allaire stated that "Circle has a very, very clear performance obligation under the law. Circle follows the rule of law, and we are able to undertake actions such as freezing a wallet at the direction of law enforcement or the courts." But Allaire explained that Circle would not freeze a wallet on its own volition because, in his view, Circle does not get to decide "what is the right path or not." Allaire added that Circle being freezing wallet addresses without a specific directive would put the company in a "moral quandary."

148. Circle's position that it only follows law enforcement's direction to freeze funds is the product of its stated position that it does not know who its users are. On May 27, 2026—well after being served with a restraining notice from the Kims—Circle represented, via its counsel at a hearing before Judge Margaret M. Garnett in the United States District Court for the Southern District of New York, that Circle is

not "doing any internal investigations using its own resources to try to identify wallets that are associated with North Korea."

149. Circle claimed in a sworn response to a subpoena that Circle "does not make determinations regarding whether a wallet address is linked to or associated with the Democratic People's Republic of Korea or any of its agencies, instrumentalities, or controlled entities; lacks access to information necessary to make any such determination; and does not decide whether to implement Access Denials based on any such determination by Circle."

150. Indeed, Circle has made clear that, even if it suspects that North Korea holds USDC, it will not freeze that USDC without a court order. As Circle explained in the United States District Court for the District of Massachusetts in an action involving the Drift exploit, Circle does not "block[] third parties who are not Circle customers based only on suspicion," however compelling the reason for that suspicion may be. (By "customers" Circle means people who hold Circle Mint accounts; Circle calls people who otherwise hold USDC "users.")

Aftermath

151. Drift announced that it was working to make its users whole, announcing a funded recovery framework that includes a recovery pool seeded by remaining protocol assets; funded by future exchange revenue; supported by up to $127.5 million from Tether International *S.A. de C.V.*, the company that issues USDT; and up to $20 million from other funders.

152. Now stabilized, Drift announced that it will relaunch its protocol on Solana, and it announced that it will no longer be using USDC to settle trades. Drift

decided to switch to USDT, perhaps in exchange for Tether's generous support of its recovery.

The Harm to the Kims

153. Circle, after being served with a restraining notice from terrorist victims with a judgment against North Korea, suffered the sale of hundreds of millions of USDC owned by North Korea.

154. Had Circle complied with the restraining notice and frozen the hundreds of millions of USDC owned by North Korea, Circle would have preserved those funds for the Kims, who have a judgment against North Korea, obtained leave to enforce that judgment under 28 U.S.C. § 1610(c), and registered the judgment in this District.

155. In total, Circle suffered the sale of at least $232 million worth of USDC that North Korea owned.

156. The USDC at issue in this case was owned by North Korea because North Korea obtained some of it by fraud or theft by false pretenses and obtained the rest in voluntary exchanges on the open market for assets taken by fraud or theft by false pretenses.

157. No one other than the Kims has served a writ of execution on the U.S. Marshal directed to North Korean assets held by Circle.

Claim for Relief

***Count One*: Violation of C.P.L.R. § 5222(b)**

158. Plaintiffs incorporate all prior paragraphs by reference.

159. Plaintiffs hold a valid, final, and unsatisfied money judgment against North Korea in the amount of $330,000,000, registered in this District.

160. In November 2025, the Kims served Circle with a restraining notice under N.Y. C.P.L.R. § 5222. That restraining notice put Circle on notice that the Kims have an unsatisfied judgment against North Korea, that Circle possesses North Korean assets, and that the Kims have a valid and superior interest to all assets belonging to North Korea and its agencies or instrumentalities. That restraining notice expressly applied to "all property in which [North Korea] has an interest hereafter coming into [Circle's] possession or custody," and it gave Circle the legal duty not to "make or suffer any sale, assignment, transfer or interference with any property in which" North Korea has an interest. N.Y. C.P.L.R. § 5222(b).

161. The individuals who carried out the Drift exploit and acquired and laundered the USDC were acting on behalf of the North Korean government. The USDC they acquired and held was property in which North Korea, the Kims' judgment debtor, had an interest, and thus fell within the scope of the Kims' restraining notice, because North Korea owned that property.

162. On April 1, 2026, Circle was aware, or should have been aware had it been taking reasonable care, that North Korea owned 232 million USDC.

163. Circle has the power to unilaterally freeze the USDC balance of any blockchain wallet address, and Circle has the power to cause the USDC balance of any blockchain wallet address to equal any amount.

164. Circle is in control of all assets sent through CCTP.

165. Circle, despite having the power to unilaterally freeze the USDC balance of any wallet addresses, and despite its control of CCTP, freezes the USDC balance

of wallet addresses only if a government specifically requests it and allows any person or entity to use CCTP without restriction.

166. On April 1, Circle suffered the sale, assignment, or transfer of approximately 232 million USDC. Worse, Circle actively facilitated that sale, assignment, or transfer by providing its CCTP service to North Korea.

167. Circle thus violated the restraining notice.

168. Circle's violation was willful, or at least reckless. Before the transactions, and as the transactions occurred, Circle had actual knowledge that it had been served with a restraining notice concerning North Korean property; knew or should have known that the Drift exploit was committed by North Korea; and observed, as did the public, the laundering and bridging of the stolen USDC in real time. Circle nonetheless made a deliberate decision not to act.

169. Had Circle complied with the restraining notice by freezing the USDC through access denial and by declining to operate CCTP to move the restrained property, the property would have been preserved and ordered turned over to the Kims. Because Circle did not, the property was exchanged for other assets that are beyond the Kims' reach.

170. As a direct and proximate result of Circle's violation of the restraining notice, Plaintiffs have been damaged in the amount of the restrained property that Circle transferred or suffered to be dissipated.

Prayer for Relief

Plaintiffs respectfully request:

- Compensatory damages against Defendants jointly and severally in an amount to be proven at trial, but no less than $232,000,000, plus prejudgment interest, costs, attorneys' fees where recoverable, and such other relief as the Court deems just and proper, and
- Any other relief deemed just and proper.

Respectfully submitted,

/s/ Charles Gerstein
Charles Gerstein
Jeremy Shur (*pro hac vice* application forthcoming)
GERSTEIN HARROW LLP
1319 F Street NW, Suite 301
Washington, DC 20004
charlie@gerstein-harrow.com
(202) 670-4809

/s/ Jason Harrow
Jason Harrow
GERSTEIN HARROW LLP
401 Park Ave. S. 10th Floor
New York, NY 10016
jason@gerstein-harrow.com
(323) 744-5293

/s/ Robert Tolchin
Robert Tolchin
THE BERKMAN LAW OFFICE, LLC
829 E. 15th Street, Suite Seven
Brooklyn, New York 11230
rtolchin@berkmanlaw.com
(718) 855-3627

Attorneys for Plaintiffs