IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

HAN KIM, YONG KIM, YONG HWA CHUNG KIM, CHUNG KOOK KIM, DANI BUTLER, BRIAN ERDSTEIN, KARENE ERDSTEIN, MAYAN ERDSTEIN, CHAIM KAPLAN, RIVKA KAPLAN, REUVEN KAPLAN, THEODORE GREENBERG, MAUREEN GREENBERG, JARED SAUTER, DVORA KASZEMACHER, CHAYA ALKAREIF, CHAYIM KUMER; LAURIE RAPPEPORT, MARGALIT RAPPEPORT, AVISHAI REUVANE, and ELISHEVA ARON, Plaintiffs, v. RAILGUN DAO, Defendant.	Case No. 26-CV-179 JURY TRIAL DEMANDED

COMPLAINT

Preliminary Statement

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 in this Court; and in 2025 the Reverend's widow, Yong Hwa Chung Kim, and two of his children, Dani Butler and Chun Kook Kim, won a $366,000,000 money judgment against North Korea in this Court.

2. In July and August of 2006, Hezbollah, which has been designated a terrorist organization by the United States, attacked civilians in Northern Israel using rockets. That attack was materially supported by North Korea and resulted in severe losses to the remaining Plaintiffs and their families. In 2016, the remaining Plaintiffs won a $169,439,132 money judgment against (among others jointly and severally) North Korea.

3. Plaintiffs have recently begun attempting to execute their judgments against crypto assets that North Korea acquires through its extensive, world-wide hacking, extortion, and money-laundering campaign. To do this, Plaintiffs have served writs of execution on U.S. companies that have frozen North Korean crypto assets, with which U.S. persons are forbidden to transact under federal law. *E.g.*, *Kim v. Democratic People's Republic of Korea*, No. 25-MC-527 (S.D.N.Y. Nov. 26, 2025). Plaintiffs' ability to execute their judgment thus depends on companies complying with federal law: Companies transferring money must register with the federal

government, must verify the identities of their customers, and, when that verification reveals that the customers are sanctioned entities like North Korea, must freeze any funds in their possession and decline further business.

4. Defendant Railgun DAO (pronounced "dow") is a purported "decentralized autonomous organization" operating within an international criminal network that forms the Railgun Enterprise, whose affairs Railgun DAO operates through a pattern of illegal money transmission in violation of 18 U.S.C. § 1960 and money laundering in violation of 18 U.S.C. § 1587. Railgun DAO runs a business through which users can disguise the origins of crypto transactions through technology called zero-knowledge proofs, which federal courts have held to be illegal money transmission. Railgun DAO claims that it never takes custody of users' funds during the laundering process, but this is false, and regardless would still be illegal, *see United States v. Storm*, No. 1:23-cr-00430 (KPF) (S.D.N.Y. Sep. 26, 2024) (denying motion to dismiss Section 1960 case against operator of crypto mixing service). And although Railgun DAO purports to be "decentralized" and "autonomous"—and, therefore, free of any legal accountability—it is in fact a general partnership formed by the holders of its "governance" token. *See Samuels v. Lido DAO*, 757 F. Supp. 3d 951, 960 (N.D. Cal. 2024); *Sarcuni v. bZx DAO*, 664 F. Supp. 3d 1100, 1109 (S.D. Cal. 2023).

5. In 2023, and again in 2025, the harms that the money-services laws and the Racketeering Influenced Corrupt Organizations Act ("RICO") exist to prevent materialized. In December of 2022, North Korean hackers stole hundreds of millions

of dollars' worth of crypto assets. And on February 21, 2025, North Korean hackers stole a record-breaking $1.5 billion worth of crypto assets. On both occasions North Korea laundered the stolen assets through Railgun, and during those laundering transactions Railgun had the power—and was required by clear federal law—to freeze the funds. Had Railgun done so, Plaintiffs would have served writs of execution on it and the funds would be theirs. Instead, Railgun transferred North Korean funds representing more than 70% of Railgun's total business and earning Railgun at least $260,000 in fees for the illegal transaction. *See* Javier Paz, *Did Digital Currency Group Profit From $60 Million in North Korean Crypto Money Laundering*, FORBES, Oct. 31, 2024 (explaining that Railgun DAO collected $260,000 in fees for laundering $60 million worth of assets for North Korea and that Railgun DAO partner Digital Currency Group, Inc., specifically profited).

6. Plaintiffs bring this action against Railgun DAO for conducting the affairs of the years-running and still operating Railgun Enterprise, which is a hierarchical network of people and companies operating a criminal scheme with the central aim of making money by facilitating money laundering, and for negligence. Those criminal schemes are what the money-transmitting laws exist to prevent: A sanctioned, authoritarian regime moving assets around the global financial system without being frozen and seized by Plaintiffs as compensation for the grievous harm of illegally abducting, torturing, and killing their loved one.

Parties

7. Plaintiff Yong Seok Kim is the brother of the late Reverend Dong Shik Kim. Plaintiff Yong Hwa Chung Kim is the widow of the Reverend Kim. Plainiff Han

Kim is the son of Reverend Kim. And Plaintiffs Dani Butler and Chung Kook Kim are children of Reverend Kim.

8. Plaintiffs Brian Erdstein, Karene Erdstein, Mayan Erdstein, Chaim Kaplan, Rivka Kaplan, Reuven Kaplan, Theodore Greenberg, Maureen Greenberg, Jared Sauter, Dvora Kaszemacher, Chaya Alkareif, Chayim Kumer; Laurie Rappeport, Margalit Rappeport, Avishai Reuvane, and Elisheva Aron are U.S. nationals who live or lived in Israel at the time of Hezbollah's 2006 rocket attacks and were injured by, killed in, or lost family members in those attacks.

9. Defendant Railgun DAO is a general partnership governed by votes of a crypto token called RAIL. It is headquartered in London.

Jurisdiction and Venue

10. This Court has subject-matter jurisdiction under 28 U.S.C. § 1331 because this Action arises under federal law. This Court may exercise supplemental jurisdiction over the common-law claim in this Action under 28 U.S.C. § 1367.

11. This Court may exercise personal jurisdiction over Railgun DAO under Federal Rule of Civil Procedure 4(k)(2) because (as explained in more detail below) (a) this case arises under federal law, (b) Railgun DAO is not subject to the jurisdiction of any state court, and (c) Railgun DAO's criminal conduct targeted the United States, and resulted in harm here, and is therefore consistent with the Due Process Clause of the Fifth Amendment to the United States Constitution.

The Kidnapping and Murder of Reverend Dong Shik Kim

12. 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).

13. 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. DRPK,* 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.*

14. 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 Kaplan Plaintiffs' Death and Injury Resulting From North Korea's Sponsorship of Terrorism

15. Between July 12, 2006, and August 14, 2006, Hezbollah—which is a designated foreign terrorist organization under U.S. law—fired thousands of rockets and missiles at civilians in northern Israel. *Kaplan v. Hezbollah et al.*, ECF No. 57, No. 09-cv-646 (D.D.C. July 23, 2014).

16. The rockets that landed in Israel had been sent to Hezbollah in the years prior to 2006 by North Korea, *id.*, and North Korean agents trained Hezbollah agents in military tactics for decades, *id.*

17. The *Kaplan* plaintiffs are U.S. nationals who lived in Israel during Hezbollah's 2006 rocket attacks and were injured or killed. Their individual injuries

were evaluated by a special master, whose conclusions were adopted (in large part) by the U.S. District Court for the District of Columbia. *Kaplan*, ECF No. 83 (D.D.C. Sept. 30, 2016).

Plaintiffs' Efforts to Recover

18. 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).

19. 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.

20. 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.

21. 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).

22. 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).

23. 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 crypto companies that possess North Korean assets in that district, *id.*

24. 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.*

25. In 2009 and 2010, the *Kaplan* Plaintiffs sued Hezbollah, Iran, DPRK, and many Iranian agencies and instrumentalities in the United States District Court for the District of Columbia. *Kaplan*, No. 09-cv-646; *Kaplan v. The Central Bank of the Islamic Republic of Iran*, No. 10-cv-483 (D.D.C.).

26. All of the defendants defaulted and the Court found by clear and convincing evidence that (among other parties) DPRK was a designated state sponsor of terrorism at the relevant time and that the Hezbollah attacks were an act of terrorism for which DRPK was responsible. *Kaplan*, ECF No. 57 at 14–15.

27. The Court referred the *Kaplan* Plaintiffs' damages claims to a special master and, upon receiving the master's report, entered a judgment for $38,161,966.67 in compensatory damages and $131,277,165.34 in punitive damages.

28. Plaintiffs' collection efforts against those companies are ongoing.

29. All Plaintiffs have agreed to proportional distribution of any proceeds from collection of the judgments against crypto companies.

Zero-Knowledge Cryptography And The Ethereum Blockchain

30. 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.

31. The standard hash function used to maintain most blockchains takes an arbitrarily long string of values and creates from it a unique, usually 40-character output. The standard hash function works well for this purpose because (a) it is very easy to run, and therefore very easy to verify; (b) it is impossible to reverse; and (c) because changing one bit of information in the input completely changes the output. For example, here is the standard hash function's output for the text of the poem "Ozymandias," by Percy Bysshe Shelley, as found on the Poetry Foundation's website: 84959c6489ca0029046d60cf3e4e06b820c064e13948bbfb90cdfe510149ae8c.

32. Armed with nothing but the 40-character hash output, a reader would be completely lost; there is no known algorithm that can take a hash output and find the input text, even if given millennia to run on the most sophisticated machines available. But armed with the hash output and the statement "this is the hash of the text of Shelley's 'Ozymandias,' as found on the Poetry Foundation's website," a reader could verify the statement easily: Simply copy the text of the poem at https://www.poetryfoundation.org/poems/46565/ozymandias, paste it into the standard SHA256 Generator at https://tools.keycdn.com/sha256-online-generator, and generate the same hash. So long as the input text is not altered at all, running that function will generate that precise output. By contrast, even a single change—like changing one space or line break—will generate a hash output that bears no discernable relationship to the original.

33. A zero-knowledge proof is achieved when one person (usually called "the prover") can prove to another person (usually called "the verifier") knowledge of a piece of information without revealing that piece of information.

34. In a standard example, Victoria, the verifier, holds one red and one green object that are otherwise identical. She cannot tell the difference between them because she is red–green colorblind. She asks the prover, Pete, to prove to her that the objects are indeed different colors but without revealing which is red and which is green. To do this, Pete first asks Victoria to hold up the ball in her right hand for him to see and keep the ball in her left hand behind her back and hidden. He then asks her to return the visible ball to her back; to choose to switch the balls between hands or not, without revealing to Pete whether she switched; and then to again hold up the ball in her right hand and keep the ball in her left hand hidden. Pete will then tell Victoria if she switched the balls between hands or not. Pete will of course immediately be able to recognize a switch or stay, because he can see the difference between red and green; Victoria will know if Pete is right or not, because she knows if she switched the balls from right hand to left; but Victoria will gain no knowledge of which is red and which is green, because Pete is not revealing that information and Victoria is color-blind. Although Pete could guess correctly whether the balls were switched 50% of the time if this game were performed only once, if the two repeat this game many times, the odds grow infinitesimally small that Pete is guessing and so Pete can prove to Victoria that the balls are indeed different colors without revealing which is which. *See Two Balls and The Colour-Blind Friend*, in *Zero Knowledge*

Proofs, WIKIPEDIA, https://en.wikipedia.org/wiki/Zero-knowledge_proof (last accessed Dec. 10, 2025).

35. Although today the term "blockchain" usually refers to exclusively electronic systems like Bitcoin and Ethereum used for trading crypto assets, blockchains originally operated on paper, and at least one still does. In the early nineties, a company called Surety created a blockchain for timestamping digital documents. To timestamp a document, one created a hash of the document and sent it to the company, which would create a hash of the hash associated with a unique time value. The company would then batch each stamped document into another hash value and link it to all prior batched transactions through a similar function. In this way, the company could prove to anyone who produced a document the exact time that it was stamped. And because if anyone altered a single bit in the whole string of transactions the output would be totally different, third parties could easily verify that hashes represented accurate timestamps.

36. But this process relied on trust in *the company*. After all, the company could simply backdate prior hash results by adding false timestamps. To protect against this, Surety ran a weekly notice in the New York *Times* with that week's hash value. This way, if at some time in the future someone wanted to alter a legacy entry, a person seeking to verify the transaction could check it against publicly available and practically immutable records to ensure its authenticity. A blockchain ledger, then, cannot be reversed or altered.

37. Inspired by this analog technology, a person with the pseudonym Satoshi Nakamoto created the Bitcoin blockchain in 2009. Bitcoin's purpose is to publicly and immutably record transactions in its eponymous crypto asset. Since then, thousands of blockchains have emerged. The blockchain at issue in this case is called Ethereum, and its native asset is called Ether.

The Ethereum Blockchain and Decentralized Autonomous Organizations

38. In 2015, Vitalik Buterin and others working with him created Ethereum. Ethereum at its founding worked just like Bitcoin, except Ethereum could more easily allow each block to record transactions other than simple transfers. Indeed, in Buterin's vision, Ethereum is a "virtual machine"—Ethereum's distributed ledger is theoretically capable of running any program that a computer could run. (This property is called "Turing completeness," after cryptographer Alan Turing.)

39. Users participate in the Ethereum blockchain using wallet addresses, which are digital representations of the sending and receiving ends of transactions on the blockchain. To create a wallet address on the Ethereum blockchain, a user first generates something call a "private key," which is typically a random combination of letters and numbers. The user then runs that combination through a hash function, which generates a unique 40-character "public key," to which "0x" is appended as a prefix, generating a 42-character wallet address. Because of the hash-function's properties discussed above, someone who knows the private key can instantly generate the public key, but someone who knows the public key can never figure out the private key. This enables a common form of zero-knowledge proving. One Ethereum blockchain user can prove she has the private keys to a wallet address

easily by inputting the private key and generating a trivial transaction, which proves that the user has the private key but does not reveal any knowledge about the key itself.

40. Because Ethereum is Turing complete, it allows for the creation of innovative new collective computing activities. For example, Ethereum users could create programs called "smart contracts," which, as their name suggests, automatically execute transactions when certain conditions are triggered. These smart contracts can together create "protocols," which are the rough equivalent of software on a personal computer. Some smart contracts are immutable, meaning that no one can ever change how they operate on the blockchain; others are mutable and can be altered or removed from the blockchain.

41. 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.

42. 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—such as the RAIL token at issue here—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.

Crypto Mixing Businesses

43. As explained above, Ethereum transactions are verifiable because they are public. Although this allows for Ethereum's novel forms of economic activity without centralized intermediaries, it also creates an obvious problem: Lots of people, but particularly money launderers and criminals, do not want all of their transactions to be seen by the whole world.

44. Crypto mixers arose to mitigate the problems caused by the public visibility of blockchain transactions. The most famous mixer, called Tornado Cash, was created in 2019 by Roman Storm, Alexey Pertsev, and Roman Semenov.

45. Tornado Cash operates by using a zero-knowledge proof to obscure the source of a crypto transaction. Imagine someone wants to obscure his ownership of 100 ETH using Tornado Cash. To do this, the user sends 100 ETH to a Tornado cash smart contract, which returns to the user a private key that functions like a receipt to withdraw 100 ETH from the smart contract to any wallet address. Because the withdrawal address need not be the deposit address, and because the smart contract functions as a zero-knowledge proof—which reveals nothing about the depositor except that the person with the receipt is the depositor—the smart contract breaks

any public link between the deposit and withdrawal addresses. *See, e.g.*, *Van Loon v. U.S. Dep't of the Treasury*, 122 F.4th 549, 557–58 (5th Cir. 2024) (explaining Tornado Cash mechanics).

46. But Tornado Cash depends on a critical mass of users simultaneously using the service. In the example above, the link between the depositor and withdrawer is obvious because only one transaction took place. But if there are, say, a thousand depositors and a thousand withdrawers each laundering 100 ETH, the odds of discovering who is who are infinitesimal.

47. Crucially, Tornado Cash's smart contracts are immutable. They will run identically as long as the Ethereum blockchain is in existence.

48. In 2024, the United States indicted Storm and Semenov for, among other things, operating an illegal money-transmission business in violation of 18 U.S.C. § 1960 and money laundering in violation of 18 U.S.C. § 1957. *See* Daniel Barabander, Amanda Tuminelli & Jake Chervinsky, *Through the Looking Glass: Conceptualizing Control and Analyzing Criminal Liability For Unlicensed Money Transmitting Businesses Under Section 1960*, INT'L ACADEMY OF FIN. CRIME LITIGATORS WORKING PAPERS, at 21 (2024).

49. Storm moved to dismiss the indictment on the ground that the immutable nature of the Tornado Cash smart contracts meant that no one received assets from anyone during the mixing process—no one took possession of the assets, and the protocol was "non-custodial"—and therefore no one could have done any money transmission. The Court denied the motion, agreeing with the government's

argument that an entity transmits money even if it does not take possession, as, say, a fiber optic cable "transmits" energy without "possessing" the energy in a particular sense. *See id.* at 9 n.8 (citing Transcript of Oral Ruling on Defendant Storm's Motion to Dismiss in *United States v. Storm*, No. 1:23-cr-00430 (KPF) (S.D.N.Y. Sep. 26, 2024)). Storm was convicted of violating Section 1960 and is appealing to the Second Circuit, where he will surely argue that he could not have violated that law because his smart contracts were non-custodial.

Railgun DAO Is a General Partnership Operating an Illegal Money-Transmission Business and Committing Money Laundering

50. In 2021, four cryptographers—Emmanuel Goldstein[1], Kieren (Kai) Mesquita, Alan Scott, and Andrey Kravchenko—founded Railgun DAO, in London, with the goal of operating a crypto mixing service even more effective than Tornado Cash. From the start, Railgun's founders claimed that the business was, as Tornado Cash is, "non custodial." But in Railgun's case that claim is false.

51. Railgun's system functions essentially like Tornado Cash except that users can anonymously transact their receipts *with each other*. This makes mixing exponentially more difficult to trace. For example, even if there are many Tornado Cash users at a given time, if one user moves a very large volume of assets through the mixer it will be obvious on the other side who conducted the transaction—if, say, one deposit and one withdrawal are ten times larger than all the others on a given

[1] In George Orwell's *1984*, the Leon Trotsky–inspired principal enemy of the State of Oceania was named Emmanuel Goldstein. *See* George Orwell, *Nineteen Eighty-Four* 894 (1949). It seems likely that Goldstein is a pseudonym for the founder of Railgun, but possible that he shares the name of the fictional character.

day, one could reliably conclude that those two transactions correspond to each other. But in Railgun, a user can, for example, deposit many different assets using many different wallets; trade them with himself, or trade them with other Railgun users; and then withdraw them to many different wallets. This enables extremely effective money laundering.

52. Railgun is accessible from the United States.

53. Many U.S. users transact on Railgun.

54. Since its founding, as of the time of this filing, Railgun has laundered more than $4 billion worth of assets.

55. Unlike Tornado Cash's smart contracts, Railgun's smart contracts can be altered in any way by the person who controls the wallet address that created them.

56. The person who controls the wallet address that created the Railgun smart contracts can send the assets that users move through Railgun to any other address the creator chooses.

57. That person, therefore, has possession of the assets in the Railgun crypto mixing service.

58. The wallet address that controls the Railgun smart contracts is, in turn, controlled by the votes of a token called RAIL, which is the governance token of Defendant Railgun DAO.

59. Railgun DAO charges fees for each withdrawal transaction. Those fees are sent to wallet addresses where they can be collected pro rata by the holders of RAIL.

60. The fee-collection process is manually executed by externally owned accounts operated by Railgun's collaborators (who are members of the Railgun Enterprise, but not necessarily the Railgun DAO, as explained in greater detail below). *See* CHAINARGOS, *Is it Wrong to Make Money Laundering For North Korea? A Case Study on How Railgun Investors Collected Fees Made From Laundering Funds for North Korea*, Nov. 5, 2024.

61. These externally owned accounts are not controlled by the Railgun DAO. *Id.*

62. When Goldstein, Mesquita, and Kravchenko created RAIL, they programmed a maximum supply of 100,000,000 RAIL tokens on Ethereum. (Small amounts of RAIL trade on other blockchains not relevant to this case.)

63. In January of 2022, a Connecticut-based firm called Digital Currency Group (DCG) purchased 5 million RAIL tokens in exchange for $10 million, valuing the Railgun business—of whose fees DCG stood to collect a share—at $200 million.

64. Although Railgun claims on its website that "[t]here is no RAILGUN company – RAILGUN is a system of smart contracts supported by fully-decentralized RAILGUN DAO governance," a lawyer named Edward Fricker is described in Forbes as having "advised on the deal on behalf of Railgun." Fricker claimed in Forbes that DCG sent some funds "to a fully decentralized DAO treasury in support of [the]

project," and that the treasury does not have "an[] admin[istrator] key or mutisig[nature wallet]" controlling the treasury. *See* Paz, *supra*. The treasury is, instead, controlled by the holders of RAIL.

65. The holders of RAIL work together to run Railgun DAO as a phenomenally profitable, illegal business. Railgun DAO's fees, which are currently 25 basis points per transaction, have already exceeded $100 million and it has no material expenses.

66. For a business like Railgun, the size of the fee is the critical business decision: Make the fee too high, and users will go elsewhere; make it too low and potential profits are lost.

67. Railgun DAO makes that crucial decision by ongoing votes of RAIL tokenholders. *See* Paz, *supra* (identifying at least two votes by DCG).

68. Railgun DAO is thus a collection of people and entities jointly operating the Railgun business for profit.

69. No one has incorporated Railgun DAO anywhere or registered it with any government for limited-liability protection.

70. Under the laws of the United Kingdom of Great Britain and Northern Ireland, a "[p]artnership is the relation which subsists between persons carrying on a business in common with a view of profit." *Partnership Act of 1890*, 53 & 54 Victoria 1 (1890).

71. The standard for determining a general partnership in the absence of a written agreement is substantially the same in the UK as it is in California. *Samuels*

v. Lido DAO, 757 F. Supp. 3d 951, 960 (N.D. Cal. 2024); *Sarcuni v. bZx DAO*, 664 F. Supp. 3d 1100, 1109 (S.D. Cal. 2023).

72. Railgun DAO's founders and core investors, including but not limited to DCG, actively operate the Railgun together for profit.

73. Railgun DAO is, therefore, a general partnership under UK law.

74. Railgun DAO knows that much of its profit comes from people trying to disguise the source of the proceeds of illegal wire fraud (through hacking), sanctions evasion, and financing of terrorism.

75. This fact is widely publicized and obvious from the structure of Railgun's business: Although there are lawful uses of a crypto-mixing service, the vast majority of uses are illegal. *E.g.*, *Van Loon*, 122 F.4th at 558; *see also* MULTILATERAL SANCTIONS MONITORING TEAM, THE DPRK'S VIOLATION AND EVASION OF UN SANCTIONS THROUGH CYBER AND INFORMATION TECHNOLOGY WORKER ACTIVITIES 43 (2025) ("DPRK cyber actors sometimes rapidly mix tokens before consolidating them in unhosted wallets. DPRK actors continued to use Wasabi Wallet, CryptoMixer, Tornado Cash, JoinMarket, and Railgun during the reporting period.").

The Railgun Enterprise

76. Railgun DAO is one part of an international hierarchical organization that runs illegal money-transmission businesses and launders money. This Complaint refers to that organization as The Railgun Enterprise.

77. Railgun DAO relies on non-partners to collaborate in the operation of the illegal money-services business. Specifically, non-partners create the wallet

interfaces through which users interact with Railgun and non-partners collaborate with Railgun to provide Railgun's illegal services.

78. Railgun's website indeed reads "Notice: This is an independent info site about RAILGUN smart contracts, run by enthusiasts and evangelists. Nobody is in charge of RAILGUN itself."

79. The Railgun Enterprise was founded in or around 2021 and it is still operating.

80. The Railgun Enterprise operates through the ongoing commission of many related criminal acts including operating an illegal money-services business in violation of 18 U.S.C. § 1960, and money laundering in violation of 18 U.S.C. § 1956.

81. Specifically, the Railgun DAO's crypto mixing service is an unlicensed money-transmission business. *United States v. Storm*, No. 1:23-cr-00430 (KPF) (S.D.N.Y. Sep. 26, 2024) (denying motion to dismiss Section 1960 case against operator of crypto mixing service).

82. The Railgun Enterprise, through the acts of Railgun DAO and others, commits money laundering because they "conduct . . . financial transaction[s] . . . knowing that the property involved . . . represents the proceeds of some form of unlawful activity" and "knowing that the transaction is designed in whole or in part . . . to conceal or disguise the nature, the location, the source, the ownership, or the control of the proceeds of the proceeds of [many different criminal violations]." 18 U.S.C. § 1956(a).

In January of 2023, North Korea Uses Railgun to Deprive Plaintiffs of Their Right to Collect This Court's Judgment

83. North Korea does not maintain diplomatic or economic relations with much of the world but nonetheless maintains a very expensive nuclear-weapons program.

84. To fund this program, as well as basic services, North Korea has turned to a widespread and extremely aggressive campaign of cyber-attacks. *See* MULTILATERAL SANCTIONS MONITORING TEAM, THE DPRK'S VIOLATION AND EVASION OF U.S. THROUGH CYBER AND INFORMATION TECHNOLOGY WORKER ACTIVITIES 11 (2025).

85. These efforts include hacks of crypto exchanges, *id.* at 7; ransomware attacks on hospitals to extort money, *id.* at 11; and hacks of American companies, *id.* at 15.

86. Although "DPRK actors and their launderers constantly change their laundering tactics," "there were certain platforms on which they consistently relied . . . [including] Railgun." *Id.* at 43, 44.

87. In late 2022, crypto hackers working for North Korea stole hundreds of millions of dollars' worth of crypto assets from a service called Harmony Bridge.

88. Between January 13 and January 14, 2023, the Lazarus Group, which is an agency of the North Korean government, sent more than $60 million worth of crypto-assets through Railgun DAO's crypto-mixing service. *See* CHAINARGOS, *supra*.

89. Had Railgun DAO complied with 18 U.S.C. § 1960 (which forbids the operation of an illegal money-services business), and 18 U.S.C. § 1957 (which forbids

money laundering), Railgun DAO would have frozen North Korea's assets as they passed through the Railgun DAO smart contracts and, therefore, Railgun DAO's possession on January 13 and 14, 2023.

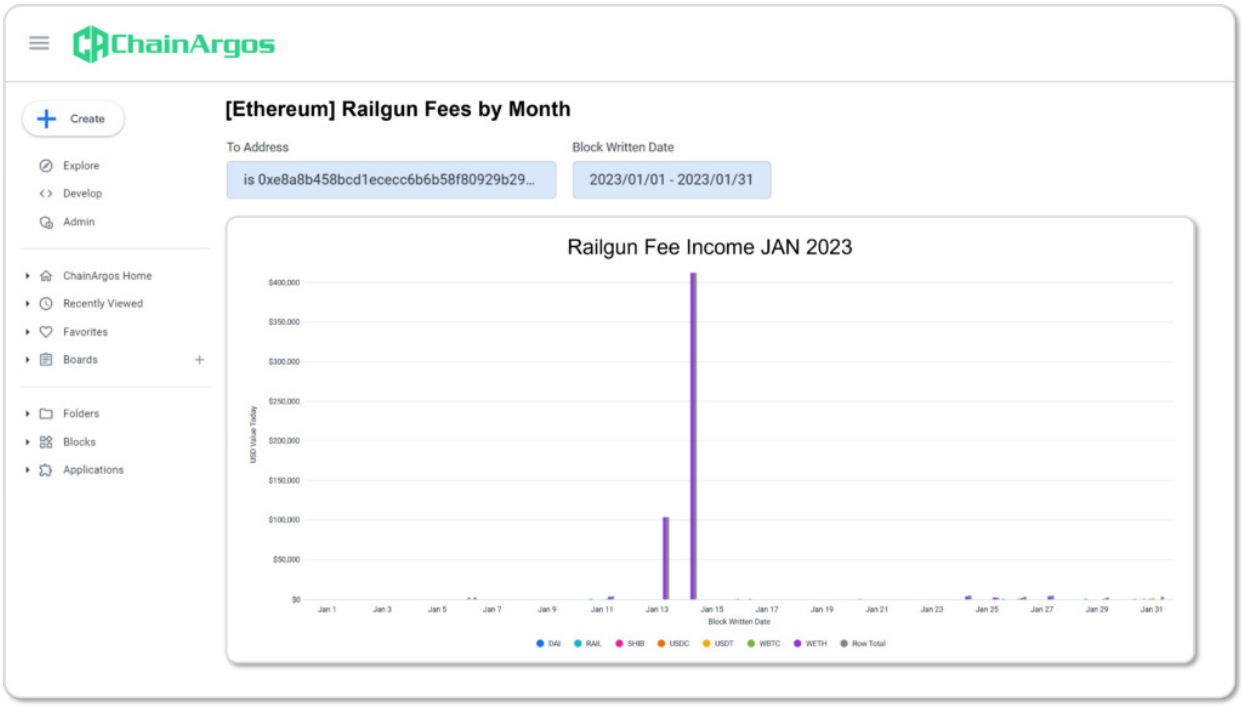
90. Plaintiffs are currently attempting to execute their judgment against crypto companies that, unlike Railgun DAO, comply—or at least attempt to comply—with U.S. law and have therefore frozen property attributable to North Korea. *See, e.g.*, *Kim v. DPRK*, 25-MC-527 (S.D.N.Y. 2025).

91. Had Railgun DAO frozen North Korea's assets, Plaintiffs could have easily, and would have in fact, executed their judgment against it by, among other things, registering the judgment in the United States District Court for the District of Connecticut and seeking to compel the turnover of North Korean property held by Railgun DAO partner DCG in that district.

92. Had Railgun DAO frozen North Korea's assets, Plaintiffs could have easily, and would have in fact, additionally domesticated their judgment in the United Kingdom and executed it against North Korean property held by Railgun DAO partners there.

93. The frustration of a judgment creditor's right to collect on a U.S. judgment is a cognizable domestic injury to property under RICO. *e.g.*, *Yegiazaryan v. Smagin*, 599 U.S. 533, 537 (2023), *Kruse v. Repp*, 611 F. Supp. 3d 666, 717 (S.D. Iowa 2020).

94. The January 13 and 14 transactions represented approximately 1,000 times more assets than Railgun DAO had ever processed in a single day before, as the following chart, *id.*, reveals:



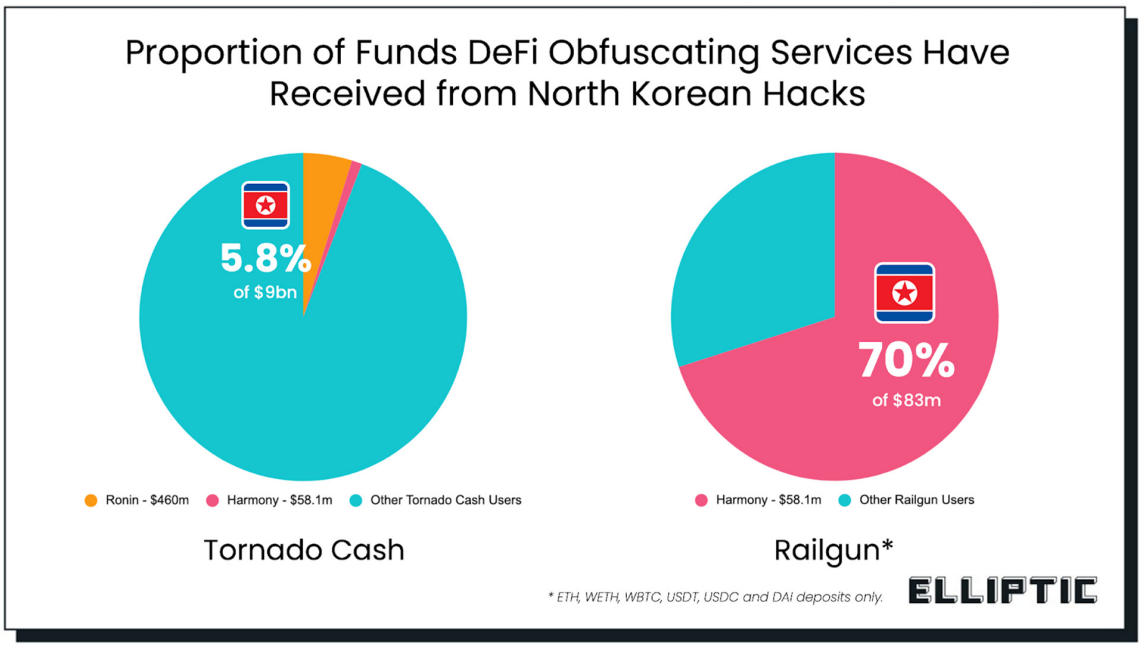
95. On January 20, externally owned addresses associated with the founders of Railgun DAO deployed a new, upgradeable smart contract to collect fees from the Railgun service.

96. That same day, approximately $500,000 worth of crypto assets was transferred from the Railgun Treasury Wallet to an externally owned wallet, which promptly sent those assets to the contract processing Railgun's fee revenues. *Id.*

97. The $500,000 represented the proceeds of North Korea's use of Railgun DAO's crypto mixing service.

98. Shortly thereafter, many RAIL tokenholders claimed their share of the fees Railgun DAO generated by laundering North Korean assets.

99. North Korean money laundering is, in fact, Railgun's core business. As of June 19, 2024, approximately *seventy percent* of Railgun's transaction volume was publicly and obviously attributable to North Korea:



100. In May 2023, Railgun DAO created a system it calls "private proof of innocence." Under this system, a user must submit a zero-knowledge proof that its wallet address is not on a specific list published by the United States Department of the Treasury.

101. This system is worthless: Because users needs not show anything about their wallets' previous transactions, all a sanctioned launderer needs to do is create a new wallet before using Railgun to obscure its transactions. Creating a new wallet address on Ethereum is free and trivially easy.

102. Railgun DAO created the private-proof-of-innocence system to whitewash its obvious money laundering.

103. Indeed Railgun, using a Twitter (now X) account that lists itself as "RAILGUN—Private & Anonymous DeFi," denied reports that North Korea used Railgun at all, writing in response to a tweet citing FBI reports of North Korean money laundering on Railgun that "This is not true and it's false reporting. Firstly, the [Lazarus] group is blocked from using the RAILGUN system by the 'Private Proofs of Innocence' system which went live over a year ago. Secondly, it was a mistaken, false allegation in the first place."

104. Both of these statements are lies: Railgun knew that North Korea can easily get around its proofs-of-innocence system and Railgun knew that the vast majority of its revenue was attributable to North Korean hackers laundering money.

105. In June 2023—more than six months after North Korea's publicly reported hacking and publicly reported laundering of funds using Railgun DAO's crypto-mixing service—DCG claimed its share of the fees. *See* Pax, *supra*.

106. DCG had previously claimed its fees promptly after they were available. *Id.*

107. Railgun DAO, through its partners DCG and the core team members and founders of Railgun DAO, knew that the $60 million worth of assets laundered through its crypto-mixing service were the proceeds of wire fraud and sanctions evasion, and yet they claimed their fees anyway.

In February of 2025, North Korea Again Uses Railgun to Deprive Plaintiffs of Their Right to Collect this Court's Judgment

108. Railgun DAO—despite knowing that its service's largest user (by a huge margin) was North Korea, and despite knowing that North Korea used the service to

launder the proceeds of wire fraud and sanctions evasion—continued to operate its illegal business.

109. And the harms that the money-services laws, the money-laundering laws, and RICO all exist to prevent happened yet again.

110. In February of 2025, North Korea, through its instrumentality the Lazarus Group, pulled off the largest crypto hack on record, stealing nearly $1.5 *billion* worth of Ethereum, a crypto asset, from a Dubai-based exchange called ByBit.

111. North Korea immediately began to launder the stolen assets through centralized exchanges, bridges, and crypto mixers.

112. In February and early March of 2025, after having transferred the initial stolen assets several times between several purchasers, North Korea used Railgun DAO's crypto mixing service to launder $1,733,062 worth of crypto assets.

113. Had Railgun DAO frozen North Korea's assets, Plaintiffs could have easily, and would have in fact, executed their judgment against it by, among other things, registering the judgment in the United States District Court for the District of Connecticut and seeking to compel the turnover of North Korean property held by Railgun DAO partner DCG in that district.

114. Had Railgun DAO frozen North Korea's assets, Plaintiffs could have easily, and would have in fact, additionally domesticated their judgment in the United Kingdom and executed it against North Korean property held by Railgun DAO partners there.

Claims for Relief

Count One: Violation of the Racketeering Influenced Corrupt Organizations Act (RICO), 18 U.S.C. § 1962(c)

115. Plaintiffs incorporate all prior paragraphs here.

116. RICO, 18 U.S.C. § 1962(c), makes it "unlawful for any person employed by or associated with any enterprise engaged in, or the activities of which affect, interstate or foreign commerce, to conduct or participate, directly or indirectly, in the conduct of such enterprise's affairs through a pattern of racketeering activity or collection of unlawful debt."

117. The Railgun Enterprise exists for the purpose of operating an illegal money-transmitting businesses in violation of 18 U.S.C. § 1960 and to commit money laundering in violation of 18 U.S.C. § 1957. Conduct violating these laws constitutes racketeering under 18 U.S.C. § 1961.

118. The Railgun Enterprise is an association-in-fact enterprise governed by Railgun DAO's founders, their associates, and Railgun DAO.

119. Defendant Railgun DAO participates in the affairs of the Enterprise through an ongoing, continuous pattern of illegal money-transmission under 18 U.S.C. § 1960 and money laundering under 18 U.S.C. § 1957.

120. Railgun DAO's racketeering activity proximately caused Plaintiffs to lose money or property: Plaintiffs' judgment debtor used Railgun DAO's illegal money-transmission business to launder funds and Railgun DAO possessed funds on

behalf of Plaintiffs' judgment debtor that they would have been required to turn over to Plaintiffs had they not engaged in a pattern of racketeering.

121. Railgun DAO is headquartered in London and is a general partnership under the laws of the United Kingdom because it is a group of people jointly carrying on a business for profit without registering for limited liability with any government.

122. In the alternative, Railgun DAO has no physical headquarters and is instead a general partnership under the law of this forum, the District of Columbia, because it is a group of people jointly carrying on a business for profit without registering for limited liability with any government.

***Count Two*: Negligence**

123. Plaintiffs incorporate all prior paragraphs by reference.

124. Railgun DAO was at all relevant times subject to federal and state laws requiring it to register its crypto mixing service as a money-transmission business.

125. The purpose of the federal and state laws requiring such registration is to prevent exactly what happened here: The laundering of assets by a state sponsor of terrorism frustrating the ability of the victim to get redress.

126. Railgun DAO thus had a duty to Plaintiffs to take reasonable measures in compliance with applicable laws to prevent their services being used to launder the assets of state sponsors of terrorism.

127. In the alternative, Railgun DAO had a duty to take reasonable precautions to prevent their services from being used for money laundering by state sponsors of terrorism.

128. Railgun DAO breached that duty *per se* by completely failing to comply with any applicable laws and regulations.

129. In the alternative, Railgun DAO breached its duty of reasonable care by failing to take *any* steps—let alone adequate steps—to prevent its services from being used for money laundering by state sponsors of terrorism.

130. Railgun DAO's breach of its duty caused Plaintiffs to be unable to collect a valid judgment against North Korea that, absent the breach breach, they would have been able to collect through writs of execution and similar procedural devices against Defendants.

131. Plaintiffs would have been able to collect assets valued at $61,733,062 and instead they collected nothing.

Prayer for Relief

Plaintiffs respectfully request:

- An award of treble damages under 18 U.S.C. § 1964(c) against Defendant Railgun DAO in the amount of $185,199,186, and
- An award of reasonable attorneys' fees under 18 U.S.C. § 1964(c), or, in the alternative,
- An award of compensatory damages against Railgun DAO in the amount of $61,733,062, and
- Any other relief that this Court deems just and proper.

Respectfully submitted,

/s/ Charles Gerstein
Charles Gerstein
GERSTEIN HARROW LLP
1629 Columbia Road NW, Suite 302
Washington, DC 20004
charlie@gerstein-harrow.com
(202) 670-4809

/s/ Jason Harrow
Jason Harrow
GERSTEIN HARROW LLP
12100 Wilshire Blvd. Ste. 800
Los Angeles, CA 90025
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