Jason Harrow
(Cal. Bar No. 308560)
GERSTEIN HARROW LLP
3243B S. La Cienega Blvd.
Los Angeles, CA 90016
jason@gerstein-harrow.com
(323) 744-5293

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF CALIFORNIA

CLÉMENT OMÉTAK, CHRISTIAN SARCUNI, PEDRO CUNHA, ALEXANDER LLOYD, SKLIAR VIKTOR, MARC SIMON, PILICI RUSTAM, SHUAI LU, EDISON HO, KIRO ALEKSANDROV, JONAS WERNECKE, PAOLO LEITE, MIRAS ISSAKHOV, SOORAJ NARAYANAN, HÉCTOR ALBERT GONZÁLEZ TERRÓN, MANNU SINGH, MARC-JULIEN LIE, SIMON SCHMID, and DANIELE PENNA, on behalf of themselves and other similarly situated,

Plaintiffs,

vs.

bZx DAO, KYLE KISTNER, TOM BEAN, HASHED INTERNATIONAL LLC, AGE CRYPTO GP LLC, OOKI DAO, LEVERAGEBOX LLC, and bZeroX LLC,

Defendants.

Case No. 22-cv-0618-LAB-DEB

FIRST AMENDED COMPLAINT

CLASS ACTION
JURY TRIAL DEMANDED

The Hon. Larry A. Burns

Date: June 27, 2022

Preliminary Statement[1]

1. This case arises from the use of novel cryptocurrencies, but it is legally straightforward. First, the Plaintiffs in this case deposited cryptocurrency with a protocol called bZx whose creators told users that they need not "ever worry about . . . getting hacked or [anyone] stealing [their] funds." Second, despite this promise of security, the bZx protocol in fact lacked reasonable safeguards and was hacked and the Plaintiffs' funds stolen. Worse, the hack and subsequent theft were not the result of some complex scheme or unknown vulnerability in the code, but rather due to bZx's simple negligence: by bZx's own account, one of the bZx developers fell for a so-called email "phishing" scam that permitted access to key passphrases that then permitted the hackers to drain Plaintiffs' accounts because the protocol had not yet implemented security measures that its operators knew were reasonably necessary to protect the protocol. The end result was a total theft of about $55 million in US Dollar equivalents: approximately $1.7 million in total from these named plaintiffs, and a substantial portion of the remainder from a proposed class of similarly situated users.

2. The Defendants are jointly responsible for making good to the Plaintiffs. Indeed, the protocol itself apparently acknowledges its responsibility for the loss, though instead of making good, it has put in place a woefully inadequate "compensation plan" where Plaintiffs could receive IOUs with no real hope of repayment. Since the protocol has failed to pay back what was taken as a result of the protocol's negligence, all of these Defendants are jointly and severally responsible for making good

[1] This Amended Complaint is filed with the written consent of all served Defendants. *See* Fed. R. Civ. P. 15(a)(2).

to the Plaintiffs. That is because the bZx protocol purports to be a so-called DAO, or de-centralized autonomous organization, that lacks any legal formalities or recognition. There is another phrase in American law for that kind of arrangement: general partnership. That means *each* of the partners is jointly and severally liable to the Plaintiffs and must make good on the full amount of its debts.

Parties

3. Plaintiff Clément Ométak is a bZx user who lost approximately $92,000 in the hack. He is a citizen of France.[2]

4. Plaintiff Christian Sarcuni is a bZx user who lost approximately $110,000 in the hack. He is a citizen of Italy.

5. Plaintiff Pedro Cunha is a bZx user who lost approximately $30,000 in the hack. He is a citizen of Portugal.

6. Plaintiff Alexander Lloyd is a bZx user who lost approximately $30,000 in the hack. He is a citizen of Canada and the United Kingdom.

7. Plaintiff Skliar Viktor is a bZx user who lost approximately $450,000 in the hack. He is a citizen of Ukraine.

8. Plaintiff Marc Simon is a bZx user who lost approximately $80,000 in the hack. He is a citizen of France.

9. Plaintiff Pilici Rustam is a bZx user who lost approximately $800 in the hack. He is a citizen of the Republic of Moldova.

[2] To prevent additional fraud and to minimize the risk of connecting individuals with specific wallet addresses that may hold additional currencies, this Complaint will not reveal the precise loss amount, cryptocurrency token type, and wallet address for each individual plaintiff. Those details are unnecessary here, but they can be disclosed using sufficient safeguards at the appropriate time in this litigation.

10. Plaintiff Shuai Lu is a bZx user who lost approximately $305,000 in the hack. He is a citizen of China. (Lu was named in the original complaint as “Daniel Lu,” using his English name; this is the same person.)

11. Plaintiff Edison Ho is a bZx user who lost approximately $25,000 in the hack. He is a citizen of the People’s Republic of China and resident in Hong Kong.

12. Plaintiff Kiro Aleksandrov is a bZx user who lost approximately $150,000 in the hack. He is a citizen of Bulgaria.

13. Plaintiff Jonas Wernecke is a bZx user who lost approximately $55,000 in the hack. He is a citizen of Germany.

14. Plaintiff Paolo Leite is a bZx user who lost approximately $14,000 in the hack. He is a citizen of Brazil.

15. Plaintiff Miras Issakhov is a bZx user who lost approximately $116,000 in the hack. He is a citizen of Kazakhstan.

16. Plaintiff Sooraj Narayanan is a bZx user who lost approximately $127,000 in the hack. He is a citizen of India.

17. Plaintiff Héctor Albert González Terrón is a bZx user who lost approximately $14,000 in the hack. He is a citizen of Spain.

18. Plaintiff Mannu Singh is a bZx user who lost approximately $44,000 in the hack. He is a citizen of Canada.

19. Plaintiff Marc-Julien Lie is a bZx user who lost approximately $1,000 in the hack. He is a citizen of Canada.

20. Plaintiff Simon Schmid is a bZx user who lost approximately $30,000 in the hack. He is a citizen of Switzerland.

21. Plaintiff Daniele Penna is a bZx user who lost approximately $180,000 in the hack. He is a citizen of Italy.

22. Defendant Kyle Kistner is an individual residing in or near San Diego, California. He is the co-founder of the bZx protocol and a member of the bZx DAO and general partnership.

23. Defendant Tom Bean is an individual residing in Alpharetta, Georgia. He is the co-founder of the bZx protocol and a member of the bZx DAO and general partnership.

24. Defendant Hashed International LLC is a Wyoming limited-liability company with its principal place of business in San Francisco, California. Hashed is an investor in the bZx protocol and a member of the DAO and general partnership.

25. Defendant AGE Crypto GP, LLC is a Nevada limited-liability company with its principal place of business in Los Angeles, California. AGE Crypto is an investor in the bZx protocol and a member of the DAO and general partnership. (AGE Crypto GP, LLC erroneously appeared in the original caption without the "GP.")

26. Defendant bZx DAO is a purported Decentralized Autonomous Organization that is a general partnership. The partnership is headquartered in or near San Diego, California, where its co-founder and primary decisionmaker lives and works. Alternatively, it is a

27. Defendant Ooki DAO is a purported Decentralized Autonomous Organization that is a general partnership. The partnership is headquartered in or near San Diego, California, where its co-founder and primary decisionmaker lives and work.

28. Defendant Leveragebox LLC is a Delaware Limited Liability Company that has a principal place of business in San Diego, California. Leveragebox LLC operated the Fulcrum trading platform and may continue to operate that platform.

29. Defendant bZeroX LLC is a Delaware Limited Liability Company that has a principal place of business in San Diego, California. bZeroX created the bZx protocol and, until August 2021, controlled the protocol.

Jurisdiction and Venue

30. This Court has subject matter jurisdiction over this action pursuant to 28 U.S.C. § 1332(a) because all Plaintiffs are foreign domiciliaries and all Defendants are U.S. domiciliaries, and pursuant to 1332(d)(2)(A) because this is a class action in which the matter or controversy exceeds the sum of $5,000,000, exclusive of interest and costs, and in which the minimal diversity requirements of that provision have been met.

31. Venue is proper in this District under 28 U.S.C. § 1391(b)(2) or (b)(3).

32. This Court has general jurisdiction over Defendants Kistner, Hashed International LLC, AGE Crypto GP LLC, bZeroX LLC, Leveragebox LLC, bZx DAO, and Ooki DAO.

33. This Court has specific personal jurisdiction over all Defendants because they purposefully entered into a general partnership controlled from California and because they are partners in a general partnership with at least one member that has conducted partnership business in California and they have directed at least some of their partnership activities at California.

34. The Court also has personal jurisdiction over bZx DAO and Ooki DAO because unincorporated entities take on the citizenship of each of their members. *See Carden v. Arkoma Associates*, 494 U.S. 185 (1990). Because at least one member of each DAO is a citizen of

California, the DAOs are citizens of California and are subject to this Court's personal jurisdiction

Background on Cryptocurrency And The Products At Issue

35. A cryptocurrency is a form of digital asset based on a network that is distributed across a large number of computers. Cryptocurrencies, at least right now, are not issued by central governments or authorities. Bitcoin is the most well-known cryptocurrency, but there are thousands of others. The value of some cryptocurrencies fluctuates with respect to the U.S. Dollar and all other fiat currencies. Other cryptocurrencies, like U.S. Dollar Coin, are so-called stablecoins because their value is pegged to a fiat currency—for U.S. Dollar Coin, the U.S. Dollar.

36. Different cryptocurrencies are typically designated by three- or four-letter symbols, like stock tickers. Bitcoin's is BTC. U.S. Dollar Coin is USDC. Coins at issue in this case include ETH, BZRX, OOKI, and several others.

37. The system by which a network of computers securely and publicly records the transactions of a given cryptocurrency is called a blockchain. There are several different blockchains that record transactions of a variety of different cryptocurrencies. The blockchains at issue in this case are called Ethereum, Polygon, and the Binance Smart Chain. Each of these blockchains has a "native" cryptocurrency, in which the computers operating the network are rewarded, and supports other cryptocurrency transactions as well. Ethereum's native cryptocurrency, for example, is Ether (ticker: ETH).

38. A cryptocurrency token is a unit of a specific virtual currency. These tokens are fungible and tradeable.

39. Cryptocurrency tokens are held via a virtual wallet. The wallet is secured using cryptography and can typically be accessed only with a lengthy passphrase, which is a form of strong password. The wallet has an address—typically a seemingly random of string of letters and numbers—that can be published on the blockchain without revealing the identity of the wallet-holder.

40. For cryptocurrency to reasonably function in a sophisticated marketplace, users must transact between currencies, crypto- or otherwise; must be able to lend and borrow; and must be able to earn some rate of return on stored assets. Transactions like these are usually executed in the traditional economy through third parties like banks. But cryptocurrency transactions are increasingly conducted through "DeFi" applications. DeFi stands for "Decentralized Finance" and uses emerging technology to remove third-parties, like banking institutions, from financial transactions. Thus, using DeFi protocols—such as bZx, at issue here—users can engage in complicated transactions using cryptocurrencies, like lending or borrowing, without interacting with banks or other established, regulated intermediaries.

41. DeFi protocols are almost always governed as "Decentralized Autonomous Organizations," or "DAOs." In a DAO, there is no formal corporate structure, no explicit liability protection, and no distinction between, say, managers and directors, or between general and limited partners. Instead, holders of specific tokens—such as the BZRX token at issue here—have governance rights that allow holders 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 dividends. Holders of governance tokens thus may participate in the governance of a protocol, they have a potential claim on its profits, and they share responsibility for its liabilities.

The bZx Protocol And Its Promises

42. bZx is a DeFi platform describing itself as "a protocol for tokenized margin trading and lending." According to its website, "[i]t is a financial primitive for shorting, leverage, borrowing, and lending that empowers decentralized, efficient, and rent-free" transactions on the blockchain.

43. There are two "products" built on the bZx protocol. The one primarily used in this case is called Fulcrum, which the protocol's website says is a "DeFi Margin Lending and Trading Platform." Fulcrum permits users to lend tokens and earn interest on those tokens when other people borrow them, like how a U.S. bank or savings-and-loan association takes deposits, lends them out, and pays back depositors with interest.

44. The other product built on the bZx protocol is Torque, which provides for "Indefinite-term Loans with Fixed Interest Rates."

45. The simplest way to use these products is to navigate to the website bZx.network and then select the desired product, either Fulcrum or Torque. Assuming a user selects Fulcrum, the user then must choose which blockchain to use to record and execute transactions. (As mentioned above, bZx products work on three blockchains: Ethereum, Polygon, and Binance Smart Chain.) After selecting a blockchain network, a user can connect a wallet and deposit cryptocurrency or

otherwise interact with the protocol. On Fulcrum, users can deposit and earn interest on a variety of different types of cryptocurrencies.

46. bZx repeatedly and prominently touts its security features. bZx claims that Fulcrum is "non-custodial," which means that "whether lending or trading, [users] maintain control of [their] own keys and assets." This, supposedly, makes the platform especially secure.

47. In reality, a single password was sufficient to access *all* of the client funds on two of the three blockchains on which Fulcrum operated. The holder of that password, therefore, had custody of the client funds and had a legal duty as custodian to exercise reasonable care to protect the funds.

48. Additional promises of safety abound. A website section called "how safe is it?" lists four reasons to think the protocol is quite safe, including "Audited Smart Contracts" and an "Insurance fund." An entire tab called "security" is linked at the very top of the Fulcrum platform, and the headline that appears on that linked page is "Security Is Our Priority." That page says that "bZx is committed to ensuring the security of user funds." It lists several steps the protocol has taken to supposedly ensure the security of deposited cryptocurrency tokens.

49. That page, in turn, links to another page explaining bZx's "World Class Security." That page claims that, as of September 2020, "all issues found ha[d] been confirmed or fixed."

50. Perhaps the most succinct summary of bZx's security promises can be found directly on bZx's homepage. Under the graphic "Minimized Risk," bZx claims, "Whether you're a lender or borrower, you stay in control of your keys. Never worry about opaque centralized exchanges getting hacked or stealing your funds."

The November 5. 2021 Hack And Theft

51. What bZx claimed users need not worry about happened on November 5, 2021. That day, the protocol was hacked and funds were stolen from named Plaintiffs and the class members. The following facts about the hack are taken primarily from bZx's own statements.

52. On November 5, 2021, according to the anonymous bZx DAO member, "[a] bZx developer was sent a phishing email to his personal computer with a malicious macro in a Word document that was disguised as a legitimate email attachment, which then ran a script on his Personal Computer. This led to his personal mnemonic wallet phrase being compromised."

53. A "phishing attack" occurs when a malicious actor, masquerading as a trusted entity, dupes a victim into opening an email, instant message, or text message with dangerous contents. The recipient is then tricked into clicking a malicious link or opening a malicious attachment, which can lead to the installation of a virus, the freezing of the system, or, as here, the revealing of sensitive information like passwords.

54. According to the blog post from an anonymous DAO member, the November 5 "phishing attack was similar to one that affected another user recently named 'mgnr.io' . . . . This attack granted the hacker access to the content of the bZx Developer[']s wallet, and also the private keys to the BSC and Polygon deployment of bZx Protocol. After gaining control of BSC and Polygon the hacker drained the BSC and Polygon protocol, then upgraded the contract to allow draining of all tokens that the contracts had given unlimited approval."

55. Or, put more simply (according to a news report), "A hacker stole millions after a developer at bZx, a crypto company, fell for a phishing attack." The estimated theft was $55 million in U.S. Dollar value.

56. The developer was working for the bZx DAO at the time of the hack. His possession of the private keys (or passcodes or passphrases) that enabled possession of users' funds and that were stolen by the hackers was within the scope of his employment because those keys were his only means of accessing the protocol and making necessary changes to it.

57. The problem, as the company reported it, was that—despite the protocol's promises to the contrary—the protocol's implementation on two of the three blockchains on which it operated was insecure. That is, the protocol was designed to work on the Ethereum blockchain, the Polygon blockchain, and the Binance Smart Chain blockchain, but only its operations on the Ethereum blockchain were secure.

58. Here is how bZx itself put it shortly after the theft, with Plaintiffs' explanatory comments in brackets. (Punctuation has been slightly cleaned up.)

> The BSC and Polygon implementation administrative private keys have not yet been transferred to the DAO yet. [As of the date of the hack, an important measure for securing secret information had not yet been taken with respect to the Binance Smart Chain and Polygon blockchains.]
>
> Therefore the BSC and Polygon Deployment did not have the protection of the DAO. [The Binance

> and Polygon blockchains were less secure than the Ethereum blockchain.]
>
> When the developer's private keys were compromised in a phishing attack, the hacker gained access to not only the individual developer's personal funds, but also gained access to the bZx deployment on BSC and Polygon. [When the bZx developer's password was hacked, the hacker was able to steal individual funds from that developer and also steal funds of others that used the Binance and Polygon blockchains because the important security step to secure those blockchains had not yet been taken.]
>
> From there, the hacker was able to upgrade the contract and perform an attack on users of the protocol and funds held within the protocol. [Once the hackers had the password, they could use it to drain funds from bZx users on the Binance and Polygon blockchains.]

59. The report also stated that some things "went right." In particular, the "bZx treasury on Ethereum DAO is safe on the Ethereum deployment because [bZx] had already fully decentralized there." In other words, funds held on the Ethereum blockchain were not impacted because the protocol's operations on that blockchain were more secure than the Polygon and Binance blockchains. That is cold comfort to these Plaintiffs, but it means that all funds that had used the protocol were not entirely wiped out, and it shows conclusively that bZx failed to meet its *own* standards for safety, let alone reasonable industry standards.

60. The stolen tokens appear at this point to be unrecoverable.

61. This was not the first hack of this protocol. In 2020, bZx suffered three hacks with total losses of approximately $9 million, although $8 million was apparently recovered eventually. And, as bZx itself mentioned, the phishing attack that one of the developers fell for was similar to another one that the protocol had already received. Despite these incidents, bZx, Fulcrum, and their partners and members did not alter their promises of security or invulnerability from hacks. Rather, they failed to take reasonable steps to secure the platform and prevent the theft that actually occurred.

The Inadequate Compensation Plan And Move To Ooki

62. The bZx DAO has recognized its responsibility to compensate the victims of the theft. Soon after the hack, a user named BadriNat sketched out a first proposal on bZx's community forum for bZx to compensate victims of the attack. BadriNat appears to be a person named Badri Natarajan, an attorney specializing in blockchain legal and regulatory risk management. In the post, BadriNat stated that he was not a member of the bZx development team and was not being paid by the DAO. It is unclear if BadriNat had spoken to, been in contact with, or been compensated by any of the named defendants here or other key members of the bZx DAO and general partnership described below.

63. After some discussion, a proposal was put to a vote for members of the DAO. BZRX tokenholders were eligible to vote. On November 21, 2021, a compensation plan was adopted without any "no" votes.

64. The compensation plan was divided into two parts. In the first part, the DAO determined that all who lost the BZRX token would be compensated in full directly from the bZx DAO by either replacing that

token on a 1-to-1 ratio with what had been lost or, for some users, replacing the lost tokens with a version of BZRX token that would fully vest over time. Full compensation was made possible in part because the BZRX token is issued by the bZx DAO itself, and there were some unassigned BZRX tokens in the DAO's "treasury," which is the equivalent of a general partnership's shared bank account. None of the Plaintiffs or proposed class held meaningful stakes of BZRX token and so did not benefit from this plan.

65. In the second part of the plan, the bZx DAO issued new "debt tokens"—essentially, IOUs—that the DAO promised would be bought back using 30% of the future revenue that comes into the DAO, which, as a practical matter, means 30% of the revenue generated through certain transaction fees that the protocol charges users. Although bZx promised that "in this way, [the DAO] will eventually reimburse all losses suffered as a result of the incident," the word "eventually" must be given a very generous reading: at the current buyback rate, full repayment will take thousands of years.

66. In December 2021, several weeks after the hack, the bZx protocol encouraged users to transfer to a successor platform called Ooki. Many BZRX tokens were transformed into OOKI tokens; an Ooki DAO was created, with control rights given to those OOKI tokenholders (many of whom received OOKI tokens as a direct result of the conversion from BZRX); and the Ooki platform was launched with much of the same functionality as Fulcrum and Torque. Thus, while Fulcrum, Torque, and bZx still exist, Ooki is a direct successor to that network and platform.

The bZx DAO And Successor Ooki DAO Are General Partnerships

67. The bZx Protocol and the platforms built on top of it, including Fulcrum, were originally controlled at least in part by two LLCs: bZeroX LLC and Leveragebox LLC. These LLCs appear to have been largely controlled by co-founders Tom Bean and Kyle Kistner.

68. In August 2021, several months before the hack, bZx outlined plans to transition both revenue from the protocol and control of aspects of the protocol to the bZx DAO. That is, "armed with tens of millions of dollars, [the DAO] will take up the task of maintaining the protocol, building new products, marketing the brand, and managing the community." At that time, the bZx treasury held approximately $80 million worth of assets. When the transition was completed "the legal entity bZeroX LLC [ceased] to exist, and in its place the DAO . . . remain[ed]." Still, despite the change, "[t]he core team [maintained] a strong desire to continue working on the project and welcomes this new chapter as the start of something even greater than what came before."

69. The bZx DAO is controlled by those who hold the BZRX token. That is, "the keys to the bZx treasury, [were] turned over to the DAO, and bZx tokenholders [became] the main drivers of governance and decision making of the bZx platform going forward." The way this works is that bZx tokenholders—that is, those who own the BZRX token—can both suggest and vote on governance proposals. If the proposals pass, the DAO takes the action. In that way, the tokenholders could, for instance, implement the compensation plan whereby BZRX tokenholders were fully compensated from the DAO treasury for the hack but Plaintiffs and

others who used different tokens on the protocol were given IOUs but little chance of repayment.

70. The Ooki DAO is a direct successor DAO to bZx because many BZRX tokens were directly converted to OOKI tokens in December 2021.

71. Given their structures and the way they operate, the bZx and Ooki DAOs are general partnerships among tokenholders. That is, they are associations of two or more persons (the tokenholders and investors), to carry on as co-owners (of the bZx and Ooki DAOs, with shared control of the bZx and Ooki treasury funds, among other assets), of a business for profit (the bZx and Ooki protocols and related products built on them, with the profits being the right to funds held in the respective treasuries). Although DAOs seem novel, many legal observers who have analyzed them have reached the same conclusion.[3]

Each Defendant's Partnership Activities

72. Defendant Kyle Kistner is a self-professed co-founder of the bZx protocol and is still listed as being employed at bZx. During the relevant time, he participated in decisionmaking of the bZx protocol and its successor the Ooki protocol. Kistner made many of the decisions from in or around San Diego, California, where he lives.

[3] For example:

- "[T]he U.S. legal system must clarify the legal status of these organizations and as such should classify the DAO as a general partnership." Laila Metjahic, *Deconstructing the DAO…*, 39 Cardozo L. Rev. 1533, 1536 (2018).
- "[A] DAO's decision to not create a legal entity does not offer protection from responsibilities that may arise in the operation of a DAO. From a legal perspective, when two or more individuals are engaged in even a tenuous business relationship, the imputed structure is that of a general partnership." David Kerr & Miles Jennings, *A Legal Framework for Decentralized Autonomous Organizations v2*, A16Z White Paper, https://bit.ly/3jYfILt.
- "[E]xisting corporate law dictates that what the members of [a] DAO have formed is a general partnership." Dave Rodman, *DAOs: A Legal Analysis*, JD Supra (Apr. 1, 2021) https://bit.ly/3jYjnZI.

73. Defendant Tom Bean is a self-professed co-founder of the bZx protocol. During the relevant time, he participated in the decisionmaking of the bZx protocol and its successor the Ooki protocol. He was aware that Kistner moved to California and intentionally communicated with Kistner in California about partnership business.

74. Defendant Hashed International LLC is a stated investor in the bZx protocol. During the relevant time, it and its members or principals participated in the decisionmaking of the bZx protocol and its successor the Ooki protocol. It has publicly disclosed that it "supported the [bZx] team," "actually witness[ed] how this team solved" a security issue, and invested in the protocol and the BZRX token.

75. Defendant AGE Crypto GP, LLC is a stated investor in the bZx protocol. During the relevant period, it and its members or principals participated in the decisionmaking of the bZx protocol and its successor the Ooki protocol. It has stated offices in Reno, Nevada, but it is likely controlled by its founder from in or around Los Angeles, California.

76. Defendant bZx DAO is a purported Decentralized Autonomous Organization that is a general partnership. Its members determine the governance of the bZx protocol, supervise those responsible for securing the protocol, and making distributions from the treasury, among other tasks.

77. Defendant Ooki DAO is a purported Decentralized Autonomous Organization that is a general partnership. Its members determine the governance of the Ooki protocol, supervise those responsible for securing the protocol, and making distributions from the treasury, among other tasks. The Ooki protocol is a direct successor to the bZx protocol.

78. Defendant Leveragebox LLC operated the Fulcrum trading platform during the relevant time and may continue to operate that platform.

79. Defendant bZeroX LLC created the bZx protocol and, until August 2021, controlled the protocol. At that time, it purportedly transferred its assets to the bZx DAO.

Class Action Allegations

80. Plaintiff proposes to move to certify the following class: All people who delivered cryptocurrency tokens to the bZx protocol and had any amount of funds stolen in the theft reported on November 5, 2021, except for people whose only cryptocurrency stolen was the BZRX token.

81. The proposed class meets Federal Rule of Civil Procedure 23's requirements, called respectively numerosity, commonality, typicality, adequacy, predominance, and superiority.

Numerosity

82. The class is so large that joinder of all parties would be impracticable. The total loss amount was approximately $40 million, and it is estimated to have been held by thousands of different people.

Commonality

83. There are questions of law and fact common to members of the class.

84. The questions of fact common to the members of the classes include, without limitation, how the theft occurred; what steps the bZx protocol should have taken to secure the funds; what steps the bZx protocol took to secure the funds; and whether the bZx protocol and other general partners have acknowledged responsibility for the loss.

85. The questions of law common to the members of the classes include, without limitation, whether the Defendants were negligent, whether they formed a general partnership, and whether the general partnership is responsible as *respondeat superior* for the negligence of the developer whose pass-phrase was stolen in the hack.

Typicality

86. The Plaintiffs each delivered some amount of cryptocurrency to the protocol using the Binance Smart Chain or Polygon blockchains and subsequently had the cryptocurrency stolen during the November 5, 2021, phishing attack through no fault of their own. The claims of the named plaintiffs are, therefore, typical of—indeed identical to—the claims of all the unnamed class members.

Adequacy

87. As explained above, the named Plaintiffs' claims are identical to the claims of other class members, and there are no known conflicts of interest with any other class member.

88. The named Plaintiffs, especially Christian Sarcuni, whom Plaintiffs propose as lead plaintiff, will adequately protect the interests of absent class members.

89. The Plaintiffs propose Gerstein Harrow, LLP as class counsel.

90. Both founding partners of Gerstein Harrow have significant experience litigating complex cases, including major class actions, and cases involving cryptocurrency.

91. Charles Gerstein has, among other things, served as lead counsel in a class action case against the City of Houston that recently settled for $1.175 million, and has served as counsel or lead counsel in several complex class actions seeking prospective relief against public

entities and officers throughout the country. As a law clerk for the U.S. District Court of the Southern District of New York and the U.S. Court of Appeals for the Second Circuit, Gerstein advised the courts on several complex class-action cases.

92. Jason Harrow has litigated complex cases on behalf of New York State and its agencies as an Assistant Solicitor General, as an associate at the national law firm Davis Wright Tremaine, LLP, and as lead counsel in the U.S. Supreme Court in *Colorado Dep't of State v. Baca*, No. 19-518 (argued May 13, 2020; decided July 6, 2020). As a law clerk for the U.S. District Court for the Southern District of New York and the U.S. Court of Appeals for the Ninth Circuit, Harrow advised the courts on several complex class-action cases.

93. In addition, Gerstein and Harrow are lead counsel in a different major case regarding cryptocurrency, *Kent v. PoolTogether Inc.*, docketed as 21-cv-6025 in the U.S. District Court for the Eastern District of New York. That case presents some overlapping issues with this one, including regarding the liability of DAOs and their general partners. Their experience there can thus inform their experience in this matter.

94. Class counsel will fairly and adequately represent the interests of the class.

Predominance and Superiority

95. The questions of fact and law common to the class predominate in this Action over any questions affecting only individual members of the class.

96. In fact, there will be no individual questions of law or fact for any of the members of the class and damages will be trivially easy to assess: Each class member delivered money to bZx and then lost it in the

November 5, 2021, theft. Those are the only requirements necessary to succeed on these claims.

97. The classes in this case will be easily managed and ascertained. The bZx protocol and the blockchains used keep a publicly accessible record of every transaction any user has ever executed, and each account is assigned a unique identification code. Thus, although the Defendants may not know the legal identities of most of their users, they can communicate with (and therefore ensure the provision of notice to) all their users; they can (and indeed have) determined the amount each is owed; and they can pay the money it owed them easily by crediting the accounts associated with each identification number.

Claims for Relief

Count One: Negligence

98. Plaintiffs incorporate all prior paragraphs by reference.

99. The bZx protocol and its partners owed Plaintiffs a duty to maintain the security of the funds deposited using the bZx protocol, including but not limited to putting in place procedures such that a phishing attack on a single developer would not result in a multi-million dollar theft; it breached that duty; and Defendants' actions in breaching their duty were the proximate and but-for cause of an injury—namely, the loss of funds deposited with the bZx protocol.

100. The bZx protocol and its partners also owed Plaintiffs a duty to supervise developers and those working on the protocol such that important passwords or security details could not be revealed through the actions of a single developer; it breached that duty; and Defendants' actions in breaching their duty were the proximate and but-for cause of an injury—namely, the loss of funds deposited with the bZx protocol.

101. The unnamed developer working on behalf of bZx owed Plaintiffs a duty to secure against malicious attacks passwords that could result in theft of millions of dollars of assets; the developer breached that duty; and the developer's actions in breaching that duty were the proximate and but-for cause of an injury—namely, the loss of funds deposited with the bZx protocol. The Defendants answer as *respondeat superior* to the negligence of the developer they employed or contracted with.

102. Defendants are therefore jointly and severally liable for Plaintiffs' injuries.

Prayer for Relief

Plaintiffs respectfully request:

- An order certifying an appropriate class;
- An award of compensatory damages to Plaintiffs and the proposed class in an amount that fully compensates Plaintiffs and the proposed class for all lost funds;
- Punitive damages as appropriate;
- Allowable costs and attorney's fees pursuant to Federal Rule of Civil Procedure 54, or any other applicable provision or principle of law; and
- Any other relief deemed just and proper.

Respectfully submitted,

/s/ Jason Harrow
Jason Harrow
(Cal. Bar No. 308560)
GERSTEIN HARROW LLP
3243B S. La Cienega Blvd.

Los Angeles, CA 90016
jason@gerstein-harrow.com
(323) 744-5293

Attorneys for Plaintiffs