IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

BYBIT TECHNOLOGY LIMITED,

Plaintiff,

v.

DEMOCRATIC PEOPLE'S REPUBLIC OF KOREA; DPRK RECONNAISSANCE GENERAL BUREAU; LAZARUS GROUP; and JOHN DOES 1-20,

Defendants.

Case: 1:26-cv-02173 JURY DEMAND
Assigned To : Unassigned
Assign. Date : 6/18/2026
Description: TRO/PI (D-DECK)

COMPLAINT

Plaintiff Bybit Technology Limited ("Bybit" or "Plaintiff"), by and through its undersigned counsel, brings this Complaint against Defendants Democratic People's Republic of Korea ("DPRK"), the Reconnaissance General Bureau ("RGB") of the DPRK, Lazarus Group, and John Does 1-20 (collectively, "Defendants"), and alleges as follows:

NATURE OF THE ACTION

1. On February 21, 2025, North Korea stole $1.5 billion. Not with guns. Not with tanks, or even threats of missiles. With a keyboard.

2. In a matter of minutes, the Democratic People's Republic of Korea (DPRK)—a nuclear-armed dictatorship and designated State Sponsor of Terrorism—used its elite state-sponsored hacking force, Lazarus Group, to execute the largest cryptocurrency theft in history. Their target was Bybit, the world's second-largest cryptocurrency exchange. Their method was a precisely engineered act of digital deception that bypassed multiple layers of security, manipulated what Bybit's own executives saw on their screens, and silently redirected $1.5 billion in assets to wallets controlled by the North Korean regime—all before anyone at Bybit knew anything had

gone wrong. This was not a mere hack. It was an act of state-sponsored piracy, designed to bankroll DPRK's weapons of mass destruction.

3. Lazarus Group, widely recognized as the most prolific state-backed cryptocurrency hacking group in the world, executed this theft through a sophisticated supply-chain compromise that exploited trusted third-party infrastructure, circumvented multiple layers of security through deception, and made detection impossible.

4. DPRK did not need to fire a missile to attack the United States. It used Amazon Web Services (AWS), one of the largest technology companies in America. The intrusion that culminated in the February 21, 2025 theft began on or about February 4, 2025, when Lazarus Group hackers compromised the workstation of a software developer at Safe{Wallet}—the third-party platform Bybit relied on to manage its multisig cold-wallet transactions—through a social-engineering attack.

5. The Lazarus Group hackers used this foothold to obtain access to Safe{Wallet}'s cloud infrastructure, hosted on AWS. As Bybit forensic investigators later determined, the attackers gained unauthorized access to a Safe{Wallet} Amazon Web Services account and associated API credentials and used that access to deploy malicious code to the Safe{Wallet} infrastructure on which Bybit's authorized signers relied. Having corrupted the platform that stood between Bybit's signers and its cold wallet, the attackers were positioned to manipulate the very transaction-approval process Bybit used to safeguard its assets.

6. Once inside Safe{Wallet}'s systems, the hackers planted a hidden code—a digital trap—designed to trigger the moment Bybit initiated a transfer. They replaced legitimate JavaScript resources served by the Safe{Wallet}interface with malicious versions specifically designed to activate when Bybit's particular wallets initiated a transaction.

7. The trap was sprung on February 21, 2025. When three Bybit executives sat down to approve what looked like a routine internal transfer of cryptocurrency, their screens showed them exactly what they expected to see: a normal transaction, with the correct destination, moving cryptocurrency to the right place. It was all a lie. In reality, the hidden, malicious code caused the signers to unknowingly approve an unauthorized upgrade of Bybit's cold-wallet smart contract to a malicious implementation contract that the attackers had pre-deployed, which contained concealed backdoor functions.

8. The moment the executives approved it, the hackers used the backdoors to drain $1.5 billion in Ethereum and Ethereum-based digital assets from Bybit's wallet, transferring the stolen funds into wallets controlled by North Korean operatives. It was only after the transaction was complete that Bybit realized something had gone catastrophically wrong.

9. Bybit moved fast to protect the people who trusted it with their money. Despite facing the largest hack in the history of cryptocurrency—a theft so large it sent shockwaves through global markets and caused Bitcoin prices to plunge—Bybit refused to freeze customer withdrawals, a measure other exchanges have taken under far less dire circumstances. Bybit honored more than $4 billion in customer withdrawal requests in the twelve hours following the attack, completing approximately 99.994% of the over 350,000 requests it received in the first ten hours. Bybit also secured emergency financing and launched an aggressive program to trace and recover stolen funds, paying out over $2.3 million in bounties to blockchain investigators. An independent audit confirmed that Bybit remained fully solvent and maintained a reserve ratio above 100% for all tokens within a day after the attack. No Bybit customer lost a dollar. But Bybit

did—to the tune of $1.5 billion, absorbed entirely by the company so that its customers would not have to bear the consequences of North Korea's crime.

10. This attack was not an isolated incident. It was the latest—and largest—strike in a systematic, years-long campaign by the North Korean regime to rob the global financial system at gunpoint. Lazarus Group has stolen billions of dollars from cryptocurrency exchanges, banks, and technology companies around the world, including from numerous American companies and institutions. DPRK has built an industrial-scale cybercrime operation—one that the U.S. government has described as posing a direct and ongoing threat to American national security, American businesses, and American citizens. A 2024 United Nations report estimated that DPRK stole approximately $3 billion in cryptocurrency between 2017 and 2023 alone, undoubtedly funneling every dollar directly into its nuclear and ballistic missile programs. The $1.5 billion stolen from Bybit represents the single largest contribution yet to that arsenal.

11. Although Bybit's world-class response ensured that no customer lost funds, the hack inflicted significant and far-reaching harm—on Bybit, on the global cryptocurrency ecosystem, and on the United States in particular. While Bybit is not a U.S.-based company, the hack's effects reverberated directly into the United States for several independent reasons establishing a clear, substantial domestic nexus.

12. First, the hack directly facilitated DPRK's circumvention of U.S. sanctions—delivering illegal revenue to a regime the United States has spent decades working to isolate economically.

13. Second, the cyberattack sent shockwaves through the U.S. crypto market, triggering an approximately 5% same-day drop in Bitcoin prices—erasing over $70 billion in market value—

part of a broader decline of over 20% from Bitcoin's mid-January highs, and rattling investor confidence at a critical moment for the industry.

14. Third, on information and belief, a portion of the proceeds of the attack have been or will be laundered through crypto exchanges operating in the United States.

15. Fourth, forensic reports confirm that Defendants facilitated the hack through an AWS server—directly exploiting the infrastructure of one of America's largest technology companies to carry out state-sponsored crime.

16. Given the severity of this attack and the direct threat it poses to the United States, including because of DPRK's use of stolen assets to fund the regime's illegal nuclear program, the Federal Bureau of Investigation took swift and decisive action to investigate the attack and disrupt the laundering of these stolen assets. Yet despite the FBI's efforts, Lazarus Group and DPRK have operated with impunity. In 2025, DPRK-affiliated cyber actors stole approximately $2.02 billion in cryptocurrency—a 51% increase year-over-year—with Bybit's approximately $1.5 billion theft accounting for the substantial majority. Through April 2026, DPRK actors had been responsible for approximately 76% of all cryptocurrency stolen globally in 2026—$577 million of $759 million total.[1] Their thievery has not slowed.

17. The consequences of this attack reach deep into the United States. DPRK used American technology—AWS—as the primary weapon in this attack. The theft triggered an approximately 5% drop in Bitcoin prices and rattled investor confidence at a uniquely critical moment: just days before the United States established its Strategic Bitcoin Reserve and U.S.

[1] *North Korea Stole 76% of All Crypto Hack Value in 2026 with Just Two Attacks*, TRM Labs (April 30, 2026), https://www.trmlabs.com/resources/blog/north-korea-stole-76-of-all-crypto-hack-value-in-2026-with-just-two-attacks (last visited June 14, 2026)

Digital Asset Stockpile on March 6, 2025, signaling the nation's commitment to digital assets as a matter of national economic policy. A portion of the stolen funds are, on information and belief, being laundered through cryptocurrency exchanges that operate in the United States. And in a deeply alarming development, an independent blockchain investigator has traced a portion of the stolen assets to Iran, another U.S.-sanctioned nation that, upon information and belief, actively funds designated terrorist organizations. The proceeds of a single hack are thus potentially fueling the weapons and terror programs of not one, but two of the most dangerous regimes on the face of the earth—one of which is currently at war with the United States.

18. Yet despite the largest theft in cryptocurrency history, despite an FBI investigation, and despite international sanctions, North Korea's hackers have faced no consequences. As of the date of this filing, only approximately 5.3% of the stolen funds (approximately $75.5 million of the total stolen cryptocurrency) have been frozen or recovered. The remaining assets—some still traceable—are at imminent risk of being laundered beyond recovery. Every day without court intervention is a day North Korea moves closer to making $1.5 billion disappear into its coffers. This case seeks to change that.

19. Bybit brings this lawsuit because no entity—not even a rogue nuclear-armed state—should be permitted to steal $1.5 billion and walk away untouched. This action seeks three things: (i) to hold DPRK and Lazarus Group legally accountable for the largest state-sponsored financial crime in the history of digital assets; (ii) to recover the stolen assets before they are forever dedicated to DPRK's terrorist operations and weapons of mass destruction programs, including by establishing that Defendants' theft constitutes an unlawful expropriation of alien property under international law and that traceable proceeds of the theft are present in the United States; and (iii) to send an unambiguous message to every government, criminal organization, and

rogue regime in the world—that American courts, American law, and the American commitment to the rule of law will not stand aside while state-sponsored pirates loot the global financial system to build nuclear weapons. If they can steal $1.5 billion and face no consequences, no company, no exchange, and no financial institution in the world is safe.

PARTIES

A. Plaintiff

20. Plaintiff Bybit Technology Limited ("Bybit") is the developer of the second largest cryptocurrency exchange platform in the world, serving over 80 million users in almost 250 countries with daily average trading volume exceeding $10 billion. The company's headquarters is in Dubai.

21. Since its founding in 2018, Bybit has grown from a small startup into one of the most trusted and widely used digital asset platforms in the world, recognized across the industry for its commitment to transparency, user protection, and security. Bybit conducts regular independent Proof of Reserves audits and publishes them publicly, stores the majority of user funds in offline "cold" wallets for maximum security, and maintains robust data protection measures including encryption and strict authorization controls.

B. Defendants

22. Defendant Lazarus Group is one of the world's most dangerous state-sponsored cybercriminal organizations, operating as an arm of DPRK's Reconnaissance General Bureau (RGB), DPRK's primary foreign intelligence service. Lazarus Group is known for high-profile

criminal operations, such as the 2014 cyberattack on Sony Pictures Entertainment and the 2017 WannaCry ransomware outbreak that crippled over 300,000 computers worldwide.

23. Lazarus Group's cybercrimes have not been limited to the private sector; Lazarus Group's malicious cyber actors have also attacked international defense contractors and stolen sensitive data from U.S. government agencies.

24. Defendant the Democratic People's Republic of Korea (DPRK) has consistently been designated by the United States as a state sponsor of terrorism, a status maintained due to its flagrant disregard for international law, including its involvement in international assassinations and its continued support for disruptive global activities. The country's cyber operations have reached a level of sophistication comparable to those of major world powers, often targeting cryptocurrency exchanges to fund the country's illegal weapons of mass destruction (WMD) and ballistic missile programs. Beyond serving as military funding sources, these cryptocurrency heists also allow DPRK to support its economic activities in ways that international sanctions are designed to make impossible. Put differently, funds from crypto heists allow DPRK to access significant capital even though U.S. and international sanctions otherwise effectively cut DPRK off from major global economies.

25. Defendant DPRK Reconnaissance General Bureau ("RGB") is DPRK's primary foreign intelligence service. RGB directs and controls DPRK's state-sponsored cyber operations, including those carried out by Lazarus Group. The U.S. Department of the Treasury's Office of Foreign Assets Control has designated RGB as a controlled entity of DPRK pursuant to Executive Order 13722. RGB is an agency or instrumentality of DPRK within the meaning of 28 U.S.C. § 1603(b).

26. Defendants John Does 1–20 are individuals and entities whose true names and capacities are currently unknown to Plaintiff but who, on information and belief, are responsible in whole or in part for receiving, laundering, holding, transferring, or otherwise exercising control over the stolen funds, and are associated with the DPRK government, the Reconnaissance General Bureau (RGB), Lazarus Group, or persons acting in concert with them.

27. The John Doe Defendants include, without limitation, natural persons and entities—whose identities will be ascertained through discovery—who control wallets to which proceeds traceable to the February 21, 2025 Bybit theft have been transferred or who have otherwise received, held, or facilitated the transfer of such proceeds at the direction of and for the benefit of Defendants. Plaintiff will amend this Complaint to identify the John Doe Defendants by their true names and capacities when ascertained.

28. Service of process on Defendants shall be effected in accordance with 28 U.S.C. § 1608.

JURISDICTION AND VENUE

29. This Court has subject matter jurisdiction and personal jurisdiction over DPRK and Lazarus Group pursuant to 28 U.S.C. § 1330 and the Foreign Sovereign Immunities Act (FSIA), 28 U.S.C. § 1602 et seq., because their conduct falls within exceptions to the FSIA, including under both 28 U.S.C. § 1605(a)(2) and (a)(3). As detailed further below, the Bybit hack was connected to a commercial activity of the DPRK which caused a direct effect on the United States. On information and belief, the hack also involved property taken in violation of international law. On information and belief, traceable proceeds of the expropriation are presently held on cryptocurrency exchanges that operate in or maintain infrastructure in the United States.

30. Defendants' conduct constitutes "commercial activity" within the meaning of 28 U.S.C. § 1605(a)(2). The act of stealing cryptocurrency for financial gain—even by a sovereign

state—is commercial in nature, not sovereign or governmental, regardless of how the DPRK may subsequently deploy the proceeds. The theft was executed through fraudulent business transactions involving cryptocurrency exchanges, digital wallets, and cloud computing services, all of which are commercial in character.

31. Defendants' commercial activity had a "direct effect" in the United States within the meaning of 28 U.S.C. § 1605(a)(2). On information and belief, the attack caused immediate and substantial disruption to U.S. interests in numerous ways, including, among other things, significant disruption to U.S. cryptocurrency markets (including an approximately 5% drop in Bitcoin prices), undermining of U.S. sanctions enforcement, the expenditure of substantial FBI resources for investigation and response, and the laundering of stolen assets through U.S.-based cryptocurrency exchanges.

32. Defendants' conduct was also performed "in connection with" commercial activity of DPRK carried on in the United States within the meaning of 28 U.S.C. § 1605(a)(2). DPRK's broader pattern of cryptocurrency theft operations, including the deployment of fraudulent IT workers at U.S. companies and the use of U.S.-based infrastructure and exchanges to launder stolen assets, constitutes commercial activity carried on in the United States. The February 21, 2025 hack was part of and connected to this broader commercial enterprise.

33. Defendants' conduct also falls under 28 U.S.C. § 1605(a)(3), which provides an exception to sovereign immunity where "rights in property taken in violation of international law are in issue and that property or any property exchanged for such property is present in the United States in connection with a commercial activity carried on in the United States by the foreign state." Defendants' theft of approximately $1.5 billion in cryptocurrency from Plaintiff constitutes a taking of alien property in violation of international law, including customary international law

prohibiting the uncompensated expropriation of foreign nationals' property. The stolen cryptocurrency was subsequently converted and laundered through multiple blockchain transactions, and a traceable portion of the stolen assets—or property exchanged for such assets—is presently held on cryptocurrency exchanges that operate in or maintain infrastructure in the United States. The presence of these traceable proceeds on exchanges doing business in the U.S., in connection with Defendants' commercial activity of laundering and converting stolen cryptocurrency through U.S. commercial channels, satisfies the jurisdictional requirements of § 1605(a)(3). *See Republic of Hungary v. Simon*, 604 U.S. 115 (2025) (holding that a plaintiff satisfies the expropriation exception by tracing expropriated property or its exchange proceeds to a United States account).

34. This Court additionally has subject matter jurisdiction over this action pursuant to 28 U.S.C. § 1350 because this case involves a tort committed by alien Defendants, in violation of the law of nations. As detailed below, Defendants' theft of Bybit's digital assets amounts to digital piracy.

35. This Court also has subject matter jurisdiction over this action pursuant to 28 U.S.C. § 1331 because this case involves a federal question under the Computer Fraud and Abuse Act (18 U.S.C. § 1030, et seq.) and the Racketeer Influenced and Corrupt Organizations Act, 18 U.S.C. §§ 1961–1968.

36. Plaintiff's state law claims for conversion, trespass to chattels, fraud, and tortious interference with contract are governed by the substantive law of the District of Columbia. The District of Columbia has the most significant relationship to the occurrence and the parties with respect to the particular issues raised by Plaintiff's state law claims.

37. This Court has supplemental jurisdiction over Plaintiff's state law claims pursuant to 28 U.S.C. § 1367(a) because those claims are so related to the federal claims in this action as to form part of the same case or controversy.

38. The Defendants have sufficient minimum contacts with the United States to support the exercise of personal jurisdiction. The Defendants purposefully directed their conduct at the United States in numerous ways, including, among other things, by: (i) using U.S.-based AWS infrastructure as the primary vector for the attack; (ii) targeting a cryptocurrency exchange knowing that the theft would affect U.S. markets, U.S. investors, and U.S. regulatory interests; (iii) laundering stolen assets through U.S.-based cryptocurrency exchanges; and (iv) engaging in a systematic pattern of cryptocurrency thefts and related commercial activity affecting the United States.

39. The exercise of jurisdiction over Defendants comports with due process because they purposefully availed themselves of the privilege of conducting activities within the United States, and Plaintiff's claims arise out of or relate to Defendants' contacts with the United States.

40. Venue is proper in this judicial district under 28 U.S.C. § 1391(f)(4) because Defendant DPRK is a foreign state.

41. Venue is also proper in the District of Columbia because the hack had significant effects in the United States, including effects on U.S. regulatory interests, U.S. national security, the U.S. cryptocurrency market, and U.S. technological infrastructure, as detailed further below. Moreover, U.S. regulatory enforcement actions and Treasury Department sanctions designations relevant to this case—including OFAC's designations of DPRK, RGB, and Lazarus Group—are administered from the District of Columbia.

STATEMENT OF FACTS

A. Background on Cryptocurrency

42. Cryptocurrency is a form of digital currency. Unlike traditional currency issued by governments—such as U.S. dollars—cryptocurrency exists only in electronic form. The electronic nature of cryptocurrency affords numerous benefits, including lower transaction costs and faster transaction speeds (including across geographic borders), as well as increased transparency enabled through publicly viewable ledgers. Well-known cryptocurrency examples include Bitcoin and Ethereum.

43. Cryptocurrency is maintained through a technology known as a "blockchain"—essentially a digital record book that permanently logs every transaction. This record book is not stored in any single location. Instead, identical copies are maintained across a global network of computers, including massive computers and data storage facilities located in the United States. Because the record exists in many places simultaneously, no single person or entity controls it, and past transactions cannot be secretly altered or deleted.

44. Cryptocurrency is held in digital accounts called "wallets," which function in certain respects like bank accounts. Each wallet has two components: a public address and a private key. The public address is like an account number—it can be shared with others so they know where to send funds. The private key is like a password—whoever possesses the private key controls the wallet and can authorize transfers of the cryptocurrency it contains.

45. Cryptocurrency can be exchanged for traditional government-issued currency (such as U.S. dollars) or for other types of cryptocurrency. These exchanges occur electronically, often through online platforms called "exchanges." When cryptocurrency is transferred from one wallet to another, that transaction is permanently recorded on the blockchain, generally creating a traceable chain of custody.

46. Cryptocurrency can be stored in "cold wallets," which are offline crypto asset solutions that offer maximum security relative to other types of wallets. Cryptocurrency can also be stored in "warm wallets," which are connected to the internet and therefore allow faster and convenient transactions. Because of this security-accessibility tradeoff, cryptocurrency exchanges commonly maintain both cold and warm wallets, keeping the majority of reserves in cold wallets and regularly replenishing warm wallets to support customer transactions.

B. Bybit Builds a Leading Global Crypto Exchange

47. Bybit was founded in late 2018 by CEO Ben Zhou, a former foreign exchange and investment banking professional, with a vision to build a next-generation cryptocurrency exchange that would combine institutional-grade infrastructure with accessibility for everyday users.

48. Zhou and his co-founders launched Bybit's first product in December 2018, a Bitcoin inverse contract (BTCUSD Inverse Perpetual Contract). Bybit quickly gained momentum. In 2019, Bybit celebrated its break-even point and processed 10% of global Bitcoin trading volume. By 2020, Bybit surpassed $4 billion in daily trading volume. In 2021, Bybit diversified its product offerings to become a more comprehensive crypto exchange, with its customer base beginning to grow significantly to millions of new users each year and daily trading volume surpassing $70 billion.

49. In 2024, Bybit reached over 40 million users worldwide, becoming the world's second-largest crypto exchange. That growth has continued—Bybit now has over 80 million users worldwide, with daily average trading volume of over $10 billion.

C. DPRK's Egregious Crimes and Terrorist Activities

50. To understand the full gravity of the attack on Bybit, it is necessary to understand the nature of the regime that orchestrated it.

51. DPRK poses one of the gravest threats to international peace and security. For decades, DPRK has pursued an unlawful nuclear weapons program in direct defiance of its obligations under the Treaty on the Non-Proliferation of Nuclear Weapons and multiple binding U.N. Security Council resolutions. DPRK has conducted six nuclear weapons tests—in 2006, 2009, 2013, and three in 2016–2017—each escalating in yield and sophistication. U.S. intelligence assessments estimate that DPRK currently possesses sufficient fissile material for dozens of nuclear warheads and continues to produce additional weapons-grade plutonium and enriched uranium.

52. In parallel with its nuclear program, DPRK has developed and tested an increasingly advanced arsenal of ballistic missiles, including intercontinental ballistic missiles ("ICBMs") that the United States and allied governments have assessed as capable of reaching the continental United States. Since 2017, DPRK has repeatedly tested ICBM-class systems—including the liquid-fuel Hwasong-15 and Hwasong-17 and, more recently, the solid-fuel Hwasong-18 and successor systems—in direct violation of U.N. Security Council Resolutions 1718 (2006), 1874 (2009), 2087 (2013), 2094 (2013), 2270 (2016), 2321 (2016), 2371 (2017), 2375 (2017), and 2397 (2017). These weapons programs exist for the purpose of enabling DPRK to threaten the United States, its allies, and the international community with nuclear devastation, and to coerce concessions through that threat. DPRK's provocations have continued in the months leading up to the filing of this Complaint: in the first five months of 2026, DPRK has conducted multiple ballistic missile launches into the waters surrounding the Korean Peninsula, repeatedly

timed to coincide with lawful U.S.–Republic of Korea joint military exercises. The United States Department of State, the United States Indo-Pacific Command, and the Governments of the Republic of Korea and Japan have publicly condemned each of these launches as violations of multiple U.N. Security Council resolutions.

53. DPRK's conduct extends far beyond weapons proliferation. The U.S. Department of State has designated DPRK a State Sponsor of Terrorism since 2017, reflecting the regime's long history of international assassinations, hostage-taking, and support for terrorist activity. In 2017, DPRK agents assassinated Kim Jong Nam—the half-brother of DPRK leader Kim Jong Un—at a Malaysian airport using the VX nerve agent, a chemical weapon of mass destruction. DPRK has also been responsible for abducting foreign nationals, maintaining a system of political prison camps holding an estimated 80,000 to 120,000 people, and systematically subjecting its own citizens to forced labor, starvation, and extrajudicial killings, as documented by the U.N. Commission of Inquiry on Human Rights in DPRK. In 2018, this Court entered a default judgment against DPRK for its "torture, hostage taking, and extrajudicial killing" of Otto Warmbier.

54. The U.N. Security Council has found that DPRK funds these programs, in significant part, through illicit revenue generated by cybercrime and cryptocurrency theft. A 2024 report by the U.N. Panel of Experts estimated that DPRK stole approximately $3 billion in cryptocurrency between 2017 and 2023, with the proceeds funneled directly into the regime's weapons of mass destruction and ballistic missile programs. Thus, every dollar of cryptocurrency stolen by DPRK-affiliated actors—including the $1.5 billion stolen from Bybit—contributes to DPRK's capacity to threaten the United States and the international community with nuclear weapons.

D. Lazarus Group and DPRK's Cybercrime Activity

55. DPRK utilizes malicious cyber activities, referred to by the U.S. government as "HIDDEN COBRA," to generate revenue while circumventing the comprehensive economic sanctions imposed on DPRK by both the United States and the United Nations. DPRK is designated by the U.S. Department of the Treasury's Office of Foreign Assets Control ("OFAC") as one of the most heavily sanctioned nations in the world, subject to a near-total trade embargo that prohibits virtually all financial transactions involving DPRK or its agents and effectively bars DPRK from accessing the U.S. financial system. The U.N. Security Council has similarly imposed sweeping sanctions on DPRK through multiple resolutions, including Resolutions 1718, 2087, 2094, 2270, 2321, 2371, 2375, and 2397. By stealing cryptocurrency, DPRK circumvents these sanctions. These DPRK cyber actors continue to target U.S. critical infrastructure to conduct espionage and deploy ransomware to generate illicit revenue.

56. The U.S. government has identified Lazarus Group as the North Korean state-sponsored Advanced Persistent Threat (APT) group responsible for a number of cryptocurrency thefts and criminal cyber activity, detailed further below. The U.S. Government believes DPRK created Lazarus Group as early as 2007. Lazarus Group is part of the Reconnaissance General Bureau (RGB)—a controlled entity of DPRK as designated by OFAC. The following examples illustrate only a fraction of Lazarus Group's prolific and escalating pattern of cyberattacks.

57. In 2014, Lazarus Group conducted a destructive cyberattack against Sony Pictures Entertainment (SPE) in retaliation for the film *The Interview*, a comedy that depicted the fictional assassination of the DPRK's leader. In that hack, Lazarus Group stole massive amounts of sensitive data of American citizens, leaked unreleased films, and deployed "wiper" malware that deleted data from thousands of corporate computers.

58. In 2016, Lazarus Group plotted a massive theft from the Bangladesh Bank's account at the U.S. Federal Reserve Bank of New York through credentials that hackers stole through phishing emails sent to bank employees. Lazarus Group successfully exfiltrated nearly $100 million before a mistake halted the remaining transfers.

59. In 2017, Lazarus Group was responsible for the "WannaCry 2.0" ransomware attack, where Lazarus Group encrypted data in approximately 300,000 computers across 150 countries (including the United States) and demanded Bitcoin payments in return for decryption.

60. In March 2022, Lazarus Group stole approximately $620 million in cryptocurrency from the blockchain project Ronin, which was developed in Vietnam to support a popular video game with global users, including in the United States. The group then stole another $100 million from American cryptocurrency firm Harmony in June 2022.

61. In late 2025, the U.S. Department of Justice filed civil forfeiture complaints to seize over $15 million in USDT (Tether) from virtual wallets linked to Lazarus Group actors involved in 2023 cryptocurrency platform heists.

62. DPRK utilizes a global network of fake "IT workers" who use fraudulent identities to gain employment at U.S. and European firms, subsequently using their access to facilitate cyber intrusions, steal intellectual property, and funnel their high salaries back to the North Korean regime's weapons programs.

63. The threat posed by Lazarus Group to U.S. national security is so severe that it has mobilized the full weight of the U.S. national security and law enforcement apparatus. In 2022, the FBI issued a joint Cybersecurity Advisory with CISA and the Treasury Department to highlight Lazarus Group's malicious cyber activity targeting the blockchain technology and cryptocurrency industry. The report stated that "North Korea's Lazarus Group actors have targeted various firms,

entities, and exchanges in the blockchain and cryptocurrency industry using spearphishing campaigns and malware to steal cryptocurrency," and warned that "[t]hese actors will likely continue exploiting vulnerabilities of cryptocurrency technology firms, gaming companies, and exchanges to generate and launder funds to support the North Korean regime."

E. DPRK and Lazarus Group Steal Approximately $1.5 Billion in Crypto Assets

64. On February 21, 2025, Bybit suffered the largest cryptocurrency theft in history when hackers stole approximately $1.5 billion worth of Ethereum and Ethereum-based digital assets during what was supposed to be a routine internal transfer of funds. The stolen assets comprise approximately 401,347 ether (ETH), 90,375 Staked Ether (stETH), 8,000 Mantle Staked Ether (mETH), 15,000 Mantle Restaked Ethereum (cmETH), and 90 Tether (USDT).

65. The theft occurred when Bybit attempted to move ETH from a cold wallet to a warm wallet. To authorize this transfer, three Bybit executives were required to digitally sign off on the transaction, a measure known as "multisig" (short for multi-signature). The multisig process adds a layer of security by ensuring that no single individual can approve a transaction. The hackers exploited this process by manipulating transfer addresses for the transaction, even though Bybit's executives were unable to see any manipulation in the addresses.

66. The intrusion that culminated in the February 21, 2025 theft began on or about February 4, 2025, when the attackers compromised the workstation of a software developer at Safe{Wallet}—the third-party platform Bybit relied on to manage its multisig cold-wallet transactions—through a social-engineering attack, and used that foothold to obtain access to Safe{Wallet}'s cloud infrastructure.[2]

[2] *See* Sygnia, Sygnia's Investigation into the Bybit Hack: What We Know So Far (Mar. 16, 2025), https://www.sygnia.co/blog/sygnia-investigation-bybit-hack/

67. By on or about February 18, 2025, the hackers had reached Safe{Wallet}'s cloud-hosted infrastructure. Bybit's forensic investigators later determined that the attackers gained unauthorized access to a Safe{Wallet} Amazon Web Services account and associated API credentials and used that access to deploy malicious code to the Safe{Wallet} infrastructure on which Bybit's authorized signers relied. Having corrupted the platform that stood between Bybit's signers and its cold wallet, the attackers were positioned to manipulate the very transaction-approval process Bybit used to safeguard its assets.

68. Once inside Safe{Wallet}'s systems, the hackers replaced legitimate JavaScript resources served by the Safe{Wallet} interface with malicious versions specifically designed to activate when Bybit's particular wallets initiated a transaction. When Bybit executives went to approve the routine transfer on February 21, their screens displayed what appeared to be a normal transaction sending funds to the correct destination. But in reality, the malicious code caused the signers to unknowingly approve an unauthorized upgrade of Bybit's cold-wallet smart contract to a malicious implementation contract that the attackers had pre-deployed and that contained concealed backdoor functions. The hackers then invoked those backdoors to drain the wallet, transferring its contents to wallets under their control.

69. The hackers' actions were all carried out without Bybit's knowledge or authorization, constituting a clear violation of access protocols and effecting a fraud on Bybit and a theft of assets from Bybit and its customers for the financial gain of Lazarus Group and DPRK.

70. Forensic investigators, including leading cybersecurity firms Sygnia and Verichains, determined that Defendants carried out the attack through the third-party Safe{Wallet} infrastructure—a type of attack known as a "supply chain compromise," in which hackers target a

trusted vendor or service provider of the ultimate victim. In other words, the hackers exploited a vulnerability in Safe{Wallet}'s systems, not Bybit's systems.

71. Notwithstanding that the initial compromise occurred at Safe{Wallet}, Defendants' unauthorized access to Safe{Wallet}'s systems, theft of credentials, injection of malicious code that appeared on Bybit's executives' computers, and theft of Bybit's cryptocurrency constituted the direct and proximate cause of Plaintiff's damages. Defendants unlawfully exploited vulnerabilities for the specific purpose of stealing Bybit's assets. Any security measures that Safe{Wallet} may or may not have had in place do not diminish or excuse Defendants' criminal conduct or break the causal chain between Defendants' intentional acts and Plaintiff's resulting harm.

72. In the aftermath of the hack, Bybit worked closely with law enforcement, particularly the FBI, in investigation efforts and efforts to freeze the pilfered digital assets.

73. On February 26, 2025, the FBI issued a Public Service Announcement officially attributing the Bybit hack to DPRK. The FBI specifically referred to this North Korean malicious cyber activity as "TraderTraitor," a DPRK hacking group tied to Lazarus Group.

74. The FBI's February 26 Announcement also included a list of Ethereum addresses used by the hackers to launder the stolen assets. The FBI urged cryptocurrency service providers to block transactions linked to those addresses.

75. The FBI has obtained one or more seizure warrants under 18 U.S.C. § 981 directed at a portion of the stolen Bybit assets, including a portion of the assets held at one or more cryptocurrency platforms. However, the law-enforcement preservation reaches only a small fraction of the stolen $1.5 billion. The balance remains at imminent risk of being laundered beyond recovery absent court-ordered preservation through this action.

76. On November 4, 2025, the U.S. Department of the Treasury designated a network of DPRK banking officials, front companies, and 53 cryptocurrency addresses for laundering the proceeds of cybercrime on behalf of the DPRK regime. Treasury expressly identified the February 21, 2025 hack of Bybit as part of the larger pattern of DPRK cybercrime that the designation was intended to address. On March 12, 2026, Treasury further expanded the designations, adding six individuals, two entities, and an additional 21 cryptocurrency addresses associated with DPRK's IT-worker and laundering operations.

77. Forensic tracing has further identified at least one wallet under Defendants' control that holds both separately identifiable proceeds of the February 21, 2025 Bybit theft and separately identifiable proceeds of a January 2025 cryptocurrency theft from Phemex, an unrelated cryptocurrency exchange. The Phemex theft has been publicly attributed to DPRK and Lazarus Group. The presence of both tranches—each individually traceable on the public blockchain ledger—in a single wallet under common control evidences a unified DPRK laundering apparatus operating across multiple criminal incidents.

F. Bybit Protects Its Customers at Enormous Cost to Itself

78. Despite experiencing the largest ever hack in the crypto industry, Bybit kept all customer funds safe—at enormous cost to itself. As expected, the hack prompted a significant run on Bybit to the tune of $4 billion in one day. While many leaders in the crypto industry encouraged Bybit to freeze customer withdrawals, Bybit never did. In fact, Bybit met all customer withdrawal demands in just 12 hours following the attack. To do so, Bybit secured emergency bridge financing, deployed crisis management resources, and launched the LazarusBounty program—

ultimately spending millions of dollars to ensure that no customer bore the consequences of the DPRK's crime.

79. Just one day after the hack, an independent audit concluded that Bybit's diversified asset holdings and strong financial position allowed the platform to maintain full solvency and successfully reestablish a healthy reserve ratio above 100% for all tokens, demonstrating the exchange's resilience and dedication to user fund security. But while Bybit's customers were made whole, Bybit itself was not. Bybit absorbed the full financial impact of the theft and, to this day, remains out much of the $1.5 billion in stolen assets that have never been recovered or reimbursed. The costs Bybit incurred in responding to the crisis—including emergency financing, bounty payments, enhanced security measures, and crisis management—have compounded those losses further. In short, Bybit bore the entire burden of the DPRK's crime so that its customers would not have to, and it continues to bear that burden today.

G. The Hack Has a Significant Direct Effect in the U.S.

80. The theft of $1.5 billion in virtual assets by Lazarus Group directly undermines U.S. regulatory interests by providing the regime with a massive influx of untraceable capital to fund DPRK's weapons program and other aspects of DPRK's isolated economy.

81. Further, after stealing the funds, Lazarus Group has utilized cryptocurrency mixers to obscure the origin of the stolen assets. This not only creates hurdles to investigation efforts, but also challenges the efficacy of U.S. Anti-Money Laundering and Know Your Customer frameworks mandated by the Treasury Department's Financial Crimes Enforcement Network (FinCEN).

82. The FBI's immediate involvement and investigation of the cyberattack and deployment of blockchain intelligence resources to track Lazarus Group's actions throughout this

hack underscore the significance of the event to U.S. interests and the substantial resources required to mitigate the global fallout of the theft.

83. The sheer scale of the $1.5 billion theft—the largest crypto theft in history—sent shockwaves through the global crypto market. Bitcoin prices dropped approximately 5% in the immediate aftermath of the hack—erasing over $70 billion in market value—part of a broader decline of over 20% from mid-January highs, and increased volatility rattled U.S. investor confidence at a uniquely consequential moment: just days before the United States established its Strategic Bitcoin Reserve on March 6, 2025—a permanent reserve holding over $17 billion in Bitcoin obtained through criminal or civil asset forfeiture, making the federal government the largest state Bitcoin holder globally. North Korea's largest-ever heist thus threatened to destabilize the U.S. cryptocurrency market at the very moment the United States was signaling its commitment to digital assets as a matter of national policy.

84. The FBI identified that stolen funds were rapidly dispersed across thousands of addresses on multiple blockchains, with the potential for significant funds to flow through exchanges that do business in the U.S.

H. Current State of Assets from the Hack and Increasing Risks without Intervention

85. Following the theft, the hackers rapidly converted approximately 86% of the stolen Ethereum and Ethereum-based digital assets into Bitcoin. They further obscured the money trail using cryptocurrency "mixers" (services that blend transactions from many users together to make individual funds untraceable—in this context, akin to money laundering), decentralized exchanges, and cross-chain bridges (tools for moving assets between different blockchain networks).

86. Forensic tracing has identified specific laundering vehicles through which Defendants processed the stolen Bybit assets. Defendants' use of this multi-vehicle laundering chain is consistent with established Lazarus Group tradecraft documented by both the U.S. government and independent blockchain forensics firms, and provides direct evidence of Defendants' knowledge that the assets had been unlawfully obtained and of their intent to conceal the source, ownership, and disposition of those assets in furtherance of the underlying racketeering activity.

87. Multiple U.S. government officials, United Nations reports, and the U.S. Treasury have stated that North Korea uses cryptocurrency theft operations to fund the regime's nuclear weapons and ballistic missile programs. The U.N. Multilateral Sanctions Monitoring Team reported in 2025 that DPRK cyber actors had stolen at least $1.65 billion in cryptocurrency in early 2025 alone, predominantly from the Bybit hack.

88. Despite extensive sanctions imposed by the U.N. Security Council and the United States, North Korea's state-sponsored hackers continue to operate with near-total impunity. They are modern-day pirates flying a sovereign flag. These cyber operatives lurk in the open sea of digital space, carrying out devastating raids on cryptocurrency exchanges that hold billions in assets. They exploit the borderless nature of digital assets and the jurisdictional fragmentation of international law to plunder wealth from the global financial system, retreat behind the shield of a nuclear-armed state, and funnel the proceeds into weapons programs that threaten international peace and security—all while remaining effectively beyond the reach of law enforcement or legal accountability.

89. On information and belief, DPRK also uses cryptocurrency obtained from hacks as a form of payment for goods and services, including the sale and transfer of military equipment as

well as raw materials such as gold and copper. As such, DPRK uses the proceeds of its cryptocurrency heists to prop up its isolated economy, thereby circumventing U.S. sanctions policy.

90. As of filing, only approximately 5.3% ($75.5 million of the $1.5 billion) of the stolen cryptocurrency had been frozen or recovered, despite efforts by Bybit, law enforcement, and industry partners. Bybit launched the LazarusBounty program offering rewards for tracing and freezing stolen funds and paid out over $2.3 million in bounties.

91. Approximately 90.2% of the stolen Bybit assets is currently untraceable, having been laundered through mixers, cross-chain bridges, and over-the-counter cryptocurrency dealers to the point of complete obfuscation. The balance—approximately 9.8% of the stolen funds—has been traced by Bybit and independent forensic analysts to identifiable wallet addresses across multiple blockchain networks; of those traced assets, however, only a small fraction has been frozen or otherwise placed beyond Defendants' dominion.

92. On information and belief, a portion of the traceable stolen funds are held on cryptocurrency exchanges that operate in or maintain infrastructure in the United States, further establishing the domestic nexus of this action. The presence of these traceable assets—which constitute property exchanged for property taken in violation of international law—on exchanges doing business in the U.S. provides an independent basis for this Court's jurisdiction under 28 U.S.C. § 1605(a)(3).

93. Although some portion of the stolen funds have remained in the wallets to date, they can be instantly transferred by Defendants to other accounts if they know that the funds might be seized. If the funds are transferred to other wallets for further laundering, the ability of Bybit to recover funds will likely be lost forever. A significant portion of stolen Bybit assets currently sits

in freezing-order or seizure-warrant status at cryptocurrency intermediaries cooperating with U.S. law enforcement, with a significant portion preserved by cryptocurrency intermediaries at the request of the FBI. But if those crypto intermediaries decide to stop cooperating with U.S. law enforcement, those assets are at imminent risk of dissipation without court-ordered preservation. And there are significant traced assets that have not yet been frozen—assets that will undoubtedly move to DPRK for terrorist funding without court-ordered preservation.

94. Funds in these wallets should be frozen, seized and held, or blocked from further transfer by the exchange platforms to prevent the permanent loss of the funds until the Court has the opportunity to adjudicate this action.

95. Bybit contacted the cryptocurrency exchange platforms where the wallets holding stolen funds are located and requested that the platforms cooperate to freeze, or seize and hold, or block from further transfer the funds in the Doe Defendants' wallets until such time that this Court can determine the identities of the Doe Defendants and adjudicate the right of Bybit to recover the stolen funds. Certain platforms have signaled their willingness to cooperate after a court order is received.

96. If the known funds in the wallets are not frozen, seized and held, or blocked from further transfer, the funds are in imminent danger of being lost forever and Plaintiff will be irreparably harmed.

97. Furthermore, DPRK will continue to use these stolen assets to fund activities that pose significant U.S. national security threats from DPRK and beyond. In a deeply alarming development, an independent blockchain investigator has traced some of the assets from the Bybit heist to Iran—another nation sanctioned by the United States for its nuclear program and its support for designated terrorist organizations. The stolen proceeds of a single hack are thus

potentially funding the weapons and terror programs of not one, but two of the most dangerous regimes on earth.

98. The hackers have no right to retain the funds being held in the Wallets that Plaintiff seeks to have frozen, seized and held, or blocked from further transfer, and therefore will not be harmed by the granting of injunctive relief in the form of a temporary restraining order and preliminary injunction until the Court can hear evidence and decide the legal issues.

99. The public interest will be served and not harmed by ordering that the assets in the wallets are frozen, seized and held, or blocked from further transfer by the Defendants until such time that this Court can determine the identities of the parties and adjudicate the right of Plaintiff to recover the stolen funds.

100. Plaintiff intends to seek emergency relief from this Court, including a temporary restraining order and preliminary injunction to freeze the traceable stolen assets and prevent their further dissipation, as well as expedited discovery to identify the John Doe Defendants and trace additional stolen assets.

101. Indeed, strong action from the Court is urgently needed to curtail DPRK's accelerating campaign of cyber theft. In 2025 alone, DPRK operatives stole an additional $500 million in crypto assets *after* the Bybit hack—bringing the regime's total haul to over $2 billion in a single year. That pace has not slowed. In January 2026, DPRK completed twice as many exploits compared to January of the prior year, as reported by Elliptic—a leading blockchain analytics company for financial crime risk management. Without decisive judicial intervention, DPRK will continue to treat the global cryptocurrency ecosystem as its personal treasury.

I. The Act of State Doctrine Does Not Shield Defendants' Conduct

102. The act of state doctrine poses no barrier to this Court's adjudication of Plaintiff's claims.

103. Defendants' conduct is commercial, not governmental, in nature. The theft of cryptocurrency for financial gain—even if the proceeds are ultimately diverted to fund government programs—is indistinguishable from private criminal conduct and does not constitute a sovereign act entitled to judicial deference.

104. Moreover, Defendants' conduct violates well-established principles of international law, including customary international law, U.N. Security Council resolutions, and treaties to which DPRK is a party. State-sponsored theft, cyber intrusions, and circumvention of international sanctions are precisely the types of conduct that fall outside any claim of sovereign deference.

105. Adjudication of this action is fully consistent with clearly articulated U.S. policy. The United States has repeatedly condemned DPRK's cyber operations, designated DPRK as a state sponsor of terrorism, imposed comprehensive sanctions on DPRK, and specifically attributed this attack to DPRK through official FBI statements. Permitting DPRK to retain the proceeds of this theft would directly contravene U.S. policy to combat state-sponsored cybercrime and enforce sanctions against DPRK.

106. This case presents a straightforward application of U.S. and international law. The Court need only determine that Defendants' cyber intrusion into U.S. and third-party computer systems and theft of Plaintiff's property was unlawful—a determination that requires no inquiry into, let alone invalidation of, any official act of DPRK taken within its own territory.

CAUSES OF ACTION

COUNT I

Computer Fraud and Abuse Act, 18 U.S.C. § 1030(a)

107. Plaintiff realleges and incorporates by reference all preceding paragraphs.

108. On February 21, 2025, Defendants utilized malicious code to intrude into protected computers and change the intended destination of the cryptocurrency in Bybit's cold wallet to wallets controlled by DPRK operatives. By doing so, Defendants accessed or caused to be accessed the protected computers of Bybit, Safe{Wallet}, and AWS without authorization, ultimately causing Bybit's computers to display false information.

109. Defendants violated 18 U.S.C. § 1030(a)(2) because they intentionally accessed and caused to be accessed Plaintiff's and Plaintiff's vendors' computers without authorization and, on information and belief, obtained data therefrom.

110. Defendants violated 18 U.S.C. § 1030(a)(4) because they knowingly and with intent to defraud accessed and caused to be accessed Plaintiff's protected computers without authorization, and by means of such conduct furthered the intended fraud and obtained cryptocurrency of approximately $1.5 billion in value.

111. Defendants violated 18 U.S.C. § 1030(a)(5) because they knowingly and intentionally caused the transmission of a malicious code and intentionally caused damage without authorization to Plaintiff's protected computers.

112. Defendants violated 18 U.S.C. § 1030(b) by conspiring and attempting to commit the violations alleged in the preceding paragraphs.

113. Defendants' conduct caused a loss to Plaintiff in excess of $5,000 during a one-year period. Defendants' actions caused Plaintiff to incur a loss as defined in 18 U.S.C. § 1030(e)(11), including the cost of investigating and remediating Defendants' unauthorized

access. Plaintiff's damages and losses include, but are not limited to: (i) the value of approximately $1.5 billion in stolen Ethereum and Ethereum based digital assets; (ii) costs incurred in responding to and investigating the attack, including filing police reports and related remedial actions in foreign jurisdictions; (iii) over $2.3 million paid out through the LazarusBounty program; (iv) costs incurred in securing replacement cryptocurrency through emergency loans; (v) costs of enhanced security measures; and (vi) consequential business losses, reputational harm, and the costs of crisis management and communications. Plaintiff is entitled to be compensated for losses and damages, and any other amount to be proven at trial.

COUNT II

Alien Tort Statute, 28 U.S.C. § 1350

114. Plaintiff realleges and incorporates by reference all preceding paragraphs.

115. Plaintiff is an "alien" within the meaning of the ATS, as it is a corporation organized under the laws of the British Virgin Islands.

116. The Alien Tort Statute, 28 U.S.C. § 1350, confers upon this Court "original jurisdiction of any civil action by an alien for a tort only, committed in violation of the law of nations or a treaty of the United States."

A. Violation of the Law of Nations: State-Sponsored Theft and Piracy

117. Since its enactment in 1789, the ATS has been understood to provide a cause of action for piracy and theft committed in violation of the law of nations. Piracy is one of the three historical torts recognized under the ATS at the time of its adoption. *See Sosa v. Alvarez-Machain*, 542 U.S. 692, 724 (2004).

118. Defendants' conduct constitutes a modern form of piracy and theft in violation of the law of nations. Acting as agents and instrumentalities of DPRK, Defendants systematically

infiltrated Plaintiff's and Plaintiff's vendors' computer systems and stole approximately $1.5 billion in cryptocurrency assets through unauthorized access, deception, and fraud.

119. The prohibition against state-sponsored expropriation of alien property without compensation is among the longest-established and most universally recognized norms of customary international law, satisfying the "specific, universal, and obligatory" standard articulated in *Sosa*, 542 U.S. at 732. This norm is codified in the Restatement (Third) of Foreign Relations Law § 712 and reaffirmed in the Restatement (Fourth) § 210; recognized by the Permanent Court of International Justice in Factory at Chorzów, 1928 P.C.I.J. (ser. A) No. 17, and by the International Court of Justice in Barcelona Traction, 1970 I.C.J. 3; enshrined in U.N. General Assembly Resolution 1803 (XVII) on Permanent Sovereignty over Natural Resources—which the sole arbitrator in *Texaco Overseas Petroleum Co. v. Libyan Arab Republic*, 53 I.L.R. 389 (Arb. Trib. 1977), held reflects customary international law—and further reinforced by the ILC Articles on State Responsibility (2001), Articles 1, 2, and 31, which confirm that every internationally wrongful act of a state, including the taking of foreign nationals' property, entails an obligation of full reparation. Defendants' orchestrated theft of $1.5 billion in cryptocurrency belonging to foreign nationals constitutes precisely the kind of state-directed expropriation that this centuries-old norm prohibits, carried out not for any legitimate public purpose but to fund weapons programs in violation of binding UN Security Council resolutions.

B. Violation of the Law of Nations: Unlawful Expropriation of Alien Property

120. In the alternative, Defendants' conduct constitutes an unlawful expropriation of alien property in violation of customary international law. The prohibition against uncompensated expropriation of foreign nationals' property is a well-established norm of customary international law.

121. Under customary international law, a state's taking of a foreign national's property violates international law unless it is (a) for a public purpose, (b) non-discriminatory, (c) accompanied by due process, and (d) accompanied by prompt, adequate, and effective compensation. Defendants' theft of Plaintiff's cryptocurrency assets satisfied none of these requirements.

122. Expropriation under international law does not require a formal decree or official acknowledgment by the expropriating state. International law recognizes *de facto* and indirect expropriation, and applies an effect-based test that looks to the deprivation suffered by the property owner, not the form or characterization of the state's conduct.

123. DPRK is not the state of Plaintiff's nationality. Plaintiff is organized under the laws of the British Virgin Islands. The "domestic takings rule" is inapplicable.

C. Attribution of Conduct to the DPRK

124. Defendants' conduct is attributable to DPRK as a state act under customary international law, including the International Law Commission's Articles on State Responsibility. Lazarus Group operates under the direction and control of DPRK's Reconnaissance General Bureau. The U.S. Department of the Treasury has designated Lazarus Group pursuant to Executive Order 13722, the FBI has attributed the February 21, 2025 attack to DPRK, and the Department of Justice has obtained indictments against DPRK operatives for related cybercriminal activity.

D. Domestic Application

125. Plaintiff's ATS claims involve a permissible domestic application of the statute. The hack had a significant direct effect in the United States, including effects on U.S. regulatory interests, U.S. national security, the U.S. cryptocurrency market, and U.S. technological infrastructure. Plaintiff's claims "touch and concern the territory of the United States" with

sufficient force to overcome the presumption against extraterritorial application. *See Kiobel v. Royal Dutch Petroleum Co.*, 569 U.S. 108, 124-25 (2013). Defendants executed the theft by exploiting AWS infrastructure physically located in the United States, making U.S.-based servers the instrumentality through which the tortious conduct was carried out. *See RJR Nabisco, Inc. v. European Cmty.*, 579 U.S. 325 (2016). Moreover, the hack disrupted U.S. cryptocurrency markets, triggered an active FBI investigation, resulted in OFAC sanctions activity, and a material portion of the stolen assets were laundered through exchanges operating within the United States—each independently establishing the requisite territorial nexus.

E. Damages

126. As a direct and proximate result of Defendants' violations of the law of nations, Plaintiff has suffered damages in excess of approximately $1.5 billion, including the value of the stolen cryptocurrency assets, the costs of investigating and remediating the attack, and consequential business losses.

COUNT III

Racketeer Influenced and Corrupt Organizations Act, 18 U.S.C. §§ 1961-1968

127. Plaintiff realleges and incorporates by reference all preceding paragraphs.

128. At all relevant times, Plaintiff is and has been a "person" within the meaning of 18 U.S.C. § 1961(3), and a "person injured in his business or property by reason of a violation of" RICO within the meaning of 18 U.S.C. § 1964(c).

129. At all relevant times, each Defendant is and has been a "person" within the meaning of 18 U.S.C. §§ 1961(3) and 1962(c).

130. DPRK is a "person" within the meaning of 18 U.S.C. § 1961(3), which defines "person" to include "any individual or entity capable of holding a legal or beneficial interest in property." DPRK demonstrably holds a beneficial interest in the stolen cryptocurrency proceeds:

the U.N. Panel of Experts has documented that DPRK claims and exercises control over the proceeds of Lazarus Group's cryptocurrency thefts, directing those funds to its weapons of mass destruction and ballistic missile programs. The FSIA itself recognizes foreign states and their instrumentalities as legal entities capable of holding property. 28 U.S.C. § 1603(b); *cf. Pfizer Inc. v. Government of India*, 434 U.S. 308, 318 (1978) (holding that the Sherman Act's definition of "person" includes foreign governments). Even if the Court declines to treat DPRK itself as a person, however, Plaintiff's RICO claim against the DPRK survives because, as the Court has recognized, the FSIA permits RICO claims against foreign states. *Southway v. Central Bank of Nigeria*, 198 F.3d 1210, 1218 (10th Cir. 1999) (holding that the FSIA confers jurisdiction over civil RICO claims against foreign states when a statutory exception applies); *see also Turkiye Halk Bankasi A.S. v. United States*, 598 U.S. 264 (2023) (holding that the FSIA does not immunize foreign states from criminal proceedings).

131. Defendants John Does 1–20 are likewise "persons" within the meaning of 18 U.S.C. § 1961(3). On information and belief, the John Doe Defendants are individuals and/or entities who hold or control wallets containing traceable stolen assets and who have participated in laundering the proceeds of the theft. Each is capable of holding a legal or beneficial interest in property, as demonstrated by their possession and control of cryptocurrency wallets containing stolen assets.

132. Under 18 U.S.C. § 1964(c), Plaintiff is entitled to recover treble damages plus costs and attorneys' fees from Defendants.

A. RICO Enterprise

133. Lazarus Group is a group of persons associated together in fact for the common purpose of carrying out an ongoing criminal enterprise, as described in the foregoing paragraphs

of this Complaint. Specifically, Lazarus Group has executed numerous criminal schemes that harm and threaten to continue to harm Plaintiff, its users, and the general public.

134. Defendants act with the common purpose of enriching themselves by fraudulently obtaining sensitive information and stealing valuable assets.

135. Defendants constitute an association-in-fact enterprise within the meaning of 18 U.S.C. §§ 1961(4) and 1962(c). At all relevant times, Lazarus Group has been engaged in cybercriminal activities, and its activities have affected interstate and foreign commerce within the meaning of 18 U.S.C. § 1962(c).

B. Pattern of Racketeering Activity and RICO Predicate Acts

136. At all relevant times, Defendants have conducted or participated in, directly or indirectly, the conduct, management, and/or operation of Lazarus Group's activities through a pattern of racketeering activity within the meaning of 18 U.S.C. § 1961(5) and in violation of 18 U.S.C. § 1962(c).

137. Defendants have directly or indirectly engaged in an unlawful pattern of racketeering activity involving multiple RICO predicate offenses, including wire fraud in violation of 18 U.S.C. § 1343, money laundering in violation of 18 U.S.C. § 1956, and violations of the Computer Fraud and Abuse Act in violation of 18 U.S.C. § 1030.

138. Defendants' pattern of racketeering activity includes at least the following separate incidents: (i) the February 21, 2025 hack of Bybit resulting in the theft of $1.5 billion; (ii) the March 2022 theft of approximately $620 million from the Ronin blockchain project; (iii) the June 2022 theft of $100 million from Harmony; and (iv) the 2023 cryptocurrency platform heists that resulted in DOJ civil forfeiture actions.

139. Defendants' pattern of racketeering activity further includes the January 2025 theft of cryptocurrency assets from Phemex, an incident publicly attributed to DPRK and Lazarus Group. Forensic tracing has established that separately identifiable proceeds of the Bybit theft and separately identifiable proceeds of the Phemex theft are held in at least one wallet under Defendants' common control, demonstrating an integrated laundering operation that spans multiple hacks and confirming the existence of an ongoing criminal enterprise rather than a series of unconnected incidents.

140. Wire Fraud (18 U.S.C. § 1343): Defendants, with intent to defraud and obtain money or property by means of false or fraudulent pretenses, committed wire fraud in violation of 18 U.S.C. § 1343 by transmitting malicious JavaScript code through AWS servers in interstate commerce, transmitting unauthorized commands that redirected approximately $1.5 billion in Ethereum and Ethereum-based digital assets to wallets controlled by Defendants, and transmitting subsequent wire communications transferring and converting the stolen cryptocurrency through mixers, exchanges, and cross-chain bridges to obscure the funds' origin.

141. Money Laundering (18 U.S.C. § 1956): In using such cryptocurrency mixers, cross-chain bridges, and decentralized cryptocurrency exchanges to evade detection, Defendants conducted financial transactions involving cryptocurrency assets stolen from Bybit. Defendants conducted these transactions knowing that the assets represented proceeds of racketeering activity and that the transactions were designed to conceal the nature, source, or ownership of the proceeds.

142. Computer Fraud (18 U.S.C. § 1030): As alleged in Count I, by using malicious code to access or cause to be accessed protected computers of Bybit, Safe{Wallet}, and AWS without authorization and ultimately causing damage, Defendants violated the Computer Fraud and Abuse Act, 18 U.S.C. § 1030, which is a RICO predicate offense under 18 U.S.C. § 1961(1)(B).

C. Conspiracy

143. Defendants have not undertaken the practices described herein in isolation, but rather as part of a common scheme. In violation of 18 U.S.C. § 1962(d), each Defendant unlawfully, knowingly, and willfully agreed and conspired together to violate 18 U.S.C. § 1962(c) as described above.

144. Defendants knew that they were engaged in a conspiracy to commit multiple predicate offenses and that the predicate offenses were part of a pattern of racketeering activity. This conduct constitutes a conspiracy to violate 18 U.S.C. § 1962(c), in violation of 18 U.S.C. § 1962(d).

145. Plaintiff has been directly injured by Defendants' criminal enterprise perpetrating wire fraud, money laundering, and Computer Fraud and Abuse Act violations. But for the alleged pattern of racketeering activity, Plaintiff would not have incurred damages.

COUNT IV

Unjust Enrichment

146. Plaintiff realleges and incorporates by reference all preceding paragraphs.

147. The digital tokens stolen and converted by the Defendants were the personal property of Plaintiff and some of those tokens are currently being held in the wallets controlled by the Defendants. The stolen cryptocurrency assets and their exchange proceeds, including proceeds held in wallets or accounts controlled by the Doe Defendants or held by cryptocurrency exchanges, Virtual Asset Service Providers ("VASPs"), custodial platforms, or financial institutions, are directly traceable to the theft perpetrated by the Defendants. The stolen assets constitute property taken in violation of international law, and Defendants' continued retention of such property—including traceable proceeds held on U.S.-based cryptocurrency exchanges—constitutes unjust enrichment warranting the imposition of a constructive trust.

148. The Defendants acquired the digital tokens and fiat currencies in the wallets illegally and have no right to maintain possession of these digital tokens and fiat currencies.

149. Any and all assets being held by Defendants in the wallets must be held in trust for Plaintiff's benefit, and Defendants are not entitled to the benefit of wrongfully misappropriated, converted and stolen cryptocurrency assets that were taken from Plaintiff.

COUNT V

Conversion

150. Plaintiff realleges and incorporates by reference all preceding paragraphs.

151. As more fully alleged above, Defendants misappropriated Plaintiff's funds.

152. Defendants have converted Plaintiff's funds to their own use or to the use of others not entitled thereto and have exercised dominion and control over the funds to Plaintiff's exclusion and detriment.

153. In converting these funds, Defendants acted with willful disregard of Plaintiff's rights to use and possess them.

154. Plaintiff is entitled to compensatory and punitive damages proximately caused by Defendants' willful conversion of Plaintiff's property.

COUNT VI

Replevin (D.C. Code § 16-3701 et seq.)

155. Plaintiff realleges and incorporates by reference all preceding paragraphs.

156. Plaintiff was, and remains, the rightful owner of and entitled to immediate possession of the approximately $1.5 billion in cryptocurrency assets stolen from it on February 21, 2025, and the proceeds for which any portion of those assets has been exchanged.

157. Defendants, through Lazarus Group and the John Doe Defendants acting at Defendants' direction and for their benefit, wrongfully took possession of those assets on February

21, 2025, and continue to wrongfully detain those assets—and the proceeds for which those assets have been exchanged—in wallets under Defendants' control.

158. The stolen cryptocurrency and its exchange proceeds are specific, identifiable personal property. Each tranche of stolen assets, and each transaction in which a stolen tranche has been exchanged for other digital assets, is independently and individually recorded on the public blockchain ledger and remains traceable to the February 21, 2025 theft. Bybit has traced a significant portion of the stolen assets and their proceeds through public blockchain forensics.

159. The stolen assets are personal property within the meaning of D.C. Code § 16-3701 because they are intangible things subject to ownership. The District of Columbia recognizes electronic and digital assets as personal property. *See United States v. Navarro*, 664 F. Supp. 3d 48, 60–61 (D.D.C. 2023).

160. To the extent any portion of the stolen assets has been concealed, transferred through mixing services, or otherwise placed beyond ready reach of judicial process, Defendants have eloigned those assets within the meaning of D.C. Code §§ 16-3712 and 16-3713, and the Court may assess damages sufficient to compel their return.

161. Bybit demands the return of its stolen cryptocurrency and the exchange proceeds thereof. In the alternative, to the extent return in specie is not possible, Bybit is entitled to the value of the stolen assets, plus damages for the detention.

COUNT VII

Trespass to Chattels

162. Plaintiff realleges and incorporates by reference all preceding paragraphs.

163. Defendants intentionally and without authorization accessed, interfered with, and exercised dominion over Plaintiff's computer systems and Plaintiff's digital assets, including approximately 401,347 ETH, 90,375 stETH, 8,000 mETH, 15,000 cmETH, and 90 USDT

(together, valued at approximately $1.5 billion at the time of the theft) held in Plaintiff's multi-signature cold wallet. Plaintiff held a possessory interest in both the computer systems through which the digital assets were managed and in the digital assets themselves, which constitute intangible personal property—i.e., chattels—under District of Columbia law. Defendants' unauthorized intrusion into Plaintiff's computer systems and their unauthorized transfer and dispossession of Plaintiff's digital assets intermeddled with and dispossessed Plaintiff of those chattels, proximately causing actual damages to Plaintiff and Plaintiff's customers.

164. Defendants' trespass to Plaintiff's chattels was willful, malicious, and conducted as part of a state-sponsored campaign of cybertheft. Plaintiff is entitled to recover from Defendants all damages proximately caused by Defendants' trespass to chattels, including but not limited to the full value of the digital assets of which Plaintiff was dispossessed, consequential damages, punitive damages, and any other relief the Court deems just and proper.

COUNT VIII

Fraud

165. Plaintiff realleges and incorporates by reference all preceding paragraphs.

166. On February 21, 2025, Defendants made false representations to Plaintiff by causing Plaintiff's computer systems to display materially inaccurate information about a multisig transaction. Specifically, Defendants replaced legitimate JavaScript resources served by the Safe{Wallet} interface with malicious versions specifically designed to activate when Bybit's particular wallets initiated a transaction. When three Bybit executives went to approve what they understood to be a routine transfer of Ethereum and Ethereum-based assets from a cold wallet to a warm wallet, their screens displayed what appeared to be a legitimate transaction sending funds to the correct Bybit wallet address. However, unbeknownst to the executives, the malicious code caused them to unknowingly approve an unauthorized upgrade of Bybit's cold-wallet smart

contract to a malicious implementation contract that the attackers had pre-deployed. The malicious contract contained hidden backdoor functions, which, once triggered, the attackers used to swiftly redirect the $1.5 billion in digital assets to wallets controlled by the DPRK operatives.

167. Defendants made these false representations with knowledge of their falsity, with actual intent to induce Plaintiff's executives to approve the fraudulent transaction, and with willful disregard for Plaintiff's rights to use and possess the underlying funds. In reasonable reliance on the information displayed on their screens, three Bybit executives digitally signed and approved the transaction, believing it to be a routine internal transfer.

168. As a direct and proximate result of Defendants' fraud, approximately $1.5 billion in Ethereum and Ethereum-based digital assets was redirected from Plaintiff's cold wallet to wallets controlled by Defendants, against Plaintiff's will and without Plaintiff's knowledge or consent. To the extent that additional details regarding the identities and specific roles of individual Defendants remain unknown, such information is peculiarly within Defendants' knowledge and control, and Plaintiff will seek to identify such details through discovery.

169. Plaintiff is entitled to compensatory and punitive damages as a result of Defendants' fraud.

COUNT IX

Tortious Interference with Contract

170. Plaintiff realleges and incorporates by reference all preceding paragraphs.

171. At the time of the attack, Plaintiff maintained contractual relationships with (i) Safe{Wallet}, which provided multisig transaction management services to Plaintiff pursuant to a service agreement, and (ii) its customers, who maintained digital assets on Plaintiff's platform pursuant to Plaintiff's terms of service.

172. Defendants were aware of these contractual relationships. Defendants specifically targeted Plaintiff's relationship with Safe{Wallet}, selecting Safe{Wallet}'s infrastructure as the attack vector for the express purpose of compromising the services Safe{Wallet} provided to Plaintiff.

173. Defendants intentionally and improperly interfered with Plaintiff's contract with Safe{Wallet} by infiltrating Safe{Wallet}'s systems, stealing developer credentials, and injecting malicious JavaScript code into Safe{Wallet}'s AWS-hosted infrastructure. This interference caused Safe{Wallet} to fail to perform its core contractual obligation of providing secure multisig transaction management to Plaintiff. Defendants' conduct caused Safe{Wallet}'s performance to fail by subverting the very security infrastructure that Safe{Wallet} was contractually obligated to maintain, and that failure was the direct mechanism through which Defendants stole Plaintiff's assets.

174. Defendants also intentionally interfered with Plaintiff's contractual relationships with its customers. Defendants' theft placed Plaintiff in a position where it would have been unable to meet its custody obligations to its customers absent extraordinary emergency measures. Plaintiff was forced to secure emergency bridge financing, deploy crisis management resources, and expend millions of dollars to ensure that all customer withdrawal demands were met within 12 hours of the attack.

175. As a direct and proximate result of Defendants' interference, Plaintiff has suffered significant losses, including the full value of the approximately $1.5 billion in stolen assets, the costs of emergency financing, crisis management, enhanced security measures, bounty payments, and reputational harm to its customer and vendor relationships.

176. The actions of Defendants were malicious and illegal and were done without any lawful justification and for the purpose of causing harm to Plaintiff. As a result, Plaintiff is also entitled to recover punitive damages against Defendants for their tortious interference.

COUNT X

Declaratory Judgment, 28 U.S.C. § 2201

177. Plaintiff realleges and incorporates by reference all preceding paragraphs.

178. An actual controversy exists between Plaintiff and Defendants concerning the ownership of and rights to the cryptocurrency assets stolen from Plaintiff on February 21, 2025, and their exchange proceeds, currently held in wallets and accounts controlled by Defendants.

179. Plaintiff seeks a declaration of rights under the Declaratory Judgment Act, 28 U.S.C. § 2201, which provides that "in a case of actual controversy within its jurisdiction . . . any court of the United States . . . may declare the rights and other legal relations of any interested party seeking such declaration."

180. Plaintiff seeks a declaratory judgment that: (i) the cryptocurrency assets stolen from Plaintiff on February 21, 2025, and their exchange proceeds, are the rightful property of Plaintiff; (ii) Defendants have no legitimate claim, right, title, or interest in such assets; (iii) all such assets were acquired by Defendants through unlawful means including unauthorized computer access, fraud, and theft; (iv) Plaintiff is entitled to the immediate return of all such assets or their equivalent value; and (v) the cryptocurrency wallets and accounts under Defendants' control contain property stolen from Plaintiff.

181. A declaratory judgment on these issues will clarify the parties' rights and obligations, facilitate the recovery of stolen assets, and assist cryptocurrency exchanges and other third parties in determining how to respond to Plaintiff's requests to freeze or return the stolen assets. Plaintiff has no adequate remedy at law for the resolution of this controversy.

182. Upon information and belief, Defendants John Does 1 through 20 are individuals and/or entities who, acting at the direction of, in concert with, or for the benefit of DPRK, have received, transferred, converted, commingled, or otherwise exercised control over Plaintiff's stolen digital assets or their traceable proceeds. Plaintiff has traced the stolen assets and their proceeds through public blockchain forensics to identifiable wallets and intermediaries in which they presently reside. The John Doe Defendants hold or control those traceable assets without any legitimate ownership interest, legal right, or colorable claim of title, and their possession of such assets is the direct and proximate result of the theft and laundering scheme described herein. Plaintiff is entitled to a declaration pursuant to 28 U.S.C. § 2201 that (a) the John Doe Defendants have no legal or equitable right, title, or interest in the stolen digital assets or their traceable proceeds; (b) such assets remain the property of Plaintiff; and (c) any interest asserted by the John Doe Defendants in those assets is void and of no force or effect.

183. Plaintiff is further entitled to a declaration that any cryptocurrency exchange, custodial platform, or other third-party intermediary identified through tracing that holds, controls, or maintains accounts containing Plaintiff's stolen digital assets or their traceable proceeds is obligated, upon identification of the John Doe Defendants and the accounts they control, to freeze, sequester, and ultimately return such assets to Plaintiff. An actual and justiciable controversy exists between Plaintiff and the John Doe Defendants—and between Plaintiff and the exchanges and platforms that hold the traceable assets—regarding the ownership, control, and disposition of those assets, and a declaratory judgment will serve the useful purpose of clarifying the parties' rights and guiding the exchanges in discharging their legal obligations with respect to the stolen property.

PRAYER FOR RELIEF

Plaintiff demands a trial by jury and respectfully requests that this Court:

184. Grant judgment in favor of Plaintiff and against Defendants on all causes of action;

185. Enter a declaratory judgment that: (i) the cryptocurrency assets stolen from Plaintiff on February 21, 2025, are the rightful property of Plaintiff; (ii) Defendants have no legitimate claim, right, title, or interest in such assets; and (iii) Plaintiff is entitled to the immediate return of all such assets;

186. Declare that Defendants' conduct constitutes violations of the statutes and common law cited herein, including the Computer Fraud and Abuse Act, the Racketeer Influenced and Corrupt Organizations Act, and the Alien Tort Statute;

187. Grant Plaintiff's motion for a temporary restraining order prohibiting Defendants from further transferring, converting, or disposing of any stolen assets;

188. Grant all appropriate injunctive relief, including but not limited to orders: (i) requiring Defendants to disgorge and return to Plaintiff all stolen cryptocurrency assets and their proceeds; (ii) requiring Defendants to provide an accounting of all stolen assets and their disposition; and (iii) prohibiting Defendants from further transferring, converting, or disposing of any stolen assets; (iv) requiring any cryptocurrency exchange, custodial platform, or other VASP identified through tracing as holding, having held, or having received traceable proceeds of the February 21, 2025 theft to disclose: (a) the identification information for account holders controlling any wallet or account containing traceable proceeds; (b) the full transaction history of all accounts associated with such traceable proceeds; and (c) the current balance of all such accounts; and (v) authorizing Plaintiff to serve notice of this Court's orders on any downstream VASP or financial institution that receives transfers from wallets identified as containing traceable stolen proceeds, and directing such VASPs to freeze any such assets upon receipt of notice;

189. Order the return in specie to Plaintiff of the stolen cryptocurrency assets and their exchange proceeds pursuant to D.C. Code § 16-3701 et seq.; and, in the alternative, to the extent return in specie is not possible, award Plaintiff the full value of the stolen assets plus damages for the detention pursuant to D.C. Code §§ 16-3710 and 16-3713;

190. Impose a constructive trust on all stolen cryptocurrency assets and their traceable exchange proceeds, wherever held—including in wallets or accounts controlled by the John Doe Defendants, or held at any cryptocurrency exchange, VASP, custodial platform, or financial institution—for the benefit of Plaintiff;

191. Award Plaintiff compensatory damages in an amount to be proven at trial, including but not limited to: (i) the value of approximately $1.5 billion in stolen cryptocurrency; (ii) costs of forensic investigation and response; (iii) costs of the LazarusBounty program; (iv) costs of securing replacement reserves; (v) enhanced security costs; and (vi) consequential business losses;

192. Award Plaintiff treble damages pursuant to 18 U.S.C. § 1964(c) for Defendants' violations of the Racketeer Influenced and Corrupt Organizations Act;

193. Award Plaintiff punitive damages in an amount sufficient to punish Defendants for their malicious, willful, and wanton conduct and to deter similar conduct in the future;

194. Award Plaintiff reasonable costs and expenses, including reasonable attorneys' fees, pursuant to 18 U.S.C. § 1964(c) and other applicable law;

195. Award pre-judgment and post-judgment interest at the maximum rate permitted by law; and

196. Grant all such other and further relief as the Court may deem just and proper.

Dated: June 18, 2026

Respectfully submitted,

Travis LeBlanc (DC Bar # 496844)
Brian E. Nelson (DC Bar # 978426)
(Pro Hac Vice Forthcoming)
Carlton Forbes (DC Bar # 1656612)
Cooley LLP
1299 Pennsylvania Avenue, NW, Suite 700
Washington, District of Columbia 20004
Telephone: (202) 842-7800
Facsimile: (202) 842-7899
tleblanc@cooley.com
brian.nelson@cooley.com
cforbes@cooley.com

William Pao *(Pro Hac Vice Forthcoming)*
Jonathan Waxman *(Pro Hac Vice Forthcoming)*
Cooley LLP
350 South Grand Avenue, Suite 3200
Los Angeles, CA 90071
Telephone: (213) 561-3250
Facsimile: (213) 561-3244
wpao@cooley.com
jwaxman@cooley.com

Attorneys for Plaintiff Bybit Technology Limited