UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

| | |
|---|---|
| UNITED STATES OF AMERICA,<br><br>Plaintiff,<br><br>v.<br><br>ALL USDC ASSOCIATED WITH 36 VIRTUAL CURRENCY ADDRESSES ON 18 DIFFERENT BLOCKCHAINS,<br><br>Defendants *In Rem*. | Civ. No. 26-4150 |

**UNITED STATES' VERIFIED COMPLAINT FOR FORFEITURE *IN REM***

COMES NOW, Plaintiff, the United States of America (the "United States"), by and through the United States Attorney's Office for the District of Columbia, the Computer Crime and Intellectual Property Section of the Criminal Division, and the National Security Cyber Section of the National Security Division, which brings this verified complaint for forfeiture *in rem*, in accordance with Supplemental Rule G(2) of the Federal Rules of Civil Procedure, and alleges as follows:

**NATURE OF THE ACTION AND DEFENDANTS *IN REM***

1. This *in rem* forfeiture action arises out of an investigation by the U.S. Secret Service ("USSS"), the Federal Bureau of Investigation ("FBI"), and the Internal Revenue Service Criminal Investigation Division ("IRS-CI") into the recent hack of Binance where, on or about October 29, 2026, unauthorized criminal actors accessed Binance's network by unlawfully accessing Binance's protected computers and criminally obtained approximately $6 billion worth of virtual currency. Representatives from Binance confirmed that the transfer of these funds from its

business addresses was unauthorized. Because of that unauthorized access, the criminal actors were able to access approximately $6 billion worth of virtual currency from Binance and transfer it to addresses controlled by the criminal actors, including the addresses listed below.

2. The USSS, FBI, and IRS-CI assess that the hack and the subsequent theft of funds from Binance were perpetrated by members of North Korean military hacking groups known within the cybersecurity community as both the Lazarus Group and Advanced Persistent Threat 38[1] ("APT38") (hereinafter "Lazarus Group/APT38" or "criminal actors"). The USSS, FBI, and IRS-CI make that assessment based on technical indicators associated with the compromise and the patterns and methods used to launder the funds after they were criminally obtained.

3. The defendants *in rem* in this action are a portion of the virtual currency criminally obtained from Binance by the criminal actors and include all the USDC associated with the following virtual currency addresses (collectively, the "Defendant Property"):

a. The USDC associated with virtual currency address 0x5227f603c1ee34ce3c06efe6477003bdfccb2f8c on the Ethereum Network (or "Ethereum") (Subject Address A).

b. The USDC associated with virtual currency address 0xA97bF7836F8A08F9Ed91D41453D371493FAE8d10 on the Ethereum Network (Subject Address B).

[1] APT or "Advanced Persistent Threat" is a term used to define and identify groups of organized, highly skilled, and well-resourced cyber actors who maintain focused efforts on specific tasks such as intelligence gathering against specific business sectors or governments. APTs are known to gain access to computer networks while remaining undetected for extended periods. APTs are often nation-state or state-sponsored groups. Upon identification, the group is assigned a unique number as an identifier by the community: in this case, "APT38."

c. The USDC associated with virtual currency address 0xB3ddeC0cCC5C3ba733FCdf5a15f98c95Ec5a5FdB on the Ethereum Network (Subject Address C).

d. The USDC associated with virtual currency address 0xc39e690bea48448cc47e7acddfe30e6453e09824 on the Ethereum Network (Subject Address D).

e. The USDC associated with virtual currency address 0x28C6c06298d514Db089934071355E5743bf21d60 on the Ethereum Network (Subject Address E).

f. The USDC associated with virtual currency address 0x28C6c06298d514Db089934071355E5743bf21d60 on the Polygon PoS Network (or "Polygon") (Subject Address F).

g. The USDC associated with virtual currency address 0x28C6c06298d514Db089934071355E5743bf21d60 on the Arc Network (or "Arc") (Subject Address G).

h. The USDC associated with virtual currency address 0x28C6c06298d514Db089934071355E5743bf21d60 on the Arbitrum One Network (or "Arbitrum") (Subject Address H).

i. The USDC associated with virtual currency address 0x28C6c06298d514Db089934071355E5743bf21d60 on the Base Network (or "Base") (Subject Address I).

j. The USDC associated with virtual currency address 0xEe7aE85f2Fe2239E27D9c1E23fFFe168D63b4055 on the Arbitrum One Network (Subject Address J).

k. The USDC associated with virtual currency address 0xEe7aE85f2Fe2239E27D9c1E23fFFe168D63b4055 on the Arc Network (Subject Address K).

l. The USDC associated with virtual currency address 0xEe7aE85f2Fe2239E27D9c1E23fFFe168D63b4055 on the Avalanche Network (or "Avalanche") (Subject Address L).

m. The USDC associated with virtual currency address 0xEe7aE85f2Fe2239E27D9c1E23fFFe168D63b4055 on the Base Network (Subject Address M).

n. The USDC associated with virtual currency address 0xEe7aE85f2Fe2239E27D9c1E23fFFe168D63b4055 on the Celo Network (or "Celo") (Subject Address N).

o. The USDC associated with virtual currency address 0xEe7aE85f2Fe2239E27D9c1E23fFFe168D63b4055 on the Ethereum Network (Subject Address O).

p. The USDC associated with virtual currency address 0xEe7aE85f2Fe2239E27D9c1E23fFFe168D63b4055 on the Polygon PoS Network (Subject Address P).

q. The USDC associated with virtual currency address 0xEe7aE85f2Fe2239E27D9c1E23fFFe168D63b4055 on the OP Mainnet Network (or "Optimism") (Subject Address Q).

r. The USDC associated with virtual currency address 0xEe7aE85f2Fe2239E27D9c1E23fFFe168D63b4055 on the Sei Network (or "Sei") (Subject Address R).

s. The USDC associated with virtual currency address 0xEe7aE85f2Fe2239E27D9c1E23fFFe168D63b4055 on the Sonic Network (or "Sonic") (Subject Address S).

t. The USDC associated with virtual currency address 0xEe7aE85f2Fe2239E27D9c1E23fFFe168D63b4055 on the World Chain Network (or "World Chain") (Subject Address T).

u. The USDC associated with virtual currency address FzbcyEZ9m8xjtergWgWDq7mfPoHEbboBF791B6cTpzbq on the Solana Network (or "Solana") (Subject Address U).

v. The USDC associated with virtual currency address 0x8C1c499b1796D7F3C2521AC37186B52De024e58c on the Ethereum Network (Subject Address V).

w. The USDC associated with virtual currency address 0x28C6c06298d514Db089934071355E5743bf21d60 on the Avalanche Network (Subject Address W).

x. The USDC associated with virtual currency address 0x28C6c06298d514Db089934071355E5743bf21d60 on the Celo Network (Subject Address X).

y. The USDC associated with virtual currency address 0x28C6c06298d514Db089934071355E5743bf21d60 on the HyperEVM Network (or "HyperEVM") (Subject Address Y).

z. The USDC associated with virtual currency address 0x28C6c06298d514Db089934071355E5743bf21d60 on the Linea Network (or "Linea") (Subject Address Z).

aa. The USDC associated with virtual currency address 0x28C6c06298d514Db089934071355E5743bf21d60 on the Monad Network (or "Monad") (Subject Address AA).

bb. The USDC associated with virtual currency address 0x28C6c06298d514Db089934071355E5743bf21d60 on the OP Mainnet Network (Subject Address BB).

cc. The USDC associated with virtual currency address 0x28C6c06298d514Db089934071355E5743bf21d60 on the Plasma Network (or "Plasma") (Subject Address CC).

dd. The USDC associated with virtual currency address 0x28C6c06298d514Db089934071355E5743bf21d60 on the Sei Network (Subject Address DD).

ee. The USDC associated with virtual currency address 0x28C6c06298d514Db089934071355E5743bf21d60 on the Sonic Network (Subject Address EE).

ff. The USDC associated with virtual currency address 0x28C6c06298d514Db089934071355E5743bf21d60 on the Unichain Network (or "Unichain") (Subject Address FF).

gg. The USDC associated with virtual currency address 0x28C6c06298d514Db089934071355E5743bf21d60 on the World Chain Network (Subject Address GG).

hh. The USDC associated with virtual currency address 0x28C6c06298d514Db089934071355E5743bf21d60 on the XDC Network (or "XDC") (Subject Address HH).

ii. The USDC associated with virtual currency address 0xEe7aE85f2Fe2239E27D9c1E23fFFe168D63b4055 on the HyperEVM Network (Subject Address II).

jj. The USDC associated with virtual currency address 0xEe7aE85f2Fe2239E27D9c1E23fFFe168D63b4055 on the Linea Network (Subject Address JJ).

4. The virtual currency addresses above are referred to herein collectively as the "Subject Addresses." The Subject Addresses hold the following balances of USDC tokens:

| Virtual Currency Address | Blockchain Network | USDC Amount | Subject Address |
|---|---|---|---|
| 0x5227f603c1ee34ce3c06efe6477003bdfccb2f8c | Ethereum | 823,000,000.00 | A |
| 0xA97bF7836F8A08F9Ed91D41453D371493FAE8d10 | Ethereum | 123,175.5279 | B |
| 0xB3ddeC0cCC5C3ba733FCdf5a15f98c95Ec5a5FdB | Ethereum | 33,005.1171 | C |
| 0xc39e690bea48448cc47e7acddfe30e6453e09824 | Ethereum | 1,563,812.7833 | D |
| 0x28C6c06298d514Db089934071355E5743bf21d60 | Ethereum | 52,363.1195 | E |
| 0x28C6c06298d514Db089934071355E5743bf21d60 | Polygon | 50.0747 | F |
| 0x28C6c06298d514Db089934071355E5743bf21d60 | Arc | 1.7109 | G |
| 0x28C6c06298d514Db089934071355E5743bf21d60 | Arbitrum | 37.0135 | H |
| 0x28C6c06298d514Db089934071355E5743bf21d60 | Base | 604.3822 | I |
| 0xEe7aE85f2Fe2239E27D9c1E23fFFe168D63b4055 | Arbitrum | 3.0006 | J |
| 0xEe7aE85f2Fe2239E27D9c1E23fFFe168D63b4055 | Arc | 258927250.1328 | K |
| 0xEe7aE85f2Fe2239E27D9c1E23fFFe168D63b4055 | Avalanche | 3.0006 | L |
| 0xEe7aE85f2Fe2239E27D9c1E23fFFe168D63b4055 | Base | 60,000,000.0009 | M |
| 0xEe7aE85f2Fe2239E27D9c1E23fFFe168D63b4055 | Celo | 155,865.6557 | N |
| 0xEe7aE85f2Fe2239E27D9c1E23fFFe168D63b4055 | Ethereum | 2,956,093.6542 | O |
| 0xEe7aE85f2Fe2239E27D9c1E23fFFe168D63b4055 | Polygon | 3.0003 | P |
| 0xEe7aE85f2Fe2239E27D9c1E23fFFe168D63b4055 | Optimism | 3.0000 | Q |
| 0xEe7aE85f2Fe2239E27D9c1E23fFFe168D63b4055 | Sei | 3.0001 | R |
| 0xEe7aE85f2Fe2239E27D9c1E23fFFe168D63b4055 | Sonic | 16,670,009.5325 | S |
| 0xEe7aE85f2Fe2239E27D9c1E23fFFe168D63b4055 | World Chain | 662,591.9626 | T |
| FzbcyEZ9m8xjtergWgWDq7mfPoHEbboBF791B6cTpzbq | Solana | 1,972,502.7817 | U |
| 0x8C1c499b1796D7F3C2521AC37186B52De024e58c | Ethereum | 914,131.6968 | V |
| 0x28C6c06298d514Db089934071355E5743bf21d60 | Avalanche | 0 | W |
| 0x28C6c06298d514Db089934071355E5743bf21d60 | Celo | 0 | X |
| 0x28C6c06298d514Db089934071355E5743bf21d60 | HyperEVM | 0 | Y |
| 0x28C6c06298d514Db089934071355E5743bf21d60 | Linea | 0 | Z |
| 0x28C6c06298d514Db089934071355E5743bf21d60 | Monad | 0 | AA |
| 0x28C6c06298d514Db089934071355E5743bf21d60 | Optimism | 0 | BB |
| 0x28C6c06298d514Db089934071355E5743bf21d60 | Plasma | 0 | CC |
| 0x28C6c06298d514Db089934071355E5743bf21d60 | Sei | 0 | DD |
| 0x28C6c06298d514Db089934071355E5743bf21d60 | Sonic | 0 | EE |
| 0x28C6c06298d514Db089934071355E5743bf21d60 | Unichain | 0 | FF |
| 0x28C6c06298d514Db089934071355E5743bf21d60 | World Chain | 0 | GG |
| 0x28C6c06298d514Db089934071355E5743bf21d60 | XDC | 0 | HH |
| 0xEe7aE85f2Fe2239E27D9c1E23fFFe168D63b4055 | HyperEVM | 0 | II |
| 0xEe7aE85f2Fe2239E27D9c1E23fFFe168D63b4055 | Linea | 0 | JJ |

5. The Defendant Property was restrained pursuant to a Temporary Restraining Order issued by the U.S. District Court for the District of Columbia on November 12, 2026, pursuant to 18 U.S.C. § 983(j) and 28 U.S.C. § 1355(d), and served on U.S.-based Circle Internet Financial, LLC ("Circle") the same day.

6. The Defendant Property is subject to forfeiture pursuant to 18 U.S.C. § 981(a)(1)(C) as property representing proceeds of computer fraud in violation of 18 U.S.C. § 1030.

7. The Defendant Property is also subject to forfeiture pursuant to 18 U.S.C. § 981(a)(1)(C) as property representing proceeds of wire fraud, 18 U.S.C. § 1343, and a conspiracy to commit wire fraud, 18 U.S.C. § 1349.

8. The Defendant Property is also subject to forfeiture pursuant to 18 U.S.C. § 981(a)(1)(A) because it is property involved in money laundering and a conspiracy to commit money laundering, in violation of 18 U.S.C. § 1956, with the intent to promote or conceal specified unlawful activities, *viz.*, computer fraud, in violation of 18 U.S.C. § 1030, wire fraud, in violation of 18 U.S.C. § 1343, and conspiracy to commit wire fraud, in violation of 18 U.S.C. § 1349.

**JURISDICTION AND VENUE**

9. This Court has subject matter jurisdiction over a United States forfeiture action and *in rem* jurisdiction over the Defendant Property pursuant to 28 U.S.C. §§ 1345 and 1355.

10. Venue is also proper within this judicial district pursuant to 28 U.S.C. § 1395.

11. Additionally, as explained above and below, this case involves Lazarus Group/APT38 actors hacking into a victim's online network and conducting unauthorized withdrawals of virtual currency. These transactions caused "damage without authorization" to "protected computers"—namely, nodes (i.e., computers) running as part of the Ethereum Network and various other blockchain networks. *See* 18 U.S.C. §§ 1030(a)(5)(A) and (e)(2)(B). More

specifically, Ethereum Network data was damaged, without authorization, when the criminal actors initiated transactions that caused the data to reflect these unauthorized transfers. The Ethereum Network operates via a web of interconnected computers all around the world, including in the U.S. Those nodes in the U.S. are the protected computers in this case. Notably, there were multiple Ethereum Network nodes running in Washington, D.C. at the time the transactions discussed herein took place.

**STATUTORY AUTHORITY**

12. This investigation relates to violations of 18 U.S.C. § 1030 (the Computer Fraud and Abuse Act); 18 U.S.C. § 1343 (Wire Fraud); 18 U.S.C. § 1349 (Conspiracy to Commit Wire Fraud); 18 U.S.C. § 1956 (Money Laundering); and 18 U.S.C. § 1956(h) (Conspiracy to Commit Money Laundering).

13. **Computer Fraud and Abuse**: Title 18, United States Code, Section 1030(a)(2) makes it a crime, *inter alia*, to intentionally access a computer without authorization and thereby obtain information from any protected computer. Title 18, United States Code, Section 1030(a)(4) makes it a crime, *inter alia*, to knowingly and with intent to defraud, access a protected computer without authorization, and by means of such conduct further the intended fraud and obtain anything of value. The term "protected computer" is defined in Title 18, United States Code, Section 1030(e)(2) and includes, *inter alia*, a computer used in or affecting interstate or foreign commerce or communication, including a computer located outside the United States that is used in a manner that affects interstate or foreign commerce or communication of the United States. *See Van Buren v. United States*, 141 S. Ct. 1648, 1652 (2021) (definition of protected computer under 18 U.S.C. § 1030(e)(2)(B) includes "at a minimum . . . all computers that connect to the Internet").

14. **Wire Fraud**: Title 18, United States Code, Section 1343 makes it a crime for anyone, having devised or intending to devise any scheme or artifice to defraud, or for obtaining money or property by means of false or fraudulent pretenses, representations, or promises, to transmit or cause to be transmitted by means of wire, radio, or television communication in interstate or foreign commerce, any writings, signs, signals, pictures, or sounds for the purpose of executing such scheme or artifice.

15. **Conspiracy to Commit Wire Fraud**: Title 18, United States Code, Section 1349 criminalizes a conspiracy to violate Title 18, United States Code, Section 1343.

16. **Money Laundering**: Title 18, United States Code, Section 1956(a)(1)(A)(i) makes it a crime to conduct or attempt to conduct a financial transaction, knowing that the property involved in the transaction represents the proceeds of some form of unlawful activity, and which in fact involves the proceeds of specified unlawful activity, with the intent to promote the carrying on of specified unlawful activity. This offense is sometimes referred to as promotional money laundering. Title 18, United States Code, Section 1956(a)(1)(B)(i) makes it a crime to conduct or attempt to conduct a financial transaction, knowing that the property involved in the transaction represents the proceeds of some form of unlawful activity, and which in fact involves the proceeds of specified unlawful activity, knowing that the transaction is designed in whole or in part to conceal or disguise the nature, the location, the source, the ownership, or the control of the proceeds of specified unlawful activity. This offense is sometimes referred to as "concealment" money laundering.

17. The term "specified unlawful activity" is defined in Title 18, United States Code, Sections 1956(c)(7) and 1961(1), and it includes violations of Title 18, United States Code,

Section 1030 (computer fraud and abuse), Title 18, United States Code, Section 1343 (wire fraud), and Title 18, United States Code, Section 1349 (wire fraud conspiracy).

18. **Conspiracy to Commit Money Laundering**: Title 18, United States Code, Section 1956(h) criminalizes a conspiracy to violate Title 18, United States Code, Section 1956.

**FORFEITURE AUTHORITY**

19. Forfeiture of the Defendant Property is authorized pursuant to 18 U.S.C. § 981(a)(1)(C) (forfeiture of "proceeds" of criminal offenses and property traceable thereto) and 18 U.S.C. § 981(a)(1)(A) (forfeiture of property "involved in" money laundering and property traceable thereto).

20. **Forfeiture of criminal "proceeds":** Pursuant to 18 U.S.C. § 981(a)(1)(C), any property, real or personal, which constitutes or is derived from "proceeds" traceable to a violation of an offense involving specified unlawful activity as defined in 18 U.S.C. §§1956(c)(7) and 1961(1) (which includes computer fraud and wire fraud violations), or a conspiracy to commit such offenses, is subject to civil forfeiture.

21. **Forfeiture of property "involved in" specific offenses**: Pursuant to 18 U.S.C. § 981(a)(1)(A), "[a]ny property, real or personal, involved in a transaction or attempted transaction in violation of section 1956, 1957 or 1960 of this title, or any property traceable to such property" is subject to forfeiture to the United States.

22. Forfeiture pursuant to these statutes applies to more than just the proceeds of the crime. These forfeitures encompass all property "involved in" the crime or the attempted crime, which includes "clean" money that is commingled with "tainted" money derived from illicit sources. *See* 18 U.S.C. § 983(c)(3); *see, e.g.*, *United States v. Silver*, 864 F.3d 102 (2d Cir. 2017); *United States v. Rutgard*, 116 F.3d 1270, 1286 (9th Cir. 1997). This commingling is a laundering

technique that facilitates the scheme because it obfuscates the trail of the illicit funds. *See United States v. Huber*, 404 F.3d 1047, 1058 (8th Cir. 2005) (the presence of legitimate funds does not make a money laundering transaction lawful; it is only necessary to show that the transaction involves criminal proceeds).

## FACTS GIVING RISE TO FORFEITURE

### I. Relevant Background Regarding Virtual Currency Concepts

23. **Virtual Currency**: Virtual currencies are digital tokens of value circulated over the Internet as substitutes for traditional fiat currency. Virtual currencies are not issued by any government or bank like traditional fiat currencies (such as the U.S. dollar) but are generated and controlled through computer software and a computer network. Bitcoin is currently the most well-known virtual currency in use.

24. **Virtual Currency Address**: Virtual currency addresses are the virtual locations to which such currencies are sent and received. A virtual currency address is analogous to a bank account number and is represented as a string of alphanumeric characters.

25. Each virtual currency address is controlled using a unique corresponding private key, a cryptographic equivalent of a password needed to access the address. Only the holder of an address's private key can authorize a transfer of virtual currency from that address to another address.

26. **Virtual Currency Wallet:** A virtual currency wallet is a software application that interfaces with the virtual currency's specific blockchain and generates and stores a user's addresses and private keys. A virtual currency wallet also allows users to send and receive virtual currencies. Multiple addresses can be stored in a wallet.

27. **Virtual Currency Exchanges (VCEs)**: Companies known as virtual currency "exchanges" may hold the value associated with a customer's virtual currency in that exchange's own wallet. Such a wallet is known as a custodial wallet because the exchange is the third-party custodian of the virtual currency. Alternatively, a user of virtual currency may elect to keep their virtual currency in their own wallets (i.e., self-hosted or non-custodial wallets). A custodial wallet is the functional equivalent of a bank holding a customer's funds. Criminals often seek to use exchanges to exchange illicitly obtained virtual currency for currency.

28. **Blockchain**: Many virtual currencies publicly record all their transactions on what is known as a "blockchain." The blockchain is essentially a distributed public ledger on a computer network, run by a decentralized network of trusted persons, designed to contain an immutable and historical record of every transaction utilizing that blockchain's technology. The blockchain can be updated multiple times per hour by the trusted persons and records every virtual currency address that ever received that virtual currency. It also maintains records of every transaction and all the known balances for each virtual currency address. There are different computer network blockchains for different types of virtual currencies.

29. **USDC**: USDC is a "stablecoin"—a type of virtual currency pegged to a commodity's price, such as gold, or to a fiat currency, such as the U.S. dollar. Stablecoins achieve their price stability via collateralization (backing) or through algorithmic mechanisms of buying and selling the reference asset or its derivatives. USDC is pegged to the price of the U.S. dollar and is minted (i.e., issued or created) by Circle, a company headquartered in New York. As explained below, USDC is held in virtual currency addresses that exist on various blockchains, including the Ethereum network.

30. **Circle Internet Financial, LLC:** Circle is a company that issues USDC and manages the smart contracts and the treasury (i.e., the funds held in reserve) for USDC. Circle, as the issuer of USDC, has the technical ability to block individual addresses on blockchains where Circle issues USDC from sending or receiving USDC, a process known as "blocklisting" or "access denial."

31. **Mixing Services:** A service that uses pooling, redistribution, or other transaction techniques to obscure the connection between cryptocurrency received and cryptocurrency subsequently transferred. Such services can make it more difficult to trace funds and identify the parties associated with particular transfers.

32. **Smart Contracts:** Smart contracts allow developers to create markets, store registries of debts, and move funds in accordance with the instructions provided in the contract's code, without any type of middleman or counterparty controlling a desired or politically motivated outcome, all while using blockchain distributed ledger protocols to maintain transparency. Smart contract technology is one of the distinguishing characteristics of the Ethereum network (as well as many other blockchains) and an important tool for companies or individuals executing trades on various blockchains. When engaged, smart contracts automatically execute according to the terms of the contract written into lines of computer code. A transaction contemplated by a smart contract occurs on the Ethereum blockchain and is both trackable and irreversible.

33. **Contract Call:** A request to execute a specific function of a smart contract, which is a computer program deployed on a blockchain, such as Ethereum. Depending on the function requested, a contract call may retrieve information or initiate an action, such as transferring virtual currency or authorizing another party to transfer virtual currency.

## II. Background Regarding Circle's Ability to Blocklist Addresses Containing USDC and to Issue an Equivalent Amount of USDC

34. As previously explained, all of the USDC associated with the Subject Addresses is collectively referred to herein as the Defendant Property. The United States cannot access the Defendant Property because the blocklisted Subject Addresses remain under the control of Lazarus Group/APT38 criminal actors. Circle advises the United States that it does not have the technical ability to transfer the Defendant Property from the blocklisted Subject Addresses to the United States but has agreed to voluntarily issue new USDC in an amount equivalent to the amount of the Defendant Property (the "Substitute USDC") and transfer the Substitute USDC to the United States upon receipt of an Order of Forfeiture from the Court.

## III. Background Regarding U.S. Law Enforcement's Investigation of the North Korean Military Group Known as the Lazarus Group/APT38

35. The USSS, FBI, and IRS-CI are currently investigating numerous criminal schemes perpetrated by the criminal actors, in which the criminal actors commit unlawful intrusions into victims' computers via trick, fraud, and/or advanced computer intrusion methods, and then criminally obtain the victims' virtual currency. The criminal actors then launder these criminally-obtained proceeds through a sophisticated network of transactions. This type of criminal scheme is referred to hereafter as a "heist."

36. The USSS, FBI, and IRS-CI assess that the Lazarus Group/APT38 appears to be responsible for these heists based on, among other things, distinctive tactics, techniques, and procedures observed in other virtual currency heists linked to the Lazarus Group/APT38. Since at least late-2014, these criminal actors have engaged in cyber-attacks, intrusions, and attempted intrusions into computers and networks of, among others, U.S. and foreign entertainment companies, U.S. and foreign banks, U.S. cleared defense contractors and energy companies, U.S. and foreign virtual currency exchanges, information security researchers, and pharmaceutical

companies. The criminal actors have exhibited a particular focus on leveraging their malicious cyber activity to criminally obtain money and virtual currency from their victims. Since at least late 2014, the criminal actors have targeted banks and virtual currency exchanges and have successfully initiated fraudulent transfers at both. From at least 2017 through the present, the criminal actors have continued this targeting, and successfully conducted multiple virtual currency heists, netting billions of U.S. dollars of virtual currency. Below is a non-exhaustive list of recent examples:

a. In August 2021, Lazarus Group/APT38 criminally obtained approximately $90 million in virtual currency from Japan-based virtual currency exchange Liquid.

b. In March 2022, Lazarus Group/APT38 criminally obtained approximately $615 million in virtual currency from Singapore-based company Sky Mavis.

c. In June 2022, Lazarus Group/APT38 criminally obtained approximately $105 million in virtual currency from the U.S.-based blockchain platform Harmony.

d. In November 2023, Lazarus Group/APT38 criminally obtained approximately $138 million in virtual currency from Panama-based virtual currency exchange Poloniex.

e. In November 2023, Lazarus Group/APT38 criminally obtained approximately $107 million in virtual currency from Seychelles-based virtual currency exchange HTX.

f. In May 2024, Lazarus Group/APT38 criminally obtained approximately $308 million in virtual currency from Japan-based virtual currency exchange DMM Bitcoin.

g. In July 2024, Lazarus Group/APT38 criminally obtained approximately $235 million in virtual currency from India-based virtual currency exchange WazirX.

h. In February 2025, Lazarus Group/APT38 criminally obtained approximately $1.5 billion in virtual currency from United Arab Emirates-based virtual currency exchange Bybit.

i. In July 2026, Lazarus Group/APT38 criminally obtained approximately $24.15 million in virtual currency from virtual currency exchange AFX Trade.

37. Those involved in Lazarus Group/APT38-related activities appear to be part of an ongoing criminal conspiracy that appears to include the Binance heist, discussed below, and have regularly used U.S.-based computer infrastructure to facilitate intrusions that are part of these virtual currency heists.

## IV. Background Regarding the Binance Heist

38. The investigation thus far has revealed that on or about October 29, 2026, Binance employees learned that criminal actors had unlawfully accessed Binance's network and hot wallets (which are virtual currency wallets connected to the Internet) without authorization. Because of that unauthorized access, the criminal actors were able to access approximately $6 billion worth of virtual currency from Binance and transfer it to addresses controlled by the criminal actors.

39. After conducting an internal investigation, Binance informed law enforcement that the compromise of its computer was most likely caused by a Binance employee. In sum, the employee was contacted by a purported job recruiter. The Binance employee was interested in applying for the job and agreed to an interview. During the interview, the employee was told to download software. Unbeknownst to the Binance employee, that software contained malware. The

employee's compromised device allowed the criminal actors to install an EIP-7702 injection on the device.

40. EIP-7702 was introduced in a 2025 update to the Ethereum network. In practice, EIP-7702 is valuable to Ethereum users because it transforms regular Ethereum wallets into programmable smart contract wallets, allowing them to temporarily borrow advanced code execution features. For example, it allows users to combine multiple actions into one, such as requesting approval for a swap and the swap itself simultaneously. This saves time and money on transaction fees because, in a traditional setup, performing a swap of one token for another requires at least two separate sequential transactions: Transaction 1 approves the transfer of the tokens; Transaction 2 executes the actual trade. Each independent transaction has a cost associated with it. EIP-7702 temporarily behaves like a smart contract so that a user can bundle these actions into a single transaction payload.

41. Because an EIP-7702 delegation hands over control of an entire account's behavior, rather than granting a single token approval, signing a malicious authorization allows attackers to hijack the wallet's execution logic. This feature can be used by criminal actors to take control of or gain unauthorized access to smart contracts under another individual's control. In this instance, Binance has indicated that the unauthorized criminal actors exploited EIP-7702 and took control of Binance's hot wallets. The criminal actors then used EIP-7702 to send transactions containing authorizations that called a "sweeper" contract, which was used to automatically transfer (i.e., "sweep up") funds as soon as they were received.

## V. Following the Trail of Stolen Binance Funds

42. In this case, once the criminal actors obtained control over Binance's hot wallets, they were able to access USDC (and other types of virtual currencies) from Binance and then

transfer the funds to addresses on several blockchain networks. For the purposes of this filing, only those transactions that are relevant to the Subject Addresses are discussed below:

43. First, on October 29, 2026, at approximately 20:41 UTC, the unauthorized criminal actors conducted a transfer from Binance on the Ethereum network for approximately $780 million in USDC to address 0x5227f603c1ee34ce3c06efe6477003bdfccb2f8c (Subject Address A).

44. Then, at 20:59 UTC on October 29, 2026, the criminal actors conducted a transfer from Binance on the Ethereum Network for approximately $43 million in USDC to the same address, Subject Address A.

45. Next, at 22:39 UTC on October 29, 2026, the criminal actors conducted a transfer from Binance on the MASK network for 1,141,407.06 USDC to address: 0xA97bF7836F8A08F9Ed91D41453D371493FAE8d10 (Subject Address B).

46. Notably, law enforcement's review of blockchain activity revealed additional transfers from Binance at around the same time. For instance, at 20:24 UTC on October 29, 2026, the criminal actors accessed 9,707,546.77 USDe—a collateral stablecoin issued by the Ethena Labs protocol—from Binance and transferred the funds to Subject Address A. Following the deposit into Subject Address A, at 20:56 UTC on October 29, 2026, the criminal actors transferred the 9,707,546.77 USDe to address 0xB3ddeC0cCC5C3ba733FCdf5a15f98c95Ec5a5FdB (Subject Address C), where the 9,707,546.77 USDe was exchanged for 33,005.11 USDC on the Ethereum Network.

47. At 20:35 UTC on October 29, 2026, the unauthorized criminal actors accessed 573,469 AVAX (a type of virtual currency that is native to the Avalanche blockchain) and transferred it to Subject Address A. Following the deposit into Subject Address A, the funds were

transferred in two separate transactions to address 0x80358c5b8f9b2cc27147a1e0f2a6c9a30eb2c397.

48. The criminal actors continued to break up, disperse, and distribute the AVAX through other virtual currency wallets, where a portion of the funds were reconsolidated with other funds obtained from the heist. The funds were then sent through virtual currency bridge networks and swapping services (i.e., virtual currency platforms that allow users to go from one blockchain to another and/or from one virtual currency to another) until they amounted to 1,563,812.78 USDC on the Ethereum network and transferred to address 0xc39e690bea48448cc47e7acddfe30e6453e09824 (Subject Address D).

49. Blockchain data analyzed by U.S. law enforcement indicates that the wallets used to collect the funds from the Binance heist also received transfers sourced from other illicit funds including the commingling of funds from a previous exploit attributed to the Lazarus Group/APT38. Specifically, in September of 2026, Bitget, a VCE, reported to U.S. law enforcement and the general public that they suffered a loss of around $387 million in virtual currency after criminal actors hacked into Bitget's network.[2] U.S. law enforcement's review of blockchain analysis regarding the movement of the funds stolen from Bitget revealed that the criminal actors responsible for the Bitget heist moved the funds in a similar manner/pattern as the Binance heist. For example, some of the wallets that received funds from the Binance heist received stolen funds from Bitget.

50. The act of swapping of virtual currency to other tokens and across other networks, combined with the action of breaking larger token amounts into smaller token amounts makes the

[2] https://www.reuters.com/legal/government/crypto-exchange-bitget-pauses-withdrawals-after-350-million-stolen-hack-2026-09-25/

tracing more difficult insofar as it changes or shrouds the nature, location, source, ownership, or control of the property, which are concealing purposes of money laundering while having no apparent legitimate business purpose.

51. On or about October 29, 2026, Circle voluntarily denied access to the USDC associated with Subject Addresses A- D. Additionally, Circle voluntarily denied access to the USDC associated with Subject Addresses E-JJ, which are smart contract and hot wallet addresses on Binance's platform. The criminal actors compromised Subject Addresses E-JJ using EIP-7702 in the same manner described above to compromise access to other Binance-controlled addresses, conduct platform transfers, and override signature authorizations. Thus, although Subject Addresses E-JJ are on Binance's platform, it appears Binance no longer controlled them. The criminal actors depleted some, but not all, funds from Subject Addresses E-JJ before Circle implemented its voluntary access denial measure.

**COUNT ONE – FORFEITURE**
**18 U.S.C. § 981(a)(1)(C)**

52. The United States further incorporates by reference the allegations set forth in Paragraphs 1 to 51 above as if fully set forth herein for the purpose of alleging forfeitures pursuant to Title 18, United States Code, Sections 981(a)(1)(C).

53. The Defendant Property is subject to forfeiture pursuant to 18 U.S.C. § 981(a)(1)(C) as property which constitutes or is derived from proceeds traceable to violations of 18 U.S.C. §§ 1030, 1343, 1349.

**COUNT TWO – FORFEITURE**
**18 U.S.C. § 981(a)(1)(A)**

54. The United States incorporates by reference the allegations set forth in Paragraphs 1 to 51 above as if fully set forth herein for the purpose of alleging forfeitures pursuant to Title 18, United States Code, Sections 981(a)(1)(A).

55. The Defendant Property is subject to forfeiture pursuant to 18 U.S.C. § 981(a)(1)(A) as property involved in violations of 18 U.S.C. § 1956(a)(1)(A)-(B) and (h) and any property traceable to such property.

WHEREFORE, Plaintiff prays that all persons who reasonably appear to be potential claimants with interests in the Defendant Property appear herein and respond to the complaint; that the Defendant Property be forfeited and condemned to the United States of America; that upon Final Order of Forfeiture, the United States Marshal dispose of the Defendant Property according to law; and that Plaintiff have such other and further relief as this Court deems proper and just.

Dated: November 23, 2026
Washington, D.C.

Respectfully submitted,

JEANINE FERRIS PIRRO
UNITED STATES ATTORNEY

By: */s/ Rajbir Datta*
RAJBIR DATTA
N.Y. Bar 5206073
Assistant United States Attorney

[redacted]

JAFER AFTAB
N.J. Bar 050341997

[redacted]

JESSICA C. PECK

[redacted]

MAXWELL K. COLL
C.A. Bar No. 312651
Trial Attorney
[redacted]

**VERIFICATION**

I, [redacted], a Special Agent with the United States Secret Service, declare under penalty of perjury, pursuant to 28 U.S.C. § 1746, that the foregoing Verified Complaint for Forfeiture *In Rem* is based upon reports and information known to me and/or furnished to me by other law enforcement representatives and that everything represented herein is true and correct.

Executed on this 23rd day of November 2026.

[redacted]