IN THE UNITED STATES DISTRICT COURT

FOR THE NORTHERN DISTRICT OF OHIO

EASTERN DIVISION

UNITED STATES OF AMERICA, Plaintiff, v. ALL USDC CRYPTOCURRENCY (NAMELY, APPROXIMATELY 65,028.09 USDC VALUED AT APPROXIMATELY $65,028.09) HELD AT THE CRYPTOCURRENCY ADDRESS BEGINNING/ENDING 0x6d3c . . . 9d81 ON THE ETHEREUM BLOCKCHAIN, Defendant.	)	CASE NO. 1:26-CV-2947 JUDGE BRIDGET MEEHAN BRENNAN **COMPLAINT IN FORFEITURE**

NOW COMES plaintiff, the United States of America, by its attorneys, David M. Toepfer, United States Attorney for the Northern District of Ohio, and James L. Morford, Assistant U.S. Attorney, and files this Complaint in Forfeiture, respectfully alleging on information and belief as follows in accordance with Supplemental Rule G(2) of the Federal Rules of Civil Procedure:

I. *JURISDICTION AND INTRODUCTION.*

1. This Court has subject matter jurisdiction over an action commenced by the United States under 28 U.S.C. Section 1345, and over an action for forfeiture under 28 U.S.C. Section 1355(a). This Court also has jurisdiction over this particular action under 18 U.S.C. Section 981(a)(1)(C) (civil forfeiture authority: wire fraud/conspiracy).

2. This Court has *in rem* jurisdiction over the defendant USDC pursuant to: (i) 28 U.S.C. Section 1355(b)(1)(A) because acts or omissions giving rise to the forfeiture occurred in

this district; and, (ii) 28 U.S.C. Section 1355(b)(1)(B), incorporating 28 U.S.C. Section 1395, because the action accrued in this district.

3. Venue is proper in this district pursuant to: (i) 28 U.S.C. Section 1355(b)(1)(A) because acts or omissions giving rise to the forfeiture occurred in this district; and, (ii) 28 U.S.C. Section 1395 because the action accrued in this district.

4. The defendant USDC is subject to forfeiture to the United States under 18 U.S.C. Section 981(a)(1)(C) as property which constitutes, or is derived from, proceeds traceable to an offense(s) constituting "specified unlawful activity" (SUA) - as defined in 18 U.S.C. Section 1956(c)(7), with reference to 18 U.S.C. Section 1961(l); namely: wire fraud, in violation of 18 U.S.C. Section 1343, and conspiracy to commit wire fraud, in violation of 18 U.S.C. Section 1349.

II. *DESCRIPTION OF THE DEFENDANT USDC.*

5. The following property is the defendant property in the instant case: All USDC cryptocurrency (namely, approximately 65,028.09 USDC valued at approximately $65,028.09) held at the cryptocurrency address 0x6d3ca488b86fcc12f8ce08857ef1bb8b473a9d81 on the Ethereum blockchain.

6. On May 20, 2026, a federal seizure warrant was issued by U.S. Magistrate Judge James E. Grimes, Jr., for the defendant USDC. On the same date, the seizure warrant was served by e-mail on Circle Internet Financial, LLC ("Circle").

7. Also on May 20, 2026, Circle confirmed receipt of the seizure warrant and, further, confirmed that the subject address (namely, 0x6d3ca488b86fcc12f8ce08857ef1bb8b473a9d81 on the Ethereum blockchain) has been blocklisted. "Blocklisting" prevents any inflow or outflow of USDC at the subject address. At the time of the blocklisting, the subject address contained a

balance of approximately 65,028.09 USDC. Pursuant to an Agreement between Circle and the U.S. Attorney's Office, Northern District of Ohio - and should the United States prevail in the instant case - Circle will transfer the USDC equivalent of the defendant USDC to the United States upon the entry of an order of forfeiture.

III. *STATUTES.*

8. *Offense Statutes*. This Complaint in Forfeiture relates to violations of 18 U.S.C. Section 1343 (wire fraud) and conspiracy to commit wire fraud, in violation of 18 U.S.C. Section 1349.

9. *Wire fraud*: 18 U.S.C. 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.

10. *Forfeiture Statute* (*Wire Fraud*): Under 18 U.S.C. Section 981(a)(1)(C) (civil forfeiture authority), any property - real or personal - which constitutes or is derived from proceeds traceable to a violation of 18 U.S.C. Section 1343 (wire fraud), or a conspiracy to commit such offense, is subject to civil forfeiture.

IV. *BACKGROUND ON CRYPTOCURRENCY.*

11. *Virtual Currency*: Virtual currencies are digital tokens of value circulated over the internet. Virtual currencies are typically not issued by any government or bank like traditional fiat currencies, such as the U.S. dollar, but rather are generated and controlled through computer software. Different virtual currencies operate on different blockchains, and there are many

different, widely used virtual currencies currently in circulation. Bitcoin ("BTC") and Ether ("ETH") are currently the most well-known virtual currencies in use. BTC exists on the BTC blockchain and ETH exists on the Ethereum network.

12. *USDC and Circle*: 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).

a.) Stablecoins achieve their price stability via collateralization (backing) or through algorithmic mechanisms of buying and selling the reference asset or its derivatives.

b.) USDC is pegged to the price of the U.S. dollar and is minted (*i.e.*, issued or created) by Circle, a U.S.-based company.

c.) Circle also maintains the treasury/reserves (*i.e.*, funds backing) for all the USDC that Circle issues.

d.) According to Circle's website, "USDC is a digital dollar . . . and is redeemable 1:1 for U.S. dollars." *https://www.circle.com/usdc* (last visited November 6, 2026).

e.) Further, according to Circle's website: (i) "USDC is 100% backed by highly liquid cash and cash-equivalent assets, with holdings that equal or exceed the amount in circulation." *https://www.circle.com/usdc* (last visited November 6, 2026); and, (ii) "USDC is deeply liquid around the world, making it easier to move value where and when you need to." *https://www.circle.com/usdc* (last visited November 6, 2026).

f.) USDC is held in virtual currency addresses that exist on numerous blockchains.

13. *Virtual Currency Address*: Virtual currency addresses are the specific 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 letters and numbers.

14. *Private Key*: Each virtual currency address is controlled using a unique corresponding private key, a cryptographic equivalent of a password, which is needed to access the funds associated with the address. Only the holder(s) of an address' private key can authorize a transfer of virtual currency from that address to another address.

15. *Virtual Currency Wallet*: There are various types of virtual currency wallets, including software wallets, hardware wallets, and paper wallets. A software wallet is a software application that interfaces with the virtual currency's specific blockchain and generates and stores a user's address(es) and private key(s). A virtual currency wallet allows users to store, send, and receive virtual currencies. A virtual currency wallet can hold many virtual currency addresses at the same time.

16. *Hosted Wallets / Unhosted Wallets*: Wallets that are hosted by third parties are referred to as "hosted wallets" because the third party retains the customer's funds until the customer is ready to transact with those funds. An "unhosted wallet," also known as cold storage or self-custody, is a cryptocurrency wallet that is not hosted or controlled by a cryptocurrency exchange. Unhosted wallets allow users to exercise total, independent control over their funds.

17. *Virtual Currency Exchanges (VCEs):* VCEs are trading and/or storage platforms for virtual currencies. Many VCEs store their customers' virtual currency in virtual currency wallets. As previously stated, these wallets can hold multiple virtual currency addresses associated with a user on the VCE's network. Because VCEs act as money services businesses, they are legally required to conduct due diligence of their customers - *i.e.*, Know Your Customer ("KYC") checks - and to have anti-money laundering programs in place to the extent they operate and service customers in the United States.

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

19. *Blockchain Explorer*: These explorers are online tools that operate as a blockchain search engine allowing users the ability to search for and review transactional data for any address on a particular blockchain. A blockchain explorer is software that uses API and blockchain nodes to draw data from a blockchain and uses a database to arrange and present the data to a user in a searchable format.

20. API stands for application programming interface, which is a set of definitions and protocols for building and integrating application software.

21. For all cryptocurrency transactions detailed herein, dates, times, amounts, and valuations are all approximations.

V. *BACKGROUND OF INVESTIGATION.*

22. The FBI Cleveland Field Office is investigating cryptocurrency confidence fraud scams perpetrated on victims throughout the United States, including in the Northern District of Ohio.

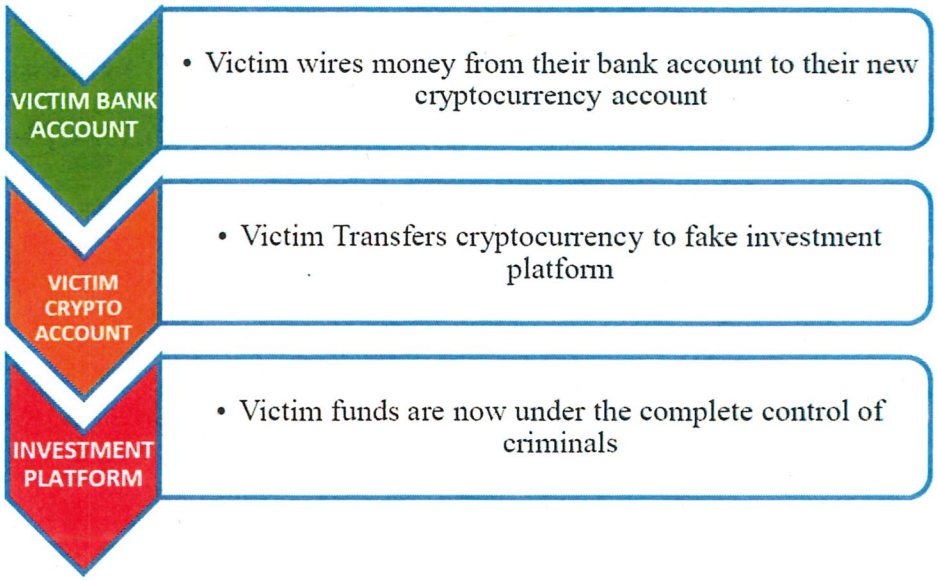
23. The fraud scheme outlined below is a particular type of investment fraud scheme and is known by a particularly unsavory term - not repeated here - derived from the foreign-language phrase used to describe the scheme.

24. Based on data submitted to the FBI's Internet Crime Complaint Center ("IC-3") in 2025, the particular type of investment fraud scheme detailed below targeted tens of thousands of victims in the United States and resulted in the loss of over $8.6 billion in private assets, much of which was sent overseas. The scheme begins with fraudsters contacting potential victims through seemingly misdirected text messages, dating applications, or professional meet-up groups. Next, using various means of manipulation, the fraudster gains the victim's affection and trust.

25. Once trust is established, the fraudster recommends cryptocurrency investments by touting their own success, or that of an associate. Means of carrying out the scheme vary, but a common tactic is to direct a victim to a fake "investment platform" hosted on a website.

26. These websites, and the "investment platforms" hosted there, are created by fraudsters to appear to be legitimate platforms. The fraudster assists the victim with opening a cryptocurrency account, often on a U.S.-based virtual currency exchange (VCE) such as Coinbase or Crypto.com, and then walks the victim through transferring money from a bank account to that cryptocurrency account. Next, the victim will receive instructions on how to transfer their cryptocurrency assets to the fake investment platform.

27. On its surface, the fake investment platform shows lucrative returns, encouraging further investment; underneath, all transferred funds are routed to a cryptocurrency wallet address controlled completely by the fraudsters.



28. Perpetrators of the particular type of investment fraud scheme detailed below frequently allow victims to withdraw some of their "profits" early in the scheme to engender trust and help convince victims of the legitimacy of the platform. As the scheme continues, however, victims are unable to withdraw their funds and are provided various excuses as to why. For example, the fraudsters will often refer to a fake "tax" requirement, stating that taxes must be paid on the proceeds generated from the platform. This is just an 11th-hour effort by the fraudsters to elicit more money from victims. Ultimately, victims are locked out of their accounts and lose all their funds.

29. First employed by Chinese organized crime groups, the particular type of investment fraud scheme detailed below initially targeted victims inside China then expanded worldwide during the global pandemic. Frequently operating from compounds in Cambodia and Myanmar, these criminal syndicates often operate by forcing human trafficking victims in Southeast Asia to participate in the schemes against their will. The schemes take advantage of

the ability of cryptocurrency to be transferred securely and globally, without the intermediaries and safeguards established, and inherent to, the traditional financial system.

VI. *N.D. OHIO VICTIM.*

30. On or about April 28, 2026, a complaint was filed with the FBI's Internet Crime Complaint Center ("IC-3") regarding the fraud loss of a victim in Eastlake, Ohio - with the initials "J.S.". Based on a review of the IC-3 complaint, interviews conducted by the FBI, and blockchain analysis, the FBI learned that J.S. began communicating with an individual using the name "Jake Williams". J.S. first spoke to Williams when Williams made an unsolicited call to J.S. Williams purported to be a financial adviser and an expert in cryptocurrency trading.

31. Williams convinced J.S. to transfer approximately $600,000.00 from J.S.' retirement account to J.S.' bank account at Citizens Bank. Williams then instructed J.S. to make bank transfers in amounts that exceeded $100,000.00 from J.S.' account at Citizens Bank to Coinbase, a cryptocurrency exchange based in the United States.

32. After the funds were sent to Coinbase, Williams deceived J.S. into giving him (Williams) remote access control of J.S.' laptop. In this regard - according to what Williams told J.S. - Williams could not make remote access withdrawals from J.S.' bank account because the bank had online security to detect if the laptop was being accessed remotely.

33. Once Williams took remote access control of J.S.' laptop, he (Williams) made transfers from J.S.' account at Coinbase to two cryptocurrency addresses. The earliest transfer sent from the Coinbase account was in December of 2025.

34. After Williams purportedly traded with J.S.' funds, Williams showed J.S. a cryptocurrency wallet - supposedly belonging to J.S. - that showed J.S.' account purportedly

valued at approximately $860,000.00, which included supposed investment gains. J.S. did not have access to this account, nor - when interviewed by the FBI - could J.S. independently locate where these funds were supposedly held.

35. When J.S. told Williams that he wanted to withdraw funds, Williams told J.S. that the Internal Revenue Service ("IRS") told Williams that the IRS froze J.S.' account because there were issues with J.S.' Certified Public Accountant ("CPA"). According to Williams, J.S.' CPA had not filed any taxes with the IRS since 2021.

36. Based on records reviewed by the FBI and blockchain analysis, the FBI learned that from on or about December 17, 2025 to March 31, 2026, a total of approximately 60 transfers from J.S.' Coinbase account were made as a result of this scam. The transfers totaled approximately $198,232.92 and were made to addresses controlled by the fraudsters. J.S. was not returned any of the funds.

37. The FBI has received additional fraud complaints through IC-3 relating to other victims who lost funds in other fraud schemes to an individual named "Jake." "Jake" used the same telephone number as Williams.

VII. *FORFEITURE OF ALL USDC CRYPTOCURRENCY (NAMELY, APPROXIMATELY 65,028.09 USDC VALUED AT APPROXIMATELY $65,028.09) HELD AT THE CRYPTOCURRENCY ADDRESS BEGINNING/ENDING 0x6d3c . . . 9d81 ON THE ETHEREUM BLOCKCHAIN.*

Tracing of Funds from Victim J.S. to the cryptocurrency address beginning/ending 0x6d3c . . . 9d81 on the Ethereum blockchain (ADDRESS-3):

38. From on or about February 6, 2026 through February 13, 2026, 22 transfers were sent from J.S.' Coinbase account to the cryptocurrency address beginning/ending 0x6522…b31e (ADDRESS-1). These transfers totaled approximately 103,848 USDC.

39. The first transaction on the blockchain involving ADDRESS-1 occurred on February 6, 2026.

40. From the inception of ADDRESS-1 through February 13, 2026, ADDRESS-1 received a total of 0.001778 USDC - worth less than $0.01 - from sources other than J.S.' Coinbase account. From February 6, 2026 to February 13, 2026, ADDRESS-1 sent 17 transfers - totaling 103,845 USDC - to the cryptocurrency address beginning/ending 0x157d…1af4 (ADDRESS-2).

41. When ADDRESS-2 received the first of these 17 transfers from ADDRESS-1, ADDRESS-2 had a balance of 0.00 USDC. From February 6, 2026 through February 13, 2026, ADDRESS-2 received a total of 103,846 USDC, 103,845 of which was traced from J.S.' Coinbase account.

42. On February 13, 2026, ADDRESS-2 made two transfers, one for 10,020 USDC and one for 90,006 USDC, to the cryptocurrency address beginning/ending 0x6d3c…9d81 (ADDRESS-3), the subject address.

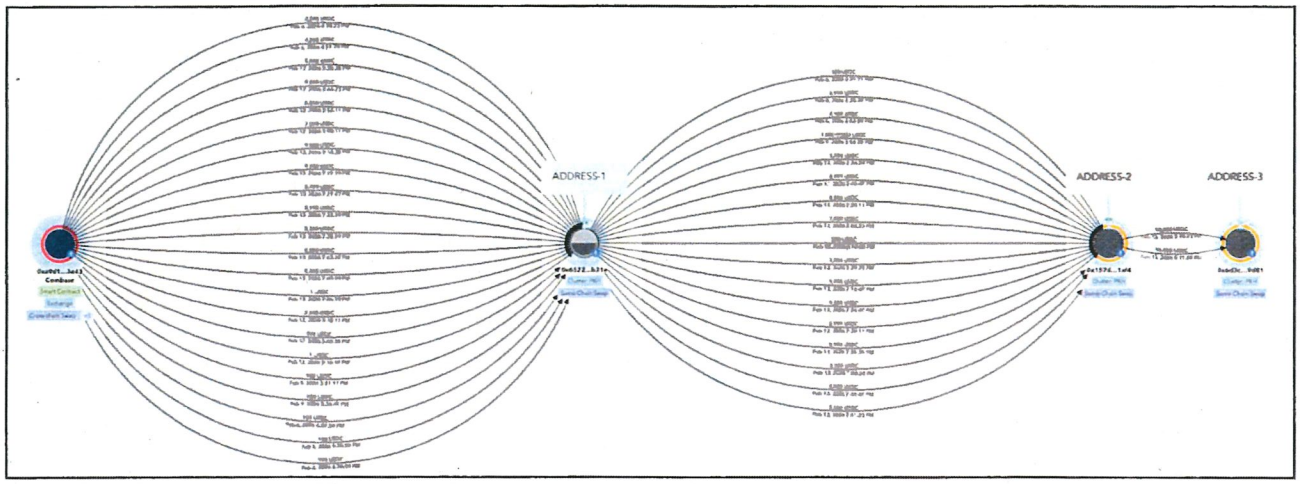
43. When ADDRESS-3 received these transfers from ADDRESS-2, ADDRESS-3 had a balance of 1.00 USDC. Following ADDRESS-3's receipt of the two transfers from ADDRESS-2, ADDRESS-3 received a total of 1.09 USDC from other sources and sent out a total of 35,000 USDC. This 35,000 USDC was returned to ADDRESS-2.

44. At the time ADDRESS-3 was blocklisted by Circle, ADDRESS-3 contained a balance of approximately 65,028.09 USDC,[1] approximately 65,026.00 of which is attributable to

[1] *i.e.*, 1.00 USDC + 10,020.00 USDC + 90,006.00 USDC + 1.09 USDC - 35,000.00 USDC = 65,028.09 USDC.

victim J.S. The remaining 2.09 USDC was received through numerous small "dust" receipts of USDC.

45. The graph below shows the tracing of victim J.S.' funds to ADDRESS-3:



VIII. *CONCLUSION.*

46. Based upon the foregoing, the defendant USDC (approximately 65,028.09 USDC) is subject to forfeiture to the United States under 18 U.S.C. Section 981(a)(1)(C) (civil forfeiture authority) as property which constitutes, or is derived from, proceeds traceable to wire fraud, in violation of 18 U.S.C. Section 1343, and conspiracy to commit wire fraud, in violation of 18 U.S.C. Section 1349.

47. The identity of the owner(s) of ADDRESS-3 is unknown. The only available information to law enforcement is the cryptocurrency address itself. Notice of this action will be messaged via the Ethereum blockchain to the address with a link to a copy of this Complaint in Forfeiture.

WHEREFORE, plaintiff, the United States of America, requests that the Court enter judgment condemning the defendant USDC and forfeiting it to the United States, and directing Circle Internet Financial, LLC ("Circle") to transfer the USDC equivalent of the defendant

USDC to the United States for disposition in accordance with law and for such other relief as this Court may deem proper.

Respectfully submitted,

David M. Toepfer
U.S. Attorney, Northern District of Ohio

By: _____
James L. Morford (Ohio: 0005657)
Assistant United States Attorney, N.D. Ohio
Carl B. Stokes U.S. Court House
801 West Superior Avenue, Suite 400
Cleveland, Ohio 44113
216.622.3743 / James.Morford@usdoj.gov

VERIFICATION

STATE OF OHIO)
) SS.
COUNTY OF CUYAHOGA)

I, James L. Morford, under penalty of perjury, depose and say that I am an Assistant United States Attorney for the Northern District of Ohio, and the attorney for the plaintiff in the within entitled action. The foregoing Complaint in Forfeiture is based upon information officially provided to me and, to my knowledge and belief, is true and correct.

James L. Morford (Ohio: 0005657)
Assistant United States Attorney, N.D. Ohio

Sworn to and subscribed in my presence this 9th day of November, 2026.

Notary Public

ANNA J DUDAS
Notary Public
State of Ohio
My Comm. Expires
December 5, 2026