UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF MICHIGAN
SOUTHERN DIVISION

United States of America,

Plaintiff,

vs.

Civil Case No. 25-cv-12246

Honorable
Magistrate Judge

Bitcoin cryptocurrency funds from two Paxful, Inc. accounts, with the affiliated deposit addresses 3KHvW3kGJGs1KnCLJ4171b5bBBgWLvgXze and 3DE6F3W1eLa5vFhyGxNdx4a7TMuF5tHDrr,

Ethereum cryptocurrency funds from two Paxful, Inc. accounts, with the affiliated deposit addresses 0x3FE0a6843317F73d977649bA6FB3e39225fC2E94 and 0x19C9c94B153F95Aa6a32c2738babB9e0Fa361AAB,

Defendants *in Rem.*

Complaint for Forfeiture

Plaintiff, United States of America, by and through its undersigned attorneys, states the following in support of this Complaint for Forfeiture:

Jurisdiction and Venue

1. This is an *in rem* civil forfeiture action pursuant to 18 U.S.C. § 981(a)(1)(A) and 18 U.S.C. § 981(a)(1)(C), resulting from violations of 18 U.S.C. §§ 1343, 1956, and 1957.

2. This Court has original jurisdiction over this proceeding pursuant to 28 U.S.C. § 1345 because this action is being commenced by the United States of America as plaintiff.

3. This Court has jurisdiction over this forfeiture action under 28 U.S.C. § 1355(b)(1)(A) because acts giving rise to the forfeiture occurred in the Eastern District of Michigan.

4. Venue is proper before this Court under 28 U.S.C. § 1391(b)(2) because a substantial part of the events or omissions giving rise to the government's claims occurred in the Eastern District of Michigan.

5. Venue is also proper before this Court under 28 U.S.C. § 1395 because the action accrued in the Eastern District of Michigan.

Defendants *in rem*

6. The defendants *in rem* consist of the following "Defendant Cryptocurrency":

a. Bitcoin cryptocurrency funds from two Paxful, Inc. accounts, with the affiliated deposit addresses 3KHvW3kGJGs1KnCLJ4171b5bBBgWLvgXze and 3DE6F3W1eLa5vFhyGxNdx4a7TMuF5tHDrr; and

b. Ethereum cryptocurrency funds from two Paxful, Inc. accounts, with the affiliated deposit addresses

0x3FE0a6843317F73d977649bA6FB3e39225fC2E94 and

0x19C9c94B153F95Aa6a32c2738babB9e0Fa361AAB.

7. The Defendant Cryptocurrency was seized as proceeds of wire fraud and/or money laundering pursuant to a seizure warrant executed on March 18, 2024, by Homeland Security Investigations ("HSI").

Underlying Criminal Statutes

8. 18 U.S.C. § 1343 ("Wire Fraud") prohibits anyone from devising or intending to devise any scheme or artifice to defraud, or to obtain 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.

9. 18 U.S.C. § 1956(a)(1)(B)(i) makes it a federal offense for anyone, knowing that the property involved in a financial transaction represents the proceeds of some form of unlawful activity, to conduct or attempt to conduct a financial transaction 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, location, source, ownership, or control of the proceeds.

10. 18 U.S.C. § 1957 makes it unlawful for any person to knowingly engage or attempt to engage in a monetary transaction in criminally derived property of a

value greater than $10,000.00 if the property is, in fact, derived from specified unlawful activity.

Statutory Basis for Civil Forfeiture

11. 18 U.S.C. § 981(a)(1)(A) provides for civil forfeiture of any property, real or personal, involved in a transaction or attempted transaction in violation of 18 U.S.C. §§ 1956 and/or 1957, or any property traceable to such property.

12. 18 U.S.C. § 981(a)(1)(C) provides for civil forfeiture of any property, real or personal, which constitutes or is derived from proceeds traceable to a violation of a specified unlawful activity, which includes violations of 18 U.S.C. § 1343 (Wire Fraud), 18 U.S.C. § 1956 (Money Laundering), and 18 U.S.C. § 1957 (Spending).

Factual Basis in Support of Forfeiture

13. The Defendant Cryptocurrency is forfeitable to the United States as property that constitutes or is derived from the proceeds of wire fraud in violation of 18 U.S.C. § 1343 and as property involved in money laundering in violation of 18 U.S.C. §§ 1956, 1957. The facts supporting this evidentiary determination include, but are not limited to, the following:

a. In December 2022, the Michigan State Police ("MSP") Cyber Command Center received a complaint from an individual ("Victim 1") that cryptocurrency had been taken from his Coinbase account.

Coinbase is a centralized cryptocurrency exchange that allows for online buying and selling of cryptocurrency.

b. Victim 1, a resident of Michigan, reported that he had received a phishing email, an attempt to steal personal information or break into online accounts using deceptive emails that look like sites already used by the victim.

c. Victim 1 reported he received an email that appeared to be from PayPal, called the phone number provided within the email, and ultimately spoke with a person that identified themselves as an employee of PayPal. The purported Paypal employee advised Victim 1 that his device had been hacked.

d. Victim 1 reported that while he was on the call with the person purporting to be an employee of PayPal, he received alerts from Coinbase about cryptocurrency transfers from his account that he did not make. Victim 1 contacted Coinbase to lock his account; however, the transfers continued until his account showed a negative balance.

e. Victim 1 provided MSP with an Ethereum (ETH) address and a Bitcoin (BTC) address, neither of which he could access or control, that received Victim 1's stolen funds from his Coinbase account:

- One transfer totaling 0.294958 ETH was made to 0x3Ef8Bf05dC53D066CcfcDC19dA382B2725377753 ("Address 7753");
- Two transfers totaling approximately 0.06317359 BTC were made to bc1qhuety945ejg8487u3m9u82yvtut89zqrt4wrgv ("Address wrgv").

f. A Task Force Officer (TFO) with Homeland Security Investigations (HSI), who has received specialized training conducting cryptocurrency investigations that require analysis of cryptocurrency transactions on the blockchain, was able to trace Victim 1's funds.

g. Through blockchain analysis, HSI traced the ETH transferred from Victim 1's Coinbase account to Address 7753, and then to the cryptocurrency conversion exchange N. Exchange. On or about December 8, 2022, Victim 1's ETH was converted into .02122 BTC at N. Exchange and was then deposited into Address wrgv.

h. Through blockchain analysis, HSI conducted a trace of Victim 1's funds from Address wrgv to the following addresses held by two accounts at Paxful, a peer-to-peer cryptocurrency exchange:

- 3KHvW3kGJGs1KnCLJ4171b5bBBgWLvgXze (Address gXze)

- 3DE6F3W1eLa5vFhyGxNdx4a7TMuF5tHDrr (Address HDrr

i. Blockchain analysis shows that the same two Paxful accounts received BTC and ETH from other addresses with links back to Coinbase.

j. On or about January 6, 2023, MSP served a state search warrant and freeze order to Paxful for the two Paxful accounts, one that held Address gXze and one that held Address HDrr.

k. On or about January 9, 2023, Paxful complied with the state search warrant and provided MSP with identifying information for the two Paxful accounts that held the addresses.

l. The identifying information produced by Paxful for one account ("Account 1") indicated that it was created on or about June 21, 2022, and a named individual with initials R.C. was listed as the owner the account. Account 1 held the following addresses:

- Address gXze (BTC)
- 0x3FE0a6843317F73d977649bA6FB3e39225fC2E94 ("Address 2E94") (ETH)

m. The identifying information produced by Paxful for the second account ("Account 2") indicated that it was created on or about October 3, 2022,

and a named individual with initials S.Y. was listed as the owner of the account. Account 2 held the following addresses:

- Address HDrr (BTC)
- 0x19C9c94B153F95Aa6a32c2738babB9e0Fa361AAB ("Address 1AAB") (ETH)

n. On January 6, 2023, Account 1 and Account 2 were frozen with the following balances:

Account	BTC balance	ETH balance
Account 1	4.69247956 BTC (Address gXze)	7.316972409 ETH (Address 2E94)
Account 2	6.36842647 BTC (Address HDrr)	43.958908148 ETH (Address 1AAB)

o. On or about July 13, 2023, HSI interviewed R.C., the listed owner of Account 1. R.C. denied having a Paxful account and denied knowledge of Account 1.

p. On or about January 12, 2024, HSI interviewed S.Y., the listed owner of Account 2. S.Y. claimed no ownership of Account 2, nor any other cryptocurrency account.

q. Website IC3.gov, is the web address for the Internet Crime Complaint Center (IC3), which is operated by the Federal Bureau of

Investigations. Victims of internet crimes can file a complaint with the FBI via this website.

r. Utilizing IC3.GOV, MSP conducted a search for additional complaints linked to Address wrgv and located two additional victims claiming to have had their cryptocurrency stolen after responding to an email purportedly from PayPal.

s. On or about January 31, 2023, MSP served Paxful with a state seizure warrant instructing Paxful to seize 0.38827689 BTC and 0.29568082 ETH, the funds stolen from Victim 1's Coinbase account, and 5.00338181 BTC and 0.184028 BTC, the funds stolen from the two additional identified victims.

t. On or about February 28, 2023, MSP received the funds from Paxful and ultimately returned the funds to the victims.

u. Utilizing IC3.gov and tracing from Coinbase, MSP and HSI identified eleven additional victims. Each victim was interviewed and claimed to have fallen victim to a similar email phishing scam involving Paypal.

v. Using blockchain analysis, HSI traced funds from the Coinbase account of each of the eleven identified victims to addresses linked to Account 1 or Account 2.

w. Below is a summary of the tracing of cryptocurrency from each victim's Coinbase account to the suspect addresses:

Victim	Type of Crypto Transferred	Amount of Cryptocurrency	Date of Transfer[1]	Address of Deposit
Victim 2	BTC	0.7705941	December 18, 2022	Address HDrr
Victim 3	BTC	0.05345644	January 3, 2023	Address gXze
Victim 4	BTC	0.2965951	December 26, 2022	Address gXze
Victim 5	BTC	1.37683741	December 11, 2022	Address HDrr
Victim 7	ETH	35.55483629	January 3, 2023	Address 1AAB
Victim 8	ETH	2.38577394	January 4, 2023	Address 1AAB
Victim 8	BTC	0.20453	January 4, 2023	Address HDrr
Victim 9	ETH	1.00994466	December 22, 2022	Address 2E94
Victim 9	BTC	0.05748837	December 22, 2022	Address gXze
Victim 10	ETC	0.06608559	January 2, 2023	Address 1AAB
Victim 11	ETC	0.76029014	December 28, 2022	Address 2E94
Victim 11	ETC	0.04000666	December 28, 2022	Address 2E94

x. HSI identified additional suspected victims by tracing funds received by Addresses held in Account 1 and Account 2 back to an attributed address, like an exchange. HSI traced those funds back to twenty-two unattributed addresses that each received funds from Coinbase via different transaction IDs not previously linked to a known victim. Each of the transactions followed the same pattern as that of the victims already identified, i.e., the transaction occurred during the same period,

[1] All the Victims' funds were moved between various addresses before ultimately ending up in the identified suspect address. The date of transaction listed is the initial withdrawal of the funds from their Coinbase account.

funds went from Coinbase to an unattributed address, and then ultimately to addresses in Account 1 or Account 2.

y. HSI provided Coinbase with a spreadsheet of those twenty-two addresses linked to Account 1 and Account 2. Coinbase located 289 transactions associated with 152 customers linked to the twenty-two unattributed addresses that transferred funds to addresses in Account 1 and Account 2.

z. Although investigators were unable to match IC3.gov complaints to the 152 customers, based on training and experience, it is believed those customers were also victims of the scheme.

aa. The funds stolen from each victim were moved through various cryptocurrency wallets before ultimately being deposited into the suspect addresses. Victim funds were also exchanged for other types of cryptocurrencies.

bb. HSI also identified transactions between Account 1's Address gXze and Account 2's Address HDrr.

cc. Conducting numerous transactions within a short period of time and using cryptocurrency swaps and exchanges, are methods to conceal or disguise the source of the funds. The number of hops the victims' funds went through are a strong indication that the victims' funds were moved

in a manner intended to conceal or disguise their nature, location, source, ownership, or control.

dd. On April 21, 2023, a warrant was issued by a federal Magistrate Judge in the Eastern District of Michigan to seize Defendant Cryptocurrency and was executed by HSI.

Claim

14. Plaintiff re-alleges and incorporates by reference each and every allegation contained in paragraphs one through 13 above, including all their subparts.

15. Based upon the facts outlined above and the applicable law, the Defendant Cryptocurrency is forfeitable to the United States under 18 U.S.C. § 981(a)(1)(A) and 18 U.S.C. § 981(a)(1)(C), as proceeds of wire fraud and as property involved in money laundering.

Conclusion and Relief

Plaintiff respectfully requests that a warrant for arrest of the defendants *in rem* be issued; that due notice be given to all interested parties to appear and show cause why the forfeiture should not be decreed; that judgment be entered declaring that the defendants *in rem* be condemned and forfeited to the United States of America for disposition according to law; and that the United States be granted such other relief

as this Court may deem just and proper, together with the costs and disbursements of this action.

Respectfully submitted,

JEROME F. GORGON, J.R
United States Attorney

s/Kelly Fasbinder
Kelly E. Fasbinder (P80109)
Assistant United States Attorney
211 W. Fort St., Ste. 2001
Detroit, MI 48226
(313) 226-9520
Kelly.Fasbinder@usdoj.gov

Dated: July 23, 2025

VERIFICATION

I, Jennifer Schlaufman, am a Task Force Officer with the Homeland Security Investigations. I have read the foregoing Complaint for Forfeiture and assert under penalty of perjury that the facts contained therein are true to the best of my knowledge and belief, based upon knowledge possessed by me and/or on information that I received from other law enforcement agents and/or officers.

Jennifer Schlaufman, Task Force Officer
Homeland Security Investigations

Dated: July 17, 2025