IN THE DISTRICT COURT OF THE UNITED STATES
FOR THE DISTRICT OF SOUTH CAROLINA
COLUMBIA DIVISION

UNITED STATES OF AMERICA, Plaintiff, vs. 250,000 in USDT, Defendant *in Rem*.	)	CIVIL ACTION NO.: 3:24-3151-JFA

UNITED STATES' COMPLAINT FOR FORFEITURE *IN REM*

The Plaintiff, United States of America, brings this complaint and alleges as follows, in accordance with Rule G(2) of the Supplemental Rules for Admiralty and Maritime Claims and Asset Forfeiture Actions.

NATURE OF THE ACTION

1. This is a civil action *in rem* to forfeit to the United States of America funds in the amount of 250,000 USDT ("Defendant Funds"), pursuant to 18 U.S.C. § 981(a)(1)(A) and 18 U.S.C. § 981(a)(1)(C). The United States seeks forfeiture based upon a reasonable belief that the Government will be able to meet its burden of proof at trial to show that the Defendant Funds constitutes, or is traceable to:

a. property involved in wire fraud transactions, attempted wire fraud transactions, or conspiracy thereof in violation of 18 U.S.C. §§ 1343, 1349;

b. property involved in money laundering transactions or attempted transactions in violation of 18 U.S.C. § 1956(a)(1)(A)(i), and/or § 1956(a)(1)(B)(i) and/or 1957;

c. property involved in an illegal money transmitting business, in violation of 18 U.S.C. § 1960; and/or

d. proceeds of some other form of specified illegal activity set forth in 18 U.S.C. § 1956(c)(7) and;

e. proceeds of some other form of specified illegal activity set forth in 18 U.S.C. § 1956(h) and;

f. property involved in money transactions in criminally derived property or attempted monetary transactions, in violation of 18 U.S.C. § 1957.

JURISDICTION AND VENUE

2. This Court has subject matter jurisdiction over an action commenced by the United States pursuant to 28 U.S.C. § 1345, and over an action for forfeiture by virtue of 28 U.S.C. § 1355. This Court has *in rem* jurisdiction over the Defendant Funds pursuant to:

(a) 28 U.S.C. § 1355(b)(1)(A), because acts or omissions giving rise to the forfeiture occurred in the District of South Carolina; and

(b) 28 U.S.C. § 1355(b)(1)(B), because venue properly lies in this district pursuant to 28 U.S.C. § 1395.

THE DEFENDANT *IN REM*

3. The Defendant Funds consists of 250,000 USDT valued at approximately $250,000.00 in United States Currency, obtained by agents with the United States Secret Service ("USSS") during an investigation into a transnational criminal organization running an investment fraud scheme. The funds were seized from a cryptocurrency custodial wallet under the control of OKX, in wallet TJDvJatYWrCvvDBm2aNAeVK6tvyHd7f1Yp ("Subject Account") and under the name of Chen Chun-Lung ("Lung").

4. USSS agents seized the OKX WALLET, TJDvJatYWrCvvDBm2aNAeVK6tvyHd7f1Yp, for federal forfeiture. The Defendant Funds are currently restrained and pending deposit to an account under the control of United States Secret Service.

5. In accordance with the provisions of 19 U.S.C. § 1606, the Defendant Funds have a total domestic value of approximately $250,000.00 in United States Currency.

KNOWN POTENTIAL CLAIMANTS

6. The known individual whose interests may be affected by this litigation are:

a. Chen Chun-Lung who may have an interest in the Defendant Funds because he was the named account holder of the account seized by USSS during this investigation.

BASIS FOR FORFEITURE

7. Pursuant to the pleading requirements of Supplemental Rule G(2)(f), Plaintiff alleges that there is a factual basis to support a reasonable belief that the Government will be able to meet its burden of proof at trial to show that the Defendant Funds are subject to forfeiture to the United States, based in part upon the following:

a. On November 16, 2023, Victim 1 filed a report with Richland County Sheriff's Department, Case # 2311041916, reporting that she was scammed out of approximately $46,129.70 through several cryptocurrency transactions. Victim 1 stated the unknown attackers developed a connection with her through the dating and communication applications Zoe and Telegram. The victim lives and works in the Columbia, S.C. area.

b. Victim 1 contacted the United States Secret Service to investigate. Special Agent Matthew Hannon, with the United States Secret Service has received training, research, education, and experience in cryptocurrency. He is familiar with the following relevant terms and definitions as they relate to cryptocurrency:

(1) Cryptocurrency: Cryptocurrency, a type of virtual currency, is a decentralized, peer-to-peer, network-based medium of value or exchange that may be used as a substitute for fiat currency to buy goods or services or exchanged for fiat currency or other cryptocurrencies.[1] Examples of cryptocurrency are Bitcoin (BTC), Litecoin (LTC), Ethereum (ETH) and Tether (USDT). Cryptocurrency can exist digitally on the Internet, in an electronic storage device, or in cloud- based servers. Although not usually stored in any physical form, public and private keys (described below) used to transfer cryptocurrency from one person or place to another can be printed or written on a piece of paper or other tangible object. Cryptocurrency can be exchanged directly person to person, through a cryptocurrency exchange, or through other intermediaries. Generally, cryptocurrency is not issued by any government, bank, or company; it is instead generated and controlled through computer software operating on a decentralized peer-to-peer network. Most cryptocurrencies have a "blockchain," which is a distributed public ledger, run by the decentralized network, containing an immutable and historical record of every transaction.[2] Cryptocurrency is not illegal in the United States.

(2) USDC: USDC is a digital stablecoin that is pegged to the United States dollar. USDC is managed by a consortium called Centre, which was founded by Circle and includes members from the cryptocurrency exchange Coinbase and Bitcoin mining company Bitmain, who are investors in Circle. Initially released in September 2018, the coin's goal is to mirror the value of the United States dollar as a digital currency investment platform that matches the performance of the New York Stock Exchange as an alternative investment portfolio holding.

(3) Tether and Ethereum: Tether (USDT) and Ethereum (ETH) is a type of cryptocurrency like Bitcoin[3] (BTC).

(4) Wallet: Cryptocurrency is stored in a virtual account called a wallet. Wallets are software programs that interface with blockchains and generate and/or store public and private keys used to send and receive cryptocurrency. A public key or address is akin to a bank account number, and a private key is akin to a PIN number or password that allows a user the ability to access and transfer value associated with the public address or key. To

[1] Fiat currency is currency issued and regulated by a government such as the U.S. dollar, euro, or Japanese yen.

[2] Some cryptocurrencies operate on blockchains that are not public and operate in such a way to obfuscate transactions, making it difficult to trace or attribute transactions.

[3] Since Bitcoin is both a cryptocurrency and a protocol, capitalization differs. Accepted practice is to use "Bitcoin" (singular with an uppercase letter B) to label the protocol, software, and community, and "bitcoin" (with a lowercase letter b) to label units of the cryptocurrency. That practice is adopted here.

conduct transactions on a blockchain, an individual must use the public address (or "public key") and the private address (or "private key"). A public address is represented as a case- sensitive string of letters and numbers, 26–36 characters long, and is somewhat analogous to a bank account number. Each public address is controlled and/or accessed through the use of a unique corresponding private key—the cryptographic equivalent of a password or PIN—needed to access the address. Only the holder of an address' private key can authorize any transfers of cryptocurrency from that address to another cryptocurrency address.

(5) Cryptocurrency Wallet Services: Some companies offer cryptocurrency wallet services which allow users to download a digital wallet application onto their smart phone or other digital device. A user typically accesses the wallet application by inputting a user-generated PIN code or password. Users can store, receive, and transfer cryptocurrencies via the application; however, many of these companies do not store or otherwise have access to their users' funds or the private keys that are necessary to access users' wallet applications. Rather, the private keys are stored on the device on which the wallet application is installed (or any digital or physical backup private key that the user creates). As a result, these companies generally cannot assist in seizing or otherwise restraining their users' cryptocurrency. Nevertheless, law enforcement could seize cryptocurrency from the user's wallet directly, such as by accessing the user's smart phone, accessing the wallet application, and transferring the cryptocurrency therein to a law enforcement-controlled wallet. Alternatively, where law enforcement has obtained the recovery seed for a wallet (see above), law enforcement may be able to use the recovery seed phrase to recover or reconstitute the wallet on a different digital device and subsequently transfer cryptocurrencies held within the new wallet to a law enforcement-controlled wallet.

(6) Use of Cryptocurrency in Criminal Activity: Although cryptocurrencies such as Bitcoin, Ethereum and Tether have legitimate uses, cryptocurrency is also used by individuals and organizations for criminal purposes such as money laundering and is often used as payment for illegal goods and services. By maintaining multiple wallets, those who use cryptocurrency for illicit purposes can attempt to thwart law enforcement's efforts to track transactions.

(7) ETH and BTC Value in U.S. Dollars: As of November 27, 2023, one ETH is worth approximately $2,009.98 and one BTC is worth approximately $36,993, though the value of ETH and BTC is generally much more volatile than that of fiat currencies. USDT value is directly tied to the value of the US Dollar and is traded on the ETH blockchain.

(8) Exchanges: Cryptocurrency "exchangers" and "exchanges" are

individuals or companies that exchange bitcoin for other currencies and cryptocurrencies, including U.S. dollars and Tether/USDT. Exchanges can be brick-and-mortar businesses or online businesses (exchanging electronically transferred money and virtual currencies). According to Department of Treasury, Financial Crimes Enforcement Network ("FinCEN") guidance issued on March 18, 2013, virtual currency administrators and exchangers, including an individual exchanger operating as a business, are considered money services businesses.[4] Such exchanges and exchangers are required to register with FinCEN and have proper state licenses (if required under applicable state law). Based on my training and experience, I know that registered money transmitters are required by law to follow Bank Secrecy Act anti-money laundering ("AML") regulations, "Know Your Customer" ("KYC") protocols, and other verification procedures similar to those employed by traditional financial institutions. For example, FinCEN-registered cryptocurrency exchangers often require customers who want to open or maintain accounts on their exchange to provide their name, address, phone number, and the full bank account and routing numbers that the customer links to an exchange account. As a result, there is significant market demand for illicit cryptocurrency-for-fiat currency exchangers, who lack AML or KYC protocols and often also advertise their ability to offer customers stealth and anonymity. These illicit exchangers routinely exchange fiat currency for cryptocurrencies by meeting customers in person or by shipping cash through the mail. Due to the illicit nature of these transactions and their customers' desire for anonymity, such exchangers are frequently able to charge a higher exchange fee, often as high as 9–10% (in contrast to registered and BSA-compliant exchangers, who may charge fees as low as 1–2%).

(9) Exchange Transactions: Exchangers and users of cryptocurrencies store and transact their cryptocurrency in a number of ways, as wallet software can be housed in a variety of forms, including on a tangible, external device ("hardware wallet"), downloaded on a PC or laptop ("desktop wallet"), with an Internet-based cloud storage provider ("online wallet"), as a mobile application on a smartphone or tablet ("mobile wallet"), printed public and private keys ("paper wallet"), and as an online account associated with a cryptocurrency exchange. Because these desktop, mobile, and online wallets are electronic in nature, they are located on mobile devices (e.g., smart phones or tablets) or at websites that users can access via a computer, smart phone, or any device that can search the Internet. Moreover, hardware wallets are located on some type of external or removable media device, such as a USB thumb drive or other commercially available device designed

[4] See "Application of FinCEN's Regulations to Person Administering, Exchanging, or Using Virtual Currencies," available at https://www.fincen.gov/resources/statutes- regulations/guidance/application-fincens-regulations-persons-administering.

> to store cryptocurrency (e.g. Trezor, Keepkey, or Nano Ledger). In addition, paper wallets contain an address and a QR code[5] with the public and private key embedded in the code. Paper wallet keys are not stored digitally. Wallets can also be backed up into, for example, paper printouts, USB drives, or CDs, and accessed through a "recovery seed" (random words strung together in a phrase) or a complex password. Additional security safeguards for cryptocurrency wallets can include two-factor authorization (such as a password and a phrase). I also know that individuals possessing cryptocurrencies often have safeguards in place to ensure that their cryptocurrencies become further secured in the event that their assets become potentially vulnerable to seizure and/or unauthorized transfer.

c. Further, based on SA Hannon's training and experience, he knows that classic money laundering often consists of three phases - Placement, Layering, and Integration as follows:

> (1) ***Placement Phase***: The process of placing, through deposits or other means, unlawful cash proceeds into traditional financial institutions. I know from training and experience that the "Placement Phase" is the most common phase of money laundering detected by law enforcement.
>
> (2) ***Layering Phase***: The process of separating the proceeds of criminal activity from their origin through the use of layers of complex financial transactions. I also know, based on my training and experience, that in cryptocurrency frauds in particular it is common for targets to layer complex financial transactions through numerous cryptocurrency transfers on the blockchain with the goal or effect to make it too difficult for law enforcement or victims to trace where stolen funds were transferred and therefore preventing their recovery.
>
> (3) ***Integration Phase***: The process of using an apparently legitimate transaction to disguise the illicit proceeds, allowing the laundered funds to be disbursed back to the criminal. I know in the third and final common phase, "dirty" funds are co-mingled with legitimate funds in a way that is designed to conceal the origins of the illicit proceeds.

b. On October 11, 2023, Victim 1 received a message on Zoe, a dating app, from an unknown individual who identified themselves as "Erin Rossi." The conversation began by

[5] A QR code is a matrix barcode that is a machine-readable optical label.

sharing personal interests and the conversation turned quickly into talk about cryptocurrency and investing. The two continued to communicate by text with the target(s) using the number XXX-XXX-3221 (after the victim identified as being from South Carolina on the dating website). "Erin Rossi" offered to become the victim's friend, she claimed she lived in Charleston, and she eventually convinced Victim 1 to switch their communication to the Telegram platform.

c. On Telegram, the user @zxc2500 operating with the profile name "Little lazy cat," provided further instructions to Victim 1 regarding cryptocurrency investing. Victim 1 was instructed to download the Coinbase application for trading cryptocurrency; Victim 1 stated she already had the app downloaded, to which "Little lazy cat" replied, "within the Coinbase wallet application, use the browser and navigate to https://www.ironfxebs.com/." In doing so, the target(s) directed the victim to the particular website that facilitated this scheme.

d. When navigating to that website, a user sees the homepage of ironfxebs.com with instructions showing how to download a Coinbase Wallet application. The genuine Iron FX is a legitimate forex / currency broker that operates from the website www.ironfxglobal.com/en/; the website Victim 1 was directed to was slightly different by adding -ebs and removing -global from the end of the legitimate Iron FX website URL.

e. Based on SA Hannon's, experience, and this investigation, he believes it is significant that the target shifted the conversation to Telegram. Telegram is an end-to-end encrypted chat platform. Targets commonly prefer end-to-end encrypted communications to facilitate criminal activity, including cryptocurrency fraud schemes, because such platforms provide real or perceived protections against detection and recovery of the content of

communications.

f. As a result of her communications with the target on Telegram, Victim 1 was convinced to transfer money into cryptocurrency wallets as directed by user(s) of the chat application at the URL https://www.ironfxebs.com/. The chat box inside that fraudulent website led to a separate pop-up window hosted at the URL https://lcvrdnos.tmabwadkyqcqngc.xyz. In turn, that URL provided detailed information on how to invest and what wallet addresses to send money to under the premise that Victim 1 was investing in a legitimate cryptocurrency investment vehicle. In truth and fact, as described below, there is probable cause to believe she was being scammed by the target(s) out of substantial sums of money.

g. Specifically, between October 13, 2023, and November 15, 2023, Victim 1 completed several digital currency transfers from her fiat bank account into digital currency accounts at the direction of the chat user at the fraudulent website described herein, including from the URL https://lcvrdnos.tmabwadkyqcqngc.xyz, in the amount of approximately $46,129.70.

h. Once the funds were successfully received as USDT (which is a type of cryptocurrency as described in paragraphs 6(a)), Victim 1 was sent to a website that showed false balances of her "investment account." As described below, there is evidence the website was designed to closely resemble a legitimate digital currency platform, Iron FX, which would lead visitors to believe it was associated with Iron FX when in truth and fact it was not. The link Victim 1 was induced to navigate to was https://www.ironfxebs.com/ rather than the legitimate URL, www.ironfxglobal.com/en/. The link provided was made to imitate the legitimate Iron FX URL, but the addition of "-ebs" indicates it instead was a

fraudulent and spoofed website made to appear as the legitimate website. In fact, Victim 1 was specifically directed by the target(s) to not go to the traditional Iron FX mobile application, but instead to go to the URL provided. All of this provides evidence that the website provided is associated with a well-organized and intentional fraud scheme.

i. As directed, Victim 1 then engaged in a series of cryptocurrency fund transfers from her account into accounts as directed by the target(s). Specifically, Victim 1 purchased and sent (hereinafter "Transfers A") cryptocurrency ETH to the wallets given by a chat online service accessed through the fraudulent website https://www.ironfxebs.com/.

j. The target(s) provided Victim 1 with website addresses as the wallets to which she was to transfer her money. There were a total of about 15 transfers into those accounts. Those funds were then transferred throughout the blockchain ultimately to the Target Cryptocurrency Wallet.

k. After the transfers, Victim 1 began to believe she was victim of a fraud scheme. On or about November 15, 2023, Victim 1 requested "customer service chat personnel" at the fraudulent website return all funds she had transferred to https://www.ironfxebs.com/ accounts; the user operating that chat function refused to do so unless Victim 1 paid an additional amount of U.S. dollars in 'taxes' to release the money. At that time, the target(s) ceased all communications with Victim 1.

l. Based on SA Hannon's experience, he knows that a demand for victims to pay an additional fee for "taxes" is a common way targets attempt to defraud victims out of additional funds even after victims confront targets. Based on this pattern and others described, SA Hannon believes it is likely that the targets(s) are involved in an organized and experienced scheme that has defrauded victims beyond Victim 1. This provides additional

evidence that accounts controlled by the target(s) such as OKX WALLET TJDvJatY-WrCvvDBm2aNAeVK6tvyHd7f1Yp are likely used to launder proceeds of wire fraud.

m. On November 20, 2023, SA Hannon sent the above wallet addresses to USSS Financial Analyst Cassandra Carpentier ("Analyst Carpentier"), who performs cryptocurrency tracing for USSS. Analyst Carpentier located the wallets and determined they were maintained by the cryptocurrency exchange OKX.

n. Analyst Carpentier then traced the transactions of funds associated with Transfers A across the blockchain and determined that Victim 1's funds associated with those transfers were sent to USDT addresses, which ultimately were deposited into to OKX WALLET TJDvJatYWrCvvDBm2aNAeVK6tvyHd7f1Yp.

o. The manner in which the funds were transferred in this case is also significant. The tracing in this case that shows that Victim 1's funds were disbursed into numerous wallets only to be re-constituted on their way to the OKX WALLET TJDvJatY-WrCvvDBm2aNAeVK6tvyHd7f1Yp. This is a common tactic consistent with a design to obfuscate the source of the funds. Based on Agent Hannon's experience, this activity indicates the user intended to move funds with the purpose of concealing the origin and destination of the proceeds.

p. There is additional evidence of money laundering. For example, in October 2023 the OKX WALLET TJDvJatYWrCvvDBm2aNAeVK6tvyHd7f1Yp moved 86,274.44 USDT, co-mingled those funds with an additional 30,000 USDT, and then transferred a newly combined 100,000 USDT back into OKX WALLET TJDvJatY-WrCvvDBm2aNAeVK6tvyHd7f1Yp. That is, funds were removed from the OKX WALLET TJDvJatYWrCvvDBm2aNAeVK6tvyHd7f1Yp, placed in another wallet, co-mingled

with other funds, and then re-deposited into the OKX WALLET TJDvJatY-WrCvvDBm2aNAeVK6tvyHd7f1Yp. Based on Agent Hannon's experience, a pattern of transferring funds out, comingling the funds with other funds, and then re-depositing the same back into an account is consistent with an effort to obfuscate the origin of the funds.

q. On November 21, 2023, Agent Hannon requested account information for the accounts described above associated with the target(s) from OKX. He received an e-mail from the investigations team at OKX, who confirmed the above listed wallets were held at OKX. OKX also provided basic customer information for the OKX WALLET TJDvJatY-WrCvvDBm2aNAeVK6tvyHd7f1Yp which showed the target(s) are likely located in Southeast Asia.

r. On November 27, 2023, Analyst Carpentier and Agent Hannon continued to research investigative leads related to the fraudulent website ironfxebs.com. The investigation produced evidence that the targets(s) associated with that website appear to have registered numerous websites through NameCheap.com located in Iceland, all of which appear to be designed to look as if they are legitimate cryptocurrency investment vehicles, when in truth and in fact they are not. That is, the target(s) who controls the OKX WALLET TJDvJatYWrCvvDBm2aNAeVK6tvyHd7f1Yp appears to have engaged in this scheme on a broader scale. According to the open-source databases listed below, the fraudulent website associated with this scheme was registered by and is currently registered to a subject with the name Zuxin Pan and an e-mail address of zhongcaishan32@163.com. Those same identifiers appear to have registered as many as three spoofed URLs associated with the Iron FX exchange platform used in this scheme, and as many as 76 spoofed URLs associated with other financial platforms.

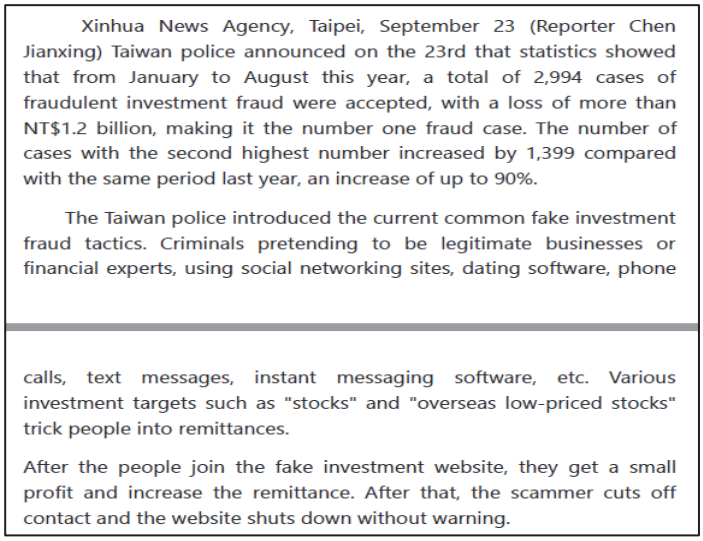
s. On December 1, 2023, OKX financial case associates asked for permission to share a contact email to the OKX WALLET TJDvJatYWrCvvDBm2aNAeVK6tvyHd7f1Yp holder, Chen. I provided approval to share cftfsc@usss.dhs.gov with Chen. On December 6, 2023, an email was received from draxlife@gmail.com, which appears to belong to Chen. In that e-mail, CHEN claimed to work for a company NewHigh Cloud Technology PTE.LTD. as a Sales Director. CHEN claimed that he receives his salary, incentive, and bonus into his OKX account that ends in -3776. The account that ends in -3776 is the account that holds the Target Cryptocurrency Wallet. CHEN provided a copy of his work authorization identification that shows a start date of June 29, 2023.

t. Deposits after June 29, 2023, are inconsistent with traditional salary, incentive, and bonus payments made from an employer. Instead, for example, the account that ends in -3776 received a total of 445,091.292916 USDT (that is, a value of more than $445,000 in U.S. dollars) between July 11, 2023, and November 16, 2023. Similarly, the OKX WALLET TJDvJatYWrCvvDBm2aNAeVK6tvyHd7f1Yp received 312,810.292916 USDT (that is, worth more than $312,000 in U.S. dollars) between July 11, 2023, and November 16, 2023.

u. During that same time period there was only one withdrawal, which occurred on October 20, 2023 – which is not a pattern consistent with Chen using these funds for daily living expenses as he claimed. On that date, 86,274.44 USDT was sent to a wallet that ends in -GRm5, and on October 21, 2023, that wallet received an additional 30,000 USDT from yet another wallet (one that ends in -9gSj) to combine with the 86,274.44 USDT (the full addresses are in the bulleted list at paragraph 17). Then, on October 23, 2023, a combined 100,000 USDT was deposited back in OKX WALLET

TJDvJatYWrCvvDBm2aNAeVK6tvyHd7f1Yp. The practice of transferring funds out of an account, co-mingling it with other funds, and then transferring it back in is consistent with money laundering.

v. Other law enforcement agencies are investigating nearly identical schemes as the one involving OKX WALLET TJDvJatYWrCvvDBm2aNAeVK6tvyHd7f1Yp. For example, below is a statement believed to have been issued by the Taiwan Police identifying a nearly identical model of fraudulent investment schemes:



Xinhua News Agency, Taipei, September 23 (Reporter Chen Jianxing) Taiwan police announced on the 23rd that statistics showed that from January to August this year, a total of 2,994 cases of fraudulent investment fraud were accepted, with a loss of more than NT$1.2 billion, making it the number one fraud case. The number of cases with the second highest number increased by 1,399 compared with the same period last year, an increase of up to 90%.

The Taiwan police introduced the current common fake investment fraud tactics. Criminals pretending to be legitimate businesses or financial experts, using social networking sites, dating software, phone calls, text messages, instant messaging software, etc. Various investment targets such as "stocks" and "overseas low-priced stocks" trick people into remittances.

After the people join the fake investment website, they get a small profit and increase the remittance. After that, the scammer cuts off contact and the website shuts down without warning.

8. Based on the information and allegations set forth herein, there is a factual basis to support a reasonable belief that the Government will be able to meet its burden of proof at trial to show that the Defendant Funds constitutes, or is traceable to:

b. property involved in wire fraud transactions, attempted wire fraud transactions, or conspiracy thereof in violation of 18 U.S.C. §§ 1343, 1349;

b. property involved in money laundering transactions or attempted transactions in violation of 18 U.S.C. § 1956(a)(1)(A)(i), and/or § 1956(a)(1)(B)(i) and/or 1957;

c. property involved in an illegal money transmitting business, in violation of 18 U.S.C. § 1960; and/or

d. proceeds of some other form of specified illegal activity set forth in 18 U.S.C. § 1956(c)(7) and;

e. proceeds of some other form of specified illegal activity set forth in 18 U.S.C. § 1956(h) and;

f. property involved in monetary transactions in criminally derived property, in violation of 18 U.S.C. § 1957

CONCLUSION

10. By reason of these premises, and pursuant to 18 U.S.C. § 981(f) and 21 U.S.C. § 881(h), whereby the Plaintiff's right, title and interest in and to the Defendant Funds relates back to the commission of the act giving rise to the forfeiture, the Defendant Funds has become and is forfeited to the United States of America, to be disposed of pursuant to Supplemental Rule G(7)(c) for Admiralty or Maritime Claims and Asset Forfeiture Actions, 18 U.S.C. § 981(d), 21 U.S.C. § 881(e), and other applicable laws.

WHEREFORE, Plaintiff prays that due process issue to enforce the forfeiture of the Defendant Funds, *in rem*; that a Warrant for the Arrest of the Defendant Funds be issued; that due Notice be given to all interested persons to appear, make claim, answer and show cause why the forfeiture should not be decreed; that the Defendant Funds be decreed condemned and forfeited to the United States of America for disposition according to law; and that Plaintiff have such other and further relief as the Court may deem just and proper, together with the costs and disbursements of this action.

Respectfully submitted,

Adair F. Boroughs
UNITED STATES ATTORNEY

By: *s/Carrie Fisher Sherard*
Carrie Fisher Sherard #10134
Assistant United States Attorney
55 Beattie Place, Suite 700
Greenville, SC 29601
(864) 282-2100

May 22, 2024