

UNITED STATES DISTRICT COURT

for the

District of Columbia

In the Matter of the Seizure of)
(Briefly describe the property to be seized))

ONE DOMAIN NAME FOR VIOLATIONS)
OF 18 U.S.C. §§ 1349, 1956)
)

Case No. 25-sz-52

WARRANT TO SEIZE PROPERTY SUBJECT TO FORFEITURE BY TELEPHONE

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests that certain property located in the jurisdiction of the District of Columbia be seized as being subject to forfeiture to the United States of America. The property is described as follows:

ONE DOMAIN NAME FOR VIOLATIONS OF 18 U.S.C. §§ 1349, 1956, FUTURE DESCRIBED IN ATTACHMENT A, HEREBY INCORPORATED BY REFERENCE.

I find that the affidavit(s) and any recorded testimony establish probable cause to seize the property.

YOU ARE COMMANDED to execute this warrant and seize the property on or before

12/15/2025

(not to exceed 14 days)

☐ in the daytime – 6:00 a.m. to 10:00 p.m.

☒ at any time in the day or night, as I find reasonable cause has been established.

Unless delayed notice is authorized below, you must also give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

An officer present during the execution of the warrant must prepare, as required by law, an inventory of any property seized and the officer executing the warrant must promptly return this warrant and a copy of the inventory to United States Magistrate Judge

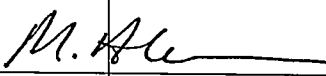
Moxila A. Upadhyaya

(name)

☐ I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized (check the appropriate box) ☐ for _____ days (not to exceed 30).

☐ until, the facts justifying, the later specific date of _____

Date issued: 12/01/2025


Judge's signature

City and state: District of Columbia

Moxila A. Upadhyaya, U.S. Magistrate Judge
Printed name and title

**UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA**

**IN THE MATTER OF THE SEIZURE OF
ONE DOMAIN NAME FOR
VIOLATIONS OF 18 U.S.C. §§ 1349, 1956**

CASE NO. 25-sz-52

FILED UNDER SEAL

Reference: USAO No. 2025R00982

AFFIDAVIT IN SUPPORT OF SEIZURE WARRANT

I, [REDACTED], a Special Agent with Federal Bureau of Investigation (FBI), being duly sworn, depose and state as follows:

1. I make this affidavit in support of an application for a seizure warrant for one domain name,¹ tickmilleas.com (**TARGET DOMAIN NAME**). The **TARGET DOMAIN NAME** to be seized is described in the following paragraphs and in Attachment A.

2. A search of publicly available WHOIS² domain name registration records revealed that **TARGET DOMAIN NAME** was registered on or about November 5, 2025, through the registrar³ GNAME (gname.com), believed to be headquartered at 8 Temasek Boulevard #21-04

¹ A domain name is a string of text that maps to an IP address and serves as an easy-to-remember way for humans to identify devices on the Internet (e.g., “justice.gov”). Domain names are composed of one or more parts, or “labels,” delimited by periods. When read right-to-left, the labels go from most general to most specific. The right-most label is the “top-level domain” (TLD) (e.g., “.com” or “.gov”). To the left of the TLD is the “second-level domain” (SLD), which is often thought of as the “name” of the domain. The SLD may be preceded by a “third-level domain,” or “subdomain,” which often provides additional information about various functions of a server or delimits areas under the same domain. For example, in “www.justice.gov,” the TLD is “.gov,” the SLD is “justice,” and the subdomain is “www,” which indicates that the domain points to a web server.

² WHOIS is a protocol used for querying databases that store registration and other information about domains, IP addresses, and related Internet resources.

³ A registrar is a company that has been accredited by the Internet Corporation for Assigned Names and Numbers (ICANN) or a national country code top-level domain (such as .uk or .ca) to register

Suntec Tower Three, Singapore, 038988. The top-level domain for **TARGET DOMAIN NAME** is “.com.” VeriSign, Inc., a U.S. company, manages all “.com” domains and is the registry⁴ for **TARGET DOMAIN NAME**.

3. I am a “federal law enforcement officer” within the meaning of Federal Rule of Criminal Procedure 41(a)(2)(c), that is, a government agent engaged in enforcing the criminal laws and duly authorized by the Attorney General to request a seizure warrant.

4. I am a Special Agent with the FBI and have been employed in this capacity since January 2019. I am assigned to a [REDACTED].

As a Special Agent, I have experience investigating cases involving the major fraud schemes, international criminal syndicates, and money laundering. During my career, I have received training and gained experience in interviewing subjects and victims, search warrant applications, the execution of searches and seizures, blockchain analysis of various cryptocurrencies, and various criminal laws and procedures. Through my training, education, and experience, I have become familiar with how various federal offenses are committed. In addition, I have been the affiant on federal arrest warrant, search warrant, and seizure warrant applications. Based upon my training and experience, I am familiar with the strategies and techniques utilized by criminal syndicates conducting investment fraud schemes through the internet, including cryptocurrency investment fraud schemes.

and sell domain names. Registrars act as intermediaries between registries and registrants. Registrars typically maintain customer and billing information about the registrants who used their domain name registration services.

⁴ A domain name registry is an organization that manages top-level domains, including by setting usage rules and working with registrars to sell domain names to the public.

PURPOSE OF AFFIDAVIT

5. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents, witnesses, and agencies. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant. It does not set forth all my knowledge, or the knowledge of others, about this matter. Based on my training and experience and the facts as set forth in this affidavit, I respectfully submit that there is probable cause to believe that violations of 18 U.S.C. §§ 1343, 1349 (Fraud by wire, radio, or television, and conspiracy), and 18 U.S.C. § 1956 (a)(2)(A) & (h) (Laundering monetary instruments and conspiracy) have been committed by numerous unknown individuals operating out of the Burma-based scam compound named “Tai Chang” and their co-conspirators. There is also probable cause to seize the **TARGET DOMAIN NAME** described in Attachment A as property subject to forfeiture pursuant to 18 U.S.C. §§ 981(a)(1)(A), 982(a)(1), and 28 U.S.C. § 2461(c).

SUMMARY OF AFFIDAVIT

6. The United States is investigating international criminal organizations operating cryptocurrency investment fraud (CIF) scams.⁵ According to information developed through the investigation and ample public reporting, in CIF scams, victims (often in the United States) are targeted and, over time, deceived into fraudulent investment schemes on fake websites and platforms. Relevant here, these platforms are controlled by criminal actors overseas, primarily associated with Chinese organized crime syndicates, and while the platforms purport to show that victims are making substantial returns on their cryptocurrency “investments,” in reality, all victim funds are funneled directly to the scammers.

7. Numerous CIF schemes are run out of industrial-scale scam compounds in Burma. The criminal syndicates behind these compounds often lure unsuspecting persons to travel to

nearby Thailand with the offer of high paying technical jobs. However, many of these persons instead have their identification documents seized and are trafficked to Burma to work in these scam compounds. Within these compounds, these trafficked persons, themselves victims, are forced to work long hours to conduct CIF schemes against fraud victims from the United States and other countries.

8. According to publicly available reporting, discussed in more depth below, “Tai Chang Park” (also known as “Taichang,” “Ko Sai Casino,” and “Kyauk Khat Casino”) (described in detail below), located in the town of Kyaukhat, is one of the major scam compounds in Burma. Also according to public reporting, trafficked persons brought to work at the Tai Chang compound, have been subject to rape, torture, and murder. The compound is reportedly secured through a mix of Chinese criminal actors and members of the Democratic Karen Benevolent Army (DKBA). DKBA has acknowledged the high number of trafficked persons in their territory. On November 12, 2025, the Department of the Treasury’s Office of Foreign Assets Control (OFAC) designated the DKBA, a Burmese armed group, along with four of its senior leaders (Sai Kyaw Hla, Saw Steel, Saw Sein Win, and Saw San Aung), for supporting cyber scam centers in Burma that target Americans using fraudulent investment schemes. OFAC also designated Trans Asia International Holding Group Thailand Company Limited (Trans Asia), which is linked to Chinese organized crime and has worked with the DKBA and other armed groups to develop these scam centers.

9. On or about November 10, 2025, U.S. Magistrate Judge Matthew J. Sharbaugh issued a seizure warrant in case no. 25-sz-47 for two domains used in CIF scams linked to Tai

⁵ In public reporting, these scams are sometimes referred to as “pig butchering,” a term derived from the Chinese phrase used to describe this scheme.

Chang. The seizure warrant's affidavit, incorporated by reference, also details more than a dozen identified CIF victims whose scammers were determined to be in the Tai Chang scam compound.

10. The government has continued its investigation into Tai Chang and has identified and is seeking to seize another target domain name, **TARGET DOMAIN NAME**. As detailed below, **TARGET DOMAIN NAME** was involved in money laundering offenses, in violation of 18 U.S.C. § 1956(a)(2)(A), and therefore should be seized pursuant to 18 U.S.C. §§ 981(a)(1)(A), 982(a)(1).

STATUTES, JURISDICTION, AND VENUE

11. Title 18, United States Code, Section 1343 criminalizes devising 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, transmits or causes 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.” Title 18, United States Code, Section 1349 criminalizes the conspiracy to commit wire fraud, as defined in Section 1343.

12. Title 18, United States Code, Section 1956(a)(2)(A) criminalizes “transport[ing], transmit[ing], or transfer[ing], or attempts to transport, transmit, or transfer a monetary instrument or funds from a place in the United States to or through a place outside the United States or to a place in the United States from or through a place outside the United States with the intent to promote the carrying on of specified unlawful activity.” Violations of 18 U.S.C. §§ 1343, 1349

qualify as specified unlawful activity under the statute. Title 18, United States Code, Section 1956(h) criminalize the conspiracy to commit money laundering, as defined in Section 1956(a).

13. This Court has jurisdiction to issue the requested warrant. Section 853(f) of Title 21 of the U.S. Code authorizes the government to obtain a seizure warrant from the court in the same manner as a search warrant under Federal Rule of Criminal Procedure 41. Further, Section 853(l) provides that a federal court has “jurisdiction to enter orders as provided in this section *without regard to the location of any property which may be subject to forfeiture*” (emphasis added). Section 853(f) provides that a court shall issue a criminal seizure warrant if it determines that the property to be seized would, in the event of a conviction, be subject to forfeiture and that a restraining order would be inadequate to assure the availability of the property for forfeiture. Neither a restraining order nor an injunction is sufficient to guarantee the availability of the **TARGET DOMAIN NAME** for forfeiture. By seizing the **TARGET DOMAIN NAME** and redirecting traffic, the government will prevent third parties from controlling or acquiring **TARGET DOMAIN NAME** and using it to commit additional violations of 18 U.S.C. §§ 1343, 1349, and 1956.

14. This affidavit also is being submitted in support of a civil seizure warrant for the property pursuant to 18 U.S.C. § 981(b)(2). Such a warrant requires a finding of probable cause and may be obtained on an *ex parte* basis. Section 981(b) applies to all property subject to civil forfeiture under § 981(a). Under § 981(a)(1)(A), property subject to forfeiture to the United States includes “[a]ny property, real or personal, involved in a transaction or attempted transaction in violation of [18 U.S.C. §1956].” As discussed below, there is probable cause to believe that violations of 18 U.S.C. §§ 1343, 1349, and 1956 have been committed by numerous unknown

individuals operating out of the Burma-based scam compound named Tai Chang and the individuals responsible for the use of **TARGET DOMAIN NAME**.

15. Further, the criminal offenses under investigation began or were committed upon the high seas, or elsewhere out of the jurisdiction of any particular State or district, and no offender is known to have, or have had, residence within any United States district. *See* 18 U.S.C. § 3238.

BACKGROUND ON CRYPTOCURRENCY

16. **Virtual Currency:** Virtual currencies are digital representations of value that, like traditional coin and paper currency, function as a medium of exchange (i.e., they can be digitally traded or transferred and can be used for payment or investment purposes). Virtual currencies are a type of digital asset separate and distinct from digital representations of traditional currencies, securities, and other traditional financial assets. The exchange value of a particular virtual currency generally is based on agreement or trust among its community of users. Some virtual currencies have equivalent values in real currency or can act as a substitute for real currency, while others are specific to particular virtual domains (e.g., online gaming communities) and generally cannot be exchanged for real currency. Cryptocurrencies, like Bitcoin and Ether, are types of virtual currencies that rely on cryptography for security. Cryptocurrencies typically lack a central administrator to issue the currency and maintain payment ledgers. Instead, cryptocurrencies use algorithms, a distributed ledger known as a blockchain, and a network of peer-to-peer users to maintain an accurate system of payments and receipts.

17. **Blockchain:** A blockchain is a digital ledger run by a decentralized network of computers referred to as “nodes.” Each node runs software that maintains an immutable and historical record of every transaction utilizing that blockchain’s technology. Many digital assets, including virtual currencies, publicly record all their transactions on a blockchain, including all of

the known balances for each virtual currency address on the blockchain. Blockchains consist of blocks of cryptographically signed transactions, and blocks are added to the previous block after validation and after undergoing a consensus decision to expose and resist tampering or manipulation of the data. There are many different blockchains used by many different virtual currencies. For example, Bitcoin in its native state exists on the Bitcoin blockchain, while Ether (or “ETH”) exists in its native state on the Ethereum network.

18. **Blockchain Analysis:** Law enforcement can trace transactions on blockchains to determine which virtual currency addresses are sending and receiving particular virtual currency. This analysis can be invaluable to criminal investigations for many reasons, including that it may enable law enforcement to uncover transactions involving illicit funds and to identify the person(s) behind those transactions. To conduct blockchain analysis, law enforcement officers use reputable, free open source blockchain explorers, as well as commercial tools and services. These commercial tools are offered by different blockchain-analysis companies. Through numerous unrelated investigations, law enforcement has found the information associated with these tools to be reliable.

19. **Virtual Currency/Cryptocurrency Address:** A virtual currency address is an alphanumeric string that designates the virtual location on a blockchain where virtual currency can be sent and received. A virtual currency address is associated with a virtual currency wallet.

20. **Virtual Currency/Cryptocurrency Exchange:** A virtual currency exchange (“VCE”), also called a cryptocurrency exchange, is a platform used to buy and sell virtual currencies. VCEs allow users to exchange their virtual currency for other virtual currencies or fiat currency, and vice versa. Many VCEs also store their customers’ virtual currency addresses in hosted wallets. VCEs can be centralized (i.e., an entity or organization that facilitates virtual

currency trading between parties on a large scale and often resembles traditional asset exchanges like the exchange of stocks) or decentralized (i.e., a peer-to-peer marketplace where transactions occur directly between parties).

21. **Virtual Currency/Cryptocurrency Wallet:** A virtual currency wallet (e.g., a hardware wallet, software wallet, or paper wallet) stores a user's public and private keys, allowing a user to send and receive virtual currency stored on the blockchain. Multiple virtual currency addresses can be controlled by one wallet.

22. **Unhosted Wallet:** An unhosted wallet, also known as a self-hosted, non-custodial wallet, is a virtual currency wallet through which the user has complete control over storing and securing their private keys and virtual currency. Unhosted wallets do not require a third party's involvement (e.g., a virtual currency exchange) to facilitate a transaction involving the wallet. Unhosted wallets allow users to generate and manage their own Private Addresses.

23. **Stablecoins:** Stablecoins are a type of virtual currency whose value is pegged to a commodity's price, such as gold, or to a fiat currency, such as the U.S. dollar, or to a different virtual currency. For example, Tether (also known as USDT) is a stablecoin pegged to 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.

24. **Tether Limited:** Tether Limited ("Tether Ltd") is a company that manages the smart contracts and the treasury (i.e., the funds held in reserve) for USDT tokens.

25. **Ether:** Ether ("ETH") is a cryptocurrency that is open source, public, has a blockchain, and is distributed on a platform that uses "smart contract" technology. The public ledger is the digital trail of the Ethereum blockchain, which allows anyone to track the movement of ETH.

PROBABLE CAUSE

I. Background on Cryptocurrency Investment Fraud

26. CIF is a confidence/investment scam perpetrated against victims for financial gain. The perpetrators contact victims, usually online, and form a strong relationship, romantic or otherwise, over days, weeks, or longer. After the subject has gained the victim's trust, the subject introduces the victim to the idea of investing in cryptocurrency. The subject then directs the victim to a specific scam website or app disguised as a legitimate investment platform.

27. The scam websites to which the victims are directed are often accessible on traditional web browsers and mobile applications (or "apps"). However, it is increasingly common for them to also be accessible within a Web3 portal.⁶ When fraud victims are interacting with these scam platforms, they are provided cryptocurrency addresses to fund their account. The victims are instructed to open an account on a cryptocurrency exchange to exchange fiat currency (U.S. dollars) for cryptocurrency and send that cryptocurrency to the cryptocurrency address(es) provided by the websites.

28. The fraud victims believe sending cryptocurrency to a cryptocurrency address provided by one of these scam websites constitutes depositing money into a legitimate investment platform; in actuality, the victims are sending funds directly to scammers, who are then free to move those funds along to associates. The scam websites purport to show the victims' returns on their investment, prompting the victims to "invest" more cryptocurrency into the platform. This

⁶ A Web3 Portal is essentially a web browser that allows users to access decentralized websites running on the blockchain. It is common for victims to mistake their cryptocurrency wallet application as the location of their investments, while the scam websites they access through the Web3 Portal are completely unrelated.

scam is continued until a victim becomes aware of the scam or runs out of money, at which time the scammer ceases contact.

29. While fraud victims from numerous countries throughout the world are impacted by CIF schemes, the United States is one of the primary targets due to its global economic status. According to the United States Institute of Peace (USIP), “the size of this criminal market is still extremely difficult to estimate due to the lack of reporting on what represents a novel form of criminality [but,] as of the end of 2023, a conservative estimate of the annual value of funds stolen by these scam syndicates worldwide now approaches \$64 billion a year and involves millions of victims.”⁷

30. According to the FBI’s Internet Crime Complaint Center (IC3), in 2023, investment scams became the most often reported crime type to the IC3, with CIF comprising 83% of that category. CIF schemes have continued to grow, and the IC3 calculated that the reported losses from CIF scams rose, from \$3.96 billion in 2023, to \$5.8 billion in 2024, an increase of 47%.⁸ These numbers, largely based on losses reported by victims, are likely severely underrepresenting the true loss amounts incurred by Americans, since most fraud victims do not report to IC3. Individual victims of financial frauds will often incorrectly blame themselves and carry a guilt with them that results in widespread underreporting.

⁷ Transnational Crime in Southeast Asia: A Growing Threat to Global Peace and Security (May 2024) (“A Growing Threat (May 2024)”), available at https://www.usip.org/sites/default/files/2024-05/ssg_transnational-crime-southeast-asia.pdf (last accessed on November 6, 2025).

⁸ IC3 (2024) Federal Bureau of Investigation Internet Crime Report. IC3, available at https://www.ic3.gov/AnnualReport/Reports/2024_IC3Report.pdf (last accessed on November 6, 2025).

II. Background on the Origins of CIF Scam Compounds in Burma

31. Based on publicly available sources, in 2017, the first Chinese investors who would later construct CIF scam compounds arrived in Burma's Kayin State.^{9, 10} This remote area of eastern Burma, adjacent to the Thai border, has seen decades of conflict from various civil wars and disputes that continue to this day. Throughout these conflicts, regional militias have been formed throughout Burma, including in Kayin State, with the now-renamed Karen National Army (KNA),¹¹ formerly branded as the "Border Guard Force" (BGF).¹² While the Karen BGF was allied with the Burma military, it held immense power in this remote region while the military was, and still is, fighting a war against the Burmese government.¹³

32. As described further below, one of the first major scam centers of Kayin was developed by completely reshaping the town of Shwe Kokko. A reported partnership between the Karen BGF, including BGF Colonel Saw Chit Thu and She Zhijiang, a Chinese businessman,

⁹ *A Growing Threat* (May 2024), *supra* note 9.

¹⁰ The Kayin State was previously referred to as the Karen State. BBC News, Burma Government Signs Ceasefire with Karen Rebels (Jan. 12, 2012), available at <https://www.bbc.com/news/world-asia-16523691> (last accessed on November 6, 2025).

¹¹ Myanmar Now, Karen BFG to Rename Itself Karen National Army (Mar. 6, 2024), available at <https://myanmar-now.org/en/news/karen-bgf-to-rename-itself-karen-national-army/> (last accessed on November 6, 2025).

¹² The Karen BGF has since renamed itself the Karen National Army after distancing itself from the Burma Military, while retaining regional control.

¹³ "The Karen Border Guard Force/Karen National Army Criminal Network Exposed" (May 22, 2024), available at <https://www.justiceformyanmar.org/stories/the-karen-border-guard-force-karen-national-army-criminal-business-network-exposed> (last accessed on November 6, 2025). The Karen BGF renamed itself the KNA in 2024. VOA News, "261 trafficking victims rescued from Myanmar scam center," available at <https://www.voanews.com/a/trafficking-victims-rescued-from-myanmar-scam-center/7972816.html> (last accessed on November 6, 2025).

coordinated this development. She Zhijiang was arrested in Thailand in 2022 and sanctioned by the United Kingdom (UK) in 2023 for links to human trafficking.¹⁴

33. In 2020, the Karen BGF/Saw Chit Thu/She Zhijiang partnership reportedly established a 46.3 square mile “special economic zone” along the Burma-Thailand border in Shwe Kokko, since renamed “Yatai New City.”¹⁵ Yatai IHG, the company behind these developments, advertised the development as a “smart city,” with high-end housing and casinos; it is also a region “impervious to law enforcement and regulation” in which the company controls security, public utilities, and health services.¹⁶ According to the USIP, “under the armed protection of . . . a paramilitary unit that reports to the Burmese armed forces, Yatai IHG has secretly developed numerous illegal structures throughout Shwe Kokko . . . to host ‘technology’ and ‘entertainment’ companies in this remote part of the Karen State.”¹⁷ USIP further reported that thousands of Chinese workers had been “lured” to this location to build and work in these structures.¹⁸

34. One of the original goals of the Yatai New City was to host gambling operations, both online and in-person, for Chinese customers—an activity that is illegal in China. After the COVID-19 pandemic crushed business plans for gambling centers in special economic zones like Yatai IHG’s, Chinese criminal organizations in these zones turned to fraud schemes, especially

¹⁴ UK Press Release, “UK and allies sanction human rights abusers” (Dec. 8, 2023), available at <https://www.gov.uk/government/news/uk-and-allies-sanction-human-rights-abusers> (last accessed on November 6, 2025).

¹⁵ Priscilla A. Clapp and Jason Tower, “Myanmar: Transnational Networks Plan Digital Dodge in Casino Enclaves,” United States Institute of Peace (July 23, 2020), available at <https://www.usip.org/publications/2020/07/myanmar-transnational-networks-plan-digital-dodge-casino-enclaves> (last accessed on November 6, 2025).

¹⁶ *Id.*

¹⁷ *Id.*

¹⁸ *Id.*

CIF, as a new source of revenue.¹⁹ And as lockdowns and border controls meant Chinese workers could not travel to Burma, these organizations began trafficking workers from around the world.²⁰ USIP reported that beginning in 2021, criminals began “large-scale trafficking of alternative labor into the zones and develop[ed] new tools for international investment or crypto-currency-fraud schemes that rely on large numbers of scammers building personal contacts with potential victims on social media.”²¹

35. The U.S. Office of Foreign Assets Control (OFAC) added She Zhijiang to its Specially Designated Nationals (SDN) list on September 8, 2025. OFAC designated She Zhijiang and two associated business entities, Yatai International Holdings Group Limited, and Myanmar Yatai International Holding Group Co., Ltd, “pursuant to E.O. 13818, for being foreign persons who are responsible for or complicit in, or who have directly or indirectly engaged in, serious human rights abuse.”²² OFAC’s press release stated:

She Zhijiang is the creator and largest shareholder of the Yatai New City compound. Adopting Burmese and Cambodian citizenship, he has operated for years under a plethora of pseudonyms. In 2022, She Zhijiang was arrested in Thailand based on an Interpol Red Notice issued by China, which has continued to seek his extradition from Thailand ever since.²³

¹⁹ Priscilla A. Clapp and Jason Tower, Myanmar’s Criminal Zones: A Growing Threat to Global Security, United States Institute of Peace (Nov. 9, 2022), available at <https://www.usip.org/publications/2022/11/myanmars-criminal-zones-growing-threat-global-security> (A Growing Threat (Nov. 2022)) (last accessed on November 6, 2025).

²⁰ *Id.*

²¹ *Id.*

²² U.S. Dep’t of the Treasury, “Treasury Sanctions Southeast Asian Networks Targeting Americans with Cyber Scams” (Sep. 8, 2025), available at <https://home.treasury.gov/news/press-releases/sb0237> (last accessed on November 6, 2025.)

²³ *Id.*

36. In May 2025, the KNA (formerly Karen BGF) and Saw Chit Thu, also sanctioned by the UK, were sanctioned by the United States for facilitating cyber scams, human trafficking, and cross-border smuggling.²⁴

37. Since 2021, scam center developments have proliferated along the Burma/Thailand border. This map, published by the Irrawaddy, a Burma-focused news outlet, shows the development of “Chinese-backed projects” in the region:

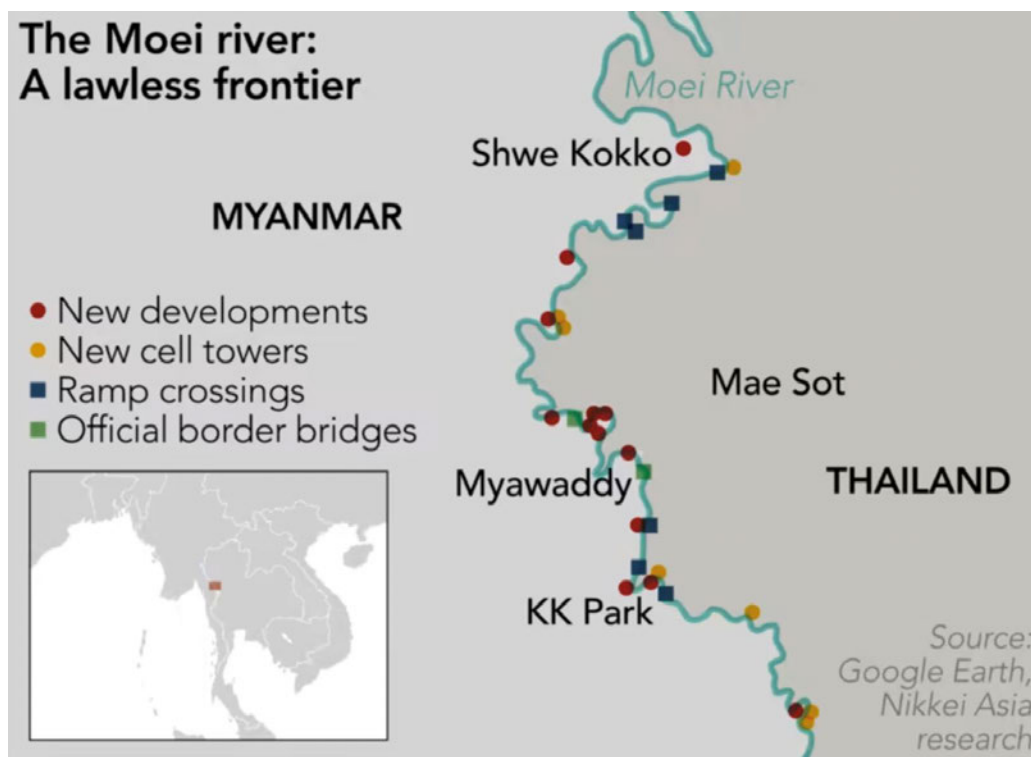


Figure 1 – Several compound developments are identified along the Moei river in Burma.²⁵

²⁴ U.S. Dep’t of the Treasury, “Treasury Sanctions Burma Warlord and Militia Tied to Cyber Scam Operations” (May 5, 2025), available at <https://home.treasury.gov/news/press-releases/sb0129> (last accessed on November 6, 2025).

²⁵ Irrawaddy, “Karen National Union Under Pressure Over Crime Hub” (Feb 28, 2023), available at <https://www.irrawaddy.com/news/burma/karen-national-union-under-pressure-over-crime-hub.html> (“KNU Under Pressure”) (last accessed on November 6, 2025).

38. CIF compounds are often “city-like” and reminiscent of “penal colonies.”²⁶ For instance, KK Park, a compound located on the Burma/Thai border town of Myawaddy, reportedly contained “as many as 10,000 people . enslaved there, tortured or, according to some accounts, threatened with having their organs harvested if they fail to generate adequate revenue from operating scams.”²⁷ Public reporting on KK Park and other Southeast Asian CIF compounds includes accounts of beatings, electrocutions, and murder.²⁸ Victims are frequently required to pay for the ability to leave these compounds; some are “subjected to violence and torture, which is sometimes filmed and sent to relatives to spur them to send ransoms.”²⁹ Those who cannot or do not pay are sometimes sold between companies.³⁰

39. One common method criminals use to imprison these victims is to lure them to the area with the false promise of employment before trafficking them to these compounds.³¹ A June 8, 2022 article published by *Free Malaysia Today*, a Malaysian online news site, detailed the

²⁶ Priscilla A. Clapp and Jason Tower, “Myanmar’s Criminal Zones: A Growing Threat to Global Security,” United States Institute of Peace (Nov 9, 2022), available at <https://www.usip.org/publications/2022/11/myanmars-criminal-zones-growing-threat-global-security> (last accessed on November 6, 2025).

²⁷ *Id.*; *KNU Under Pressure*, *supra* note 27.

²⁸ *A Growing Threat* (Nov. 2022), *supra* n. 21; Shaun Turton, Cyber Slavery: Inside Cambodia’s Online Scam Gangs, *Nikkei Asia* (Sept 1, 2021), available at <https://asia.nikkei.com/Spotlight/The-Big-Story/Cyber-slavery-inside-Cambodia-s-online-scam-gangs> (“Cyber Slavery”) (last accessed on November 6, 2025); Tessa Wong, Bui Thu, and Lok Lee, Cambodia Scams: Lured and Trapped into Slavery in South East Asia, *BBC News* (Sept 20, 2022), available at <https://www.bbc.com/news/world-asia-62792875> (“Cambodia Scams”) (last accessed on November 6, 2025).

²⁹ *Cyber Slavery*, *supra* note 30; *see also Cambodia Scams*, *supra* note 30.

³⁰ *Cyber Slavery*, *supra* note 30; *Cambodia Scams*, *supra* note 30.

³¹ Mary Wambui, Kenya ‘Overwhelmed’ by Job Scam Victims in Myanmar, *The East African* (Aug 23, 2022), available at <https://www.theeastafrican.co.ke/tea/news/east-africa/kenya-overwhelmed-by-job-scam-victims-in-myanmar-3923668> (last accessed on November 6, 2025); Indian Workers Rescued from Digital Job Scams in Southeast Asia, *Al Jazeera* (Oct 8, 2022), available at <https://www.aljazeera.com/news/2022/10/8/indian-workers-rescued-from-digital-job-scams-in-southeast-asia> (last accessed on November 6, 2025); *Cyber Slavery*, *supra* note 30; *Cambodia Scams*, *supra* note 30.

account of a 19-year old Malaysian man who was imprisoned in KK Park after responding to an online job advertisement for a waiter position in Thailand.³² After reporting for the position, he was trafficked into Burma via the border town of Mae Sot.³³ Upon arriving at KK Park, he was housed in a four-story building with approximately 300 other Malaysian victims per floor and was forced to target victims in the United States through romance-based “pig butchering” scams.³⁴ After refusing to work, he was reportedly beaten with a baseball bat and later pushed out of a building from the third floor, resulting in a broken leg and rib.³⁵ Ultimately, he was released after his family paid a ransom.³⁶

III. The Tai Chang Compound

A. Background on the Tai Chang Compound and Its Organization

40. Tai Chang is in Kyaukhat, Burma, along the Thailand border. The compound was reportedly established in January 2020 by Brigadier General Sai Kyaw Hla, leader of the DKBA, and by Chinese investors from the Trans-Asia International Holding Group Co., Ltd.³⁷ According to public reporting, the Tai Chang compound also goes by the names Ko Sai Casino or Kyauk Khat Casino.³⁸

³² Faisal Asyraf, Trafficked Teen Returns Home, Claims ‘Hundreds’ Still Held Captive in Myanmar, Free Malaysia Today (Jun 8, 2022), available at <https://www.freemalaysiatoday.com/category/nation/2022/06/08/trafficked-teen-returns-home-claims-hundreds-still-held-captive-in-myanmar/> (last accessed on November 6, 2025).

³³ *Id.*

³⁴ *Id.*

³⁵ *Id.*

³⁶ *Id.*

³⁷ China Forces Myanmar Scam Syndicates to Move to Thai Border (Apr 22, 2024), available at <https://www.usip.org/publications/2024/04/china-forces-myanmar-scam-syndicates-move-thai-border> (“China Forces”) (last accessed on November 6, 2025).

³⁸ *Id.*; Radio Free Asia (Apr. 13, 2023), available at <https://www.rfa.org/english/news/laos/trafficked-04112023170154.html> (“According to a geolocation pin sent to RFA by several parents of Lao teens trapped at the Casino Kosai, the site

41. The Tai Chang compound is located approximately 25 miles southeast of the Shwe Kokko.³⁹ A map of Kyaukhath, Burma, and the border with Thailand, is shown below.



*Figure 2 – Map of the Burma (left) and Thailand (right) border. Kyaukhath is depicted southeast of Shwe Kokko.*⁴⁰

42. The following satellite imagery, obtained from two different providers, shows the area of the Tai Chang compound between 2020 and 2025, and the development of multiple buildings into the creation of a north and south compound. As described further herein, these compounds appear to contain operations of a CIF scheme to target U.S. victims.

appears to be a warehouse some 20 miles south of Myawaddy city, across the border from a Thai town.”) (“Radio Free Asia (Apr. 13, 2023)”) (last accessed on November 6, 2025).

³⁹ C4ADS, Hot Lines: Tracing Movements to and from Myanmar’s Scam Centers (Mar 27, 2025), available at https://c4ads.org/commentary/hot-lines/#_ftnref46 (last accessed on November 6, 2025); *China Forces*, *supra* note 39.

⁴⁰ Google Maps,

https://www.google.com/maps/place/16%C2%B028'16.1%22N+98%C2%B038'49.5%22E/@16.471143,98.6445031,835m/data=!3m2!1e3!4b1!4m4!3m3!8m2!3d16.471143!4d98.647078?entry=tu&g_ep=EgoyMDI1MTEwNC4xIKXMDSoASAFQAw%3D%3D

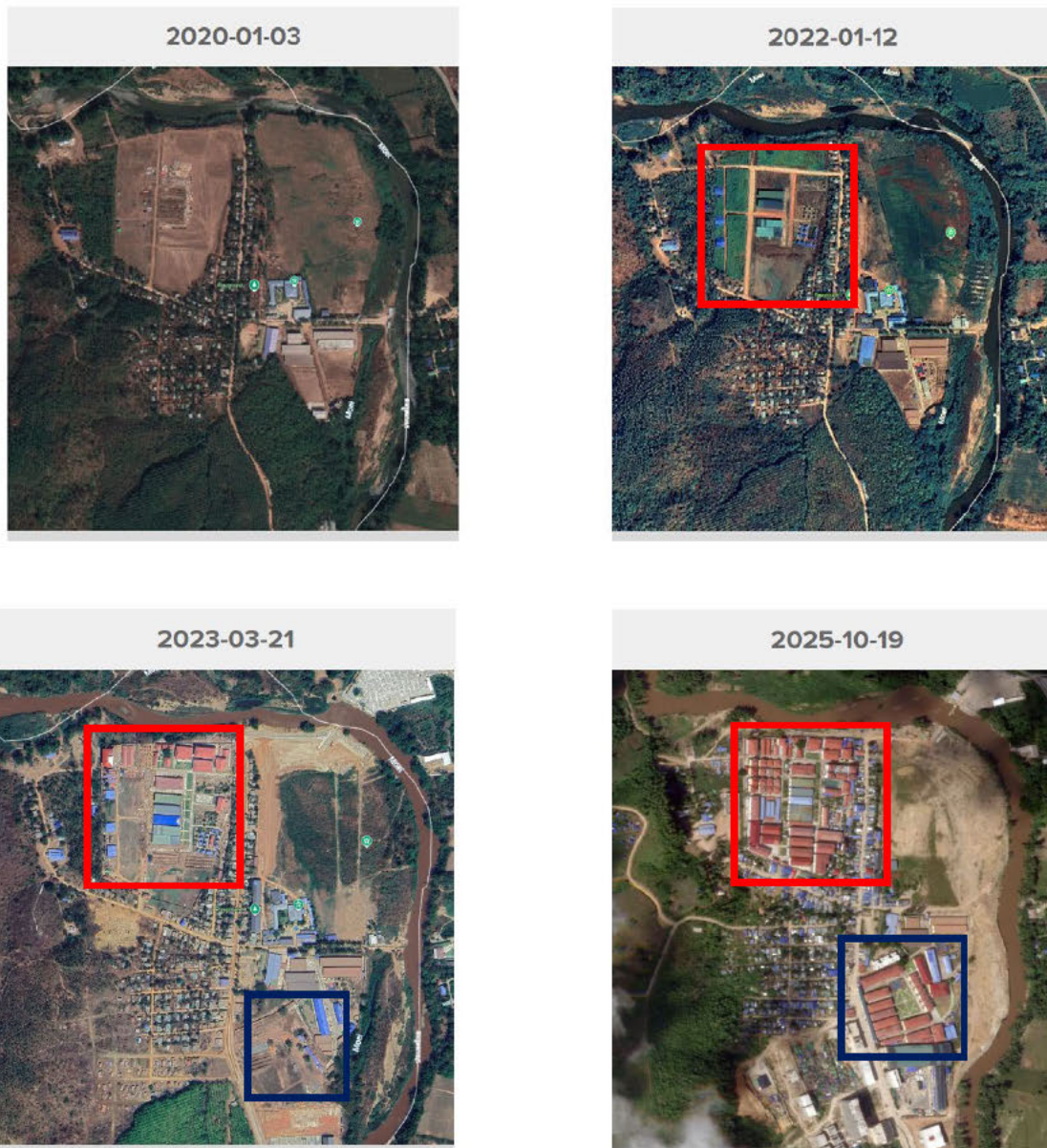


Figure 3 – Satellite imagery showing development of Tai Chang compound.

43. Based on reporting published in *The Guardian*, the Tai Chang compound is on the opposite side of the Moei river that separates Thailand and Burma.⁴¹ An aerial photograph of the compound taken in or around August 2025 and included in this reporting, is shown below:

⁴¹ “Revealed: the huge growth of Myanmar scam centres that may hold 100,000 trafficked people” (Sept. 7, 2025), available at <https://www.theguardian.com/global-development/2025/sep/08/myanmar-military-junta-scam-centres-trafficking-crime-syndicates-kk-park> (“Revealed”) (last accessed on November 6, 2025).



Figure 4 – Tai Chang as seen from the Thai border.

44. The compound is reportedly secured through a mix of Chinese criminal actors and members of the DKBA. DKBA is a separate entity from KNA, and also friendly with the ruling Burmese Junta.⁴² The DKBA is run by General Saw Steel,⁴³ Colonel Saw Sein Win,⁴⁴ and Brigadier General Sai Kyaw Hla.⁴⁵ Victims trafficked to the Tai Chang compound have reported their location and local sources have reported that the area is under the control of the DKBA, and

⁴² Jason Tower, Priscilla Clapp, “Chinese Crime Networks Partner with Myanmar Armed Groups” (April 20, 2020), available at <https://www.usip.org/publications/2020/04/chinese-crime-networks-partner-myanmar-armed-groups> (last accessed on November 6, 2025).

⁴³ Myanmar Now (Aug. 30, 2022), available at <https://myanmar-now.org/en/news/ethnic-karen-leaders-come-to-historic-agreement-to-reunite-knu-dkba/> (last accessed on November 6, 2025).

⁴⁴ DVB (Jan. 23, 2023), available at <https://english.dvb.no/dkba-demands-answers-after-junta-airstrike-on-commanders-housing-compound/> (last accessed on November 6, 2025); Radio Free Asia (Jan. 23, 2023), available at <https://www.rfa.org/english/news/myanmar/juntadkbairstrike-01232023164117.html> (last accessed on November 6, 2025).

⁴⁵ Radio Free Asia (Apr. 13, 2023), *supra* note 40.

Brigadier General, Sai Kyaw Hla.⁴⁶ The same report noted that kidnapped victims may refer to the Tai Chang compound as “Casino Kosai” because “a portmanteau of the word ‘Ko,’ meaning ‘mister’ in Burmese, and ‘Sai,’ the Shan/Thai honorific in Sai Kyaw Hla.”⁴⁷

45. An April 2024 report from the USIP linked the Trans-Asia International Holding Group to Tai Chang.⁴⁸

46. As used in this affidavit, the Tai Chang north compound (Tai Chang North) refers to the following location, demarcated in red and bounded by:

- Northwest point 16.472469N, 98.645868E
- Northeast point 16.472469N, 98.648334E
- Southeast point 16.469987N, 98.648146E
- South point 16.470037N, 98.647895E
- South point 16.469464N, 98.647601E
- Southwest point 16.470001N, 98.645875E

The Tai Chang south compound (Tai Chang South) refers to the following location, demarcated in blue and bounded by:

- Northwest point 16.467242N, 98.648357E
- Northeast point 16.467757N, 98.649580E
- Southeast point 16.465997N, 98.650514E
- Southwest point 16.465925N, 98.648786E

⁴⁶ *Id.*

⁴⁷ *Id.*

⁴⁸ *China Forces*, *supra* note 39.



Figure 5 – Tai Chang North and South Compounds.

47. As noted above, on November 12, 2025, OFAC sanctioned the DKBA, along with four of its senior leaders, and others, for supporting scam centers in Burma that target Americans with CIF. In its press release announcing these sanctions, OFAC stated, “One compound known to have housed cyber scam operations that have targeted and stolen money from Americans is Tai Chang, located near Myawaddy in Burma’s Karen State. The compound is located in territory controlled by the DKBA, an armed group that has supported Burma’s ruling military regime in the country’s civil conflict.”⁴⁹ That same day, the U.S. Attorney’s Office for the District of Columbia issued a press release that documented efforts by and successes to date of the newly created District

⁴⁹ U.S. Dep’t of the Treasury, “Treasury Sanctions Burma Armed Group and Companies Linked to Organized Crime Targeting Americans” (Nov. 12, 2025), available at <https://home.treasury.gov/news/press-releases/sb0312> (last accessed Nov. 22, 2025).

of Columbia Scam Center Strike Force aimed at combatting CIF.⁵⁰ The release specifically mentions Tai Chang and details how investigators seized websites used by Tai Chang to target Americans (referring to the seizure warrant obtained in case no. 25-sz-47).

B. [REDACTED] Tai Chang

48. [REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]:

[REDACTED]

[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

⁵⁰ U.S. Dep’t of Justice, *New Scam Center Strike Force Battles Southeast Asian Crypto Investment Fraud Targeting Americans* (Nov. 12, 2025) <https://www.justice.gov/usao-dc/pr/new-scam-center-strike-force-battles-southeast-asian-crypto-investment-fraud-targeting> (last accessed November 21, 2025).

⁵¹ [REDACTED]
[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

50.

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

51.

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

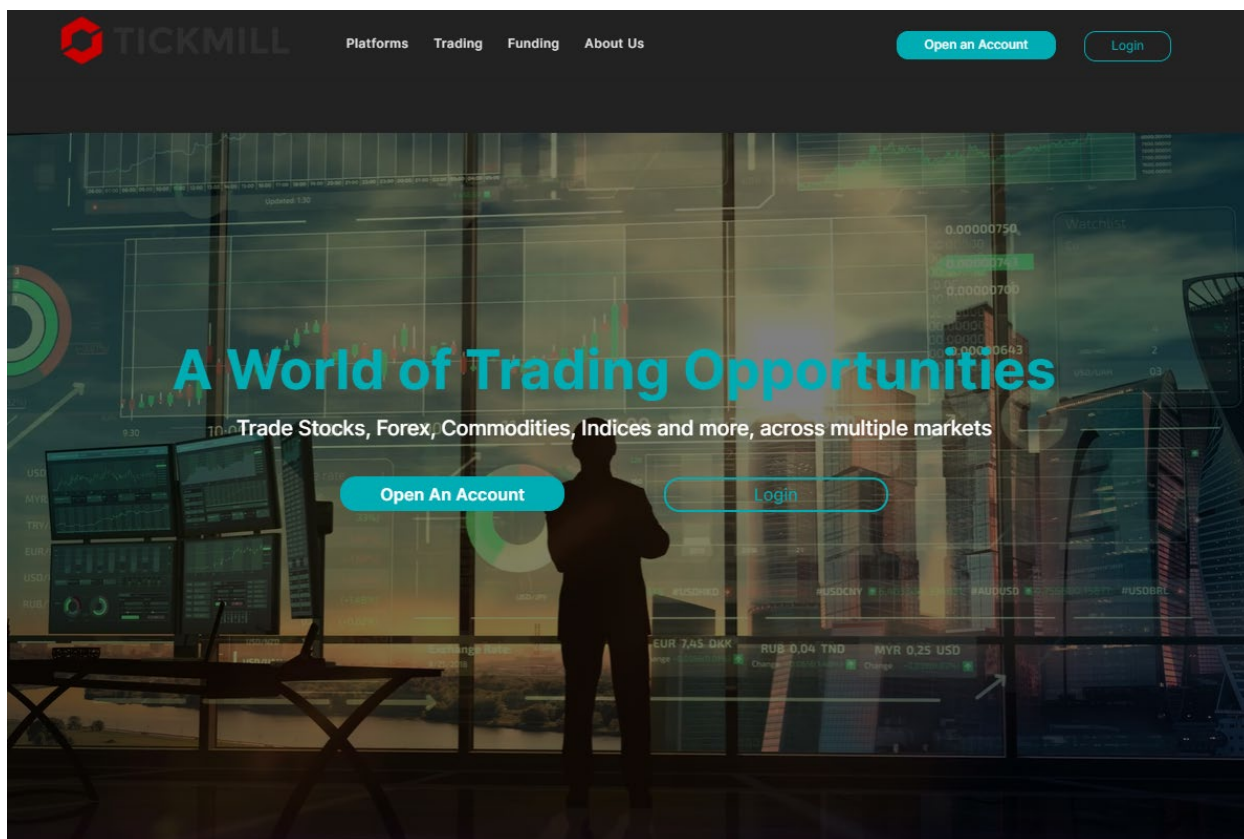
52.

53.

C. [REDACTED] **TARGET DOMAIN NAME**

54.

[REDACTED] **TARGET DOMAIN NAME** was used by Tai Chang North to defraud victims. Based on this investigation to date, [REDACTED] **TARGET DOMAIN NAME** was a website disguised as a legitimate investment platform to trick victims into depositing proceeds. On or about November 14, 2025, FBI agents reviewed the website, whose landing page—the page on a website a user will first see displayed after typing the website URL (*e.g.*, google.com)—is displayed below:



*Figure 6 – Landing Page for **TARGET DOMAIN NAME***

55. A review of the **TARGET DOMAIN NAME** website shows an option to open an account, which requires an email address and password. By clicking the “login” button, however, even without registering, the user is taken to a page appearing to display tickers for various apparent currencies, commodities, and conversion rates, shown in Figure 7 below:

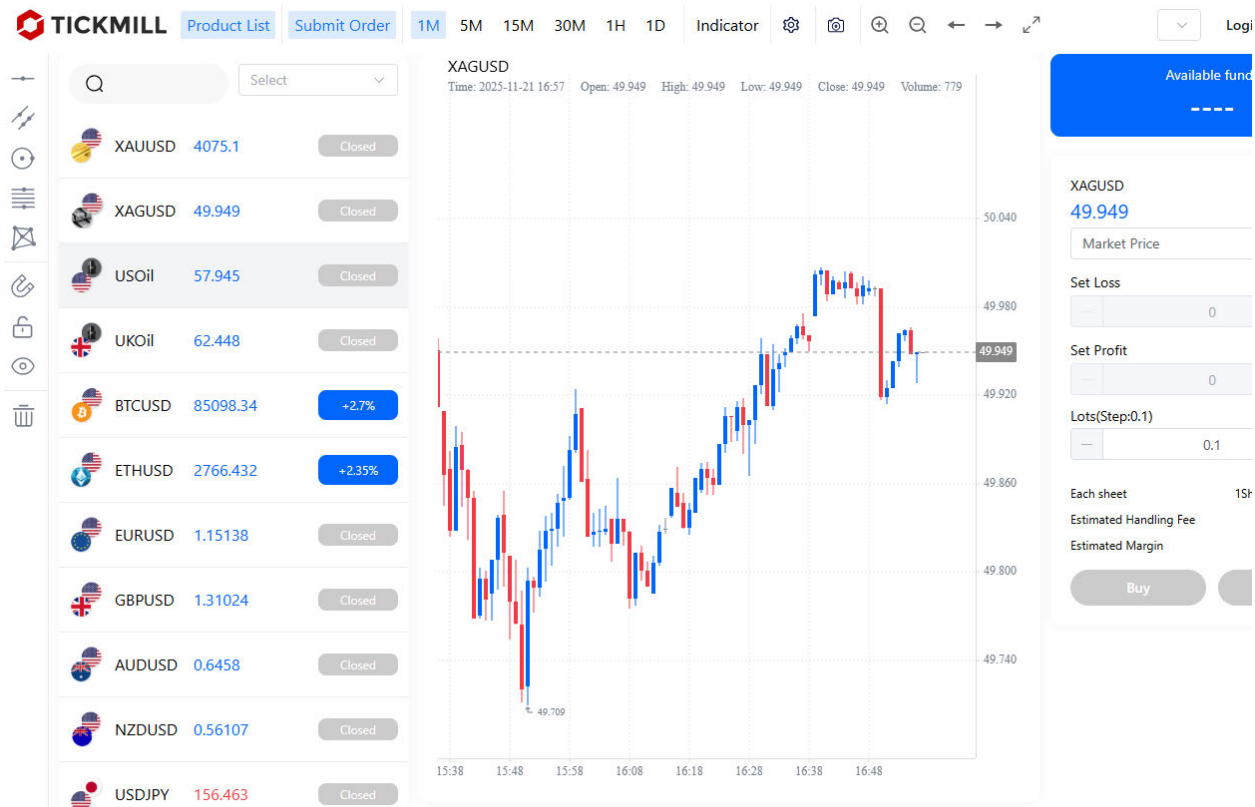
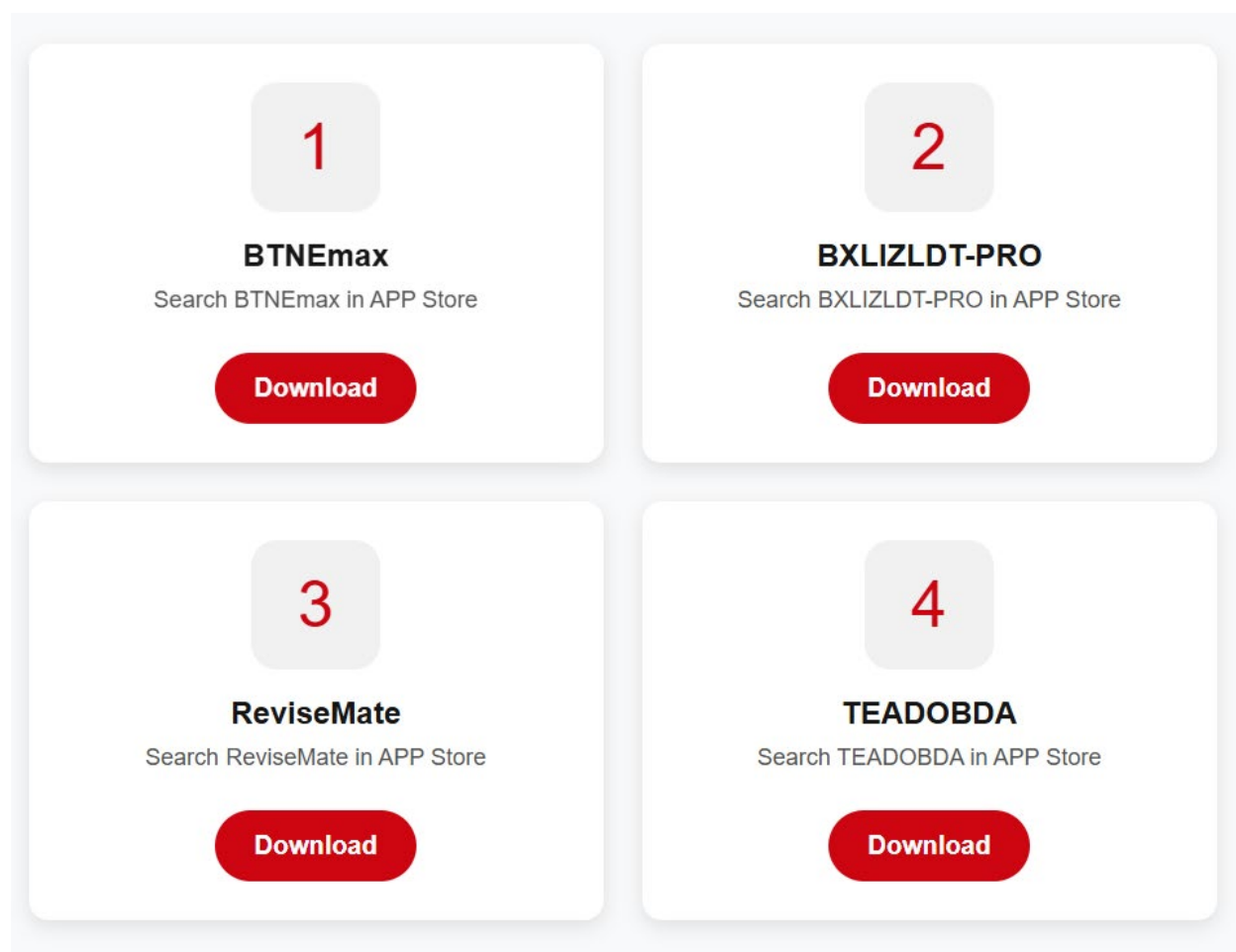


Figure 7 – “tickmilleas.com’s “ticker” page

56. The bottom of the landing page for **TARGET DOMAIN NAME** lists further information about the purported registration of the “company,” which claims that “Tickmill has a US NFA license, license number 0557897.” Based on my training and experience, I believe this is a purported reference to a “National Futures Association” number. The National Futures Association is a self-regulatory organization for the U.S. futures and derivatives markets. Membership is mandatory for many participants, including brokers, commodity pool operators, and trading advisors. Each member receives a “number,” which can be used by the public to search that member’s registration status, disciplinary history, and other background information. On or about November 21, 2025, agents conducted a search of the National Futures Association database

and confirmed no records existed for the number supplied by **TARGET DOMAIN NAME** on its landing page.

57. Under the “Platforms” tab on the landing page, there are two options, including a “Desktop” and a “Mobile” version. By clicking on the “mobile” version, the user is directed to a page advertising “Tickmill ST5 Mobile,” with links to download the application on the Google Play Store and/or the Apple App Store. As described further below, these applications appear legitimate, but they are not legitimate applications and primarily used by Tai Chang compound to further facilitate CIF. When the Apple App Store link is clicked, it shows four apps available: BTNEmax, BXLIZLDT-PRO, ReviseMate, and TEADOBDA, shown in Figure-8 below:



*Figure 8 – Application links located on **TARGET DOMAIN NAME***

58. [REDACTED]

[REDACTED]

[REDACTED] That same day, the FBI submitted these applications to both Google and Apple for internal review. As of on or about November 19, 2025, Apple confirmed to agents that all three applications ([REDACTED]) had been removed from the App Store and the developer's accounts were under investigation for termination.⁵²

59. [REDACTED]

60. Based on the [REDACTED] Apple's response, and my training and experience, I believe the above applications, both those taken down ([REDACTED]) and those still active (BTNEmax, BXLIZLDT-Pro, ReviseMate, and TEADOBDA)⁵³ on the website, were used by Tai Chang North operators as mobile applications to defraud victims, and that they are both located on and associated to **TARGET DOMAIN**

⁵² As of November 24, 2025, agents have not yet heard back from Google, LLC.

⁵³ The FBI has requested Google and Apple remove these applications as well and are awaiting a response.

NAME.⁵⁴ For legitimate companies, it rarely makes sense to create multiple applications (especially applications with dissimilar and completely unrelated names, such as those listed above) for their business because of the additional cost and likelihood of causing customer confusion. Further, from a branding and marketing perspective, companies would also want their mobile applications to match in name, logo, and style to their company and its website for brand recognition.

61. Here, however, on **TARGET DOMAIN NAME**, the embedded application BTNEmax, for example, has a different name than “Tickmill” and a different logo entirely:

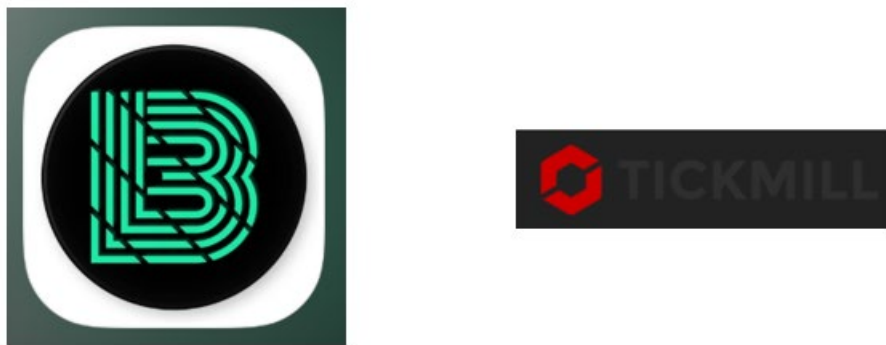


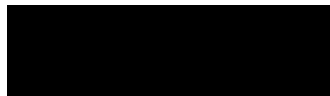
Figure 9 – BTNEmax vs. “Tickmill” Logo

62. Unlike legitimate companies, criminal organizations’ goals for using domains like **TARGET DOMAIN NAME** is to create websites that both appear legitimate and can remain active for as long as possible to build perceived legitimacy, attract more victims, and curb suspicions that would inevitably arise if the website was shut down. **TARGET DOMAIN NAME**, on its surface, appears professional and legitimate. Severing that brand (*i.e.*, “TickMill”), which first attracts victims, with the actual applications (*e.g.*, “BTNEmax”) that victims use to deposit

⁵⁴ As of November 25, 2025, [REDACTED] are all disabled and no longer on the Apple App Store.

funds and ultimately lose money from makes sense because even if those applications are shut down, the original website can remain as a platform for future fraudulent applications. This separate branding provides additional benefits for scam organizations because victims may report the application name as fraudulent but not realize that the landing website, here, **TARGET DOMAIN NAME**, is also a part of the scheme.

63. The FBI conducted open searches of the name “Tickmill” and learned that there is a legitimate company named [REDACTED] with the website [REDACTED]. Unlike **TARGET DOMAIN NAME**, which was registered in or around November 2025, a WHOIS lookup shows that [REDACTED] was registered in or around [REDACTED]. Based on a review of its website, [REDACTED] was founded in [REDACTED] and is a regulated offshore broker that provides services to clients worldwide. A search via Google shows that [REDACTED] is widely known and started as a company around when its website was registered in [REDACTED]. Based on its website, [REDACTED] has several authorized and regulated entities and uses the following logo:



64. On or about November 19, 2025, agents emailed [REDACTED], found on the [REDACTED] website and asked whether [REDACTED] had any affiliation with **TARGET DOMAIN NAME**. The Head of Customer Support responded, “We confirm that [REDACTED] is not affiliated with [REDACTED] or any of our group entities. This website is not related to our services in any capacity. Our official and legitimate website is: [REDACTED].”

65. Based on the information described above, it is evident that **TARGET DOMAIN NAME** is impersonating the legitimate company, [REDACTED], and its website [REDACTED]. **TARGET DOMAIN NAME**’s emblem, when compared against [REDACTED] is similar:



*Figure 10 – **TARGET DOMAIN NAME** logo vs. [REDACTED] Logo*

66. **TARGET DOMAIN NAME**'s content also mimics [REDACTED] such as by claiming to be regulated by the [REDACTED]. Additionally, [REDACTED] has an authorized and regulated entity in [REDACTED] and **TARGET DOMAIN NAME** claims to be authorized as a "Financial Services Provider with licensing number [REDACTED] by the Financial Services Board in [REDACTED]." Based on my experience investigating CIF, it is very common for scam domains to impersonate legitimate investment platforms and financial services companies.

67. On or about November 24, 2025, a query of IC3.gov data, the FBI's crime complaint center for frauds and scams, revealed approximately 132 victims reporting scams associated with various websites/apps referencing "Tickmill." Although none of these reports specifically reference **TARGET DOMAIN NAME**, the details in the victim narratives strongly indicate that the type of scam was CIF. Many of these victims reported meeting individuals on dating sites. Later, these victims were asked to communicate via WhatsApp before being introduced to the cryptocurrency investment opportunities that they later reported as fraudulent. To date and as detailed below, every victim contacted by agents regarding the **TARGET DOMAIN NAME** was not yet aware it was a scam. Accordingly, I believe the likely reason the query returned no reports referencing **TARGET DOMAIN NAME** in IC3.gov is **TARGET DOMAIN NAME**'s recent registration date.

D. T-Victim 1 Provides Cryptocurrency Addresses linked to TARGET DOMAIN NAME⁵⁵

68. [REDACTED] multiple cryptocurrency addresses that [REDACTED] were being used by scammers inside Tai Chaing to accept victim payments made to **TARGET DOMAIN NAME:**

- BTC address: bc1qzrtDNA9d6eeavratvXld6qvk19dwl06xakd4g (bc1qzr)
- ETH address: 0xc248c5Db7fa467B2d5660E0EE648e60C2c5e24dc (0xc248)
- USDT-ERC20 address: 0xc248c5Db7fa467B2d5660E0EE648e60C2c5e24dc (0xc248)
- USDC address: 0xc248c5Db7fa467B2d5660E0EE648e60C2c5e24dc (0xc248-2)
- USDT-TRC20 address: TM4ASkK7QEMbjTNbyNdfekzZnRdi9TZenn (TM4Ask)

69. I am aware that most CIF subjects will coach victims to send wire payment transactions to a U.S. cryptocurrency exchange to purchase and send cryptocurrency to addresses associated with the CIF investment platform controlled by the scammers and their conspirators. When an FBI forensic accountant analyzed the addresses above, the accountant observed activity consistent with their use as addresses used to receive victims' funds. For example, both the bc1qzr and 0xc248 addresses, first analyzed on or about November 18, 2025, had incoming deposits that same day directly, or one hop away, from known U.S. cryptocurrency exchanges.

E. Identification of Financial Fraud Victims

70. [REDACTED] the FBI forensic accountant, using reliable blockchain analytical tools,⁵⁶ traced backwards from several of the cryptocurrency

⁵⁵ The cryptocurrency addresses provided did not, and currently do not, maintain any cryptocurrency balance that could be frozen or seized.

⁵⁶ There are several private-sector companies that have software that allows trained agents and forensic accountants to analyze blockchain data. Since most blockchain activity is technically public, these tools provide enhanced capabilities to more readily review that public data in a productive and more expedient way.

addresses provided above to identify those recent transactions emanating from U.S.-based exchanges. After serving legal process to these exchanges, the FBI identified numerous potential victims. Eight of the identified victims (referred to as “Financial” or “F-Victims”) sent BTC or ETH totaling approximately \$126,000 in cryptocurrency to two of the addresses [REDACTED] and listed above (illustrated in Figure 11 below). The FBI interviewed F-Victim 1 and F-Victim 2; summaries of these interviews are provided below.

[Remainder of page intentionally left blank]

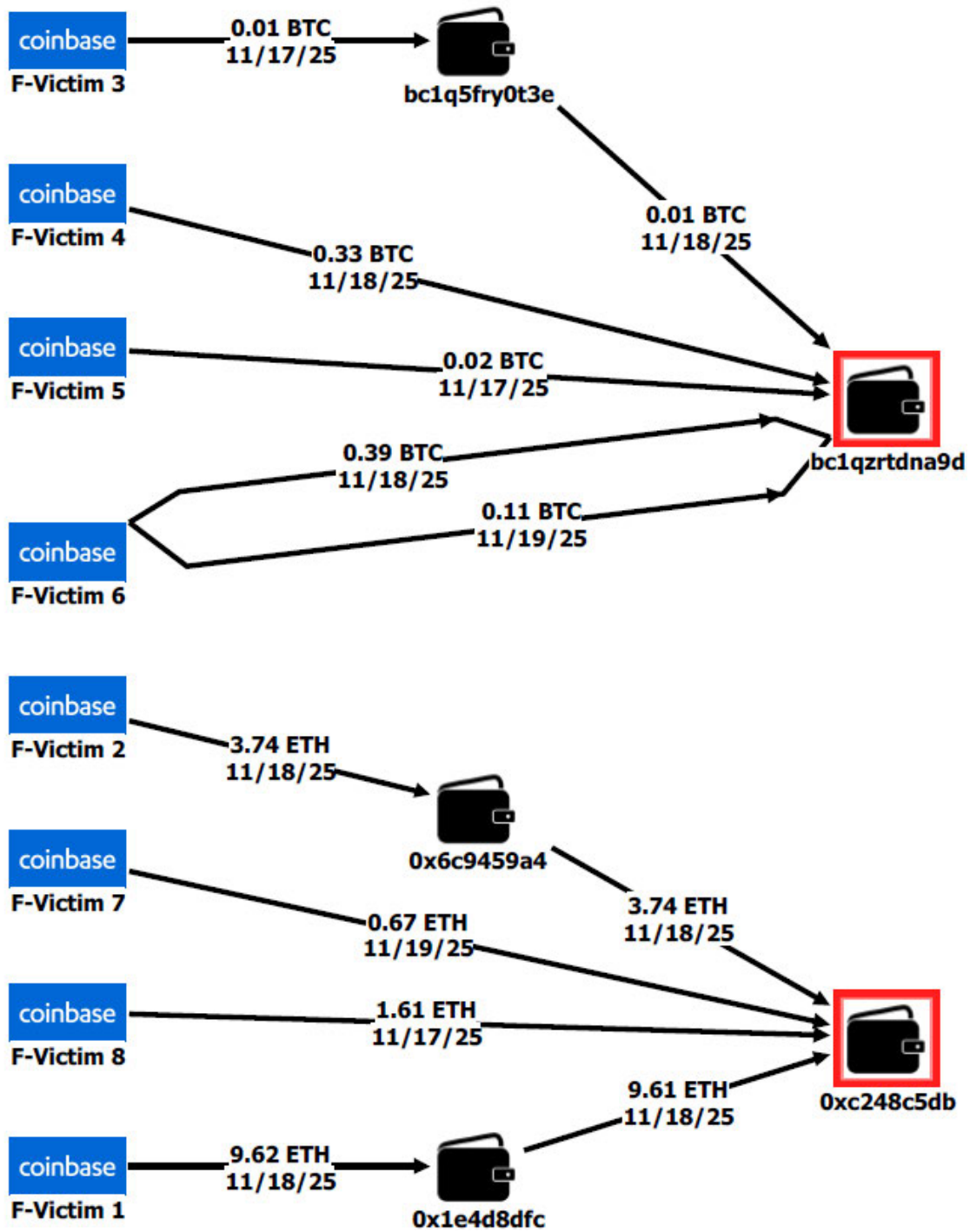


Figure 11 – Blockchain Tracing of Eight F-Victims to Addresses

F. Identification of Additional Potential Victims

71. Through legal process, the FBI has identified 21 potential victims. These victims were identified by conducting blockchain analysis using the same reliable tools mentioned above to find which U.S.-based exchanges sent money to the cryptocurrency addresses provided by F-Victim 1. The FBI has interviewed nine of those individuals, including F-Victim 2 and F-Victim 3. All nine interviewees have described situations clearly indicative of CIF schemes, and seven have specifically mentioned **TARGET DOMAIN NAME** as the investment platform they used.⁵⁷

Statement of F-Victim 1

72. In or around July 2025, F-Victim 1 reportedly met “Luca” on a dating platform. Shortly thereafter, Luca asked that they move their conversation to WhatsApp. Luca stated he was from San Francisco but had moved to Minnesota. F-Victim 1 and Luca bonded over talking about family. Over time, Luca introduced F-Victim 1 to investing. He instructed F-Victim 1 to download the [REDACTED] applications. From there, Luca showed F-Victim 1 **TARGET DOMAIN NAME** and how trades occurred on the platform. When F-Victim 1 first deposited funds using **TARGET DOMAIN NAME**, F-Victim 1 was able to withdraw those funds. Shortly thereafter, Luca stated that if F-Victim 1 deposited a larger amount, F-Victim 1 would make a larger percentage back. Luca offered to help F-Victim 1 reach that new investment tier by contributing some of his own money into F-Victim 1’s portfolio.

73. Based on what Luca told F-Victim 1, F-Victim 1 started investing more money. Just two days before the FBI called F-Victim 1, F-Victim 1 had sent approximately \$30,000 to **TARGET DOMAIN NAME**. When contacted by the FBI, F-Victim 1 was not yet aware that F-Victim 1 was a scam victim.

⁵⁷ The FBI is attempting to interview the remaining victims.

Statement of F-Victim 2

74. F-Victim 2 met a man on Tinder who went by “Matteo.” Matteo soon asked that they move the conversation off platform, and the two began conversing on [REDACTED] [REDACTED] Matteo stated he lived in a town not far from F-Victim 2. Matteo claimed he worked in real estate and cryptocurrency investments. When F-Victim 2 arranged to meet Matteo, Matteo at the last minute claimed his sister had been in a car accident.

75. Over time, Matteo introduced F-Victim 2 to investing. He instructed F-Victim 2 to open a [REDACTED] account and a [REDACTED] and ultimately guided F-Victim 2 to investing via **TARGET DOMAIN NAME**. Initially, F-Victim 2 was able to withdraw his/her invested funds, such as the \$1,000 he initially deposited. Over time, F-Victim 2 deposited approximately \$70,000 to **Target DOMAN NAME 1**. F-Victim 2 has been unable to withdraw those proceeds from the site.

G. Cryptocurrency Addresses to Which F-Victims 1-8 Were Directed

76. [REDACTED] I have determined that F-Victims 1-8, shown earlier in Figure 11, were directed by CIF scammers, who appeared to be based in Burma (as outlined above), to fund their “investment accounts” by sending cryptocurrency to the two cryptocurrency addresses noted above—namely, bc1qzr and 0xc248. I am aware that most CIF subjects will coach victims to make wire payment transactions to a cryptocurrency exchange to purchase and send cryptocurrency to addresses associated with the CIF investment platform controlled by the scammers and their conspirators. I believe that F-Victims 1-8 also were likely told to send cryptocurrency in the same way.

77. Based on my training and experience, I believe that the blockchain transaction activity detailed above in Figure 11 indicates money laundering. For example, the subjects used

various methods to attempt to thwart law enforcement's ability to trace, and ultimately recover, any illicit proceeds. These methods include:

- a. Rapid movement of funds through multiple cryptocurrency wallets: Each time a victim sent cryptocurrency to one of the subject's addresses, that cryptocurrency was then rapidly withdrawn by the subjects and sent to another wallet. In many instances, the F-Victim's cryptocurrency was withdrawn and sent to new wallets within minutes. By rapidly moving funds out of the initial addresses the F-Victims sent cryptocurrency to, the subjects complicated law enforcement's ability to detect and recover the stolen funds.
- b. The use of a consolidation wallets to commingle funds: Criminals commonly use consolidation wallets to obfuscate the source of funds and complicate tracing efforts by law enforcement. By consolidating deposits of multiple victims' funds into the same wallet, criminals make it more difficult for law enforcement to analyze the wallet activity and determine the source of funds and ultimate destination of specific victim deposits. Consolidation wallets often have hundreds, or even thousands, of transactions, further complicating law enforcement's ability to trace and recover victim funds.

H. TARGET DOMAIN NAME's Involvement in Money Laundering

78. As shown above, **TARGET DOMAIN NAME** was a CIF scam domain sent by scammers to victims to attract and support victims' fake investments and it served as key facilitating property for the wire fraud and money laundering conspiracies: Scammers located overseas, including in Burma, induced U.S. victims to send funds from the United States to cryptocurrency addresses located and controlled by CIF actors overseas, to promote wire fraud

and wire fraud conspiracy schemes. In other words, this scam domain facilitated the transfer of funds from a place in the United States to a place outside the United States with the intent to promote a specified unlawful activity, in violation of 18 U.S.C. §§ 1956(a)(2)(A), (h).

79. **TARGET DOMAIN NAME** was involved in international promotion money laundering by connecting U.S. victims to the platforms used by criminals overseas to siphon victim funds abroad in promotion of the underlying wire fraud scheme. As detailed above, seven victims reported using **TARGET DOMAIN NAME** in their interviews, referencing the domain as property that they were directed to use to make false investments. Victims described how the **TARGET DOMAIN NAME** showed lucrative returns on investment and how it would even show deposits made by the scammers to the victim's account when that scammer would walk the victim through trading.

SEIZURE PROCEDURE

80. The top-level domain for **TARGET DOMAIN NAME** is “.com.” VeriSign, Inc. (Verisign), headquartered at 12061 Bluemont Way, Reston, Virginia, manages all “.com” domains.

81. As detailed in Attachment A-1, upon execution of the seizure warrant, the registry for the “.com” top-level domain, Verisign shall be directed to restrain and lock **TARGET DOMAIN NAME** pending transfer of all right, title, and interest in **TARGET DOMAIN NAME** to the United States upon completion of forfeiture proceedings, to ensure that changes to **TARGET DOMAIN NAME** cannot be made absent court order or, if forfeited to the United States, without prior consultation with the FBI or the Department of Justice.

82. In addition, upon seizure of **TARGET DOMAIN NAME** by the FBI, Verisign will be directed to associate **TARGET DOMAIN NAME** to a new authoritative name server(s) to be designated by a law enforcement agent. The government will display a notice on the website to

which **TARGET DOMAIN NAME** will resolve indicating that the site has been seized pursuant to a warrant issued by this court.

**REQUEST TO SUBMIT WARRANT BY TELEPHONE OR OTHER RELIABLE
ELECTRONIC MEANS**

83. I respectfully request, pursuant to Rules 4.1 and 41(d)(3) of the Federal Rules of Criminal Procedure, permission to communicate information to the Court by telephone in connection with this Application for a Seizure Warrant. I submit that Assistant U.S. Attorney Jolie Zimmerman, an attorney for the United States, can identify my voice and telephone number for the Court.

CONCLUSION

84. **TARGET DOMAIN NAME**, tickmilleas.com, was used by subjects believed to be located outside the United States as a facility in a wire fraud conspiracy in which U.S. victims were instructed to send their U.S.-based funds to cryptocurrency addresses controlled by actors outside the United States, in violation of 18 U.S.C. §§ 1343, 1349. **TARGET DOMAIN NAME** was also involved in a conspiracy to commit international promotional money laundering (18 U.S.C. §§ 1956(a)(2)(A), 1956(h)) and can be seized and forfeited pursuant to 18 U.S.C. §§ 981(a)(1)(A), 982(a)(1).

85. Based on the foregoing, I submit that **TARGET DOMAIN NAME** is subject to seizure and forfeiture, pursuant to the above referenced statutes, and I request that the Court issue the proposed seizure warrant.

86. Because the warrant will be served on the registry that controls **TARGET DOMAIN NAME**, and the registry at a time convenient to them, will transfer control of **TARGET DOMAIN NAME** to the government, there exists reasonable cause to permit the execution of the requested warrant at any time of day or night.

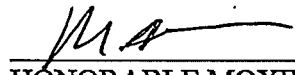
Respectfully submitted,

[REDACTED]

[REDACTED]

Special Agent
Federal Bureau of Investigation

Subscribed and sworn pursuant to Fed. R. Crim. P. 4.1 and 41(d)(3) on December 1, 2025.


HONORABLE MOXILA A. UPADHYAYA
UNITED STATES MAGISTRATE JUDGE
DISTRICT OF COLUMBIA