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. 26-sz-27

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, FUTHER 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 05/04/2026
(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 Matthew J. Sharbaugh.
(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 and time issued: 04/20/2026

Judge's signature

City and state: District of Columbia

Matthew J. Sharbaugh, U.S. Magistrate Judge
Printed name and title

Return

Case No.: 26-sz-27	Date and time warrant executed:	Copy of warrant and inventory left with:

Inventory made in the presence of:

Inventory of the property taken:

Certification

I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.

Date: _____

_____
Executing officer's signature

_____
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. 26-sz-27** **FILED UNDER SEAL**

Reference: USAO No. 2026R00224

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] fortuneprimeglobalirts.com (**TARGET DOMAIN NAME**). The **TARGET DOMAIN NAME** to be seized is described below and in Attachment A.

2. A search of publicly available WHOIS[2] domain name registration records revealed that **TARGET DOMAIN NAME** was registered on or about March 25, 2026, through the registrar[3] GMO Internet (GMO), believed to be headquartered at Cerulean Tower, 26-1

[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

Sakuragaoka-cho, Shibuya-ku, Tokyo, 150-8512, Japan. The top-level domain for **TARGET DOMAIN NAME** is ".com." VeriSign, Inc. (VeriSign), headquartered at 12061 Bluemont Way, Reston, Virginia, manages all ".com" domains and is the registry[4] for **TARGET DOMAIN NAME**.

3. I am a Special Agent with the FBI and have been so employed since approximately September 2020. As such, 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. I am currently assigned to an FBI squad that investigates scam compounds. During the course of my duties, I have received training about and participated in the execution of search warrants, and the review and analysis of both physical and electronic evidence.

PURPOSE OF AFFIDAVIT

4. 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-

---

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.

based scam compound referred to as "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

5. 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.

6. 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.

7. According to publicly available reporting, discussed in more depth below, "Tai Chang Park" (also known as "Taichang," "Ko Sai Casino," and "Kyauk Khat Casino") (Tai Chang)

[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.

(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 Tai Chang, have been subject to rape, torture, and murder. The compound—in fact, a series of compounds, as explained below—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.

8. On 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 Chang. The seizure warrant's affidavit, incorporated by reference, details probable cause to believe that these two domain names were 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). 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 compounds.

9. On December 1, 2025, U.S. Magistrate Judge Moxila A. Upadhyaya issued a seizure warrant in case no. 25-sz-52 for one domain name (tickmilleas.com) used in CIF scams linked to Tai Chang. The seizure warrant's affidavit, incorporated by reference, details probable cause to believe that tickmilleas.com 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). The affidavit also details additional CIF victims whose scammers were determined to be in the Tai Chang scam compounds.

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, there is probable cause to believe that **TARGET DOMAIN NAME**, which is almost identical to tickmilleas.com in appearance and function, is 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 referred to as 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.

PROBABLE CAUSE

I. Background on Cryptocurrency Investment Fraud

22. 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.

23. 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.

[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.

dollars) for cryptocurrency and send that cryptocurrency to the cryptocurrency address(es) provided by the websites.

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

25. 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]

26. 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

[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 Apr. 9, 2026).

from CIF scams rose, from $3.96 billion in 2023, to $5.8 billion in 2024, an increase of 47%.[8] In 2025, over $7.2 billion in losses were reported to IC3.[9] These numbers, 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.

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

27. Based on publicly available sources, in 2017, the first Chinese investors who would later construct CIF scam compounds arrived in Burma's Kayin State.[10, 11] 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),[12] formerly branded as the "Border Guard Force" (BGF).[13] 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.[14]

---

[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 Apr. 9, 2026).
[9] IC3 (2025) Federal Bureau of Investigation Internet Crime Report. IC3, available at https://www.ic3.gov/AnnualReport/Reports/2025_IC3Report.pdf (last accessed on Apr. 16, 2026).
[10] *A Growing Threat* (May 2024), *supra* note 7.
[11] 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 Apr. 9, 2026).
[12] 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 Apr. 9, 2026).
[13] The Karen BGF has since renamed itself the Karen National Army after distancing itself from the Burma Military, while retaining regional control.
[14] "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-

28. 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, 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.[15]

29. 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."[16] 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.[17] According to the USIP, "under the armed protection of . . . a para-military 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."[18] USIP further reported that thousands of Chinese workers had been "lured" to this location to build and work in these structures.[19]

---

karen-national-army-criminal-business-network-exposed (last accessed on April 09, 2026). 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 Apr. 9, 2026).

[15] 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 Apr. 9, 2026).

[16] 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://wayback.archive-it.org/3453/20230911081407/https://www.usip.org/publications/2020/07/myanmar-transnational-networks-plan-digital-dodge-casino-enclaves (last accessed on Apr. 9, 2026).

[17] *Id*.

[18] *Id*.

[19] *Id*.

30. 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 CIF, as a new source of revenue.[20] And as lockdowns and border controls meant Chinese workers could not travel to Burma, these organizations began trafficking workers from around the world.[21] 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."[22]

31. 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."[23]

---

[20] 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://web.archive.org/web/20221209195438/https://www.usip.org/publications/2022/11/myanmars-criminal-zones-growing-threat-global-security (A Growing Threat (Nov. 2022)) (last accessed on Apr. 9, 2026).

[21] *Id.*

[22] *Id.*

[23] 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 Apr. 9, 2026).

32. 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]

33. Since 2021, scam center developments have proliferated along the Burma/Thailand border.

34. CIF compounds are often "city-like" and reminiscent of "penal colonies."[25] 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."[26] Public reporting on KK Park and other Southeast Asian CIF compounds includes accounts of beatings, electrocutions, and murder.[27] 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."[28] Those who cannot or do not pay are sometimes sold between companies.[29]

---

[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 Apr. 9, 2026).
[25] A Growing Threat (Nov. 2022), *supra* note 19.
[26] *Id.;* Irawaddy, "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 Nov. 6, 2025).
[27] *A Growing Threat* (Nov. 2022), *supra* note 19; 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 Apr. 9, 2026); 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 Apr. 9, 2026).
[28] *Cyber Slavery*, *supra* note 26; *see also Cambodia Scams*, *supra* note 26.
[29] *Cyber Slavery*, *supra* note 26; *Cambodia Scams*, *supra* note 26.

35. 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.[30] A June 8, 2022 article published by *Free Malaysia Today*, a Malaysian online news site, detailed the 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.[31] After reporting for the position, he was trafficked into Burma via the border town of Mae Sot.[32] 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.[33] 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.[34] Ultimately, he was released after his family paid a ransom.[35]

[30] 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 April 09, 2026); 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 Apr. 9, 2026); *Cyber Slavery*, *supra* note 26; *Cambodia Scams*, *supra* note 26.

[31] 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 Apr. 9, 2026).

[32] *Id.*

[33] *Id.*

[34] *Id.*

[35] *Id.*

III. The Tai Chang Scam Compounds

A. Background on Tai Chang and Its Organization

36. The main Tai Chang scam compound (Tai Chang 1.0)[36] is in Kyaukhat, Burma, located at 16.467242N, 98.648357E and 16.472469N, 98.645868E, along the Thailand border. The compound reportedly was 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]

37. Tai Chang 1.0 is located approximately 25 miles southeast of Shwe Kokko.[39] A map of Kyaukhat, Burma, and the border with Thailand, is shown below.

[36] Tai Chang 1.0 encompasses Tai Chang North and Tai Chang South, as described in 25-sz-52.
[37] China Forces Myanmar Scam Syndicates to Move to Thai Border (Apr 29, 2024) ("China Forces"), available athttps://mmlibrary.uwazi.io/en/entity/sxg4pt9e9xh?file=1714378693397b5aqexbn0fd.pdf&page=4 (last accessed on Apr. 9, 2026).
[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 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 Apr. 9, 2026).
[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 Apr. 9, 2026); *China Forces*, *supra* note 36.

Figure 1 – Map of the Burma (left) and Thailand (right) border. Kyaukhat is depicted southeast of Shwe Kokko.[40]

38. The following satellite imagery, obtained from two different providers, shows the area of Tai Chang 1.0 between 2020 and 2025, and the development of multiple buildings into the creation of a north and south compound. As described further below, until recently, these compounds appear to have housed operations of a CIF scheme to target U.S. victims.

[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=ttu&g_ep=EgoyMDI1MTEwNC4xIKXMDSoASAFQAw%3D%3D (last accessed on Apr. 9, 2026).

Figure 2 – Satellite imagery showing development of Tai Chang 1.0 compound.

39. Based on reporting published in *The Guardian*, the Tai Chang 1.0 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 Apr. 9, 2026).

Figure 3 – Tai Chang as seen from the Thai border.

40. Tai Chang 1.0 is reportedly secured through a mix of Chinese criminal actors and members of the DKBA. DKBA is a separate entity from the Karen National Army (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 1.0 have reported their location and local sources have reported that the area is under the control of

[42] Jason Tower, Priscilla Clapp, "Chinese Crime Networks Partner with Myanmar Armed Groups" (Apr. 20, 2020), available at https://web.archive.org/web/20230922100816/https://www.usip.org/publications/2020/04/chinese-crime-networks-partner-myanmar-armed-groups (last accessed on March 16, 2026).
[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 Mar. 16, 2026).
[44] DVB (Jan. 23, 2023), available at https://english.dvb.no/dkba-demands-answers-after-junta-airstrike-on-commanders-housing-compound/ (last accessed on Apr. 9, 2026); Radio Free Asia (Jan. 23, 2023), available at https://www.rfa.org/english/news/myanmar/juntadkbaairstrike-01232023164117.html (last accessed on Apr. 9, 2026).
[45] *Radio Free Asia* (Apr. 13, 2023), *supra* note 37.

the DKBA, and Brigadier General, Sai Kyaw Hla.[46] The same report noted that kidnapped victims may refer to Tai Chang 1.0 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]

41. 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."[48] 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 of Columbia Scam Center Strike Force (the Strike Force) aimed at combatting CIF.[49] 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. Tai Chang – Additional Compounds

42. In early 2026, two additional, smaller compounds were identified in the area near Tai Chang 1.0. The two locations are believed to be newer Tai Chang compounds that are partially

[46] *Id*.
[47] *Id*.
[48] 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 Apr. 9, 2026).
[49] 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 Apr. 9, 2026).

operational. One of the new compounds ("Tai Chang 2.0") is located at 16.425472, 98.635806. The other new compound ("Tai Chang 3.0") is located at 16.491389, 98.58972. The following figures show satellite imagery from Google Maps and NGO-1.

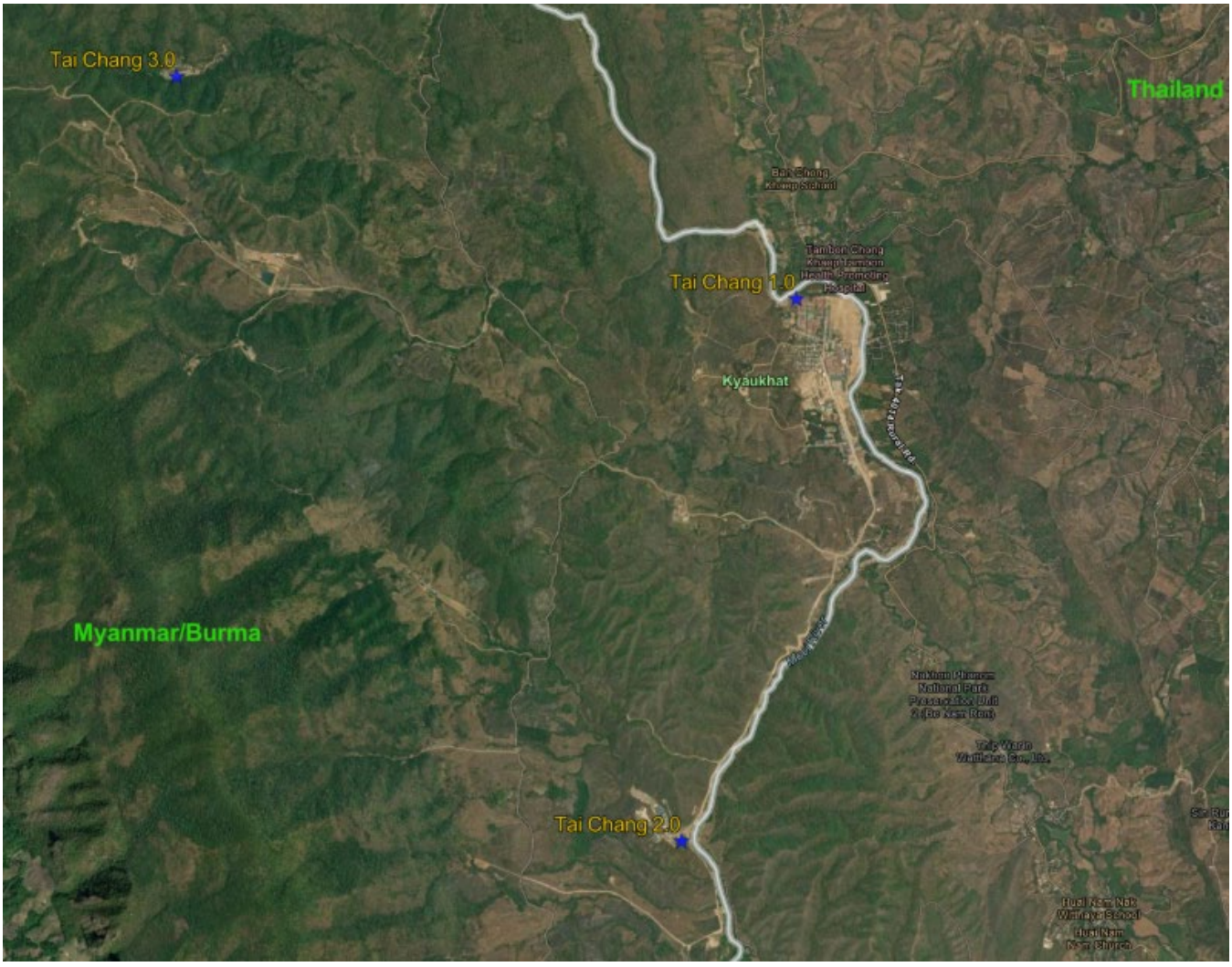

Figure 4 – Map of the Burma (left) and Thailand (right) border. Tai Chang 1.0 (center), Tai Chang 2.0 (down), Tai Chang 3.0 (up).

Figure 5 - *Google Maps Showing Tai Chang 3.0 (date unknown).*

Figure 6 - NGO-1[50] Satellite Imagery Showing Tai Chang 3.0 on April 03, 2026.

[50] NGO-1 is an international non-profit organization. NGO-1 has worked in Southeast Asia with victims of human trafficking, including victims who have been forced to work in scam compounds.

Figure 7 - NGO-1 Satellite Imagery Showing Tai Chang 3.0 Starlink/Satellite terminals on April 03, 2026.

Figure 8 - Google Maps Showing Tai Chang 2.0 (Date Unknown).

Figure 9 - NGO-1's Satellite Imagery Showing Tai Chang 2.0 on April 3, 2026.

Figure 10 - NGO-1's Satellite Imagery Showing Tai Chang 2.0 with Starlink/Satellite terminals on April 3, 2026.

Figure 11 - [redacted] *Imagery Showing Tai Chang 2.0 in April 2026.*

B. DKBA Control of Geographic Region Around Tai Chang compounds

43. The area near Tai Chang 1.0 is likely controlled by the DKBA. For example, as demonstrated below in Figure 12, per Google Maps, approximately 3.5 miles northwest of Tai Chang 1.0 main compound, there are a DKBA marijuana plantation and YABA & ICE production plants located at 16.475681, 98.598148.[52]

[51] [redacted].

[52] YABA is a combination of methamphetamine and caffeine. ICE is a common name for crystal methamphetamine. https://www.google.com/maps/place/DKBA+marijuana+plantation,YABA+%26+ICE+production+plants/@16.4760951,98.5947249,1453m/data=!3m2!1e3!4b1!4m6!3m5!1s0x30dd850003ad59ff:0xcf3249696d98a6c8!8m2!3d16.4760951!4d98.5972998!16s%2Fg%2F11yq9zbxqb?entry=ttu&g_ep=EgoyMDI2MDQwNi4wIKXMDSoASAFQAw%3D%3D

44. Additionally, just about a mile northwest of the DKBA marijuana plantation, per Google Maps, there is the mansion of General Sai Kyaw Hla, leader of the DKBA.[53] As mentioned previously, Tai Chang 1.0 was reportedly established in January 2020 by the sanctioned Brigadier General Sai Kyaw Hla, leader of the DKBA.

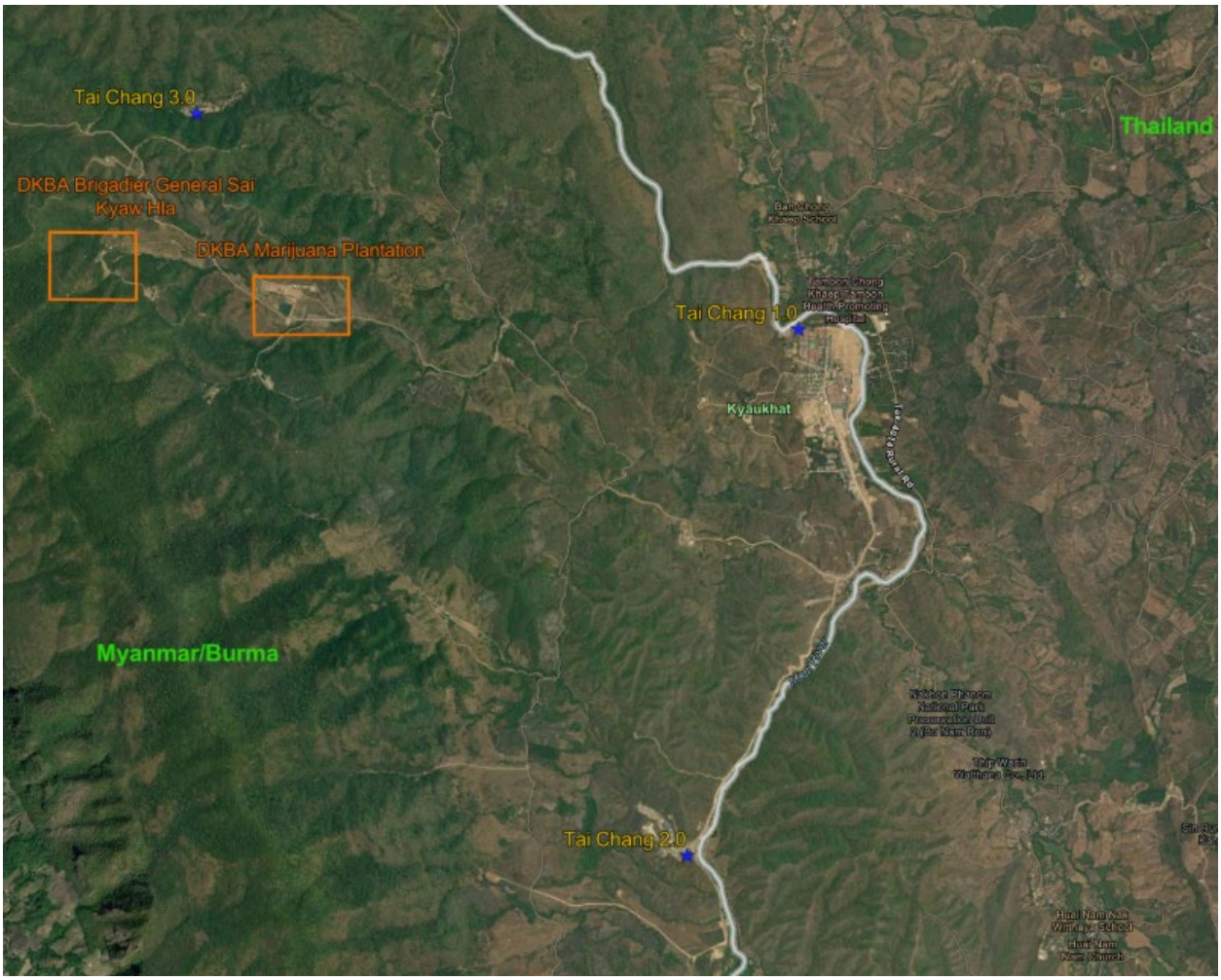

Figure 12 – Map of the Burma (left) and Thailand (right) border. Tai Chang 1.0 (center), Tai Chang 2.0 (down), Tai Chang 3.0 (up), DKBA marijuana plantation and YABA & ICE production plants (right box), mansion of General Sai Kyaw Hla (left box).

[53] https://www.google.com/maps/place/The+mansion+of+DKBA+Brigadier+General+Sai+Kyaw+Hla/@16.4704453,98.6057091,5896m/data=!3m1!1e3!4m6!3m5!1s0x30dd8500031194f1:0xba1dd3668bba85c1!8m2!3d16.4796042!4d98.5813941!16s%2Fg%2F11zkq81h05?entry=ttu&g_ep=EgoyMDI2MDQwNy4wIKXMDSoASAFQAw%3D%3D (last accessed on Apr. 10, 2026).

C. [redacted] Inside Tai Chang

45. [redacted]

[redacted]

47. [redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

D. Identification of New Tai Chang Compounds

51. [redacted]

52. [redacted]

[56] Google Maps, https://www.google.com/maps/place/16%C2%B027'46.4%22N+98%C2%B038'09.3%22E/@16.4761651,98.5966945,386m/data=!3m1!1e3!4m4!3m3!8m2!3d16.4628892!4d98.635915?entry=ttu&g_ep=EgoyMDI2MDQwMS4wIKXMDSoASAFQAw%3D%3D (last accessed on [April 09, 2026]).

[redacted]

53. [redacted] As a result, some Tai Chang personnel relocated to a new scam compound located at 16.856722, 98.342667.

54. [redacted]. NGO-1 [redacted] recent imagery of the location showing development of structures and infrastructure at the location, as shown above. NGO-1 reported that Tai Chang 2.0 was also known as Taih or Qingsong.

55. [redacted] I believe that Tai Chang's leadership has been developing new compound locations since late 2025 after the announcement of OFAC sanctions imposed on DKBA and the announcement of Strike Force aimed at combatting CIF. I further believe that Tai Chang

[57] *See* Justice Department Announces Seizure of Tai Chang Scam Compound Domain Used in Cryptocurrency Investment Fraud https://www.justice.gov/opa/pr/justice-department-announces-seizure-tai-chang-scam-compound-domain-used-cryptocurrency (last accessed on Apr. 9, 2026).

[58] [redacted]

leadership is still operating at Tai Chang 1.0 and slowly moving personnel to Tai Chang 2.0 and Tai Chang 3.0 in the nearby area controlled by the DKBA.

E. [redacted] tickmilleas.com (Tickmilleas) as a Scam Domain

56. [redacted] As noted above, on December 1, 2025, the FBI obtained a seizure warrant in case no. 25-sz-52 for the domain name tickmilleas.com; the domain name was seized by the FBI on or about December 2, 2025.[59]

57. On or about November 14, 2025, FBI agents reviewed the website. The website's landing page—the page on a website a user will first see displayed after typing the website URL (*e.g.*, google.com)—as it appeared at that time (before the FBI's seizure) is displayed below:

[59] *See* n. 57.

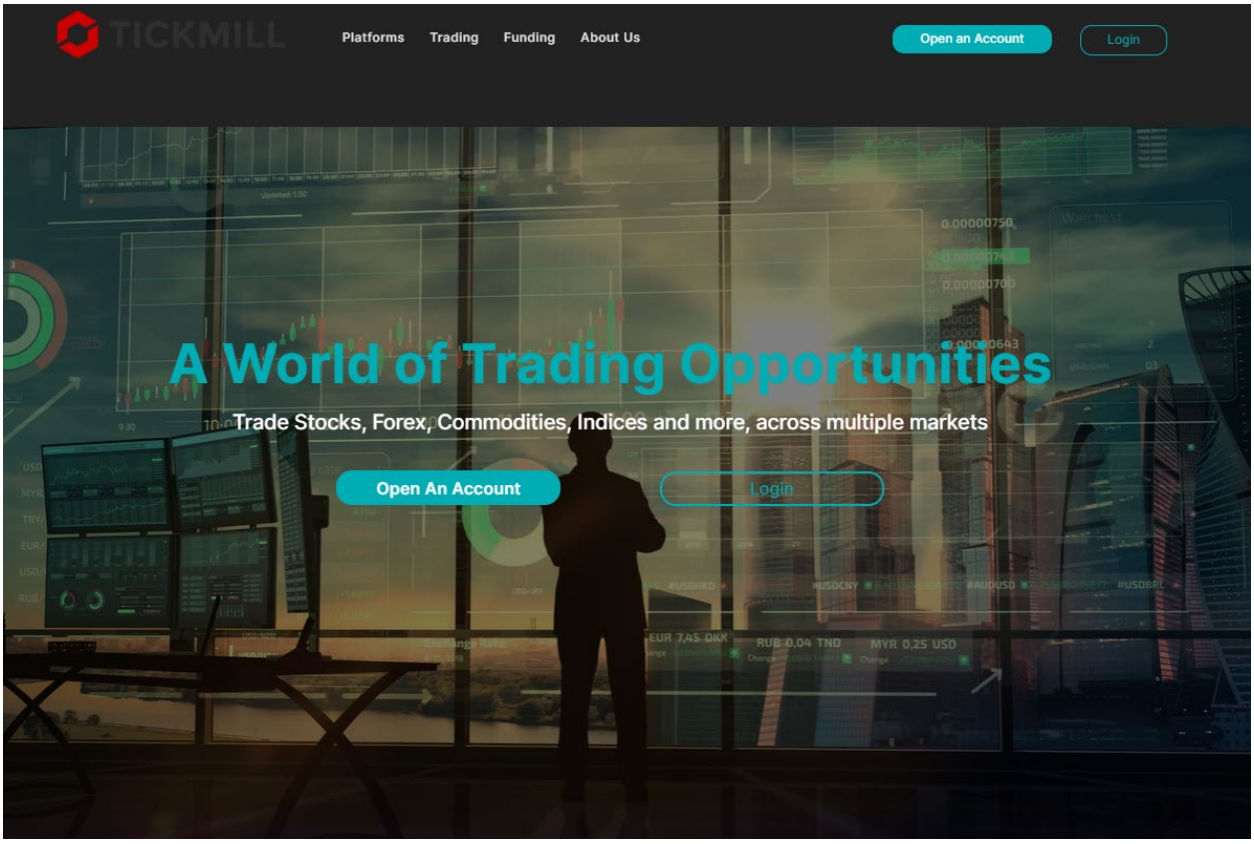

Figure 13 – Former Landing Page for Tickmilleas

58. The agents reviewing the Tickmilleas website saw an option to open an account, which required an email address and password. By clicking the "login" button, however, even without registering, the user was taken to a page appearing to display tickers for various apparent currencies, commodities, and conversion rates, shown in Figure 14 below:

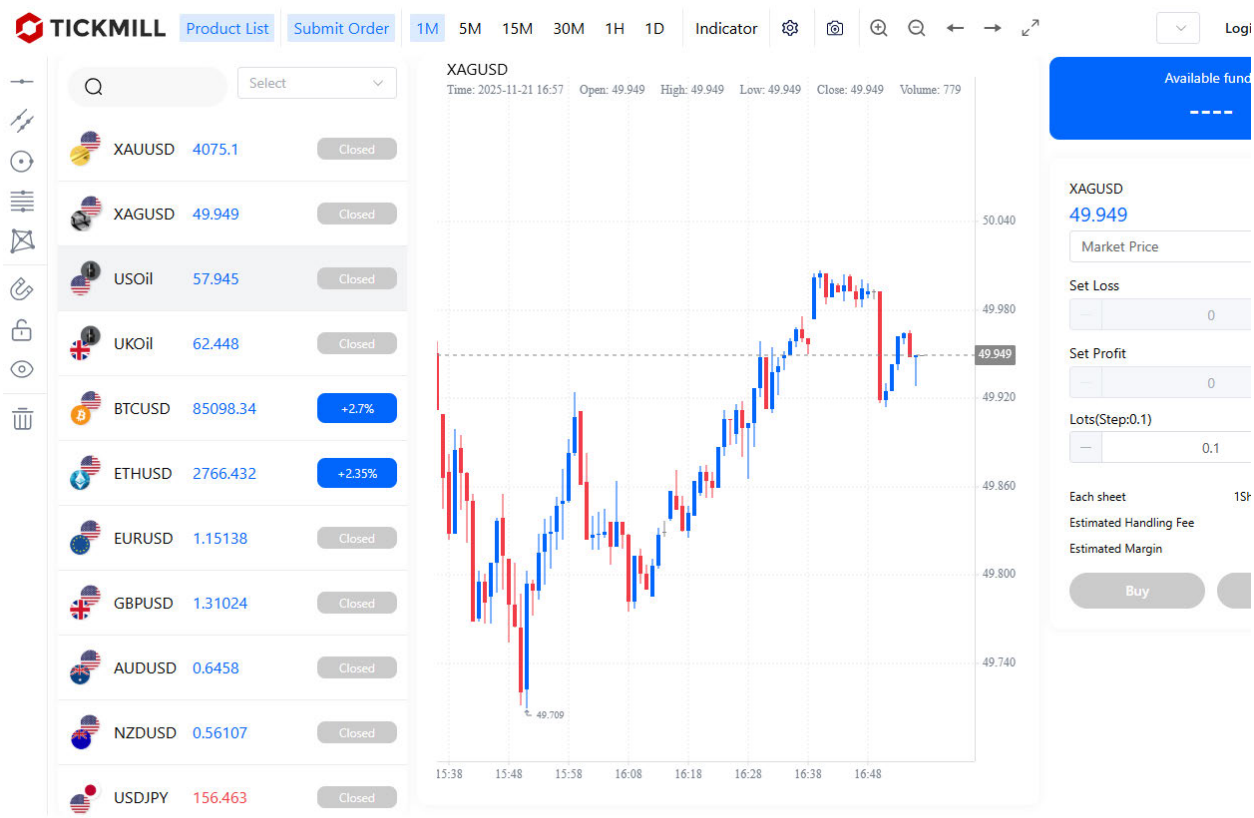

Figure 14 – tickmilleas.com's "ticker" page

59. The bottom of the landing page for Tickmilleas listed further information about the purported registration of the "company," which claimed, "Tickmill has a US NFA license, license number 0557897." Based on my training and experience, I believe this was 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 Tickmilleas on its landing page.

60. Under the "Platforms" tab on the landing page, there were two options, including a "Desktop" and a "Mobile" version. By clicking on the "mobile" version, the user was 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 appeared legitimate, but they were not legitimate applications and were primarily used by Tai Chang to further facilitate CIF. When the Apple App Store link was clicked, it showed four apps available: BTNEmax, BXLIZLDT-PRO, ReviseMate, and TEADOBDA, shown in Figure 15 below:

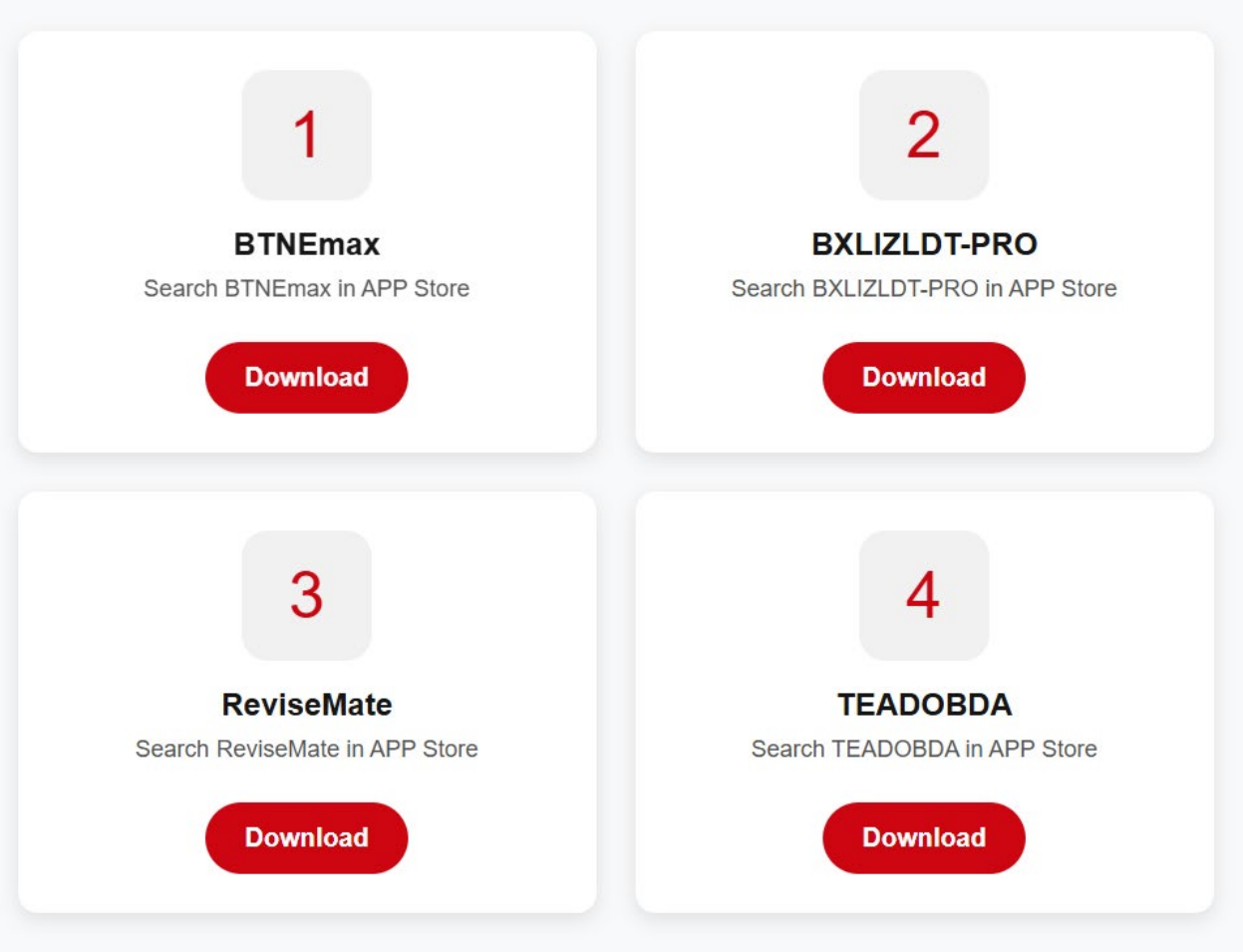

Figure 15 – Application links located on Tickmilleas

61. [redacted]

[redacted]. That same day, the FBI submitted these applications to Apple for internal review. On or about November 19, 2025, Apple confirmed to agents that all three applications ([redacted] been removed from the App Store and the developer's accounts were under investigation for termination.

62. [redacted]

That same day, the FBI submitted these applications to Apple and Google for internal review. On or about December 2, 2025, Apple confirmed to agents that all four applications [redacted] had been removed from the Apple App Store and the developer's accounts were under investigation for termination. In March 2026, Google confirmed to agents that all four applications ([redacted] been removed from the Google Play Store in mid-December 2025 and the developer's accounts were under investigation for termination.

63. Based [redacted] Apple and Google's responses, and my training and experience, I believe the above Apple and Google applications were both associated with Tickmilleas and were used by Tai Chang operators as mobile applications to defraud victims. 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 want their mobile applications to match in name, logo, and style to their company and its website for brand recognition.

64. Here, however, on Tickmilleas, the embedded application BTNEmax, for example, has a different name than "Tickmill" and a different logo entirely:

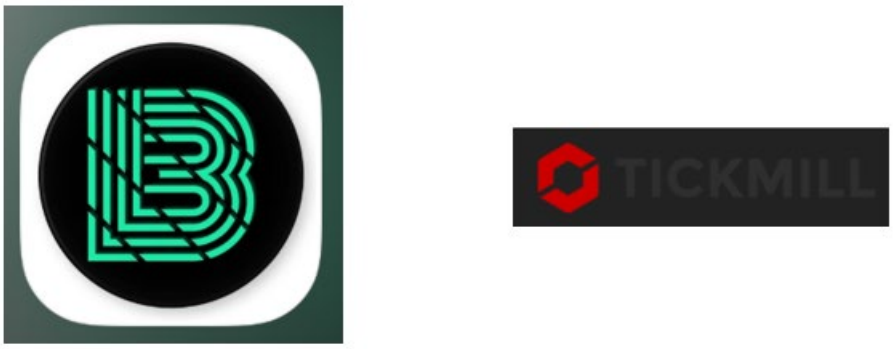

Figure 16 – BTNEmax vs. "Tickmill" Logo

65. Unlike legitimate companies, criminal organizations' goals for using domains like Tickmilleas 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. Tickmilleas, on its surface, appeared 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 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, Tickmilleas, is also a part of the scheme.

66. The FBI has conducted open searches of the name "Tickmill" and learned that there is a legitimate company named [redacted] with the website [redacted] Unlike Tickmilleas, 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:

[redacted]

67. On or about November 19, 2025, agents emailed [redacted], found on the [redacted] website and asked whether [redacted] had any affiliation with Tickmilleas. The Head of Customer Support responded, "We confirm that Tickmilleas[.]com 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]."

68. Based on the information described above, it is evident that Tickmilleas was impersonating the legitimate company, [redacted], and its website [redacted]. Tickmilleas's emblem, when compared against [redacted], is similar:

Figure 17 – Tickmilleas logo vs. [redacted] *Logo*

69. Tickmilleas's content also mimicked [redacted], such as by claiming to be regulated by the [redacted] Additionally, [redacted] has an authorized and regulated entity in [redacted] and Tickmilleas claimed 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.

70. 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 Tickmilleas**,** 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 Tickmilleas was not yet aware it was a scam. Accordingly, I believe the likely reason the query returned no reports referencing Tickmilleas in IC3.gov is because of Tickmilleas's recent registration date On December 2, 2025, the FBI seized the Tickmilleas website. Between December 2, 2025, and April 9, 2026, IC3 revealed that four victims reported scams associated directly with the seized Tickmilleas website.

F. Tickmilleas's Involvement in Money Laundering

71. [redacted] multiple cryptocurrency addresses that [redacted] were being used by scammers inside Tai Chang to accept victim payments made to Tickmilleas.[60] I know 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

[60] The cryptocurrency addresses provided did not, and as of April 9, 2026, still do not, maintain any cryptocurrency balance that could be frozen or seized.

conspirators. When an FBI forensic accountant analyzed the addresses [redacted] 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.

72. [redacted], the FBI forensic accountant, using reliable blockchain analytical tools,[61] traced backwards from several of the cryptocurrency addresses [redacted] to identify 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] listed above (illustrated in Figure 18 below). The FBI interviewed F-Victim 1 and F-Victim 2; summaries of these interviews are provided below.

[*Remainder of page intentionally left blank*]

[61] 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.

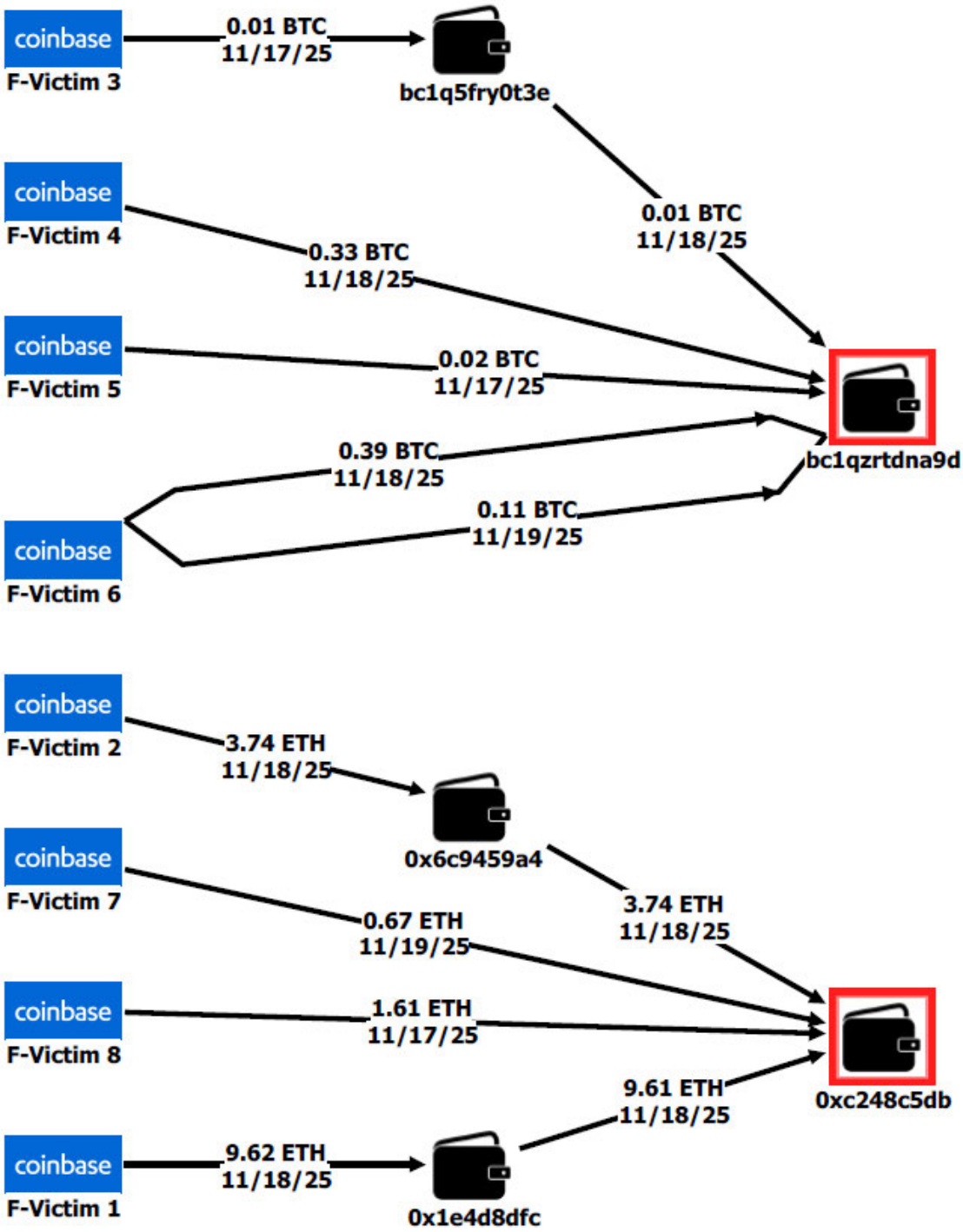

Figure 18 – Blockchain Tracing of Eight F-Victims to Addresses [redacted]

73. Through legal process, the FBI 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 funds that were ultimately deposited into the cryptocurrency addresses provided by F-Victim 1. The FBI interviewed most of the 21 identified individuals. All interviewees described situations clearly indicative of CIF schemes, and seven specifically mentioned Tickmilleas as the investment platform they had used.

Statement of F-Victim 1

74. 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 [redacted] applications. From there, Luca showed F-Victim 1 Tickmilleas and how trades occurred on the platform. When F-Victim 1 first deposited funds using Tickmilleas, 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.

75. 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 Tickmilleas. When contacted by the FBI, F-Victim 1 was not yet aware that F-Victim 1 was a scam victim.

Statement of F-Victim 2

76. 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]. 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.

77. Over time, Matteo introduced F-Victim 2 to investing. He instructed F-Victim 2 to open [redacted] account and [redacted] and ultimately guided F-Victim 2 to investing via Tickmilleas. 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 Tickmilleas. F-Victim 2 has been unable to withdraw those proceeds from the site.

78. [redacted] and the FBI's victim interviews, I have determined that F-Victims 1-8, shown earlier in Figure 18, 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.

79. Based on my training and experience, I believe that the blockchain transaction activity detailed above in Figure 18 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 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 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.

80. As shown above, before being seized by the FBI, Tickmilleas was a CIF scam domain sent by scammers to victims to attract and support victims' fake investments and 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).

81. Before its seizure, Tickmilleas 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 Tickmilleas in their interviews, referencing the domain as property that they were

directed to use to make false investments. Victims described how Tickmilleas showed lucrative returns on investment and how it would even show deposits made by the scammers to the victims' accounts when that scammer would walk victims through trading.

G. Identification of the New Domain Used by Tai Chang

82. [redacted]. A review of **TARGET DOMAIN NAME** revealed it to be almost identical to Tickmilleas in appearance and function. For example, the former landing page for Tickmilleas (before its seizure) and that of **TARGET DOMAIN NAME** are almost identical, using the same graphic, links, and language as those shown above in paras. 57 and 58:

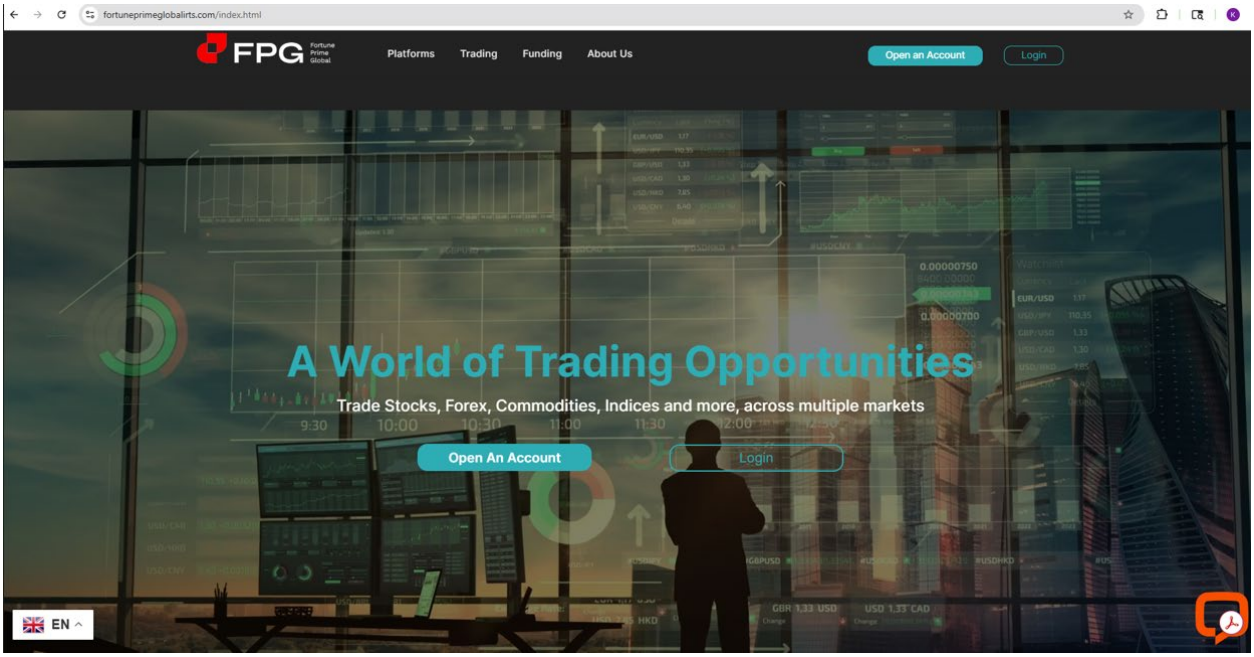

Figure 19 – Landing Page for ***Fortuneprimeglobalirts.com***

83. As was the case with Tickmilleas, a review of **TARGET DOMAIN NAME**'s 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 via the same ticker as was displayed on Tickmilleas before its seizure (shown above in para. 58):

*Figure 20 – **TARGET DOMAIN NAME'S** "Ticker" Page*

84. The ability to simply click "login" without entering a username or password and then arriving at an ambiguous "ticker" unconnected to any specific purpose is not something one would expect to find on an official business's website, where poor authentication and security protocols could negatively impact the company's reputation and potentially expose it to data breaches.

85. I believe that **TARGET DOMAIN NAME** is not in fact an official business website but the impersonation of one. Just as Tickmilleas impersonated [redacted] a legitimate company, I believe that **TARGET DOMAIN NAME** is impersonating a different legitimate company known as [redacted][62] According to its website,

[62] The FBI has emailed [redacted] to confirm that the **TARGET DOMAIN NAME** is not associated with [redacted] but as of April 15, 2026, the FBI has not yet received a response from [redacted]

[redacted],[63] [redacted] was established in [redacted] and serves as an online securities broker. Unlike **TARGET DOMAIN NAME**, which was registered on or about March 25, 2026, [redacted] website was registered in or around [redacted] uses the logo on the left, whereas **TARGET DOMAIN NAME** uses the same exact logo, only with a dark background, on the right:

[redacted]

Further, **TARGET DOMAIN NAME** uses [redacted] same physical address but a different (though similar) phone number and email address:

[redacted]

Figure 21 – [redacted] *contact information*

[63] [redacted] (last accessed on Apr. 9, 2026).

[64] Based on an open-source search, [redacted] appears to have used a different domain prior to that date. Based on my experience, it is extremely uncommon for fraudulent websites to remain active for long, especially as long as [redacted] years. Accordingly, the lasting presence of [redacted] website supports the inference that it is a legitimate company.

*Figure 22 – **TARGET DOMAIN NAME's** Contact Information*

86. Based on my training and experience and my knowledge of this investigation, I believe that **TARGET DOMAIN NAME** is impersonating [redacted] For example, by using the same physical address ([redacted]) as [redacted] **TARGET DOMAIN NAME** makes explicit its impersonation. Such a tactic is common in CIF schemes because, by using the same address as legitimate platforms, scam sites can attract traffic and deceive victims. Another common tactic in CIF schemes is modeling illegitimate investment platforms' contact information to be similar to that used by the legitimate platforms the scams are imitating or impersonating. For example, **TARGET DOMAIN NAME** uses a telephone number with a [redacted] country code, making it appear similar to [redacted] actual [redacted] number. The same is true for **TARGET DOMAIN NAME**'s email address, [redacted], which is similar to [redacted] true email address of [redacted]. Finally, **TARGET DOMAIN NAME** copied [redacted] logo, in what appears to be a further effort to deceive victims with the appearance of legitimacy while dissuading a closer look at its operations.

87. Not only do the tactics employed by the operators of **TARGET DOMAIN NAME** mirror those used by the previously seized Tickmilleas, but so do the methods used to link the

fraudulent domains to malicious applications. As Tickmilleas did, **TARGET DOMAIN NAME** distances its brand, [redacted] from the malicious applications it asks its victims to use so that the brand can be protected when the applications themselves are inevitably flagged and shut down.

88. For example, present on **TARGET DOMAIN NAME's** landing page are links to download its applications via the Google Play Store and the Apple App Store. When the Apple App Store link is clicked, it displays the following applications:

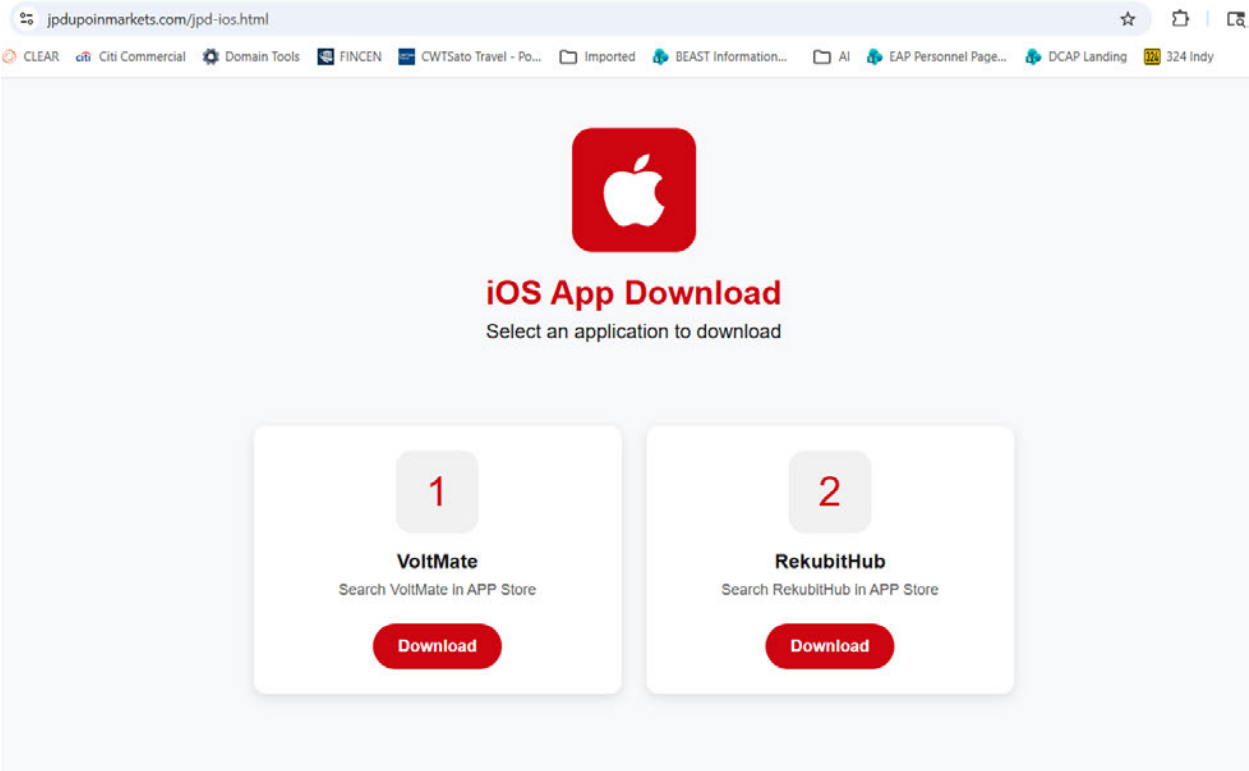

*Figure 23 – Application links located on **TARGET DOMAIN NAME***

When the user clicks the "download" button, the user is taken to the Apple App Store to download the specific app, such as "VoltMate" below:

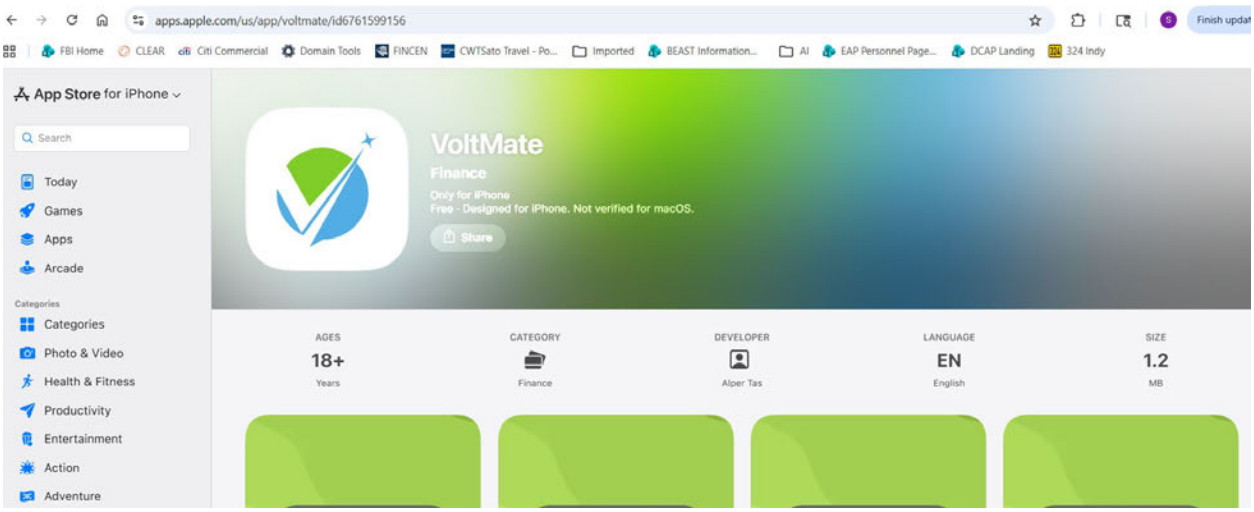

Figure 24 – Apple App Store Landing Page for VOLTMATE

89. The VoltMate application has an entirely different name and logo than [redacted] Tickmilleas was organized in the same way. Unlike legitimate companies, a criminal organization's goal for using a domain like **TARGET DOMAIN NAME** is to create a website that both appears 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 were shut down. **TARGET DOMAIN NAME**, on its surface, appears professional and legitimate. Severing that brand (*i.e.*, "[redacted] which first attracts victims, with the actual applications (*e.g.*, "VoltMate") that victims use to deposit funds and ultimately lose money from makes sense. 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.

90. This inference is supported by Apple's removal of applications that were previously linked to the **TARGET DOMAIN NAME**. On or about April 1, 2026, investigators discovered two Apple applications, "JHBHOLY" and "FIXLOGS," linked via the **TARGET DOMAIN**

NAME.[65] Investigators provided those applications to Apple which, on or about April 2, 2026, removed both applications for its store.

91. Because **TARGET DOMAIN NAME** was only registered in late March 2026, investigators could not yet find complaints by victims regarding the site via IC3.gov, the FBI's crime complaint center for Internet-based frauds and scams. As described previously, CIF schemes often occur over the span of months, so it is possible that none of the victims directed to the **TARGET DOMAIN NAME** are aware of their victimization. Furthermore, I know from my training and experience that not all CIF victims report their incidents to law enforcement or IC3.gov.

H. TARGET DOMAIN NAME'S INVOLVEMENT IN MONEY LAUNDERING

92. Based on all the facts detailed above, I believe that **TARGET DOMAIN NAME** is a CIF domain used by Tai Chang scammers to attract and facilitate victims' fake investments. There thus is probable cause to believe that it serves as key facilitating property for Tai Chang's wire fraud and money laundering conspiracies. Scammers located overseas, including in Burma, induce 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 facilitates 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).

93. **TARGET DOMAIN NAME** is involved in international promotion money laundering by connecting U.S. victims to the platforms used by criminals overseas to siphon victim

[65] Apple App Store, https://apps.apple.com/us/app/jhbholy/id6761244691, https://apps.apple.com/us/app/fixlogs/id6761248005. Because these apps were removed, these links are no longer functional.

funds abroad in promotion of the underlying wire fraud scheme. As detailed above, **TARGET DOMAIN NAME** just became active and, as a result, investigators have not yet been able to find victims associated with the specific website and/or current applications hosted there. Nevertheless, the facts in this affidavit clearly demonstrate that **TARGET DOMAIN NAME** is just the latest iteration of websites and domains used by Tai Chang to conduct these schemes. I believe that the perpetrators who control **TARGET DOMAIN NAME** are using the same tactics employed by those who controlled the previously seized Tickmilleas website. Consequently, there is probable cause to believe the new website, **TARGET DOMAIN NAME**, is merely a substitute for and copy of the prior domain (Tickmilleas), which this court already determined was involved in money laundering. There thus is probable cause to believe that **TARGET DOMAIN NAME** is likewise involved in money laundering offenses.

SEIZURE PROCEDURE

94. As detailed in Attachment A, upon execution of the seizure warrant, VeriSign the registry for the ".com" top-level domain, 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.

95. 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

96. 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

97. **TARGET DOMAIN NAME**, fortuneprimeglobalirts.com, is a domain used by subjects believed to be located outside the United States for a wire fraud conspiracy in which U.S. victims are 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** is 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).

98. 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.

99. 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]

Special Agent
Federal Bureau of Investigation

Subscribed and sworn pursuant to Fed. R. Crim. P. 4.1 and 41(d)(3) on April 20, 2026.

HONORABLE MATTHEW J. SHARBAUGH
UNITED STATES MAGISTRATE JUDGE
DISTRICT OF COLUMBIA

ATTACHMENT A: PROPERTY TO BE SEIZED

With respect to the domain name fortuneprimeglobalirts.com (**TARGET DOMAIN NAME**), VeriSign, Inc. ("VeriSign"), which is the domain registry for **TARGET DOMAIN NAME**, shall take the following actions to effectuate the seizure of **TARGET DOMAIN NAME**:

1. Take all reasonable measures to redirect **TARGET DOMAIN NAME** to substitute servers at the direction of the Federal Bureau of Investigation, by redirecting traffic from the **TARGET DOMAIN NAME** to the following authoritative name-servers:
    a. Ns1.fbi.seized.gov;
    b. Ns2.fbi.seized.gov; and/or
    c. Any new authoritative name server or IP address to be designated by a law enforcement agent in writing, including email, to VeriSign.
2. Prevent any further modification to, or transfer of, **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 the **TARGET DOMAIN NAME** cannot be made absent court order or, if forfeited to the United States, without prior consultation with Federal Bureau of Investigation.
3. Take all reasonable measures to propagate the necessary changes through the Domain Name System as quickly as practicable.
4. Provide reasonable assistance in implementing the terms of this Order and take no unreasonable action to frustrate the implementation of this Order.

The Government will display a notice on the website to which **TARGET DOMAIN NAME** will resolve. That notice will consist of the following text (or substantially similar text):

This domain has been seized in accordance with a seizure warrant issued pursuant to 18 U.S.C. § 981, 18 U.S.C. § 982, and 21 U.S.C. § 853, issued by the United States District Court for the District of Columbia as part of a joint law enforcement operation and action by:

United States Attorney's Office for the District of Columbia;

Computer Crime & Intellectual Property Section; and

Federal Bureau of Investigation

If you believe you may have been victimized as part of a cryptocurrency investment fraud scam or other cyber-enabled crime, please submit a complaint to the FBI at www.ic3.gov. Tips about the Tai Chang Scam Centers, also referred to as "Koi Sai Casino" and "Kyauk Khat Casino" can be emailed to TaiChangTIPS@fbi.gov.