UNITED STATES DISTRICT COURT

for the

District of Columbia

In the Matter of the Seizure of *(Briefly describe the property to be seized)* IN THE MATTER OF THE SEIZURE OF NINE STARLINK TERMINALS AND ASSOCIATED ACCOUNTS UNDER THE CONTROL OF SPACEX FOR VIOLATIONS OF 18 U.S.C. §§ 1349, 1956	)	Case No. 25-sz-48

APPLICATION FOR A WARRANT TO SEIZE PROPERTY SUBJECT TO FORFEITURE

I, a federal law enforcement officer or attorney for the government, request a seizure warrant and state under penalty of perjury that I have reason to believe that the following property in the jurisdiction of the District of Columbia is subject to forfeiture to the United States of America under 18 U.S.C. §§ 981, 982. and 28 U.S.C. § 2461(c).

(describe the property):

SEE ATTACHMENT A, HEREBY INCORPORATED BY REFERENCE

The application is based on these facts:

SEE ATTACHED AFFIDAVIT, HEREBY INCORPORATED BY REFERENCE.

❒ Continued on the attached sheet.

Stephanie Streeter

Applicant's Signature

Stephanie Streeter, Special Agent

Printed name and title

Attested to by the applicant in according with the requirements of Fed. R. Crim. P. 41 by telephone.

Date: 11/12/2025

Judge's signature

City and state: District of Columbia

G. Michael Harvey, U.S. Magistrate

Printed name and title

Judge

AO 109 (Rev. 12/09, modified by USAO-DC) Warrant to Seize Property Subject to Forfeiture by Telephone

UNITED STATES DISTRICT COURT

for the

District of Columbia

In the Matter of the Seizure of *(Briefly describe the property to be seized)*	)	
IN THE MATTER OF THE SEIZURE OF NINE STARLINK TERMINALS AND ASSOCIATED ACCOUNTS UNDER THE CONTROL OF SPACEX FOR VIOLATIONS OF 18 U.S.C. §§ 1349, 1956	)	Case No. 25-sz-48

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:

NINE STARLINK TERMINALS AND ASSOCIATED ACCOUNTS UNDER THE CONTROL OF SPACEX FOR VIOLATION OF 18 U.S.C. §§ 1349, 1956, 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 11/26/2025
(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 G. Michael Harvey.
(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: 11/12/2025

Judge's signature

City and state: District of Columbia G. Michael Harvey, U.S. Magistrate Judge
Printed name and title

AO 109 (Rev. 12/09) Warrant to Seize Property Subject to Forfeiture (Page 2)

Return		
Case No.: 25-sz-48	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 NINE STARLINK TERMINALS AND ASSOCIATED ACCOUNTS UNDER THE CONTROL OF SPACEX FOR VIOLATIONS OF 18 U.S.C. §§ 1349, 1956	**CASE NO. 25-sz-48** **FILED UNDER SEAL**

AFFIDAVIT IN SUPPORT OF SEIZURE WARRANT

I, Stephanie Streeter, 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 nine Starlink terminals (collectively, "the **TARGET PROPERTY**") and the associated accounts (collectively, "the **TARGET ACCOUNTS**"), as described in the following paragraphs and in Attachment A. The **TARGET PROPERTY** is located outside the United States but is controlled through electronic means by Space Exploration Technologies Corp. (SpaceX), located in Hawthorne, California. **The TARGET ACCOUNTS** are located at SpaceX in California and/or can be controlled through electronic means by SpaceX in California.

2. 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.

3. Based upon my training and experience, I am familiar with the methods of operation employed by subjects in fraud investigations to obfuscate their involvement in transactions for the purpose of circumventing U.S. law.

4. I am one of the case agents in this investigation, which is being worked out of the FBI Washington Field Office. During my work on this investigation, I have reviewed reports

prepared by agents and discussed this case and other related cases with law enforcement officers, analysts, and partners at other U.S. Government agencies who have been involved in these investigations. I submit this affidavit based upon personal knowledge derived from my participation in this investigation and information that I have received from a variety of other sources, including open-source reporting by reputable news organizations and non-governmental organizations, reporting by FBI sources, business records of U.S. providers, and reports of victims.

PURPOSE OF AFFIDAVIT

5. This affidavit is made in support of a seizure warrant for nine Starlink terminals (the **TARGET PROPERTY**) located in or around Payathonzu, Burma, near Three Pagodas Pass, and associated Starlink user accounts (the **TARGET ACCOUNTS**).

6. 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)(1)(A)(i),(a)(2)(A) & (h) (Laundering monetary instruments and conspiracy) have been committed by numerous unknown individuals operating out of Burma-based scam centers near Three Pagodas Pass, and referred to below as the "Three Pagodas Pass" scam centers. There is also probable cause to seize the **TARGET PROPERTY** and the **TARGET ACCOUNTS** as property involved in violations of 18 U.S.C. § 1956 and subject to forfeiture pursuant to 18 U.S.C. §§ 981(a)(1)(A) and 982(a)(1) and 28 U.S.C. § 2461(c).

SUMMARY OF AFFIDAVIT

7. The United States is investigating international criminal organizations operating cryptocurrency investment fraud (CIF) scams.[1] 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.

8. Numerous CIF schemes are run out of industrial-scale scam compounds and scam centers in Burma. The criminal syndicates behind these compounds and centers 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 facilities. Within these facilities, 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.

9. According to publicly available reporting, in late 2024, scam operations moved into the area around Payathonzu, in the Kayin State of south Burma, an area also described locally as Three Pagodas Pass (due to a local landmark), which was south of existing scam operations in Burma and around Myawaddy. Open-source reporting from local news organizations in October 2024 confirmed that these scam centers are within the area controlled by the Democratic Karen

[1] In public reporting, these scams are sometimes referred to as "pig butchering," a term derived from the Chinese phrase used to describe this scheme.

Benevolent Army (DKBA). DKBA has acknowledged the high number of trafficked persons in their territory. This warrant focuses on three locations in the Payathonzu area believed to be associated with scamming U.S. victims.

10. The government has identified and is seeking to seize the **TARGET PROPERTY** and the **TARGET ACCOUNTS**. As detailed below, the **TARGET PROPERTY** and the **TARGET ACCOUNTS** each were involved in a conspiracy to commit money laundering offenses, in violation of 18 U.S.C. § 1956(a)(1)(A)(i), (a)(a)(2)(A) & (h) 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, U.S. 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, U.S. Code, Section 1956(a)(1)(A)(i) criminalizes "a financial transaction which in fact involves the proceeds of specified unlawful activity—with the intent to promote the carrying on of specified unlawful activity" where the defendants "know[] that the property involved in a financial transaction represents the proceeds of some form of unlawful activity, conducts or attempts to conduct such a financial transaction . . . ." Title 18, U.S. 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 and 1349 qualify as specified unlawful activity under the statute. Title 18, United States Code, Section 1956(h) criminalize a conspiracy to commit money laundering, as defined in Section 1956(a).

13. This Court has jurisdiction to issue the requested warrant. Title 21, U.S. Code, Section 853(f) 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, § 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 PROPERTY** and the **TARGET ACCOUNTS** for forfeiture.

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]." Under § 982(a)(1), property involved in a transaction or attempted transaction in violation of 18 U.S.C. § 1956 is subject to criminal forfeiture to the United States. 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 Three Pagodas Pass scam centers and the individuals responsible for the use of the **TARGET PROPERTY** and the **TARGET ACCOUNTS.**

15. This court has the authority to issue seizure warrants for assets located in a foreign jurisdiction pursuant to 18 U.S.C. § 981(b)(3). Section 981(b)(3) provides that a seizure warrant may be issued by a "judicial officer in any district in which a forfeiture action against the property may be filed under [28 U.S.C.] section 1355(b), and may be executed in any district in which the property is found, or transmitted to the central authority of any foreign state for service in accordance with any treaty or other international agreement" (emphasis added). Pursuant to 28 U.S.C. § 1355(b), a forfeiture action may be brought in any district court where any of the acts or omissions giving rise to the forfeiture occurred, even as to property located in a foreign jurisdiction. 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.

16. The statutes described above provide the Court authority to issue a seizure warrant for the contents of the entire accounts, where the accounts are used as property involved in the illegal money laundering activity. This is true even where the account may have been used for "legitimate" or "clean" purposes. *See United States v. Bornfield*, 145 F.3d 1123 (10th Cir. 1998) (forfeiture of legitimate and illegitimate funds commingled in an account is proper as long as the government demonstrates that the defendant pooled the funds to facilitate--*i.e.*, disguise--the nature and source of his scheme); *United States v. Hawkey*, 148 F.3d 920, 928 n.13 (8th Cir. 1998) (citing *Bornfield* with approval, and noting that in some instances it may be appropriate to order the forfeiture of an account containing commingled tainted and untainted funds); *United States v.*

Trost, 152 F.3d 715 (7th Cir. 1998) (legitimate funds may be forfeited if used to disguise illegitimate funds); *United States v. Iacaboni*, 221 F. Supp. 2d 104 (D. Mass. 2002) (commingling clean money with gambling proceeds to conceal nature of transaction rendered entire sum forfeitable); *United States v. Certain Funds on Deposit in Account No. 01-0-71417*, 769 F. Supp. 80, 84-85 (E.D.N.Y. 1991).

17. Courts are empowered to grant warrants for the seizure of all contents of an account involved in money laundering transactions. *E.g.*, *United States v. Contents of Account Number 901121707*, 36 F. Supp. 2d 614 (S.D.N.Y. 1999); *United States v. Contents of Account Numbers 208-06070,* 847 F. Supp. 329, 334-35 (S.D.N.Y. 1994); *United States v. Certain Accounts*, 795 F. Supp. 391, 397 (S.D. Fla. 1992); *United States v. All Monies in Account No. 90-3617-3*, 754 F. Supp. 1467, 1473 (D. Haw. 1991).Venue is proper in this district under 18 U.S.C. § 3238 (venue for offenses committed outside any district and on the high seas). Venue is also proper within this judicial district pursuant to 28 U.S.C. § 1355(b)(2), because the **TARGET PROPERTY** is subject to forfeiture because it is located in a foreign country.

PROBABLE CAUSE

I. Background on Cryptocurrency Investment Fraud

18. CIF is a confidence/investment scam perpetrated by subjects against victims for financial gain. Subjects contact victims, often online, and form a strong relationship, romantic or otherwise, over days or weeks. 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 towards a specific scam website or app disguised as a legitimate investment platform.

19. When fraud victims are interacting with these scam websites, they are provided cryptocurrency addresses as a means to fund their account. The victims are instructed to open an

account on a cryptocurrency platform to exchange fiat currency (U.S. dollars) for cryptocurrency and send that cryptocurrency to the cryptocurrency addresses provided by the websites.

20. 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 the scammer, who is then free to move those funds along to associates. The scam websites show the victims returns on their investment, prompting the victims to "invest" more cryptocurrency into the platform. This scam is continued until a victim becomes aware of the scam or runs out of money, at which time the scammer ceases contact.

21. 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."[2]

22. 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

[2] 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).

from CIF scams rose, from $3.96 billion in 2023, to $5.8 billion in 2024, an increase of 47%.[3] 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.

II. Background on Origins of CIF Scam Compounds in Burma

23. Based on publicly available sources, in 2017, the first Chinese investors who would later construct CIF scam compounds arrived in Burma's Kayin State.[4,5] 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),[6] formerly branded as the "Border Guard Force" (BGF).[7] 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.[8]

---

[3] 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).

[4] *A Growing Threat* (May 2024), *supra* at n.2.

[5] 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).

[6] 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).

[7] The Karen BGF has since renamed itself the Karen National Army after distancing itself from the Myanmar Military, while retaining regional control.

[8] "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

24. 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.[9]

25. 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."[10] 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.[11] 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."[12] USIP further reported that thousands of Chinese workers had been "lured" to this location to build and work in these structures.[13]

---

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).

[9] 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).

[10] 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).

[11] *Id.*

[12] *Id.*

[13] *Id.*

26. 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.[14] And as lockdowns and border controls meant Chinese workers could not travel to Burma, these organizations began trafficking workers from around the world.[15] 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."[16]

27. The Department of the Treasury's 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."[17] 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

---

[14] 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).

[15] *Id.*

[16] *Id.*

[17] 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.)

issued by China, which has continued to seek his extradition from Thailand ever since.[18]

28. In May 2025, the KNA (formerly Karen BGF) and Saw Chit Thu, also sanctioned by the United Kingdom, were sanctioned by the United States for facilitating cyber scams, human trafficking, and cross-border smuggling.[19]

29. 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:

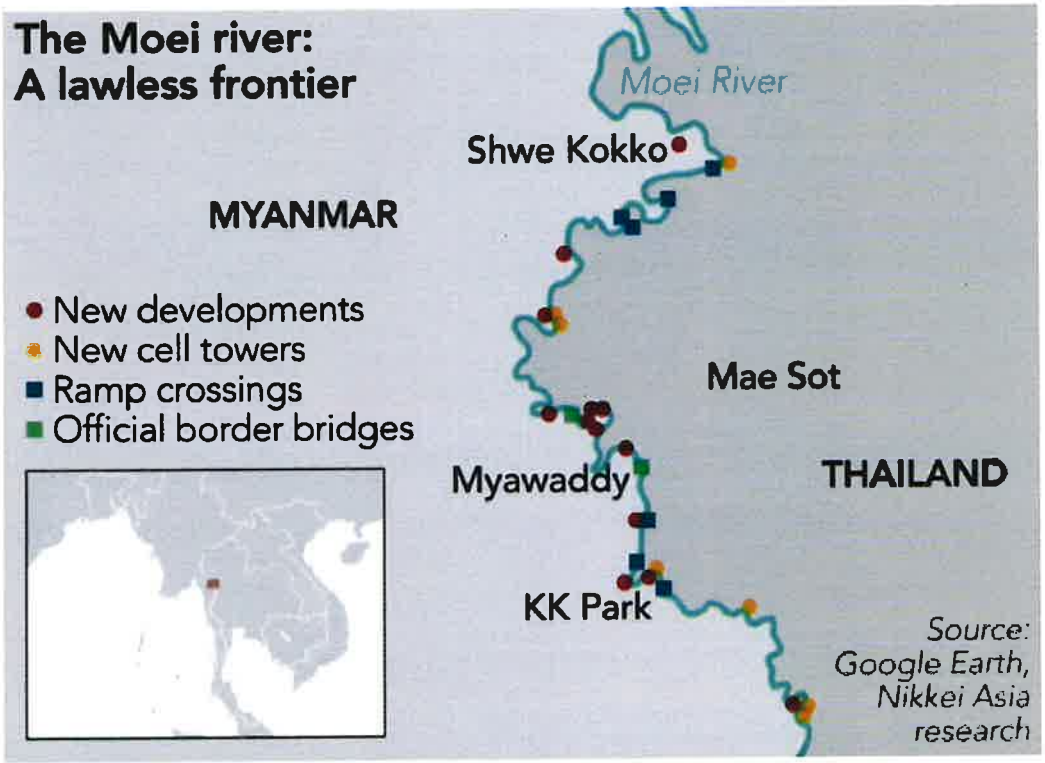


Figure 1 – Several compound developments are identified along the Moei river in Burma.[20]

---

[18] *Id.*

[19] 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.)

[20] Karen National Union Under Pressure Over Crime Hub, https://www.irrawaddy.com/news/burma/karen-national-union-under-pressure-over-crime-hub.html (Feb 28, 2023).

30. CIF compounds are often "city-like" and reminiscent of "penal colonies."[21] Public reporting on KK Park and other Southeast Asian CIF compounds includes accounts of beatings, electrocutions, and murder.[22] 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."[23] Those who cannot or do not pay are sometimes sold between companies.[24] 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.[25]

III. The Scam Centers at Three Pagodas Pass & WEALTHOB CIF Scam

A. The Democratic Karen Benevolent Army's Involvement in Scam Centers in Payathonzu, Burma

31. Public reporting shows that the Democratic Karen Benevolent Army (DKBA) is involved in scam compounds in Burma. The DKBA is a separate entity from the KNA and is also

---

[21] *A Growing Threat (Nov. 2022)*, *supra* at n. 14.

[22] *A Growing Threat (Nov. 2022)*, *supra* at n. 14; 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).

[23] *Cyber Slavery*, *supra* at n. 22; *see also Cambodia Scams*, *supra* at n. 22.

[24] *Cyber Slavery*, *supra* at n. 22; *Cambodia Scams*, *supra* at n. 22.

[25] 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*, at n. 23; *Cambodia Scams*, *supra* at n. 22.

friendly with the ruling Junta of Burma.[26] The DKBA is reportedly run by General Saw Steel,[27] Colonel Saw Sein Win,[28] and Brigadier General Sai Kyaw Hla.[29]

32. Multiple articles note the DKBA's involvement in scam compounds.[30] In February 2025, The Irrawaddy, a Burma-focused news organization, reported images of trafficked persons who reported being abused by the DKBA operating compounds in Khyauk Khet, Myawaddy.[31] The victims reported that "[t]he torture was carried out by rank-and-file DKBA soldiers at the orders of the Chinese gangs for infractions from failing to meet their scam quotas to refusing to cooperate."[32] The same report also included statements from DKBA commanders, Individual 1 and Brig. Gen. Sai Kyaw Hla, acknowledging involvement in the abuses.[33] The DKBA has likewise acknowledged the high amount of trafficked persons in their territory.[34]

33. A companion warrant, 25-sz-47, incorporated by reference, further describes the

---

[26] Jason Tower, Priscilla Clapp, *Chinese Crime Networks Partner with Myanmar Armed Groups*, U.S. Institute of Peace, https://www.usip.org/publications/2020/04/chinese-crime-networks-partner-myanmar-armed-groups (April 20, 2020) (last accessed on November 7, 2025).

[27] Myanmar Now, https://myanmar-now.org/en/news/ethnic-karen-leaders-come-to-historic-agreement-to-reunite-knu-dkba/ (Aug. 30, 2022) (last accessed on November 7, 2025).

[28] DVB, https://english.dvb.no/dkba-demands-answers-after-junta-airstrike-on-commanders-housing-compound/ (Jan. 23, 2023) (last accessed on November 7, 2025); Radio Free Asia, https://www.rfa.org/english/news/myanmar/juntadkbaairstrike-01232023164117.html (Jan. 23, 2023) (last accessed on November 7, 2025).

[29] Radio Free Asia, https://www.rfa.org/english/news/laos/trafficked-04112023170154.html (Apr. 13, 2023) ("According to a geolocation pin sent to RFA by several parents of Lao teens currently 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.")

[30] Bangkok Post, https://www.bangkokpost.com/thailand/general/2985005/pregnant-women-among-stranded-former-scam-workers (Mar. 21, 2025) (noting that a human trafficking organization had visited a camp on March 15 that was run by the DKBA, where pregnant women were being held captive).

[31] The Irrawaddy, https://www.irrawaddy.com/news/burma/freed-scam-center-victims-tell-of-torture-by-karen-militia.html (Feb. 14, 2025).

[32] *Id.*

[33] *Id.*

[34] Thai PBS, https://world.thaipbs.or.th/detail/dkba-force-to-suspend-help-for-foreigners-in-its-territory-due-to-high-costs/56598 (Feb. 20, 2025).

DKBA's control of a scam compounds, including the Tai Chang compound in Kyaukhat, Burma.

34. According to publicly available reporting, in late 2024, scam operations moved into the area around Payathonzu, in the Kayin State of south Burma, an area also described locally as Three Pagodas Pass (due to a local landmark), which was south of existing scam operations in Burma in and around Myawaddy. Based on my review of Google Maps, Payathonzu is approximately 100 miles south of Kyaukhat, Burma.

35. According to publicly available reporting, in late 2024, scam centers moved into Payathonzu from another scam compound in the area of Shwe Kokko, Burma, after pressure from local and Chinese authorities to end scam activities there:

> Since early July, online fraud gangs have been moving operations to Payathonzu, Falu, Kyauk Khet, Min Let Pan and Waw Lay near Myawaddy, Myanmar's busiest border town with Thailand. **Payathonzu is about five hours' drive south of Myawaddy.** Gangs have moved from the Shwe Kokko criminal hub in Myawaddy Township and rents have doubled, according to Payathonzu residents. **Some gangs have rented land from armed organizations near Mount Dhamma Giri above Payathonzu to run casinos.**[35]

36. In February 2025, another publicly available source noted, "New scam rooms are cropping up to the south, including along Burma's border with Thailand's Kachanburi province—Rangsiman pointed to the border along Thailand's Phop Phra district, 35 kilometers south of Mae Sot, and Payathonzu, in Burma's Karen state and across from Sangkhlaburi, 300 kilometers from Mae Sot."[36]

---

[35] *Online Scam Centers Expand on Thailand-Myanmar Border*, The Irawaddy (Oct. 1, 2024), https://www.irrawaddy.com/news/burma/online-scam-centers-expand-on-thailand-myanmar-border.html ("Online Scam Centers Expand") (last accessed on November 7, 2025) (emphasis added).

[36] *Myanmar scam operations move south along Thai border*, Voice of America (Feb. 1, 2025), https://www.voanews.com/a/myanmar-scam-operations-move-south-along-thai-border/7959295.html (emphasis added).

37. Publicly available sources also reported in February 2025 that the Thai government had admitted that organized crime syndicates were running scam operations in Payathonzu.[37]

38. Open-source reporting from local news organizations in October 2024 confirmed that these scam centers are within the area controlled by the DKBA: "The DKBA has mostly provided the administration and security for Payathonzu since mid-2023 with junta forces largely confined to their base, residents said."[38]

39. Additionally, I have obtained information from two human sources related to scam operations in Payathonzu that corroborate the public reporting. Based on the following, I believe that this information is consistent with the scam operations in Payathonzu being under DKBA control, and specifically with the scam centers described further below as the "Three Pagodas Pass" scam centers.

40. According to reporting received in the summer of 2025 from CS-1,[39] a confidential source who has traveled through and lived in Burma and who has knowledge of the area, DKBA exercises control over the physical security of the "Three Pagodas Pass" area and its scam center operations.

41. In November 2025, I obtained information from a cooperating witness (CW-1), an expert on scam compounds in Burma who is the source of multiple scholarly articles. CW-1

---

[37] *Thailand will cut power to Myanmar border to stop "scam centres" run by gangs*, ABC News Australia (Feb. 4, 2025), https://www.abc.net.au/news/2025-02-05/thailand-will-cut-to-myanmar-border-regions-to-stop-scam-centres/104897578.

[38] *Online Scam Centers Expand*, The Irawaddy (Oct. 1, 2024), https://www.irrawaddy.com/news/burma/online-scam-centers-expand-on-thailand-myanmar-border.html.

[39] CS-1, a well-placed source with excellent access, has provided early reporting substantiated by news outlets.

confirmed the presence of scam compounds in Payathonzu under DKBA control.[40] CW-1 has regularly and recently traveled to Thailand and obtained first-hand reporting from individuals about the situation on the ground in Payathonzu, Burma. CW-1 reported that:

i. CW-1's sources stated that scam operations started at the area in early 2024. The DKBA controls the area tightly.

ii. Initially, there were reports of scammers based out of hotels in Payathonzu.

iii. Over time, the scam operations consolidated into a compound. Specifically, in mid-2024, DKBA purchased land just outside the city to construct a compound, on which fifteen buildings surrounded by a 2m wall have been built. The compound is tightly controlled, with a moat to prevent easy access. CW-1 provided a location for this compound to investigators; the location is approximately 6 miles from the border with Thailand (Location C, described below).

B. Description of "Three Pagodas Pass" Scam Center Operations

42. This warrant focuses on scam operations within Payathonzu (collectively, the "Three Pagodas Pass scam centers"), including three locations described below.

43. **Location A:** As described further below, Location A is a location within Payathonzu near the Thai border.

44. The following satellite imagery, obtained from two different providers, shows the development of Location A between 2023 and 2025 and the construction of multiple buildings into

[40] I have reviewed CW-1's scholarly reporting and generally find it to be consistent with other scholarly reporting about the area, as well as information known to me generally from the investigation. CW-1 has not been paid for this information provided to the FBI.

the creation of what appears to be a scam center. As described further below, these buildings appear to contain operations of a CIF scheme, likely targeting U.S. victims.

Figure 2 – Satellite imagery depicting Payathonzu.[41]

45. As used in this affidavit, Location A refers to the area bounded generally by the following coordinates and illustrated by the yellow boundary in the photo inserted below:

a. 15°18'28"N, 98°23'45"E (Point 1)
b. 15°18'25"N 98°23'41"E (Point 2)
c. 15°18'23"N 98°23'42"E (Point 3)
d. 15°18'26"N 98°23'47"E (Point 4)

[41] Figure 2 depicts side by side imagery from Google Maps in February 2023 and Planet Labs in October 2025. Planet Labs is an earth imaging company based in the United States. The October 2025 satellite imaging suggests building development in the Three Pagodas area of Payathonzu.

Figure 3 – Location A[42]

46. Based on my review of Google Earth images taken in or around February 2023 and the recent satellite imagery described above, Location A is located to the south of a landmark noted as "Dhamma Giri" Mountain, referred to in the open-source reporting discussed above (*see supra* ¶ 35).

[42] Figure 3 was created using Google Earth imagery from November 2023 and does not reflect recent construction; however, the area contained in the yellow box generally aligns with the blue buildings shown in the yellow box in Figure 3.

Figure 4 – Google Earth image of Mt. Dhamma Giri, Payathonzu, Burma, and Location A (circled).

47. While CW-1 did not have specific knowledge about the buildings in Location A, CW-1 noted that there is an "informal" border smuggling point located a few blocks away from the Location A, which CW-1 had visited. CW-1 noted that due to the presence of the informal border crossing and the complete lack of border management at that point, criminal operations such as human trafficking would be generally undetected in that area.

48. **Location B:** Location B is a location within Payathonzu, a few blocks away from Location A. Location B was determined from a review of geolocation information for SpaceX property tied to the scheme and bounded generally by the coordinates for the points listed and illustrated below:

a. 15°18'24"N 98°23'32"E (Point 1)

b. 15°18'23"N 98°23'30"E (Point 2)

c. 15°18'22"N 98°23'30"E (Point 3)

d. 15°18'22"N 98°23'32"E (Point 4)

Figure 5 – Location A and B geographic relationship

49. **Location C:** Location C is a location approximately six miles from Payathonzu.

Figure 6 – Location C.

50. Location C was described by CW-1 as a location outside the city that DKBA had purchased from local farmers after establishing operations in the area (*see supra* ¶ 41). The Google Maps satellite imagery of Location C is consistent with the description provided by CW-1, to include the location of the facility and the moat surrounding it. Location C refers to the area bounded generally by the following coordinates and is illustrated in the photo inserted above:

a. 15°23'32"N 98°18'03"E (Point 1)

b. 15°23'25"N 98°18'01"E (Point 2)

c. 15°23'26"N 98°17'57"E (Point 3)

d. 15°23'21"N 98°17'56"E (Point 4)

e. 15°23'22"N 98°18'12"E (Point 5)

f. 15°23'30"N 98°18'13"E (Point 6)

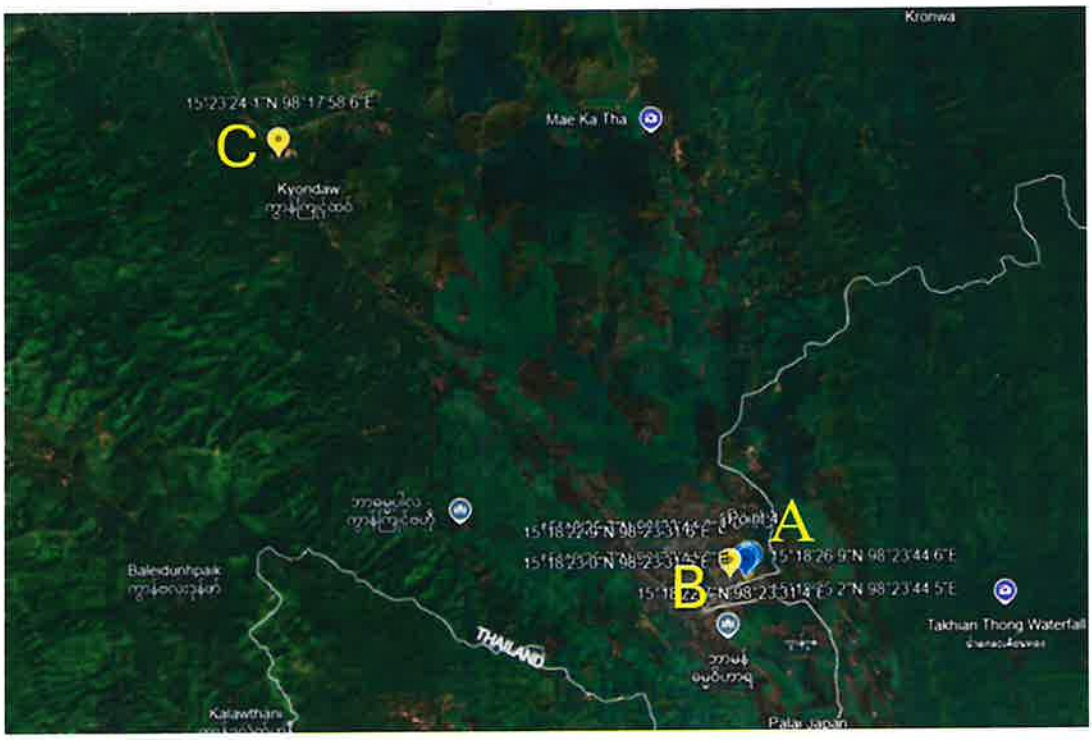


Figure 7 – Locations A, B, and C

51. According to reports from NGO-1, as of 2024, scam actors in the Myawaddy area relocated to the Three Pagodas Pass area due to pressure from the local junta. These individuals were reported to be higher level bosses. Because there was reportedly no infrastructure to support this relocation at the time, these individuals were reported to have resided in nearby hotels. NGO-1 reported observing one large compound taking shape a few miles outside the Three Pagodas Pass area (consistent with Location A). NGO-1 also reported Internet Protocol (IP) location information related to scam activity was observed in a specific hotel within the Three Pagodas area, which was consistent with bosses taking control of operations when victims sent funds to the scammers. NGO-1 cited a specific compound location that falls within the bounds of Location C (described above).

C. The WEALTHOB CIF Scam and U.S. Victims

i. IC3 Victim Reporting

52. From approximately January 2017 to November 2025, roughly 22 individuals, including U.S. persons, filed complaints with the FBI's IC3[43] relating to an alleged investment scheme that was using the brand "WEALTHOB." The aggregate estimated loss reported by the victims of this scheme is at least $6.7 million.

53. I have reviewed the complaints filed by these victims. These complaints all describe that, based on fraud perpetrated by the SUBJECT scammers, the victims moved fiat currency (USD) from bank accounts in the United States to cryptocurrency addresses through the means of wire transactions. Specifically, multiple victims described that, based on the advice of the SUBJECT scammers, they purchased cryptocurrency through the use of their U.S. bank accounts. Thereafter, these complaints describe that the cryptocurrency addresses in which the funds were deposited were later drained of funds and thereafter inaccessible to the victim. All of the victims described the use of U.S. wires (*e.g.*, Meta, bank transactions) as a means to perpetrate the fraud (as discussed further in Part III). For instance:

a. An Illinois-based victim (M.O.), who alleged losses of $255,000, stated that in February 2024, a woman named "Aurora" texted with M.O. They texted for about six months. Aurora told M.O. about the domain https://wealthob.cc/login for crypto investing. M.O. stated that Aurora had M.O. transfer funds from a U.S. bank account to a cryptocurrency exchange and then to a new wallet, which M.O. was thereafter locked out of.

b. A Virginia-based victim (VA Victim) was contacted by a scammer using the name

[43] IC3 provides an online tool by which victims of fraud can report their complaints to the FBI.

"Amy Pan" via text message in early 2024. During the course of their communication, the scammer instructed the victim on how to transfer funds from different cryptocurrency exchanges. Eventually, in or around April 2024, the scammer convinced the victim to transfer funds to an exchange called WEALTHOB. The victim believed he was engaging in stock trading and that his portfolio was growing. The scammer also showed the victim how he could make a withdrawal, a common tactic used in these types of schemes to lead the victim to believe he/she has made money trading and encourage them to invest more funds. I have reviewed tracing reports from the blockchain analysis,[44] which show the movement of funds from VA Victim's accounts in the United States to cryptocurrency addresses at a cryptocurrency exchange located outside the United States, as follows:

i. Between in or around April through in or around July 2024, the victim sent over $5 million worth of Bitcoin ("BTC"), a type of virtual currency, and ETH[45] from accounts in the United States to what the victim believed was his Wealthob account. The majority of the funds (approximately $4.2

[44] 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 cryptocurrencies, publicly record all of their transactions on a blockchain, including all of the known balances for each cryptocurrency address on the blockchain. Law enforcement can trace transactions on blockchains to determine which cryptocurrency addresses are sending and receiving particular cryptocurrency. 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.

[45] Ether ("ETH") is a cryptocurrency that is open-source and is distributed on a platform that uses "smart contract" technology

million) were sent from the victim's Strike account, via BTC, to a wallet address that appears to be unrelated to any legitimate trading platform.

ii. This BTC was then sent by the individual(s) with control of this wallet to other wallets and eventually transferred to wallets at Binance.com, a cryptocurrency exchange outside of the United States based in the Seychelles.

iii. The FBI received records from Binance.com related to the account receiving these funds, which identified the account as belonging to a female in China named 康秀花 (translated to Yasuhide Flower) (the "SUBJECT BINANCE ACCOUNT"). A review of the transaction history showed that the SUBJECT BINANCE ACCOUNT converted the BTC into USDT[46] and moved it to various wallets.

iv. The victim ultimately ended up transferring approximately $5 million in cryptocurrency through WEALTHOB from her/his accounts in the United States to wallets associated with the WHEALTHOB website. When the victim attempted to withdraw a larger sum later, the victim was told that his profit was 20,604,636.4 USDT and that he needed to pay taxes of 1,957,440.46 USDT.

v. The U.S. Attorney's Office for the Eastern District of Virginia obtained an Order of Forfeiture for nearly 2 million USDT tokens seized from three cryptocurrency addresses tied to this victim's losses. The property was

[46] Tether ("USDT") is a stablecoin pegged to the U.S. dollar

forfeited to the United States pursuant to 18 U.S.C. §§ 981(a)(1)(C) and (a)(1)(A).

54. According to information included in the IC3 complaints described above, online personas (SUBJECTS) approached the victims via unexpected text messages, pretending that they misdialed a number. The SUBJECTS would then shift their communications to encrypted communication applications such as WhatsApp or Telegram. Once trust was established with the victims, the SUBJECTS would introduce the topic of investing in cryptocurrency. The SUBJECTS claimed they had invested in cryptocurrency and told the fraud victims they could teach them how to invest in cryptocurrency.

55. In most of the cases, as detailed by the fraud victims, the SUBJECTS instructed the victims to set up accounts with cryptocurrency platforms, transfer funds from their financial accounts (in the United States) to the cryptocurrency platforms, and ultimately to a fraudulent trading platform domain: WEALTHOB.

56. The domain names the SUBJECTS provided to these fraud victims include wealthob[.]com, wealthob[.]cc, or wealthob[.]org.[47] Based on my experience investigating CIF, I know that these scams often use multiple similar domains with slight spelling differences and different top-level domains (the part of a domain that appears after the last dot). The FBI believes the CIF scheme using these domains with the brand WEALTHOB are all connected, as some of the fraud victims reported a change in the domain name from wealthob[.]com to wealthob[.]cc or wealthob[.]org. (As further described below, *see infra* Part III, through business records of U.S. providers, a phone number used in the WEALTHOB scheme was later tied geographically to the Three Pagodas Pass scam centers.)

[47] Public records searches show these domains are no longer active.

57. After investing in the trading platform, the fraud victims encountered problems when attempting to withdraw their funds through the trading platform. In an apparent effort to build trust and confidence in the trading platform, some of the fraud victims were allowed to withdraw funds. However, the fraud victims were ultimately unable to recover most or all of their funds from the trading platforms connected to WEALTHOB.

58. The following chart shows the transactions from U.S. financial institutions or U.S. money processors to cryptocurrency addresses associated with WEALTHOB in this scheme:

Transaction Date	Transaction Reported Amount	Origin Bank
3/10/2022	$8,000.00	U.S. Mobile Payment Service 1
3/10/2022	$8,000.00	U.S. Mobile Payment Service 1
3/10/2022	$8,000.00	U.S. Mobile Payment Service 1
5/3/2024	$11,576.00	U.S. Financial Institution 1
7/22/2024	$25,800.00	U.S. Financial Institution 1
7/17/2024	$16,500.00	U.S. Financial Institution 1
7/26/2024	$21,200.00	U.S. Financial Institution 1
7/11/2024	$18,790.00	Digital Currency Exchange Platform 1
6/28/2024	$15,000.00	U.S. Financial Institution 2
8/12/2024	$2,600.00	U.S. Financial Institution 3
7/10/2024	$200.00	U.S. Financial Services Platform 1
9/12/2024	$2,000.00	U.S. Financial Services Platform 1
9/17/2024	$2,000.00	U.S. Financial Services Platform 1
7/20/2024	$1,450.00	U.S. Financial Services Platform 1
7/23/2024	$1,000.00	U.S. Financial Services Platform 1
7/31/2024	$1,200.00	U.S. Financial Services Platform 1
9/5/2024	$1,000.00	U.S. Financial Services Platform 1
8/26/2024	$500.28	U.S. Financial Institution 4
8/28/2024	$2,000.00	U.S. Financial Institution 4
8/30/2014	$2,000.00	U.S. Financial Institution 4
8/30/2024	$7,500.00	U.S. Financial Institution 4

8/28/2024	$2,000.00	U.S. Financial Institution 1 Bank
8/27/2024	$2,900.00	Digital Currency Exchange Platform 2
8/29/2024	$2,900.00	Digital Currency Exchange Platform 2
8/30/2024	$5,000.00	Digital Currency Exchange Platform 2
8/30/2024	$2,864.54	U.S. Financial Institution 4
9/10/2024	$2,000.00	U.S. Financial Institution 1 Bank
9/13/2024	$200.00	U.S. Financial Institution 5 via U.S. Financial Institution 6
9/16/2024	$8,000.00	U.S. Financial Institution 5 via U.S. Financial Institution 6
9/25/2024	$750.00	U.S. Financial Institution 6
7/25/2024	$300,000.00	U.S. Financial Institution 6
10/9/2024	$110,000.00	U.S. Financial Institution 6
10/17/2024	$95,000.00	U.S. Financial Institution 6
9/20/2024	$400.00	U.S. Financial Institution 1 Bank
9/27/2024	$72.09	U.S. Financial Institution 1 Bank
10/8/2024	$31.08	U.S. Financial Institution 1 Bank
10/8/2024	$31.38	U.S. Financial Institution 1 Bank
10/10/2024	$1,029.90	U.S. Financial Institution 1 Bank
10/15/2024	$1,750.83	U.S. Financial Institution 1 Bank
10/24/2024	$1,956.81	U.S. Financial Institution 1 Bank
11/4/2024	$4,016.51	U.S. Financial Institution 1 Bank
11/12/2024	$4,634.55	U.S. Financial Institution 1 Bank
11/12/2024	$4,634.55	U.S. Financial Institution 1 Bank
10/8/2024	$9,600.00	U.S. Financial Institution 7
8/26/2024	$5,100.00	U.S. Financial Institution 8

59. Additionally, I have reviewed blockchain analysis of cryptocurrency deposited by the WEALTHOB victims (including by VA Victim, as described above) and have identified

approximately three cryptocurrency addresses[48] and numerous clusters[49] of cryptocurrency addresses related to the scheme. In general, my review of the analysis of the movement of funds is that the CIF victims in the United States generally deposited funds from U.S. financial institutions into a series of cryptocurrency addresses controlled by the SUBJECTS and/or their co-conspirators, and then the funds were sent to additional cryptocurrency addresses believed to be located outside of the United States in short order. Based on my training and experience, these transaction patterns are indicative of common tactics used in CIF schemes, and the flow of these funds indicates laundering activity to conceal the nature, location, source, ownership, or control of wire fraud proceeds.

i. FBI Undercover Employee Engagement with ALICE and WEALTHOB

60. In or around October 2024, an FBI Online Undercover Employee (OCE) communicated with an online persona name ALICE, believed to be a SUBJECT involved in the WEALTHOB scheme, via WhatsApp. ALICE instructed the OCE to register with a "short-term trading platform" using the website https://wealthob[.]com.

iii. Victim Engagement with WhatsApp Phone Number +1-850-305-2120

61. As detailed below, between approximately August 2024 and January 2025, SUBJECT(S) using the WhatsApp Phone Number +1-850-305-2120 targeted at least two individuals to invest in WEALTHOB. The circumstances surrounding these contacts bear a striking resemblance to the contacts between VA Victim and "Amy Pan," detailed above.

---

[48] A cryptocurrency address is an alphanumeric string that designates the virtual location on a blockchain where cryptocurrency can be sent and received. A cryptocurrency address is associated with a cryptocurrency wallet.

[49] A cluster is a collection of cryptocurrency addresses that is assessed to be held in the same cryptocurrency wallet or controlled by the same entity. These clusters were identified using a blockchain analytics tool.

62. **Victim 1.** On or about January 24, 2025, the FBI interviewed Victim 1, who reported communicating with the online persona named ALICE using WhatsApp number +1-850-305-2120, which also promoted the fraudulent trading platform wealthob.com to the FBI OCE. Victim 1 explained that on or about August 20, 2024, s/he received a text message from an unknown phone number, +1-657-291-7669. Victim 1 responded to the text message informing the individual they had the wrong number. The individual responded and continued the conversation and introduced herself as "ALICE."

63. Victim 1 and ALICE continued to communicate via text message in a friendly manner. ALICE then suggested they text via WhatsApp and provided Victim 1 with her WhatsApp phone number, +1-850-305-2120. In or around September 2024, ALICE suggested that Victim 1 learn how to conduct short term cryptocurrency trades. Victim 1 was suspicious and did not engage when ALICE suggested Victim 1 begin investing. By in or around early October 2024, Victim 1 and ALICE had stopped communicating.

64. On or about December 24, 2024, ALICE again contacted Victim 1. By approximately December 27, 2024, ALICE had again brought up the topic of investing in cryptocurrency.

65. On or about December 30, 2024, ALICE suggested Victim 1 begin short-term trading; ALICE suggested Victim 1 would make profits of 10-30%. ALICE said she used Digital Currency Exchange Platform 2 and U.S. Mobile Payment Service 1 to purchase cryptocurrency and sent Victim 1 a hyperlink to review material. The hyperlink was labeled "200100" but did not identify a domain name. Victim 1 did not click on the link as it seemed suspicious.

66. **Victim 2.** On February 6, 2025, the FBI interviewed "Victim 2," who also had reported communicating with an online persona named ALICE using WhatsApp number +1-850-305-2120.

67. According to Victim 2, ALICE initially contacted Victim 2 via text message and apologized stating she had the wrong number. ALICE thereafter began communicating with Victim 2 and suggested they move the conversation to WhatsApp. Victim 2 and ALICE communicated for approximately one month, during which time ALICE introduced the idea of investing in cryptocurrency. Victim 2 never invested in cryptocurrency.

68. According to screenshots of WhatsApp chats provided by Victim 2, on or about January 2, 2025, ALICE claimed she was involved in short term option investments in gold and cryptocurrency and suggested Victim 2 could purchase cryptocurrency via U.S. Financial Services Platform 1 or Digital Currency Exchange Platform 2. ALICE then suggested Victim 2 begin investing with a small amount of $200-$10,000.

69. On or about January 4, 2025, ALICE sent Victim 2 two images allegedly demonstrating ALICE's investment profits from the same day. The images ALICE shared with Victim 2 indicated that ALICE had earned $5,530 from short term option investments.

IV. Use of U.S. Wires to Commit the CIF Fraud and the Connection to the Three Pagoda Pass Scam Centers

70. As explained below, there is probable cause to believe that the perpetrators of the WEALTHOB CIF fraud scheme were connected to the Three Pagodas Pass scam centers and that the SUBJECTS have been using U.S. wires to commit CIF fraud. Moreover, the perpetrators have used the services of U.S. providers, including U.S. cellular phone providers, Meta Platforms, Inc. (Meta) and SpaceX to commit these crimes.

A. Meta and U.S. Cellular Phone Providers

71. As further described above at Part III.C, the FBI has received at least 22 CIF complaints referencing the brand WEALTHOB. A common mode of the initial contact was a text message sent to the U.S. victim over their U.S. cellular phone provider. Thereafter, the SUBJECTS shifted communications with the U.S. victims to encrypted messaging applications, including multiple instances of SUBJECTS using WhatsApp to communicate with the victims.

72. Meta is a provider of an electronic communication service, as defined in 18 U.S.C. § 2510(15), and/or a remote computing service, as defined in 18 U.S.C. § 2711(2). Meta is a provider of multiple social media networking sites, including Facebook and Instagram, and the encrypted messaging application WhatsApp.

73. On or about November 24, 2024, Meta issued a statement acknowledging that its platforms, including WhatsApp, had been susceptible to use by CIF scam compounds. Meta noted that, in 2024 alone, it had "taken down over two million accounts associated with scam centers in Cambodia, Myanmar, Laos, the United Arab Emirates and the Philippines."[50]

B. SpaceX

74. SpaceX is a provider of an electronic communication service, as defined in 18 U.S.C. § 2510(15), and/or a remote computing service, as defined in 18 U.S.C. § 2711(2). According to publicly accessible company information, SpaceX is a provider of satellite-based internet service through Starlink. Starlink is a Low Earth Orbit ("LEO") satellite communications constellation. Consumer service for Starlink began in or around October 2020 and today, Starlink provides internet service in approximately numerous different markets around the world.

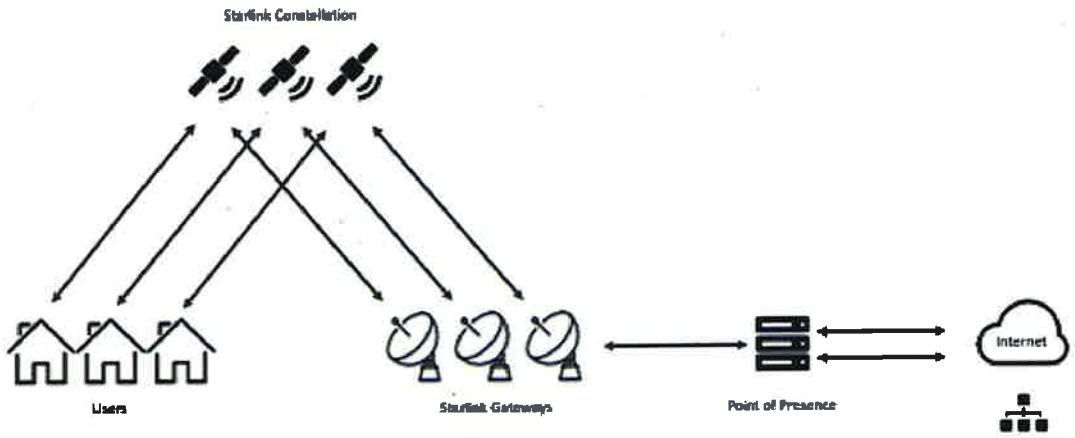
---

[50] Meta, Cracking Down on Organized Crime Behind Scam Centers, https://about.fb.com/news/2024/11/cracking-down-organized-crime-scam-centers/ (Nov. 24, 2024).

75. Starlink provides fiber-like connectivity for users, with average bandwidth speeds of approximately 100 Megabits per second download and 20 Megabits per second upload speeds. These speeds and low latency enable customers to participate in video calls, streaming services, and other high data rate activities. The Starlink constellation is comprised of more than 5,000 satellites deployed in LEO. Users access the internet via user terminals. These terminals communicate with the constellation of Starlink satellites. A Starlink user terminal comes equipped with a power supply and WiFi router. A Starlink user maintains an account with SpaceX, located in California, and pays a subscription price for the satellite internet service.

Figure 7 – SpaceX Starlink Terminal.

76. The Starlink satellites then communicate to Starlink Gateways or ground stations, which in turn route the data through ground-based international infrastructure. The network architecture is shown in the diagram below:



77. SpaceX maintains customer information related to services provided to each terminal. This includes basic subscriber information, *e.g.*, customer names, email accounts, phone numbers, account identifiers and types, activation dates, start and end service dates, payment methods/processors, service addresses, terminal IDs, Starlink router IDs, user terminal network data with source IP address(es) (identifying which user terminal used which IP address at what time), and terminal Basic Service Set Identifier (BSSID).

78. A general overview of the Starlink architecture, including Starlink user terminals, the satellite constellation, ground stations, and the H3 grid system is show below:

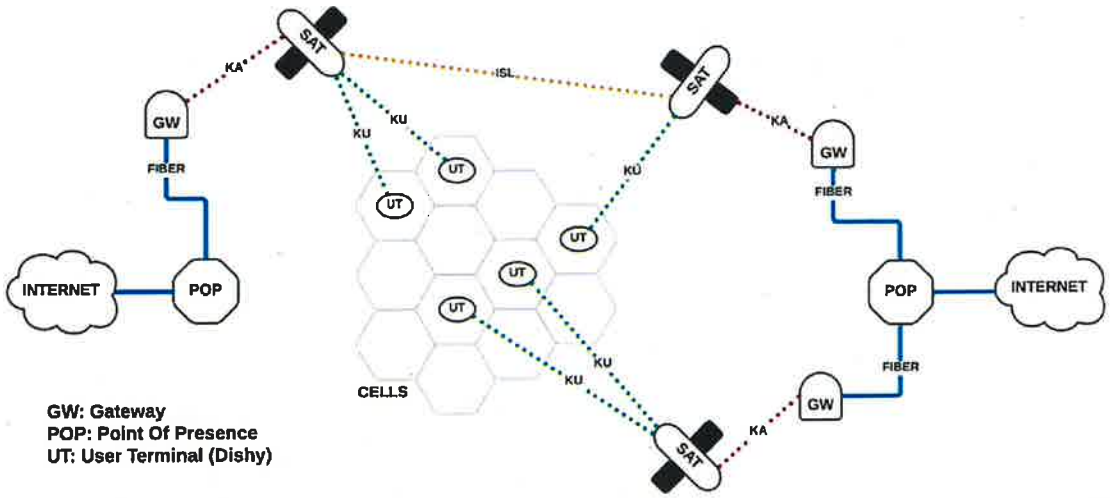


Figure 8 – SpaceX Starlink Connection Chart.

79. Starlink stores the following data pertaining to a customer: hardware identification, account identification, personal customer information, Network Address Translation (NAT) binding records with source Internet Protocol (IP) address, and cell location.

80. Starlink stores unique identifiers for its terminals, including the user terminal ID, router number, KitID, Account ID, user terminal serial number, and router serial number.

81. Starlink does not collect or track precise GPS location for its services. Instead, Starlink has divided the earth into a set of hexagons, or "cells," using Uber's H3 spatial Index, of two rough sizes: H5, with an average circumradius of 10 km, and H6, with an average circumradius of 3.7 km. Starlink adjusts the cell size based on the number of customers in a particular area. Generally, a populated area is allocated a smaller cell, and very rural or maritime cells are allocated larger cells. Depending on several factors, Starlink will change the cell size / cell dimensions we allocate to different points on earth.

i. Use of Starlink by Scam Compounds in Burma

82. Publicly available reporting states that Starlink is being openly used by scam compounds in Burma:

> [C]riminals running multibillion-dollar empires across Southeast Asia appear to be widely using the [Starlink] satellite internet network. At least eight scam compounds based around the Burma-Thailand border region are using Starlink devices, according to mobile phone connection data . . . . Between November 2024 and the start of February [2025], hundreds of mobile phones logged their locations and use of Starlink at known scamp compounds more than 40,000 times, according to mobile phone data, which was collected by an online advertising industry tool.[51]

[51] *Elon Musk's Starlink Is Keeping Modern Slavery Compounds Online*, Wired (Feb. 27, 2025), https://www.wired.com/story/starlink-scam-compounds.

The same reporting noted that "white Starlink satellite dishes" are visible on rooftops of scam compounds, and often "dozens" are placed on the same roof.[52] Additionally, the combat in Burma has resulted in "frequent internet shutdowns" and thus Starlink has become a crucial means of connectivity and stable internet.[53] Additionally, the Thai government has been attempting to disrupt traditional internet connections to Burmese scam compounds, making Starlink an alternative.[54]

83. On or about October 22, 2025, SpaceX confirmed that it had removed thousands of devices from its platform that it suspected were operating in Burmese scam compounds.[55]

ii. Starlink Terminals Associated with the Three Pagodas Pass Scam Centers

84. ***Starlink Records.*** Through review of Starlink business records, investigators tied the WhatsApp phone number used by ALICE (+1-850-305-2120) to Location A. In December 2024, the FBI served WhatsApp with a § 2703(d) order and a pen register/trap and trace (PRTT) order for subscriber information, account records, and communications transactional records associated with WhatsApp phone number +1-850-305-2120, used by SUBJECT ALICE to promote WEALTHOB "investments" to Victims 1 and 2 (as discussed above).

85. The FBI's review of transactional records sent to and from WhatsApp number +1-850-305-2120 found that, on or about December 18, 2024, the user of this number used a SpaceX (Starlink) IP address 65.181.16.7 with port number 29642. As discussed above, ALICE used this

---

[52] *Id.*
[53] *Id.*
[54] *Id.*
[55] *Elon Musk's SpaceX says it has cut Starlink services at Myanmar scam compounds*, NBC News (Oct. 23, 2024), https://www.nbcnews.com/world/asia/spacex-disables-2500-starlink-terminals-scam-compounds-myanmar-rcna239286.

number to contact Victim 1 several times in December 2024. Activity on the surrounding dates shows use of VPN service and Thailand broadband networks (as noted below).

86. Records provided by SpaceX on or about December 20, 2024, identified the following subscriber information for the Starlink terminal associated with IP address 65.181.16.7 and port number 29642. This IP address and port were observed among internet activity using VPN and non-U.S. broadband networks, which revealed the following subscriber information:

Contact(s):

- Contact Name: sam Li
- Contact Email: er116133@gmail.com
- Contact Phone: +639452390647

Account Number: ACC-4252880-57542-17 (**TARGET ACCOUNT 1**)

Device(s):

- Starlink User Terminal ID: 01000000-00000000-0088b280 (**TARGET PROPERTY 1**)

87. Additionally, in 2025, Starlink provided additional records for customer information associated with **TARGET ACCOUNT 1**. The FBI's review identified additional Starlink accounts and Starlink terminals linked to the same phone number (+639452390647) that was associated with **TARGET ACCOUNT 1,** including **TARGET ACCOUNT 2** listed below. While **TARGET ACCOUNT 2** was held under a different name and email address, as shown below, however, **TARGET ACCOUNT 2**'s registrant name was an inversion of the name used for **TARGET ACCOUNT 1** ("sam Li" and "li sam") and utilizes the common phone number:

STARLINK CUSTOMER INFORMATION ASSOCIATED WITH +639452390647

Contact(s):

Contact Name: li sam

Contact Email: samli22645@gmail.com

Contact Phone: +639452390647

Account Number: ACC-4232182-53915-10 (**TARGET ACCOUNT 2**)

Device(s):

1) Starlink User Terminal ID: 01000000-00000000-0088a66f (**TARGET PROPERTY 2**)
2) Starlink User Terminal ID: 01000000-00000000-0088077c (**TARGET PROPERTY 3**)
3) Starlink User Terminal ID: 01000000-00000000-008081a9 (**TARGET PROPERTY 4**)
4) Starlink User Terminal ID: 01000000-00000000-0051b9f2 (**TARGET PROPERTY 5**)
5) Starlink User Terminal ID: 01000000-00000000-00d377c3 (**TARGET PROPERTY 6**)
6) Starlink User Terminal ID: 01000000-00000000-008083ff (**TARGET PROPERTY 7**)
7) Starlink User Terminal ID: 01000000-00000000-00dcedf2 (**TARGET PROPERTY 8**)
8) Starlink User Terminal ID: 01000000-00000000-009567b3 (**TARGET PROPERTY 9**)

The FBI's review of Starlink's business records revealed that the two Starlink accounts (**TARGET ACCOUNTS 1 and 2**) and their nine associated Starlink terminals (**TARGET PROPERTY 1-9**) were also linked to the following Basic Service Set Identifiers (BSSIDs):[56]

BSSIDs FOR STARLINK TERMINALS LINKED TO +639452390647

[56] A BSSID is a unique identifier, typically the MAC address, assigned to a specific access point or router within a designated WiFi network. The BSSID serves as a technical fingerprint of a specific WiFi access point allowing devices to distinguish access points on the same service set identifier (SSID) for a wireless local area network (WLAN).

Phone Number	Starlink Account	Terminal	BSSIDs
639452390647	ACC-4252880-57542-17	01000000-00000000-0088b280	02:6b:de:22:37:80
			02:6b:de:32:37:80
	ACC-4232182-53915-10	01000000-00000000-0088a66f	76:c7:20:2a:26:9c
			76:c7:20:3a:26:9c
		01000000-00000000-0088077c	2e:f1:2b:22:f2:b0
			2e:f1:2b:32:f2:b0
		01000000-00000000-008081a9	c2:1b:1f:22:0a:f2
			c2:1b:1f:32:0a:f2
		01000000-00000000-0051b9f2	fa:cb:0a:2a:05:b0
			fa:cb:0a:3a:05:b0
			ce:90:bd:25:f3:7b
			ce:90:bd:35:f3:7b
		01000000-00000000-00d377c3	5e:7e:38:20:f5:76
			5e:7e:38:30:f5:76
		01000000-00000000-008083ff	56:25:ce:27:0a:17
			56:25:ce:37:0a:17
		01000000-00000000-00dcedf2	c2:7f:ba:2c:46:0e
			c2:7f:ba:3c:46:0e
		01000000-00000000-009567b3	1e:31:ca:2c:76:da
			1e:31:ca:3c:76:da

89. According to open-source information, Apple maintains a database of WiFi BSSIDs and corresponding geolocations. This database facilitates location services for Apple devices when global positioning systems ("GPS") are unavailable. This database is derived from Apple devices when devices submit nearby WiFi BSSIDs with corresponding geolocation (and thus not all WiFi facilities will be present in the tool). Researchers have reverse engineered the application programming interface (API) that Apple devices use to query for the geolocation given a WiFi BSSID. In or around January 2025,[57] the FBI queried the open-source Apple API database server

[57] I attempted to review the same BSSIDs in the Apple API tool in November 2025, before filing this affidavit. However, several of the terminals no longer showed up in the API tool. Based on my training and experience, there are numerous reasons why the devices may no longer be available in the data set, including that there were no Apple devices using those BSSIDs at that time.

for the above Starlink BSSIDs. For those with information within the Apple API tool, each BSSID plotted within the area of the Three Pagodas Pass scam centers described above, as follows:

Target Acct. No.	Target Property No.	BSSID	Latitude	Longitude	Location
1	1	02:6b:de:22:37:80	15.30745792	98.39572906	Location A
2	2	76:c7:20:2a:26:9c	15.30743122	98.39572143	Location A
2	3	2e:f1:2b:22:f2:b0	15.39002609	98.29960632	Location C
2	4	c2:1b:1f:22:0a:f2	N/A	N/A	N/A
2	5	ce:90:bd:25:f3:7b	15.30714702	98.39559936	Location A
2	5	ce:90:bd:35:f3:7b	15.30714797	98.39556121	Location A
2	6	5e:7e:38:20:f5:76	15.30634593	98.39211273	Location B
2	7	56:25:ce:27:0a:17	15.3063097	98.39204406	Location B
2	8	c2:7f:ba:2c:46:0e	15.30637931	98.39208221	Location B
2	9	1e:31:ca:2c:76:da	N/A	N/A	N/A

90. That **TARGET PROPERTY 1**, used to attempt scams on the OCE and Victims 1 and 2, is co-located with **TARGET PROPERTY 2** and **5**, further shows the connection between these **TARGET ACCOUNTS** and the use of the **TARGET PROPERTYs** for illicit purposes. Moreover, the connections between **TARGET ACCOUNT 1** and **TARGET ACCOUNT 2** show probable cause that both accounts and their contents are being used as part of the wire fraud conspiracy and money laundering conspiracy schemes.

91. Additionally, the location of the Starlink terminals associated with **TARGET ACCOUNTS 1** and **2** is consistent with the information provided by CW-1 that scam activities in the area began by using various hotels and locations (Locations A and B) and then moved their operations outside of town (Location C). Similarly, as noted above, NGO-1 also reported that IP location information related to scam activity was observed in a hotel within the Three Pagodas area, which was consistent with bosses taking control of operations when victims sent funds to the scammers. NGO-1 cited a specific compound location that falls within the bounds of Location C

(described above). Based on my training and experience, I know that when victims send funds to the scammers, they typically do so via cryptocurrency, which leads to various efforts to hide the nature, source, and location of the funds (as was the case for VA Victim, discussed above).

92. ***Imagery of Location A.*** Investigators consulted with a company doing business in imagery analysis to obtain high resolution satellite imagery of Location A.[58] The company's imagery expert obtained imagery from October 2025 showing multiple buildings in the area. Those buildings contained numerous items located on the roofs of all the buildings, which the expert opined was consistent with Starlink satellite terminals. The expert opined that there were approximately 26 Starlink terminals on the roofs of the buildings.

Figure 9 – Analysis of Starlink Terminals at Location A.

[58] The expert company is in the business of analyzing high resolution satellite imagery and provides imagery and analysis to the government, as well as to private market corporate clients. The expert has reviewed satellite imagery for multiple scam center compounds in Burma, including the scam center near Three Pagodas Pass, as well as video footage showing certain compounds in closer proximity, to conduct a general analysis of the location of Starlink terminals. The expert is also personally familiar with Starlink terminals, including their shape and size. The expert was paid for a report issued related to this work.

93. Further the expert obtained open-source WiFi network information from Instabridge, a Swedish-based application, showing at least three WiFi networks that individuals reported were operating at coordinates within the Location A. This data is consistent with use of Starlink terminals Location A to connect to the internet.

V. Involvement of the TARGET PROPERTY and the TARGET ACCOUNTS in Money Laundering

94. As described above, the WEALTHOB CIF scam, which IC3 complaints tie to 22 different victims, is a wire fraud scam. The CIF scam is a scheme to defraud victims by unlawfully obtaining their funds under the false or fraudulent pretense and representations that victims are sending their funds to SUBJECTS as part of an "investment" opportunity, when in reality, those funds are just being stolen. These false or fraudulent representations are being transmitted to the victims using wires in interstate or foreign commerce.

95. Based on my training and experience and publicly available reporting, CIF scams are not single actor operations, but rather, as described above, function as criminal conspiracies involving multiple individuals who agree to manage and operate scam centers in order to defraud victims, especially in the United States. Therefore, I believe that CIF scams such as WEALTHOB are also wire fraud conspiracies.

96. The WEALTHOB scam, like other CIF scams, consisted of SUBJECTS fraudulently convincing U.S. victims to send them cryptocurrency from their cryptocurrency accounts at U.S.-based cryptocurrency exchanges. Based on the records described above linking WEALTHOB SUBJECT ALICE to Location A in Burma, I believe that the WEALTHOB CIF scam is being run out of Burma. The SUBJECTS thus were soliciting U.S. victims to transfer their funds from the United States to cryptocurrency addresses controlled by SUBJECTS located abroad

to promote the carrying on of the aforementioned wire fraud activity, in violation of 18 U.S.C. § 1956(a)(1)(A)(i), (a)(2)(A).

97. Furthermore, based on my training and experience, and open-source reporting on CIF scams, I know that the money laundering component of CIF scams also involves multiple individuals conspiring together to siphon funds from U.S. victims to co-conspirators located overseas to promote the underlying wire fraud and wire fraud conspiracy. After receiving victim funds from the United States, CIF actors normally then send the cryptocurrency to multiple other cryptocurrency addresses outside the United States, and often various exchanges and blockchains, in an apparent effort to conceal the nature, location, source, ownership, or control of the criminal proceeds, all in violation of 18 U.S.C. § 1956(a)(1)(A)(i), (a)(B)(i).

98. VA Victim of the WEALTHOB CIF scam provided law enforcement with the cryptocurrency addresses to which the victim was directed to send funds as part of the scam. VA Victim reported losses due to sending funds to the SUBJECTS. I have reviewed blockchain analysis of these cryptocurrency addresses, and they show deposits believed to be from this victim. After receiving these funds, the cryptocurrency was soon thereafter converted to USDT and further transferred to additional addresses. Based on my training and experience and conversation with other agents, I believe this is consistent with an effort to disguise, conceal, and obfuscate the origin, location, and ownership of the stolen funds.

99. The operation of this money laundering conspiracy depends on multiple pieces of SUBJECT-controlled property, with one of the most essential being the accounts and devices enabling internet access. CIF scams such as WEALTHOB require actors to have internet access to communicate with U.S. victims and facilitate the transfer of their funds overseas to promote the underlying wire fraud scams. As described above, Starlink accounts, such as the **TARGET**

ACCOUNTS, provide CIF SUBJECTS with the internet service they need to induce U.S. victims to send their funds overseas as part of fraudulent investment opportunities. These accounts are particularly important in areas such as Payathonzu and surrounding areas in Burma where there are significantly limited internet options to run scam center operations.

100. While **TARGET ACCOUNT 1** is directly connected to the money laundering conspiracy via its use by SUBJECT ALICE, the unidentified SUBJECT(s) using the names "sam Li" and "li sam" are believed to operate an additional account, **TARGET ACCOUNT 2**, which also shares a common registrant phone number and is connected to a terminal that is believed to have been located in an additional scam center (Location C).

101. Therefore, the **TARGET PROPERTY** and the **TARGET ACCOUNTS** play a substantial role, and is therefore involved in, the WEALTHOB wire fraud and money laundering conspiracies focused on transferring U.S. victims' funds abroad to further promote the WEALTHOB wire fraud scheme.

VI. Summary of Probable Clause and Conclusion

102. Based on the foregoing, there is probable cause to believe that unknown overseas individuals have conspired to violate the wire fraud and money laundering statutes, as follows:

a. The DKBA and other unknown individuals established scam centers in the area of the Payathonzu, Burma, through which U.S. persons were targeted for CIF scams related to the WEALTHOB domains by SUBJECTS, to include ALICE. U.S. persons fell prey to the scams, reportedly investing at least $6.7 million in cryptocurrency into cryptocurrency addresses tied to the WELATHOB website.

b. The SUBJECTS utilized U.S. wires to communicate with their U.S. victims, to include cellular phone networks (through text messaging) and WhatsApp, while the SUBJECTS used a phone number tied to **TARGET PROPERTY 1** and **2**.

c. The SUBJECTS used U.S. wires to connect to the Internet to perpetrate the scheme. In particular,

   i. ALICE used **TARGET PROPERTY 1** and **TERMINAL 1** to solicit U.S. victims;

   ii. **TERMINAL 1** was physically located at the Three Pagodas Pass Scam Location A;

   iii. **TARGET ACCOUNT 2** used the same phone number as **TARGET ACCOUNT 1** and used an inverted version of the same customer name, indicating that they are likely controlled by the same user. According to location data, at least two of the terminals registered to **TARGET ACCOUNT 2** (**TERMINALS 2** and **5**) were also located at Three Pagodas Pass Scam Location A. Open-source reporting, human reporting, and satellite imagery are consistent with the operation of scam centers in these areas.

d. Accordingly, there is probable cause to believe that the SUBJECTS conspired to commit wire fraud, in violation of 18 U.S.C. §§ 1343, 1349.

e. Further, U.S. victims were defrauded through the movement of cryptocurrency from their financial accounts, located in the United States, to cryptocurrency addresses associated with the WEALTHOB scam. Next, those cryptocurrency funds were moved to other unhosted cryptocurrency addresses outside the United

States, in an apparent effort to launder the funds, in violation of 18 U.S.C. § 1956(a)(1)(A)(i), (a)(2)(A) & (h).

f. **TARGET ACCOUNTS 1** and **2** and their associated terminals provided the SUBJECTS with the internet connections needed to connect with U.S. victims and defraud them of funds sent abroad in CIF schemes. Therefore, they are = facilities involved in a conspiracy to commit wire fraud and further are involved in a conspiracy to commit money laundering.

103. Thus, there is probable cause to believe the **TARGET PROPERTY** and **TARGET ACCOUNTS** in **Attachment A** are being used by SUBJECTS located outside the United States as instrumentalities to facilitate the crimes of wire fraud and conspiracy to commit wire fraud, 18 U.S.C. §§ 1343, 1349, against U.S. victims. The **TARGET PROPERTY** and **TARGET ACCOUNTS** are also property involved in a conspiracy to commit money laundering, and therefore the **TARGET ACCOUNTS** and their associated terminals (the **TARGET PROPERTY**) are subject to seizure as property involved in a violation of 18 U.S.C. § 1956(a)(1)(A)(i),(a)(2)(A) & (h). Such property is subject to seizure and forfeiture under 18 U.S.C. §§ 981(a)(1)(A), 982(a)(1).

104. I respectfully request that the Court issue an order seizing the **TARGET ACCOUNTS** and order SpaceX to effect seizure on the **TARGET PROPERTY** by freezing and/or disconnecting the Starlink terminals from the SpaceX network.

VII. Seizure Procedures

105. SpaceX maintains the ability to terminate or suspend Starlink accounts and services.[59] As detailed in Attachment A, upon execution of the seizure warrant, SpaceX shall be directed to restrain and lock the **TARGET PROPERTY** and the **TARGET ACCOUNTS** pending transfer of all right, title, and interest in the forfeitable property in the **TARGET PROPERTY** and the **TARGET ACCOUNTS** to the United States upon completion of forfeiture proceedings, to ensure that access to or manipulation of the forfeitable property cannot be made absent court order or, if forfeited to the United States, without prior consultation by the United States.

106. As detailed in Attachment A, as part of restraining and locking of the **TARGET PROPERTY** and the **TARGET ACCOUNTS**, SpaceX will be directed to disable service to the terminals associated with the **TARGET PROPERTY** and the **TARGET ACCOUNTS**, preventing the terminals from being able to be used with other Starlink accounts.

VIII. Request to Submit Warrant by Telephone or Other Reliable Electronic Means

107. 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.

108. Because the warrant will be served on SpaceX, which controls the **TARGET PROPERTY** and the **TARGET ACCOUNTS**, and SpaceX, thereafter, at a time convenient to it,

---

[59] Starlink Terms of Service, STARLINK, https://starlink.com/legal/documents/DOC-1020-91087-64?srsltid=AfmBOoqjCAESNvwVCkAThavGo6zKDO_M6rZxz6tSjJjy7k5sIRRKJIdZ (last accessed November 7, 2025).

will lock the **TARGET PROPERTY** and the **TARGET ACCOUNTS**, there exists reasonable cause to permit the execution of the requested warrant at any time of day or night.

Respectfully submitted,

Stephanie Streeter

Special Agent Stephanie Streeter
Federal Bureau of Investigation

Subscribed and sworn pursuant to Fed. R. Crim. P. 4.1 and 41(d)(3) on November 12, 2025.

HONORABLE G. MICHAEL HARVEY
UNITED STATES MAGISTRATE JUDGE
DISTRICT OF COLUMBIA

ATTACHMENT A: PROPERTY TO BE SEIZED

I. Seizure Procedures

The seizure warrant will be transmitted electronically to personnel of the provider listed in Section II ("PROVIDER"), who is directed to make any changes necessary to restrain and lock the TARGET PROPERTY and TARGET ACCOUNTS pending transfer of all rights, title, and interest in the TARGET PROPERTY and TARGET ACCOUNTS to the United States upon completion of forfeiture proceedings.

Upon seizure of the TARGET PROPERTY and TARGET ACCOUNTS, the PROVIDER shall take all steps necessary to restrain and lock the TARGET PROPERTY and TARGET ACCOUNTS to ensure that access to or manipulation of the forfeitable property cannot be made absent a court order or, if forfeited to the United States government, without prior consultation with the United States.

The PROVIDER shall disable all access to the TARGET PROPERTY and TARGET ACCOUNTS, including services provided to all Starlink terminals associated with the TARGET PROPERTY and TARGET ACCOUNTS, except as necessary for the Subject Provider to comply with any additional legal process or engage in normal business operations.

II. PROVIDER

Space Exploration Technologies, Inc. (SpaceX)
1 Rocket Road
Hawthorne, CA 90250

III. The Target Accounts

SpaceX is directed to give effect to the seizure by suspending the accounts with the following identifiers, suspending all service to Starlink terminals associated with the accounts, including those terminals listed below, and suspending access to the same by the customer:

- ACC-4252880-57542-17
- ACC-4232182-53915-10

IV. The Target Property

SpaceX is directed to give effect to the seizure by suspending access of the following Starlink terminals to the SpaceX network:

- Starlink User Terminal ID: 01000000-00000000-0088b280 (**Target Property 1**)
- Starlink User Terminal ID: 01000000-00000000-0088a66f (**Target Property 2**)
- Starlink User Terminal ID: 01000000-00000000-0088077c (**Target Property 3**)
- Starlink User Terminal ID: 01000000-00000000-008081a9 (**Target Property 4**)
- Starlink User Terminal ID: 01000000-00000000-0051b9f2 (**Target Property 5**)
- Starlink User Terminal ID: 01000000-00000000-00d377c3 (**Target Property 6**)
- Starlink User Terminal ID: 01000000-00000000-008083ff (**Target Property 7**)
- Starlink User Terminal ID: 01000000-00000000-00dcedf2 (**Target Property 8**)
- Starlink User Terminal ID: 01000000-00000000-009567b3 (**Target Property 9**)