AO 91 (Rev. 08/09) Criminal Complaint

UNITED STATES DISTRICT COURT

for the

District of Columbia

United States of America
v.
Huang Xingshan
DOB: [redacted]

Defendant(s)

Case: 1:26-mj-00018
Assigned To: Judge Upadhyaya, Moxila A.
Assign. Date: 1/30/2026
Description: COMPLAINT W/ARREST WARRANT

CRIMINAL COMPLAINT

I, the complainant in this case, state that the following is true to the best of my knowledge and belief.

On or about the date(s) of January 2023 - January 2026 in the jurisdiction of the District of Columbia, the defendant(s) violated:

Code Section	*Offense Description*
18 U.S.C. §§ 1343, 1349	(Wire fraud conspiracy)

This criminal complaint is based on these facts:

SEE AFFIDAVIT

☐ Continued on the attached sheet.

[redacted], Special Agent
Printed name and title

Sworn to before me and signed in my presence.

Date: 01/30/2026

Judge's signature

City and state: Washington, D.C.

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

AO 442 (Rev. 01/09) Arrest Warrant

UNITED STATES DISTRICT COURT

for the

District of Columbia

United States of America
v.
Huang Xingshan

Case No. 26-MJ-18

Defendant

ARREST WARRANT

To: Any authorized law enforcement officer

YOU ARE COMMANDED to arrest and bring before a United States magistrate judge without unnecessary delay

(name of person to be arrested) Xingshan Huang,

who is accused of an offense or violation based on the following document filed with the court:

☐ Indictment ☐ Superseding Indictment ☐ Information ☐ Superseding Information ☑ Complaint

☐ Probation Violation Petition ☐ Supervised Release Violation Petition ☐ Violation Notice ☐ Order of the Court

This offense is briefly described as follows:
18 U.S.C. §§ 1343, 1349 (Wire fraud conspiracy)

REVISED
10:52 am, Apr 01, 2026

Date: 01/30/2026

Issuing officer's signature

City and state: Washington, D.C.

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

Return

This warrant was received on *(date)* _____, and the person was arrested on *(date)* _____
at *(city and state)* _____.

Date: _____

Arresting officer's signature

Printed name and title

This second page contains personal identifiers provided for law-enforcement use only and therefore should not be filed in court with the executed warrant unless under seal.

(Not for Public Disclosure)

Name of defendant/offender: Huang Xingshan

Known aliases: "Ah Zhe"

Last known residence: Thailand

Prior addresses to which defendant/offender may still have ties: unknown

Last known employment: unknown

Last known telephone numbers: unknown

Place of birth: People's Republic of China

Date of birth: [redacted]

Social Security number: none

Height: Unknown Weight: Uknown

Sex: Male Race: Asian

Hair: Black Eyes: Brown

Scars, tattoos, other distinguishing marks: unknown

History of violence, weapons, drug use: unknown

Known family, friends, and other associates *(name, relation, address, phone number)*:

FBI number:

Complete description of auto:

Investigative agency and address: Federal Bureau of Investigation [redacted]

Name and telephone numbers (office and cell) of pretrial services or probation officer *(if applicable)*:

Date of last contact with pretrial services or probation officer *(if applicable)*:

Case: 1:26-mj-00018
Assigned To: Judge Upadhyaya, Moxila A.
Assign. Date: 1/30/2026
Description: COMPLAINT W/ARREST WARRANT

AFFIDAVIT IN SUPPORT OF AN ARREST

I, [redacted], being first duly sworn, hereby depose and state as follows:

INTRODUCTION

1. I make this affidavit in support of a warrant to search the arrest of HUANG Xing Shan, also known as "Ah Zhe" (HUANG), and JIANG Wen Jie, also known as "Jiang Nan" (JIANG), for violations of violations of 18 U.S.C. §§ 1343, 1349 (Wire fraud conspiracy). Specifically, the defendants and others (generally, "the conspirators") were involved in a cryptocurrency investment fraud (CIF), run out of multiple compounds in Burma ("scam compounds"), wherein the workers were held against their will and directed to defraud U.S. persons via the use of U.S. wires. The conspirators were operating these scam operations under a specific business name ("Company-1").

2. Unless otherwise noted, wherever in this affidavit I assert that a statement was made, that statement is described in substance and is not intended to be a verbatim recitation of such statement. Wherever in this affidavit I quote statements, those quotations have been taken from draft translations which are subject to further revision.

3. I am a Special Agent with the Federal Bureau of Investigation (FBI), New York Field Office, and have been so employed since January 2015. As a Special Agent, I have investigated numerous violations of federal law, including but not limited to matters involving financial crimes and money laundering. Before joining the FBI, I was a [redacted] As such, I am an "investigative or law enforcement officer" of the United States within the meaning of 18 U.S.C. § 2510(7), that is, an officer of the United States who is empowered by law to conduct investigations of, and to make arrests for, offenses enumerated in 18 U.S.C. § 2516.

4. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents, witnesses, and agencies. Specifically, I am familiar with the facts and circumstances set forth below from my participation in the investigation; my review of the investigative file; my interviews with witnesses; my review of summaries of interviews with witnesses, including victims; a review of records, including digital evidence; and discussions with other law enforcement officials. 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.

5. Unless otherwise stated, the conclusions and beliefs I express in this affidavit are based on my training, experience, and knowledge of the investigation, and reasonable inferences I've drawn from my training, experience, and knowledge of the investigation.

JURISDICTION, STATUTES, & VENUE

6. This Court has jurisdiction to issue the requested warrant because it is a "court of competent jurisdiction" as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A), and (c)(1)(A). Specifically, the Court is "a district court of the United States . . . that – has jurisdiction over the offense being investigated." 18 U.S.C. § 2711(3)(A)(i). As discussed more fully below, 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.

7. Section 1343 of Title 18 of the U.S. Code 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." Section 1349 of Title 18 of the U.S. Code criminalizes the conspiracy to commit wire fraud, as defined in Section 1343.

8. Venue is also proper within this judicial district pursuant to 18 U.S.C. § 3238. 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.

THE DEFENDANTS

9. INDIVIDUAL-1 was a Chinese national residing in Burma until approximately November 2025.

10. HUANG Xing Shan, also known as "Ah Zhe," was a Chinese national residing in Burma until approximately November 2025. HUANG is currently in custody of the government of Thailand ("Thailand") for illegally entering Thailand.

11. JIANG Wen Jie, also known as "Jiang Nan," was a Chinese national residing in Burma until approximately November 2025. HUANG is currently in custody of the government of Thailand ("Thailand") for illegally entering Thailand.

PROBABLE CAUSE

12. 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

[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.

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.

13. 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.

14. The FBI has been investigating a fraudulent scheme by multiple targets, all citizens of the People's Republic of China, who operated one such compound in Min Let Pan, Burma, from at least in or around January 2025 to in or around December 2025.

Background Cryptocurrency Investment Fraud

15. 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.

16. 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.[2] When fraud victims are interacting with these scam platforms, they are provided cryptocurrency addresses to fund their account. The victims are instructed to open an account on a cryptocurrency exchange to exchange fiat currency (U.S. dollars) for cryptocurrency and send that cryptocurrency to the cryptocurrency address(es) provided by the websites.

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

18. 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."[3]

---

[2] 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.

[3] Transnational Crime in Southeast Asia: A Growing Threat to Global Peace and Security (May 2024) ("A Growing Threat (May 2024)"), available at

19. According to the FBI's Internet Crime Complaint Center (IC3), in 2023, investment scams became the most often reported crime type to the IC3, with CIF comprising 83% of that category. CIF schemes have continued to grow, and the IC3 calculated that the reported losses from CIF scams rose, from $3.96 billion in 2023, to $5.8 billion in 2024, an increase of 47%.[4] 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 guilt with them that results in widespread underreporting.

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

---

https://www.usip.org/sites/default/files/2024-05/ssg_transnational-crime-southeast-asia.pdf (last accessed on November 6, 2025).

[4] 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).

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

[6] 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).

[7] 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).

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

Burma military, it held immense power in this remote region while the military was, and still is, fighting a war against the Burmese government.[9]

21. One of the original goals of these compounds 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, Chinese criminal organizations in these zones turned to fraud schemes, especially CIF, as a new source of revenue.[10] And as lockdowns and border controls meant Chinese workers could not travel to Burma, these organizations began trafficking workers from around the world.[11] 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."[12]

22. 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:

---

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

[10] 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).

[11] *Id.*

[12] *Id.*

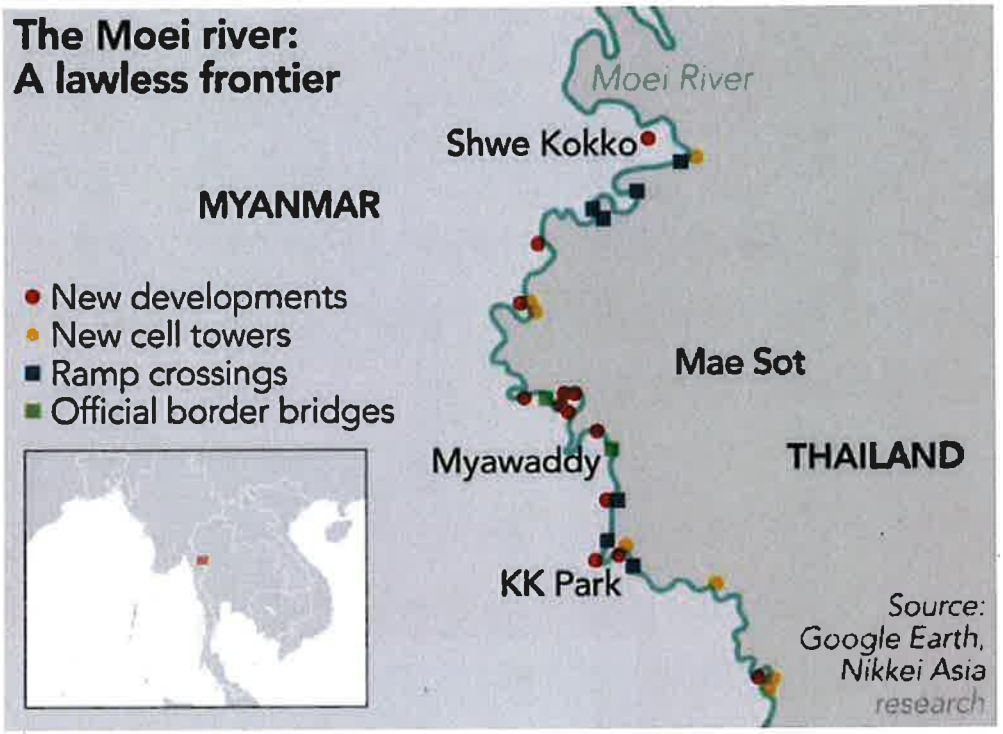


Figure 1 – Several compound developments are identified along the Moei river in Burma.[13]

23. CIF compounds are often "city-like" and reminiscent of "penal colonies."[14] 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."[15] Public reporting on KK Park and other Southeast Asian CIF compounds includes accounts of beatings, electrocutions, and murder.[16] Victims are frequently required to pay

[13] 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 November 6, 2025).
[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 (last accessed on November 6, 2025).
[15] *Id.; KNU Under Pressure*, *supra* note 27.
[16] *A Growing Threat* (Nov. 2022), *supra* n. 21; Shaun Turton, Cyber Slavery: Inside Cambodia's Online Scam Gangs, Nikkei Asia (Sept 1, 2021), available at

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."[17] Those who cannot or do not pay are sometimes sold between companies.[18]

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.[19] 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.[20] After reporting for the position, he was trafficked into Burma via the border town of Mae Sot.[21] 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.[22] After refusing to work, he was reportedly beaten with a baseball bat and later pushed out of a

---

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).

[17] *Cyber Slavery*, *supra* note 30; *see also Cambodia Scams*, *supra* note 30.

[18] *Cyber Slavery*, *supra* note 30; *Cambodia Scams*, *supra* note 30.

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

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

[21] *Id.*

[22] *Id.*

building from the third floor, resulting in a broken leg and rib.[23] Ultimately, he was released after his family paid a ransom.[24]

KK Park

25. KK Park was operating in Burma and supporting scam operations against U.S. persons, until late 2025. KK Park is located at approximately 16°37'44.6"N 98°34'03.0"E, and is pictured below:

Fig. 1. – KK Park Arial View

26. Through interviews of trafficked persons in Burma, the criminal investigation focused on a network of Chinese individuals involved in CIF scheme, which included operating Company-1. The trafficked persons stated that the Company-1 was operating in KK Park in or

[23] *Id.*
[24] *Id.*

around 2023, and thereafter then moved their operations to another compound, "Baoli Park," located directly to the west of KK Park in or around 2024.

Baoli Park

27. Baoli Park is located at approximately 16°38'00.8"N 98°32'56.7"E, and is pictured below:

Fig. 2 – Baoli Park

28. The trafficked persons also stated that the Company-1 employees moved from Baoli Park to another compound near Min Lat Pan, Burma, in and around the fall of 2025. I know, based on my training and experience, that scam compound owners often relocate their operations to new scam compound locations in response to changes in the security environment and costs.

According to publicly-available map data, Baoli Park is located approximately 4.9 miles away from this compound.

Min Let Pan & Use of U.S. Wires

29. According to publicly-available news reporting, along with interviews of trafficked persons and digital forensic reviews conducted by investigating agents (detailed further below), a forced-labor scam compound known as Shunda Park ("Shunda") was operated by the conspirators for the purpose of defrauding the citizens of multiple countries, including the United States. Shunda was located adjacent to the eastern border of the town of Min Let Pan, Burma, at approximately 16°34'48.5"N 98°34'58.3"E, as shown by the image below, and was in operation since at least January 2025.

Fig. 3 – Shunda Compound

30. Aerial imagery shows the growth of the Shunda compound between September 2024 and December 2025.

Fig. 4 – Shunda Compound Comparison September 2024 to December 2025

31. According to interviews with multiple former workers from Shunda, during its period of operation, physical security for Shunda was provided by personnel of the Democratic Karen Buddhist Army ("DKBA"), an insurgent militia. On November 12, 2025, the DKBA and its leadership were designated as sanctioned entities by the Department of Treasury's Office of Foreign Asset Control ("OFAC") for supporting cyber scam centers in Burma that target Americans using fraudulent investment schemes. According to trafficked persons who worked at the Shunda compound, the compound was secured with a combination of a high perimeter wall, barbed wire, and a solitary guarded main gate that was the only means of egress into and out of the compound. The vicinity of the compound was controlled by and patrolled by DKBA soldiers, whom the trafficked persons recognized due to the insignia on their uniforms.

32. I am aware based on information provided to me from Thai authorities, as well as a letter received by the FBI from the Karen National Liberation Army ("KNLA")[25], that on or about November 21, 2025, the KNLA seized and took control of the Shunda compound, resulting in the KNLA's discovery of Shunda's scam center operation. KNLA personnel retained a large number of cellular telephones and desktop computers from Shunda. Subsequently, in or around early December 2025, Thai authorities obtained these devices and provided them for review by the FBI. As explained below, the content of the devices associated with Shunda is broadly consistent with the administration of a scam compound and revealed successful attempts by Shunda-based personnel to defraud U.S.-located victims.

Fig. 5 – Phones seized from the Shunda Compound

[25] The KNLA is the military branch of the Karen National Union, an Burmese armed group.

Fig. 6 – Interior of the Shunda Compound After KNLA Capture[26]

52. As the resulting evidence collection showed, access to the internet was critical to the criminal operations at the Shunda Compound. As described further herein, Shunda compound trafficking victims interviewed by the FBI stated that they contacted U.S. victims of fraud through the internet, and further through the use of U.S. internet platforms.

53. There is probable cause to believe that the Shunda Compound was using, at least in part, internet services provided by SpaceX. Specifically, Trafficking Victim 1 (TV-1) visually observed approximately four to five Starlink terminals during their time at Shunda. Additionally, 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

[26] Free Burma Rangers, Exposing a Burma Scam Center Liberated from Burma Army Proxy Forces (Dec. 7, 2025), https://www.freeburmarangers.org/post/exposing-a-burma-scam-center-liberated-from-burma-army-proxy-forces.

constellation. Consumer service for Starlink began in or around October 2020 and, today, Starlink provides internet service in numerous different markets around the world.

54. 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 monthly subscription price for the satellite internet service.

Figure 7 – SpaceX Starlink Terminal.

33. 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 scam compounds more than

> 40,000 times, according to mobile phone data, which was collected by an online advertising industry tool.[27]

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.[28] Additionally, the combat in Burma has resulted in "frequent internet shutdowns" and thus Starlink has become a crucial means of connectivity and stable internet.[29] Additionally, the Thai government has been attempting to disrupt traditional internet connections to Burmese scam compounds, making Starlink an alternative.[30]

34. 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.[31]

35. Investigators consulted with a company doing business in imagery analysis to obtain high resolution satellite imagery of the Shunda Compound.[32] The company's imagery expert obtained imagery from December 4, 2025, showing multiple buildings in the area. Those buildings contained numerous items located on the roofs of all the buildings, which the expert

---

[27] *Elon Musk's Starlink Is Keeping Modern Slavery Compounds Online*, Wired (Feb. 27, 2025), https://www.wired.com/story/starlink-scam-compounds.
[28] *Id.*
[29] *Id.*
[30] *Id.*
[31] *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.
[32] 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.

opined was consistent with Starlink satellite terminals. The expert opined that there were approximately at least 45 (and possibly up to 63) Starlink terminals on the roofs of the buildings.

Fig. 8 – Analysis of Starlink Terminals (circled in red) at Shunda Compound.

36. The expert also reviewed imagery of the Shunda Compound from a publicly-available news article,[33] and noted the presence of Starlink terminals on the roof of the buildings.

[33] Beech, Hannah, *At This Office Park, Scamming the World Was the Business,* The New York Times (Jan. 13, 2026), *available at https://www.nytimes.com/2026/01/13/world/asia/myanmar-scam-center.html*

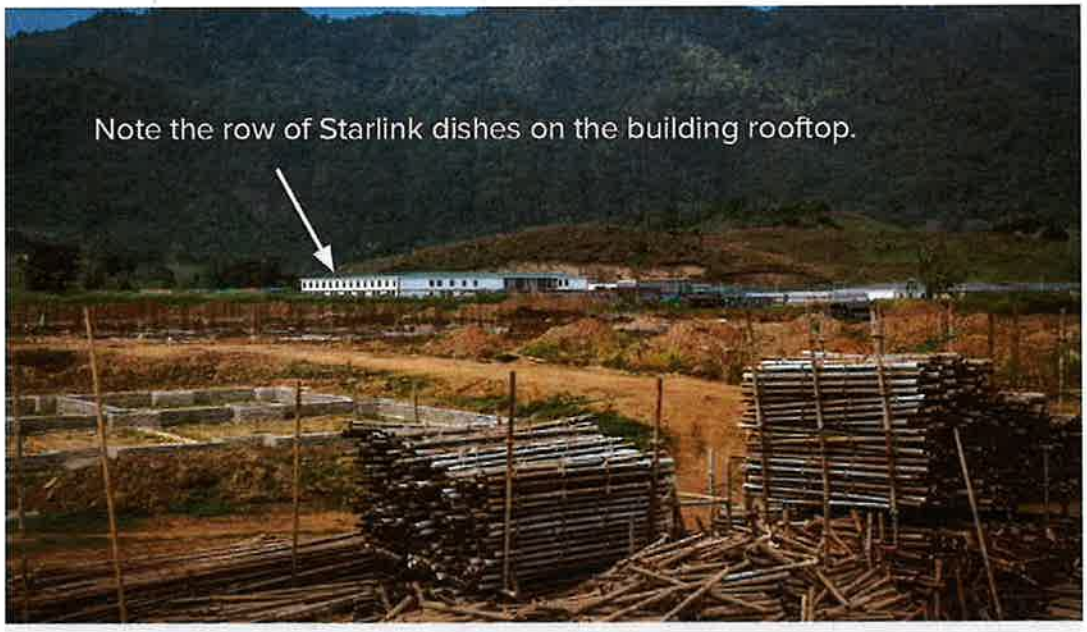


Fig. 9 – Identification of Starlink Terminals at Shunda Compound.

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

Interviews of Trafficked Persons from Min Let Pan

38. After the KNLA seized and occupied Shunda, hundreds of compound workers fled to Thailand where they were detained by Thai immigration authorities pursuant to deportation procedures. Between December 8 and December 10, 2025, the FBI interviewed approximately 18 former compound workers from Shunda. In addition, from December 2025 through January 2026 the FBI reviewed approximately 1,969 mobile devices and 68 desktop computers recovered by the Royal Thai Police from the Shunda compound and provided to the FBI. As a result of these interviews and its analysis of the digital evidence, the FBI has learned the following facts, which support probable cause that the Shunda compound was engaged in crypto investment fraud

schemes targeting U.S. persons and using U.S. wires between in and around July 2023 and in and November 2025. The interviews further illustrated the role of human trafficking and coercive physical punishment in the administration and operation of the Shunda scam center.

39. FBI interviews of former compound workers corroborated the historical movement of the criminal enterprise that operated Company-1; each time the criminal enterprise moved to a different compound, the compound workers were forcibly transferred.

40. Two such interviews were of Trafficking Victim 1 (TV-1) and of Trafficking Victim 2 (TV-2). According to TV-1, TV-1 was lured to KK Park in or around July 2023 by promises of a high paying job offer. Upon arriving, TV-1 was held against his will, and forced to work for the criminal enterprise as a [redacted], without pay. In or around July 2024, TV-1 was forcibly transferred to Baoli Park, where he continued to be held against his will by the conspirators, and was finally transferred to Shunda on or about September 20, 2025. Each time TV-1 was transferred between compounds, TV-1 was transferred under restraint and armed escort.

41. TV-2 was also initially trafficked to KK Park. TV-2 was lured to KK Park in or around June 2023 with a promise of a high paying job offer to work as a casino customer service representative but was instead forced to work there in the CIF criminal enterprise. TV-2 worked targeting individuals for scams in the European/United States market, primarily assisting in identifying and contacting potential victims in the United States. TV-2 worked at KK Park until approximately March 16, 2024, when TV-2 was transferred to Baoli under armed military escort. Later, TV-2 was transferred to Shunda in or around September 2025 in a similar fashion.

42. TV-3 was lured to KK Park in or around August 2023 with the promise of a high paying job offer. Instead, TV-3 was forced to work first as a scammer [redacted] targeting

individuals for scams in the European/United States market, and later as an [redacted]. TV-3 was transferred to Shunda in or around September 2025; [redacted]

43. The trafficking victims, including TV-1 and TV-2, described the basic premise of the investment fraud scheme. Specifically, the Company-1 managers instructed the trafficking victims as employees of the scam compound, such as TV-2, to induce the U.S. persons to invest money in purported cryptocurrency investments. The Company-1 managers instructed employees to employ "romance scam" type tactics, which included the use of online dating applications to identify and communicate with the U.S. persons using a profile of a fictitious female who would eventually gain the adoration and trust of the U.S. persons. The Company-1 managers also instructed the workers in their criminal enterprise to communicate with the U.S. persons utilizing cell phone messaging applications.

44. The U.S. persons were shown fraudulent account statements and balances indicating their investment was growing, when in reality, the U.S. persons' money was no longer accessible and had already been moved to other accounts controlled by the Company-1 managers. Several false statements were made to the U.S. persons, including but not limited to, having to send more money to pay a "tax" on requested withdrawals, when in actuality, these funds had already been misappropriated by the criminal enterprise and would never be released.

U.S. Victims of Company-1's Scam Operations

45. During the investigation, the FBI identified various digital evidence that tied Company-1's operations to victims in the United States.

A. Spreadsheets of Company-1 & Domain-1

46. The FBI reviewed of one of the desktop computers seized from Shunda, on which was found digital evidence of Company-1's operations. Multiple spreadsheets from Company-1 detailed profits from victims. For example, one spreadsheet was titled in Chinese "Miracle Client Account Recharge." In this spreadsheet, victims were listed by name, description, phone number, and amounts stolen. FBI agents then correlated these listings to reports by U.S. persons made to the FBI, through the IC3 database. A total of approximately three U.S. victims were found on this spreadsheet.

47. One such victim, Fraud Victim 1 (FV-1), located in New York, reported that they were directed by an individual they met on a U.S.-based social media site, identifying herself as "Karen Lee" (LEE), to invest in a trading platform, located at "Domain-1." (Based on my training and experience, I believe that LEE is a fictitious individual, whose identity was used by the compound for the purpose of inducing FV-1 and others to invest money.) Four individuals have reported cryptocurrency investment frauds to the FBI related to Domain-1, for a combined loss amount of approximately $3,911,175.00.

48. According to FV-1, from approximately October 2024 to March 2025, FV-1 proceeded to invest approximately $2.1 million in the Domain-1 platform by sending cryptocurrency USDC[34] through an American cryptocurrency exchange (U.S. Exchange 1) to wallets provided by LEE. (FV-1 transferred these funds through electronically from U.S. Exchange 1 through its website, located in the United States.) When FV-1 attempted to make a withdrawal in or around March 2025, LEE told FV-1 that FV-1 needed to make an additional deposit of $329,235 to complete the withdrawal. After FV-1 sent this amount in USDC through U.S.

[34] According to publicly-available descriptions, USD Coin (USDC) is a regulated, fiat-collateralized stablecoin pegged 1:1 to the U.S. dollar.

Exchange 1, LEE told FV-1 that the withdrawals had been intercepted by the Financial Crimes Enforcement Network (FINCEN). LEE told FV-1 that FV-1 now needed to make an additional deposit of approximately $44,010 in USDC through U.S. Exchange 1 to secure the release the funds. FV-1 complied with the instructions provided by LEE. I know from my training and experience that CIF scam compounds often tell victims their invest funds have been frozen or intercepted by U.S. law enforcement to create a sense of artificial urgency, and to induce the victim to invest additional funds.

49. The deposits made by FV-1 in or around March 2025 match up in sum and substance with what was listed in the spreadsheet recovered from the computer from Shunda. In this spreadsheet, one line-item lists FV-1 depositing approximately $329,062 on or about March 8, 2025. A second line-item lists FV-1 depositing approximately $43,990 on or about March 19, 2025.

50. FV-1 was interviewed by the FBI in or around January 2026, and corroborated both March 2025 deposits. Furthermore, FBI tracing of the cryptocurrency transactions conducted by FV-1 further corroborated the timing and dollar amounts of these deposits. FBI tracing found that on March 7, 2025, FV-1 sent 329,235.39 in USDC, and on March 18, 2025, FV-1 sent 44,010.11 in USDC. Per my training and experience, the discrepancy in deposit value likely reflects fees paid to an intermediate money launderer, while the discrepancy in date likely reflects a time difference between the transactions revealed by FBI tracing, recorded in UTC, and the Shunda records recorded in local time.

B. Domain-2

51. TV-2 identified another domain name, Domain-2, which was used by Company-1 to defraud fraud victims. According to TV-2, beginning in or around June 2024, at Baoli Park, TV-

2 and the members of his team were instructed by their managers to direct victims to invest in another website platform located on Domain 2, which purported to offer cryptocurrency trading. Domain-2 continued to be used at Shunda after the Company-1 criminal enterprise relocated there in 2025.

52. The FBI has identified multiple victims in the United States who invested in the platform located at Domain-2. Approximately 8 U.S. individuals reported to the FBI that they were defrauded using the Domain-2 platform.

53. In or around February 2025, FV-2, an individual located in Ohio, was contacted on a U.S.-based online dating application[35] by someone FV-2 believed to be a Ukrainian-American woman named "Sophia Elmira" (ELMIRA). ELMIRA expressed a romantic interest in FV-2 and eventually instructed FV-2 to switch the conversation over to an encrypted messaging application. (Based on my training and experience, I believe that ELMIRA is a fictitious individual, whose identity was used by the compound for the purpose of inducing FV-2 and others to invest money.)

54. According to FV-2, shortly after initiating contact, ELMIRA told FV-2 that ELMIRA worked for an "investment company" that conducted "market analysis" and developed "trade signals." ELMIRA told FV-2 that FV-2 could use the trade signals from ELMIRA's company to make profits on FV-2's investments, and ultimately convinced FV-2 to invest on the Domain-2 platform.

55. On or about early February 28, 2025, FV-2 initially invested approximately $2,000 without issue. To fund the account, on or about that date, FV-2 wired money from his bank account to U.S. Exchange 1 via U.S. Exchange 1's U.S. website, converted the money to ETH (Ethereum,

[35] The dating application, used to target FV-2, is operated by a company headquartered in the United States, but which is a subsidiary of a German company.

which is a form of cryptocurrency) and transferred the ETH to a wallet per ELMIRA's instructions. As time continued, ELMIRA convinced FV-2 to invest more money with the goal to reach $1 million. On or about April 22, 2025, ELMIRA told FV-2 that ELMIRA would be investing her own money into FV-2's account as well. At one point, on or about June 2025, FV-2 was told by "customer service" representatives purporting to work for the Domain-2 platform, that FV-2 had to pay a penalty of approximately $115,000, which FV-2 paid on or about June 21, 2025. From approximately February to June 2025, FV-2 invested approximately $240,000 into the Domain-2 platform, which falsely showed that FV-2's "investment" grew to approximately $1,300,000. FV-2 was unable to recover these funds and reported the same to the FBI.

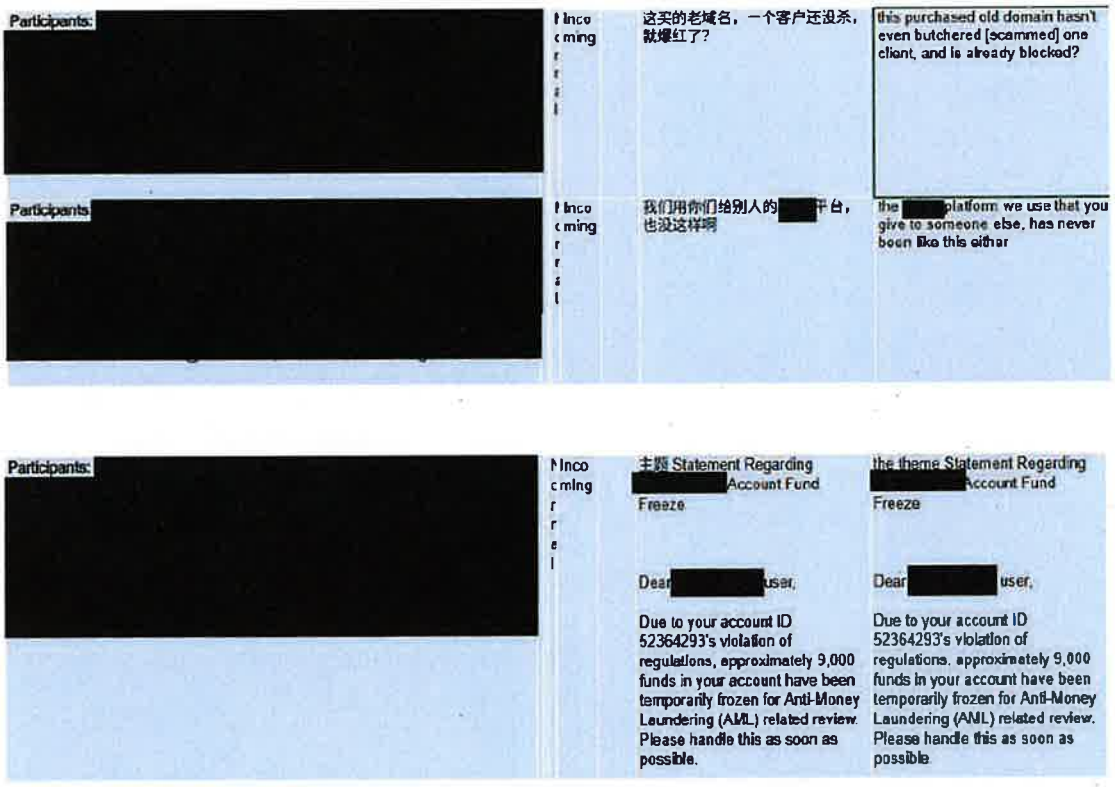
C. Compound Phone-1, Applications, & Domain-3

56. Additionally, the FBI reviewed one phone recovered from a Shunda compound worker detained by the Thai immigration authorities (Compound Phone-1). Compound Phone-1 also included limited geodata showing that the phone was in the approximate area of Shunda in or around November 2025. In addition, when shown Conversation-1 and Conversation-2, TV-1 and TV-2 both (separately) confirmed these discussions were between employees of Company-1, based on their review of the content of the conversations and knowledge of Company-1 operations.

57. Compound Phone-1 contained a conversation thread on a messaging application ("Conversation-1") in which the participants referred to multiple software applications. (Based on my training and experience, I know that software applications are able to be downloaded on Apple and Android devices through their applications stores, and that further CIF schemes sometimes distribute these applications through the applications stores in order to increase the perception of legitimacy.) Conversation-1 began on or about September 15, 2025, and ended on or about November 6, 2025. Approximately 50 individuals reported to the FBI that they were defrauded

using the applications discussed in Conversation 1. A review of these reports show that most fraud victims initially met the scammer on a U.S.-based social media platform.

58. A portion of Conversation 1 is provided below. Based on my training and experience, this conversation appeared to be between employees operating the scam center and web developers at another location, who were responsible for registering and maintaining internet-based platforms that display a fraud victim's purported investments and profits. Conversation-1 participants discuss the impersonation of existing financial companies, complain about the difficulties arising from fraudulent websites being taken down, and exchange victim-facing messages such as fake warnings of violations of anti-money laundering regulations, as exemplified below:



59. Compound Phone-1 included another conversation on the same messaging application ("Conversation-2"). Conversation-2 began on or about February 20, 2025, and ended

on or about November 24, 2025. In Conversation 2, the participants coordinated about communications with fraud victims, cryptocurrency payments, and the registration of domain names used for CIF portals, including Domain-3. While only one U.S. individual reported to the FBI that they were defrauded using the Domain-3 platform, a review of the tracing analysis for the cryptocurrency wallets involved identified at least another U.S. victim who also reported to the FBI that they were defrauded using the Domain-3 platform.

60. Conversation-2 also contained multiple cryptocurrency wallet addresses. FBI analysts traced these addresses, which revealed small payments to victim cryptocurrency wallets. In my experience investigating CIF, it is common for perpetrators to send small payments to victims purporting to be withdrawals from the victim's investment profits to convince the victim of the investment's legitimacy. This tracing also revealed additional victims, including FV-4 and FV-5, who are both located in the United States.

61. Both FV-4 and FV-5 reported to FBI that they were defrauded using Domain-3 from approximately September 2025 to December 2025, losing a combined approximate total of $300,000. Both fraud victims originally met their scammer on a U.S.-based social media website. Both fraud victims were interviewed by the FBI and confirmed that they had received the small payments from the platform revealed by the FBI tracing described above.

Money Laundering Associated with U.S. Victims

62. As a general matter, my review of the cryptocurrency transactions of U.S. victims and information provided by the trafficking victims, showed that the scheme laundered funds in the following way. First, fraud victims were convinced though direct messages from the trafficking victims to withdraw money from their bank accounts (fiat currency) and invest in cryptocurrency, often on U.S. platforms. Second, fraud victims were given instructions to access specific websites

related to the scam, which included the cryptocurrency wallets to which they should transfer funds. Third, once the funds were deposited into these wallets, over which the conspirators had control, they were quickly moved to other wallets via cryptocurrency swapping services]. Examples follow.

63. Conversation-1 and Conversation-2 included references to specific cryptocurrency wallet addresses, which were later tied to victims of fraud, showing the involvement of Shunda compound management in the laundering of funds.

64. The FBI conducted a tracing analysis on the funds sent by FV-4 and FV-5 to the cryptocurrency wallets associated with Domain-3. That analysis drew on blockchain analysis, virtual asset service provider (VASP) records, attributions from a commercially available blockchain analytics tool, open-source block explorers, and the training and experience of the investigating agents.

65. A review of Conversation-2 showed a message from September 19, 2025 ([redacted]), which contained the cryptocurrency address [redacted].

a. A review of the blockchain showed that, on the same day at [redacted], [redacted] US Dollar Coin (USDC) was sent from [redacted] to [redacted] FV-4 confirmed that [redacted] was a wallet under his control, and that this payment was represented to FV-4 by the conspirators as a "withdrawal" from his investment in the Domain-3 related platform.

b. A review of the blockchain showed that, on September 20, 2025, at [redacted], [redacted] USDC was sent from [redacted] to

[redacted]. FV-4 confirmed that this withdrawal was an investment on his part into the Domain-3 related platform.

66. A review of the blockchain showed that [redacted] has received additional USDC directly from VASPs including [redacted], in addition to unhosted wallets, including a wallet belonging to FV-5. Per my training and experience, it is highly likely that these represent additional victim funds. The total amount received by [redacted] from all sources is approximately [redacted] (USDC).

67. Nearly all USDC received into [redacted] was sent to [redacted] an instant swapping service.[36] Using [redacted]'s bridge explorer[37], agents determined that a portion of FV-4's funds were converted into Tether (USDT).

a. A portion of the originally traced funds from the victim transactions were bridged to a wallet, [redacted]. In total, [redacted] Tether (USDT) was sent to [redacted] from [redacted]. An additional [redacted] USDT was received by [redacted] from other bridging services (specifically, [redacted]).

68. Thereafter, a review of the blockchain showed the following transfers:

a. Between 1/19/25 and 9/20/25, over the course of [redacted] transfers, [redacted] sent [redacted] USDT to [redacted],

[36] An instant swapping service is a cryptocurrency exchange platform that allows users to directly swap one digital asset for another, or to move those assets between blockchains, without creating an account or supplying Know-Your-Customer (KYC) information.

[37] A bridge explorer is a publicly accessible tool that allows users to track and verify transactions that occur using a given bridge service, such as [redacted].

i. [redacted] sent [redacted] USDT to [redacted] over two transfers on September 29, 2025, for [redacted] USDT and [redacted] USDT.

ii. [redacted] sent [redacted] USDT back to [redacted] on October 4, 2025.

b. On September 27, 2025, [redacted] sent [redacted] USDT in total to [redacted], first sending [redacted] followed by an additional [redacted] USDT ten minutes later.

i. These funds were then comingled and sent with additional funds for a total of [redacted] USDT to [redacted] on September 30, 2025.

ii. In total, [redacted] sent [redacted] USDT over [redacted] transfers and [redacted] sent [redacted] USDT over [redacted] transfers. Both of these wallets are funded in part by transfers from wallets that were funded in part by [redacted] and [redacted] transfers.

Involvement of the Defendants

A. Defendants' Conduct at the Shunda Compound

69. Through interviews with the trafficking victims, including TV-1, TV-2, and TV-3, the investigation has revealed that the Shunda compound was being operated by a group of Chinese nationals, all from Fujian, China, and several of whom were related to each other. Based on my training and experience, I know that many Southeast Asian scam compounds are owned and

operated by groups of individuals made up of family members and business partners from Fujian, China. The owner-operators of Southeast Asian scam compounds are frequently from the same or neighboring cities.

70. Multiple interviews with former compound workers determined that the criminal enterprise operating at Shunda was led [redacted]. According to TV-1, TV-2, and TV-3, INDIVIDUAL-1 was in charge of the Shunda compound. Under INDIVIDUAL-1's leadership, Shunda housed operations that specialized in scamming different geographical regions known as markets, this included Company-1, which targeted the European/United States markets.

71. Multiple interviews with former compound workers, including TV-1, TV-2, and TV-3, identified HUANG as a high-level manager [redacted] who acted as a General Manager for INDIVIDUAL-1's criminal enterprise as well as an enforcer, exacting beatings on trafficked victims.

a. TV-1 identified HUANG as INDIVIDUAL-1's cousin. TV-1 personally witnessed HUANG participate in beatings of compound workers while TV-1 was at KK Park, Baoli Park, and Shunda. From in or around July 2023 until in or around July 2024, TV-1, [redacted]. TV-1 witnessed HUANG and the remaining managers discuss building Shunda as a future base for their criminal enterprise.

b. According to TV-3, TV-3 was forced to [redacted] within the criminal enterprise at KK Park. [redacted]

[redacted]. In addition, TV-3 personally observed HUANG beat four or five workers in front of the entire compound workforce. TV-3 was transferred to Shunda from KK Park in or around September 2025, where he was forced to continue to work [redacted].

c. TV-1, TV-2 and TV-3 all identified HUANG by his picture below, taken by the Royal Thai Police (RTP) after they arrested HUANG on or about January 21, 2026.

72. Multiple interviews with compound workers, including TV-1, TV-2, and TV-3, identified JIANG as a General Manager for operations targeting American victims and reported directly to HUANG at KK Park, Baoli Park, and Shunda.

a. According to TV-2, while TV-2 was at Baoli Park, TV-2 worked [redacted]

[redacted] how workers should best introduce themselves to potential victims in the United States over messaging platform applications to capture their attention and interest. [redacted].

b. [redacted]. Later, throughout TV-3's time at KK Park, [redacted]. JIANG was a team leader in charge of scamming U.S. persons. [redacted] JIANG coach his workers on how to resolve victim doubts, and how to help victims deposit cryptocurrency funds into their fictitious trading accounts.

c. In or around December 2024, while JIANG was at Baoli Park, one of JIANG's direct reports (Worker-1)[38] successfully scammed a U.S. person of approximately $3,000,000 utilizing Domain-2 under JIANG's tutelage and leadership. This successful victimization was so large in scale it became infamous and celebrated within INDIVIDUAL-1's criminal enterprise. In fact, INDIVIDUAL-1 gifted a Mercedes Maybach to JIANG to reward him for this success, which TV-1 and TV-2 saw JIANG drive around Baoli Park. Furthermore, [redacted]

[38] A search of HUANG's phone yielded Worker-1's contact in an encrypted messaging application as well as Worker-1's photo. [redacted]

JIANG talk about this success on a few occasions following the victimization.

d. In addition, TV-1, TV-2, and TV-3 all identified JIANG by his picture below, taken by the Royal Thai Police (RTP) after they arrested JIANG on or about January 21, 2026:

B. Defendants' Actions After Fall of the Shunda Compound

73. As described further herein, [redacted], after escaping from Shunda in or around the beginning of December 2025, HUANG, JIANG, [redacted], and other individuals from Shunda relocated to another scam compound located in Cambodia where they attempted to continue their CIF operation [redacted].

74. [redacted] in December 2025, shortly after the Shunda compound was seized by the KNLA, [redacted] while HUANG made arrangements with human traffickers to smuggle compound managers to safety, including JIANG. [redacted] INDIVIDUAL-1 would make arrangements to bring everyone somewhere safe.

75. [redacted] at New Peace Village for approximately ten days with 80 other former Shunda compound workers. Afterwards, this group split into two. One group traveled to the Yatai New City compound in Shwe Kokko, Burma, while the other traveled to Bokor Mountain in Cambodia. [redacted], at a compound in Bokor Mountain, Cambodia (hereinafter "the Bokor Mountain Complex") located at approximately 10°40'13.3"N 104°01'16.9"E:

76. [redacted]. HUANG appeared to [redacted] be re-establishing his criminal enterprise in a rented villa located in Subdivision 3. Several former

colleagues from KK Park and Shunda were already at the villa [redacted], including JIANG. Specifically, [redacted] this villa would become the new long-term compound for their criminal enterprise. The Cambodia branch of the criminal enterprise was named "Senyu." The new compound was laid out as follows: the 1st floor was the office for scamming operations, the 2nd floor was the dormitory for the scam workers, and the 3rd floor was reserved for management. [redacted]

77. [redacted] HUANG actively re-establish the criminal enterprise from Shunda in this new location (Senyu).

a. [redacted] HUANG procure approximately 160 phones to be used in scamming operations.[39]

b. [redacted] HUANG order workers to do renovations on the villa for Senyu, such as building a new building for visitor reception and meetings. (As explained further herein, digital evidence later discovered on one of HUANG's phones showed the same.)

c. HUANG told his workers on several occasions, in sum and substance, that they would start over again, expand, and buy or hire additional workers. [redacted], HUANG had only approximately 20 workers and thus needed to hire additional workers. HUANG only had workers to target the South-American market. In or around the beginning of January 2026, [redacted] HUANG and JIANG discuss buying more workers to scam the American market. As a result,

[39] Approximately 90 phones were discovered at the safehouse when HUANG was arrested by Thai authorities on or about January 21, 2026. [redacted] these phones were part of the same set HUANG procured for the Senyu compound.

one day HUANG drove JIANG to buy workers from another compound located in Phnom Penh, Cambodia. [redacted] HUANG and JIANG return without any new workers, and later learned from other Senyu workers that HUANG and JIANG were unsuccessful because they felt there were too many Cambodian police on the roads.

78. While at Senyu, [redacted] INDIVIDUAL-1's continued involvement in the criminal enterprise. For example, in or around the end of December 2025, another manager from Shunda had a conversation with INDIVIDUAL-1 over text message while at Senyu regarding sharing profits from successful victimizations. [redacted] HUANG explain to the management of the Bokor Mountain Complex how INDIVIDUAL-1 had arranged for Shunda workers to be smuggled over from Myanmar.

79. [redacted], due to the recent January 2026 crackdown in Cambodia on undocumented Chinese aliens within the country, HUANG, JIANG, and the Senyu co-conspirators decided to relocate back to Burma, with guidance and funding [redacted] On or about January 20, 2026, these individuals travelled together to a safehouse in Thailand as a waypoint on the way back to Burma from the Bokor Mountain Complex.

80. On or about January 21, 2026, Thai authorities conducted an operation on the safehouse location, [redacted]. Thai law enforcement located HUANG and JIANG on the premises and arrested them for illegal entry into Thailand. Also on or about January 21, 2026, Thai law enforcement recovered from on or about HUANG's person two cellular phones, in addition to approximately 90 phones in the safehouse. [redacted].

81. On or about January 21, 2026, FBI Agents interviewed HUANG in Chinese with a

Chinese speaking agent, while he was detained at a Thai police station. HUANG advised he had never been to Burma, and had smuggled himself into Cambodia illegally in or around June 2024. In Cambodia, HUANG claimed that he worked as a welder and as a "chef" at a bed and breakfast. When asked about his culinary background, he could not describe what he cooked in detail, stating he knew how to make soup. HUANG also stated that he did not want to return to China because he would be arrested upon return due to his history of illegal immigration. [redacted].

82. On or about the same day that HUANG was interviewed, FBI Agents interviewed JIANG at the same Thai police station. JIANG advised he did not know anyone in the group he had been arrested with, including HUANG. JIANG stated he had left from Sihanoukville, Cambodia, prior to illegally entering Thailand. JIANG also stated he had never been to Burma. JIANG advised he smuggled himself into Cambodia on or about December 15, 2025, from Laos to escape gambling debts he had incurred there. According to JIANG, while he was in Cambodia in December 2025 and January 2026, he primarily spent his time gambling in the casinos.

C. Evidence from HUANG's Phone

83. Subsequent to HUANG's arrest on or about January 20, 2026, the FBI executed a search warrant (approved by this Court, 26-sw-14) on two of the phones HUANG had on his person at the time of arrest, then located at the U.S. Embassy in Thailand. The contents of these two phones corroborated [redacted] the involvement of the conspirators, [redacted] HUANG, and JIANG.

84. HUANG's phone contained evidence detailing INDIVIDUAL-1's arrangement to relocate personnel from their criminal enterprise after Shunda was seized by the KNLA. For

example, one message group in an encrypted messaging application was titled "Shunda Safe House." On or about December 4, 2025, HUANG asked, "if I go up what place should I go to?" In response, INDIVIDUAL-1 sent a voice message stating, in sum and substance, that another member in the chat group should find somewhere safe for HUANG to stay, lest they get recaptured. TV-1 and TV-2 confirmed the voice in this message was INDIVIDUAL-1's.

85. Beginning on or about December 16, 2025, HUANG had a conversation on an encrypted messaging application with Business Partner-1 about hiring human traffickers to transport individuals from New Peace Village, Cambodia, to the new compound location in Yatai, Burma. Several references were made to INDIVIDUAL-1 in this conversation. For example, on or about December 20, 2025, Business Partner-1 informed HUANG in sum and substance of a payment dispute with a human trafficker [redacted] Business Partner-1 told HUANG, "I created a group for INDIVIDUAL-1 and the human trafficker, they can yell at each other." HUANG responded, in sum and substance, that he told the trafficker he was good for the money he owed the human trafficker. HUANG further added, that "the boss" had called him and asked him to explain the payment dispute with the human trafficker.

86. Similarly, on or about December 27, 2025, HUANG received a message in an encrypted messaging application from a co-conspirator listing the expenses incurred in smuggling people from Shunda, Burma, to New Peace Village, Cambodia, broken down by day, expense amount, and description.

a. On multiple line items, the description is "INDIVIDUAL-1 ordered payment", "JIANG ordered payment", "INDIVIDUAL-1 ordered payment of living expenses to [co-conspirator]", or "INDIVIDUAL-1 made arrangements for payment."

b. In response, HUANG complained about not being able to keep track of all these

expenses. He stated in a voice message, in sum and substance, "Some of these expenses are from Shunda….I was fleeing, you give me this bill, how am I supposed to remember all that?"

87. On or about December 22, 2025, HUANG sent a video of his current surroundings to another individual over an encrypted messaging application.

[redacted] the buildings in this video were the ones located in Subdivision 3 of the Bokor Mountain Complex, which HUANG was renovating as a base of operations for Senyu.

88. Later, on or about December 26, 2026, HUANG created a chat group named "Cambodia Senyu Management Group" in an encrypted messaging application. [redacted] HUANG, JIANG and other managers were present in this group. INDIVIDUAL-1 ordered other co-conspirators from the criminal enterprise to be added into the group. The group then proceeded to discuss payment of living expenses, furniture, and equipment, including payments to JIANG.

a. For example, on or about December 28, 2025, a co-conspirator sent a text message

titled "Management Advance Payments for Living Expenses." Below this, Senyu manager names were listed out with an amount next to their names, including JIANG, who had "1,000" next to his name.

b. Later, on or about December 29, 2025, HUANG sent a voice message in the same chat group, stating in sum and substance that JIANG needed money to use. Another manager in the chat group sent a screenshot of a cryptocurrency transaction for approximately 1,000 USDT with the caption "JIANG NAN's [payment], check." Afterwards, this manager sent another screenshot of a QR code for a cryptocurrency wallet with the same caption, "JIANG NAN's [payment], check." Finally, there was a screenshot sent in the message group showing the successful 1,000 USDT payment, with the caption "Arrived."

c. Similarly, on or about January 10, 2026, HUANG sent a picture of bills received from the Bokor Mountain Complex for rent and utilities, describing it as rental fees, property management fees, and renovation fees. INDIVIDUAL-1 asked in response, "renovation fee?" HUANG then responded that this was for renovations for the villa's third floor bedroom, meeting area, and reception area.

89. Review of HUANG's phone also found evidence of HUANG's involvement in re-acquiring the digital tools needed to facilitate the CIF criminal enterprise.

a. For example, HUANG's phone contained multiple pictures of a cryptocurrency wallet seedphrase. Tracing of the cryptocurrency wallet to which this seedphrase belonged found that, on or about January 12, 2026, approximately $100 was sent to a wallet associated with "[redacted]" Publicly-available research identified this wallet as one that had been flagged by [redacted] as an illicit actor and/or

organization. More specifically, it had been flagged as being associated with CIF and pig-butchering schemes.

b. Publicly-available research also identified [redacted] as a known vendor of fake social media profiles. I know based on my training and experience, purchasing fake social media profiles is a key component of CIF schemes, as these social media profiles are used by scam compound workers to contact and communicate with their victims.

c. Further review of HUANG's phone found a chat group titled "Senyu Social Media Account Seller Contact Group" within an encrypted messaging application. In this chat group, social media accounts sold by [redacted] to HUANG and his co-conspirators were listed out, along with the price paid as well as cryptocurrency wallet addresses for payment to [redacted]

90. In another chat group, titled "Senyu Operations Group," on or about December 28, 2025, an individual sent Huang a price quote for the right to use a U.S.-registered company which could be listed as the developer for apps on smartphone app stores. For 21,000 USDT, HUANG could obtain the rights to use this company's registration documents. Another one of HUANG's co-conspirators asked, "how much for a SEC license?" The vendor responded, in sum and substance, that SEC licenses were now 13,000 USDT. I know, based on my training and experience, that CIF schemes need to purchase the rights to use companies with legitimate business registrations and SEC licenses in order to be able to offer fictitious cryptocurrency trading apps for download on the Apple or Google app stores. In a separate chat, on or about January 11, 2026, a separate co-conspirator texted HUANG a screenshot containing this price quote, along with the crying emoji. HUANG responded, "Didn't we pay for this previously at KK? This the expense

for writing apps."

91. Likewise, on or about December 28, 2025, another known co-conspirator of INDIVIDUAL-1's criminal enterprise texted HUANG, asking in sum and substance, that he "had just called the boss . . . previously at Shunda, were all the workers using Apple 12's?" HUANG responded in sum and substance in a voice message, that each person in the Human Resources Department had one each. However, workers did not have them, and only team leaders and managers did. The co-conspirator responded, "Four [iPhone] 12 for each person, how do you say?" This dialogue illustrates HUANG's knowledge of INDIVIDUAL-1's criminal enterprise at Shunda. I know based on my experience and interviews with former compound workers from Shunda that only managers at INDIVIDUAL-1's criminal enterprise received newer model iPhones, specifically iPhone 11's and above. Workers only received older iPhones, such as iPhone 8s, to contact and communicate with potential victims, especially in the early stages of victimization. Furthermore, I know based on my experience that the Chinese term "Human Resources Department" used by HUANG referred to the department in scam compounds responsible for luring and trafficking victim workers.

92. HUANG's phone also contained evidence corroborating HUANG and INDIVIDUAL-1's efforts to continue their criminal enterprise at Yatai compound in Shwe Kokko, Burma, in addition to Cambodia. After leaving Shunda, HUANG [redacted] that INDIVIDUAL-1 wanted to diversify their bases of operations to reduce future risk. One of INDIVIDUAL-1's business partners (Business Partner-1) from Shunda was sent to Yatai to establish a new base of operations after Shunda was captured by the KNLA. Based on interviews with former Shunda compound workers who stayed in contact with Business Partner-1, the location in Yatai in which they re-established operations was known as "Plot Number 4."

a. On or about December 12, 2025, HUANG messaged Business Partner-1 and asked him "When are you going to Plot Number 4? How is the site? . . . . Aren't you going to Plot Number 4 to establish a site?" Business Partner-1 responded, in sum and substance, with his opinion of Plot Number 4, and sent HUANG pictures of the compound office space. Later in the same conversation, HUANG stated, "Its best if we have a space that can be sealed off, lest people run away." Business Partner-1 concurred.

b. Likewise, on or about December 26, 2025, HUANG created a chat group named "Yatai" in an encrypted messaging application. [redacted] Business Partner-1, and other former Shunda leaders were present in this group. Members of the group then proceeded to post receipts to request reimbursement for purchases of computers, approximately 88 cellular phones, a Starlink terminal, and other equipment.

c. Furthermore, on or about January 16, 2026, a bill from the Yatai compound property manager was posted in this chat group. This bill had line items for rent, property management fees, food, and utilities, totaling approximately 57,085 USDT for the months of December 2025 and January 2026. The bill was followed by discussions on how the group did not have enough money to pay this bill, and how the Property Manager was demanding payment.

REQUEST TO SUBMIT WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

93. 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 Search Warrant. I submit that AUSA Karen Seifert from the

United States Attorney's Office is capable of identifying my voice and telephone number for the Court.

CONCLUSION

94. Based on the forgoing factual allegations, there is probable cause to believe that HUANG Xing Shan, also known as "Ah Zhe," and JIANG Wen Jie, also known as "Jiang Nan," and others have committed violations of 18 U.S.C. §§ 1343, 1349 (Wire fraud conspiracy).

Respectfully submitted,

[redacted]
Special Agent, Federal Bure··· of Investigation

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by telephone on on January 30, 2026.

M. A. Upadhyaya

HONORABLE MOXILA A.UPADHYAYA
UNITED STATES MAGISTRATE JUDGE