UNITED STATES DISTRICT COURT

for the

District of Columbia

In the Matter of the Seizure of *(Briefly describe the property to be seized)* 2 CRYPTOCURRENCY WALLETS & 2 TELEGRAM CHANNELS ASSOCIATED WITH XINBI GUARANTEE PURSUANT TO 18 U.S.C. §§ 981(a)(1)(A) & (C), 982(a)(1), AND 28 U.S.C. § 2461	)	Case No. 26-sz-54

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(a)(1)(A), 981(a)(1)(C), 982(a)(1), and 982(a)(2)(A); 28 U.S.C. § 2461(c)

(describe the property):

2 CRYPTOCURRENCY WALLETS & 2 TELEGRAM CHANNELS ASSOCIATED WITH XINBI GUARANTEE PURSUANT TO 18 U.S.C. §§ 981(a)(1)(A) & (C), 982(a)(1), AND 28 U.S.C. § 2461

The application is based on these facts:

SEE ATTACHED AFFIDAVIT, HEREBY INCORPORATED BY REFERENCE.

❒ Continued on the attached sheet.

[redacted]

Applicant's Signature

[redacted]

Printed name and title

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

Date: 09/07/2026

Judge's signature

City and state: Washington, District of Columbia

Moxila A. Upadhyaya U.S. Magistrate Judge

Printed name and title

UNITED STATES DISTRICT COURT

for the

District of Columbia

In the Matter of the Seizure of *(Briefly describe the property to be seized):* 2 CRYPTOCURRENCY WALLETS & 1 TELEGRAM CHANNEL ASSOCIATED WITH XINBI GUARANTEE PURSUANT TO 18 U.S.C. §§ 981(a)(1)(A) & (C), 982(a)(1), AND 28 U.S.C. § 2461	)	Case No. 26-sz-54

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:

2 CRYPTOCURRENCY WALLETS & 2 TELEGRAM CHANNELS ASSOCIATED WITH XINBI GUARANTEE PURSUANT TO 18 U.S.C. §§ 981(a)(1)(A) & (C), 982(a)(1), AND 28 U.S.C. § 2461, 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 09/21/2026
(not to exceed 14 days)

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

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

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

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

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

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

Date and time issued: 09/07/2026

M.U. Upadhyaya
Judge's signature

City and state: Washington, District of Columbia

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

Return

Case No.: 26-sz-54	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

ATTACHMENT A-1: PROPERTY TO BE SEIZED

Pursuant to this warrant, Tether shall provide the law enforcement officer/agency serving this document with the equivalent amount of USDT tokens that are currently associated with the virtual currency addresses referenced below. Tether shall effectuate this process by (1) burning the USDT tokens currently associated with the virtual currency addresses referenced below and (2) reissuing the equivalent value of USDT tokens to a U.S. law enforcement-controlled virtual currency wallet. Tether shall provide reasonable assistance in implementing the terms of this seizure warrant and take no unreasonable action to frustrate its implementation.

1.	TWPma8xH48AEN93x2krdukV9e1j6sPsBeS	Target Wallet 1
2.	TF7LUSoZQyDFxTFzCL11saBHAqMAyPh8dK	Target Wallet 2

ATTACHMENT A-2: PROPERTY TO BE SEIZED

With respect to the Telegram channels with associated Telegram addresses of **@gqdh** and **@xbdh** (**TARGET SITES**), Telegram Messenger Inc. ("Telegram"), which is the host for the **TARGET SITES**, shall take the following actions to effectuate the seizure of **TARGET SITES**:

1. Take all reasonable measures to backup all data associated with the **TARGET SITES** at the time of seizure, and produce a copy of the same to the Federal Bureau of Investigation.
2. Take all reasonable measures to redirect **TARGET SITES** to accounts controlled by and at the direction of the Federal Bureau of Investigation, by redirecting traffic from the **TARGET SITES** to the accounts controlled by the FBI.
3. Prevent any further modification to, or transfer of, the **TARGET SITES** pending transfer of all rights, title, and interest in the **TARGET SITES** to the United States upon completion of forfeiture proceedings, to ensure that changes to the **TARGET SITES** cannot be made absent court order or, if forfeited to the United States, without prior consultation with Federal Bureau of Investigation.
4. Take all reasonable measures to propagate the necessary changes.
5. Provide reasonable assistance in implementing the terms of this Order and take no unreasonable action to frustrate the implementation of this Order.

The Government will maintain a copy of the backup data of the **TARGET SITES**. The Government will display a notice on the **TARGET SITES** after control is transferred to the government account. That notice will consist of the following text (or substantially similar text):

> This site has been seized in accordance with a seizure warrant issued pursuant to 18 U.S.C. § 981(a)(1)(A), 18 U.S.C. § 982(a)(1), and 28 U.S.C. § 2461(c) by the United States District Court for the District of Columbia.

This seizure is part of a law enforcement operation conducted by the Scam Center Strike Force, an initiative of the U.S. Attorney's Office for the District of Columbia, the U.S. Department of Justice, the Federal Bureau of Investigation, and the U.S. Secret Service.

For additional information, visit www.justice.gov/usao-dc/scam-center-strike-force

To report cybercrime, visit www.ic3.gov

UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

IN THE MATTER OF THE SEIZURE OF 2 CRYPTOCURRENCY WALLETS & 2 TELEGRAM CHANNELS ASSOCIATED WITH XINBI GUARANTEE PURSUANT TO 18 U.S.C. §§ 981(a)(1)(A) & (C), 982(a)(1), AND 28 U.S.C. § 2461	**SZ No. 26-sz-54** **FILED UNDER SEAL**

Reference: USAO Ref. #2026R00315; Target Property: See attachment A-1; @gqdh (Telegram Site 1) and @xbdh (Telegram Site 2)

AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEIZURE WARRANT

Your co-affiants, U.S. Secret Service Special Agent [redacted] and Federal Bureau of Investigation Special Agent [redacted] being duly sworn, depose and state as follows:

I. INTRODUCTION

1. Your co-affiants are both "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, the offenses enumerated in 18 U.S.C. § 2516.

2. The facts and information contained in this affidavit are based upon personal knowledge and observations; information obtained from other agents, analysts, law enforcement personnel, and witnesses; and information obtained from business records. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all the facts in this case.

3. Co-affiant [redacted] is a Special Agent with the United States Secret Service ("USSS") and has been so employed since [redacted]

[redacted]

[redacted]

4. Co-affiant [redacted] is a Special Agent with the Federal Bureau of Investigation (FBI), having been so employed since [redacted]

5. Because this affidavit is being submitted for the limited purpose of securing the requested order, we have not included each and every fact known to me concerning this investigation. We have set forth only those facts that we believe are necessary to establish probable cause for the requested search warrant. Where statements of others are set forth in this affidavit, they are set forth in substance and in part.

II. THE TARGET PROPERTY

6. This affidavit is made in support of an application for a warrant authorizing the seizure of

a. the equivalent amount of USDT as associated with the unhosted cryptocurrency addresses as described herein and listed in Attachment A-1 which were / will be processed by and through XINBI GUARANTEE ("Xinbi") (collectively, the "Target Funds"), and

b. two Telegram Channels, with the Telegram locators @gqdh (Target Site 1) and @xbdh (Target Site 2) (collectively, the "Target Sites"), hosted by **TELEGRAM**, a cloud-based, cross-platform social media and instant messaging (IM) service, registered in the British Virgin Islands (BVI) with a legal address for correspondence usually listed as Conyers Trust Company (BVI) Limited, Commerce House, Wickhams Cay 1, P.O. Box 3140, Road Town, Tortola, VG1110, British Virgin Islands.

7. As set forth in more detail below, and based on my training and experience, there is probable cause to believe that the Target Funds and Target Sites are subject to seizure and forfeiture, since any property, real or personal, that is involved in, constitutes, or is derived from proceeds traceable to violations of 18 U.S.C. §§ 1956 (Money Laundering Conspiracy), 1343 & 1349 (Wire Fraud Conspiracy), is subject to criminal and civil seizure and forfeiture under 18 U.S.C. § 981 and 28 U.S.C. § 2461(c).

III. STATUTES

A. Substantive Criminal Offenses

8. Wire fraud: 18 U.S.C. § 1343 makes it a crime for anyone, having devised 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, to transmit or cause 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. 18 U.S.C. § 1349 criminalizes any attempt or conspiracy to violate, *inter alia*, 18 U.S.C. § 1343.

9. Concealment money laundering: 18 U.S.C. § 1956(a)(1)(B)(i) makes it a crime to conduct or attempt to conduct a financial transaction, knowing that the property involved in the transaction represents the proceeds of some form of unlawful activity, and which in fact involves the proceeds of specified unlawful activity, knowing that the transaction is designed in whole or in part to conceal the nature, the location, the source, the ownership, or the control of the proceeds of specified unlawful activity.

B. Asset Forfeiture Statutes

10. Pursuant to 18 U.S.C. § 981(a)(1)(A), any property, real or personal, involved in a transaction or attempted transaction in violation of 18 U.S.C. §§ 1956 and 1957 (money laundering, engaging in monetary transactions in property derived from specified unlawful activity, and conspiracy to commit these offenses), is subject to forfeiture to the United States, as is any property traceable to such violation.

11. Pursuant to 18 U.S.C. § 982(a)(1), any property, real or personal, involved in a transaction or attempted transaction in violation of 18 U.S.C. §§ 1956 and 1957 (money laundering, engaging in monetary transactions in property derived from specified unlawful

activity, and conspiracy to commit these offenses), is subject to forfeiture to the United States, as is any property traceable to such violation. Forfeiture pursuant to these statutes applies to more than just the proceeds of the crime. These forfeitures encompass all property "involved in" the crime, which can include untainted funds that are commingled with tainted funds derived from illicit sources.

12. In cases involving a money laundering offense, the forfeiture statutes permit the government to forfeit property "involved in" money laundering. *See* 18 U.S.C. §§ 981(a)(1)(A), 982(a)(1). "It is . . . clear that Congress intended criminal forfeiture provisions to eliminate profit from certain criminal activities, including money laundering . . . ." *United States v. Casey*, 444 F.3d 1071, 1073 (9th Cir. 2006). "Consequently, when legitimate funds are commingled with property involved in money laundering or purchased with criminally derived proceeds, the entire property, including the legitimate funds, is subject to forfeiture." *United States v. Kivanc*, 714 F.3d 782, 794-95 (4th Cir. 2013); *see also United States v. Guerrero*, 2021 WL 2550154, *9 (N.D. Ill. June 22, 2021) ("[C]omingling 'clean' money with crime proceeds can 'make[ ] money laundering less difficult and may even be necessary to the successful completion of the offense .' . . . As a result, courts have found that untainted funds are 'involved for purposes of the forfeiture statute.'" (internal citations omitted)). "[I]n a money laundering charge, the commingling of tainted money with clean money taints the entire account. The money transferred from a commingled account does not need to be traceable to fraud, theft, or any wrongdoing at all. It is enough that the money, even if innocently obtained, was commingled in an account with

money that was obtained illegally." *United States v. Lazarenko*, 564 F.3d 1026, 1035 (9th Cir. 2009) (internal citations omitted).

13. Pursuant to 18 U.S.C. § 981(a)(1)(C), any property, real or personal, which constitutes or is derived from proceeds traceable to the violation of an enumerated statute constituting a specified unlawful activity "is subject to forfeiture to the United States." Specified unlawful activities are detailed therein, as well as at 18 U.S.C. §§ 1956(c)(7) and 1961(1), which enumerates wire fraud as a specified unlawful activity. This section provides both civil forfeiture authority and criminal forfeiture authority by virtue of 28 U.S.C. § 2461(c). A violation of the wire fraud statute and conspiracy to violate the wire fraud statute are defined as "specified unlawful activities" pursuant to 18 U.S.C. 1956(c)(7)(D).

14. Pursuant to 18 U.S.C. § 982(a)(2)(A), any property constituting, or derived from, proceeds obtained directly or indirectly, as the result of such violation of 18 U.S.C. §1343, is subject to forfeiture to the United States, as is any property traceable to such violation. A violation of 18 U.S.C. §§1343 and 1349 is a "specified unlawful activities" pursuant to 18 U.S.C. § 1956(c)(7)(D).

15. 18 U.S.C. §981(b) states that property subject to forfeiture under Section 981 may be seized via a civil seizure warrant issued by a judicial officer "in any district in which a forfeiture action against the property may be filed," and may be executed "in any district in which the property is found," if there is probable cause to believe the property is subject to forfeiture. 18 U.S.C. § 982(b)(1) incorporates the procedures in 21 U.S.C. § 853 (other than subsection (d)) for

all stages of a criminal forfeiture proceeding. Section 853 permits the government to request the issuance of a seizure warrant for property subject to criminal forfeiture.

16. This application seeks a seizure warrant under both civil and criminal authority because the property to be seized could easily be placed beyond process if not seized by warrant, as cryptocurrency is fungible and easily dissipated. 21 U.S.C. §853(f), made applicable by 18 U.S.C. §982(b)(1) and 28 U.S.C. §2461(c), authorizes the court to issue a criminal seizure warrant "in the same manner as provided for a search warrant." Under Section 853(f), "[i]f the court determines that there is probable cause to believe that the property to be seized would, in the event of conviction, be subject to forfeiture and that a [restraining] order under subsection [853](e) may not be sufficient to assure the availability of the property for forfeiture, the court shall issue a warrant authorizing the seizure of such property." 21 U.S.C. § 853(f).

17. We submit that a restraining order under 21 U.S.C. § 853(e) is insufficient to assure the availability of the funds sought to be seized for forfeiture because we have been advised of cases in which, even after a restraining order or similar process has been issued to a financial institution, the funds sought to be restrained were not effectively restrained by the financial institution. Furthermore, we are aware that courts have held that criminal seizure, instead of restraint, is appropriate when assets are fungible and readily transferable. *See, e.g., United States v. Dupree*, 781 F. Supp. 2d 115, 133 (E.D.N.Y. 2011) (citing *United States v. Daccarett*, 6 F.3d 37, 49 (2d Cir.1993) (holding that "seizure under the criminal statutes was thus appropriate because the seized funds could be, and had been, easily transferred in and out of the accounts.)); *see also United States v. Martin*, 460 F. Supp. 2d 669, 677 (D. Md. 2006) ("Given the fungible and readily transferable nature of the property (mostly cash) and the size and seriousness of this alleged conspiracy . . . this Court cannot conclude that there was no probable cause to believe that

a seizure warrant was necessary to secure the property"). Therefore, we submit that seizure warrants are the most effective way to assure the availability of funds in the SUBJECT ADDRESSES sought to be seized for forfeiture.

18. 18 U.S.C. § 981(b) states that property subject to forfeiture under Section 981 may be seized via a civil seizure warrant issued by a judicial officer "in any district in which a forfeiture action against the property may be filed," and may be executed "in any district in which the property is found," if there is probable cause to believe the property is subject to forfeiture. 18 U.S.C. § 982(b)(l) incorporates the procedures in 21 U.S.C. § 853 (other than subsection (d)) for all stages of a criminal forfeiture proceeding. 21 U.S.C. § 853(f) permits the government to request the issuance of a seizure warrant for property subject to criminal forfeiture.

IV. JURISDICTION AND VENUE

19. As explained in further detail below, the United States District Court for the District of Columbia has jurisdiction and venue to issue the requested civil seizure warrant, pursuant to 18 U.S.C. § 981(b)(3) and 28 U.S.C. §1355(b)(2), because the property is subject to forfeiture under the laws of the United States and is located in a foreign-domiciled account in the custody of Tether. The United States District Court for the District of Columbia also has jurisdiction to issue the requested criminal seizure warrant, pursuant to 18 U.S.C. §853(l), because district courts have jurisdiction to enter orders under Section 853, including seizure warrants under Section 853(f), without regard to the location of any property that may be subject to criminal forfeiture. The United States District Court for the District of Columbia would also be proper venue in which the United States could seek to charge the underlying criminal conduct and to seek criminal forfeiture, under 18 U.S.C. § 3238, because the criminal offenses under investigation appears to have begun or to

have been committed 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.

V. RELEVANT TERMS

Cryptocurrency Related Terms

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

21. **Blockchain:** A blockchain is a digital ledger run by a decentralized network of computers referred to as "nodes." Each node runs software that maintains an immutable and historical record of every transaction utilizing that blockchain's technology. Many digital assets, including virtual currencies, publicly record all their transactions on a blockchain, including all of the known balances for each virtual currency address on the blockchain. Blockchains consist of blocks of cryptographically signed transactions, and blocks are added to the previous block after

validation and after undergoing a consensus decision to expose and resist tampering or manipulation of the data. There are many different blockchains used by many different virtual currencies. For example, Bitcoin in its native state exists of the Bitcoin blockchain, while Ether (or "ETH") exists in its native state on the Ethereum network.

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

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

24. **Virtual Currency Exchange:** A virtual currency exchange ("VCE"), also called a virtual currency exchange, is a platform used to buy and sell virtual currencies. VCEs allow users to exchange their virtual currency for other virtual currencies or fiat currency, and vice versa. Many VCEs also store their customers' virtual currency addresses in hosted wallets. VCEs can be centralized (i.e., an entity or organization that facilitates virtual currency trading between parties on a large scale and often resembles traditional asset exchanges like the exchange of stocks) or decentralized (i.e., a peer-to-peer marketplace where transactions occur directly between parties).

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

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

27. **Transaction Fee:** A transaction fee is a fee paid by the party sending virtual currency on a blockchain to reward miners and/or validators for verifying and validating transactions. Transaction fees vary by blockchain and can fluctuate based on factors such as blockchain network traffic and transaction sizes. Senders of virtual currency can increase the transaction fees that they pay to have their transactions confirmed faster by miners and/or validators. Transaction fees are generally paid in a blockchain's native token (*e.g.*, Bitcoin on the Bitcoin blockchain).

28. **Stablecoins:** Stablecoins are a type of virtual currency whose value is pegged to a commodity's price, such as gold, or to a fiat currency, such as the U.S. dollar, or to a different virtual currency. For example, Tether (also known as USDT) is a stablecoin pegged to the U.S. Dollar. Stablecoins achieve their price stability via collateralization (backing) or through algorithmic mechanisms of buying and selling the reference asset or its derivatives.

29. **Tether:** Tether International S.A. de C.V. ("Tether") is the company that manages the smart contracts and the treasury (i.e., the funds held in reserve) for USDT tokens.

30. **USD Tether:** USD Tether ("USDT") is a "stablecoin" virtual currency with its value tied to the US dollar. USDT is issued by Tether.

31. **Ether:** Ether ("ETH") is a virtual currency that is the native token used by the Ethereum blockchain, which is a blockchain with smart contract functionality.

32. **Tron:** Tron is a blockchain with smart contract functionality.

33. **USD Coin:** USD Coin ("USDC") is a "stablecoin" virtual currency with its value tied to the US dollar. USDC is issued by Circle Internet Financial, LLC.

Telegram Related Terms[1]

34. **Telegram** is an internationally available electronic messaging service, which allows users to communicate through channels, groups, secret chats, and one-on-one chats. As opposed to traditional phone communications, Telegram users are not bound by geography; a Telegram user can communicate with any other user anywhere in the world simply through the Telegram application. For this reason, Telegram is a popular tool for those seeking to communicate internationally.

35. Additionally, Telegram features end-to-end encryption, a method of secure communication that prevents third parties from accessing data while it is transferred from one end system or device to another. Because only the intended recipient can decrypt the sent data, Telegram is broadly considered a more private and secure alternative to standard SMS or MMS communications. We know based on training and experience investigating Pig Butchering and other cybercrime matters, that likely because communications are encrypted, perpetrators commonly use Telegram to communicate with victims and associates. Telegram's encryption

[1] The following information was obtained from publicly-available information of Telegram available on its website and from Department of Justice employees who have experience with Telegram.

features allow perpetrators to conceal their communications from unwanted recipients, including law enforcement, and its international reach allows perpetrators to connect easily with victims across the globe.

36. **Telegram channels** allow one or more individuals to send messages or broadcast content to an unlimited number of "subscribers." Each Channel has an "owner," who can "broadcast messages, delete any messages, add subscribers (the first 200 only), remove subscribers, change the Channel's name, profile image and link, as well as delete the Channel completely. The owner can also add and remove administrators to help manage the channel." Only the owner or administrators of a Channel can post in the Channel. Posts are signed with the Channel's name instead of an individual user's name, although there is a setting that can identify the administrator who posts a message in the Channel. Channels can be either public or private. Any user can find and join a public channel, which has its own username. Users can only join a private channel if the Channel's owner invites them to join.

37. **Telegram groups** are separate and can have up to 200,000 "members." They can be either public or private. Any member can post (unless limited by a group administrator). By default, all members of a Group can invite new members and change the name of the Group and its profile picture. Group members can also designate "administrators" for the Group, which allows only the administrators to add new members, remove members, and change the Group information. Group members (or the Group's administrators, if enabled) can choose to make the Group public, allowing any user to view the Group's entire chat history or post messages.

38. Within a Telegram Group, members can reply to messages, mention other members (@username), and add hashtags to organize topics (#topic). In addition to plain text and hyperlinks, users can share files, such as images and documents. Users can generally "forward"

messages posted by other users. Forwarded messages include the text of the original post and can include a link to the original poster's profile.

39. **Telegram Secret Chats**, unlike other Telegram Groups, "use end-to-end encryption, leave no trace on [Telegram's] servers, support self-destructing messages and don't allow forwarding. On top of this, secret chats are not part of the Telegram cloud and can only be accessed on their devices of origin."

40. **Telegram One-on-One Chats** contain two participants who can share text and documents. Each participant can delete messages they have either sent or received, which also deletes those messages from the other participant's device. There is no time limit on the messages that a participant can delete from both devices.

VI. PROBABLE CAUSE

A. Background Related to Cryptocurrency Investment Scams

41. Based on training, experience, and research, we understand that a cryptocurrency investment fraud (CIF) schemes, also referred to by the perpetrators as "pig butchering scams," are a type of cryptocurrency-related investment, or confidence scam, that convinces victims to invest in cryptocurrency through non-existent cryptocurrency trading platforms. The scammer typically initiates contact through social media platforms and eventually forms a relationship with the victim to grow trust. Those relationships may be perceived by the victims as romantic, professional, or friendship based. The scammers often create profiles using fictitious names, locations, images, and personas, allowing the scammers to cultivate personal relationships with prospective victims.

42. The scammers promise a lucrative return of investment by manipulating an increase in balance to the victim's account on their fraudulent domain. The scammers also provide falsified

transaction photos that depict that scammers are contributing their own funds to the victim's initial investment. Often enticed by the falsified returns, the victim continues to invest, until they try to retrieve their gains, only to find that they are unable to retrieve them. The scam continues by the scammers demanding additional payments be made to the platform for their investments to be released and/or withdrawn. Examples include victims being required to pay an additional percentage to the fraudulent platform in order to guarantee the funds, prepay taxes on the balance, or to pay a fee/fine due to suspicious money laundering activities.

43. Based on a review of thousands of complaints made to the FBI through various reporting platforms, CIF schemes almost always involve use of U.S. wires to perpetrate the fraud. For instance, scammers may contact the U.S. victims via social media platforms like Facebook or dating websites like Match.com, or display fake profiles of glamorous individuals on Instagram. Scammers typically communicate with their U.S. victims via cellular phone services, texting them or using encrypted messaging applications like WhatsApp. And victims of CIF often use their U.S. bank accounts and U.S.-based cryptocurrency exchanges in order to deposit U.S. dollars into their cryptocurrency wallets, which are then used to transfer the funds to the scammers.

44. Based on our knowledge and experience, cryptocurrency-investment-scam compounds are predominantly based in Southeast Asia. These criminal organizations often use forced labor by means of human trafficked victims to perpetuate the crime globally.[2]

45. Based on training, experience, and research, we know that perpetrators of cryptocurrency investment scams are highly effective in gaining an individual's trust and/or affection in a short amount of time using manipulative tactics and language. We also know that a

---

[2] *FinCEN Alert* issued September 8, 2023, FinCEN Alert on Prevalent Virtual Currency Investment Scam Commonly Known as "Pig Butchering" *(FIN-2023-Alert005, Pg. 1-2.)*

single cryptocurrency investment scheme is often facilitated by multiple individuals with different roles and responsibilities. This is true of its operation in that there are registrants, developers, and controllers of these domains, that are prepared in advance to be used by the scammer prior to and throughout the lifecycle of victim engagement. We also know that the criminal syndicate commingles, consolidates, and coordinates their post-fraud money laundering activities of illicit victim proceeds linked to cryptocurrency investment scams.

46. 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 a U.S.-government funded study, "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]

47. According to the FBI's Internet Crime Complaint Center (IC3), cyber-enabled fraud schemes were responsible for almost 85% of all losses reported to IC3 in 2025. Within that category, CIF schemes have continued to grow, and the IC3 calculated the reported losses from CIF scams rose, from $4.57 billion in 2023, to $8.65 billion in 2025, an increase of 89%.[4] These figures, largely based on losses reported by victims, likely significantly under-represent the true loss amounts incurred by Americans, since most fraud victims do not report to IC3, if at all.[5]

---

3 U.S. Institute of Peace, *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 March 5, 2026).

4 IC3 (2025) Federal Bureau of Investigation Internet Crime Report. IC3, available at https://www.ic3.gov/AnnualReport/Reports/2025_IC3Report.pdf.

5 Statement of Gregory Heeb, Dep. Ass't Dir., FBI (Mar. 25, 2026), *available at* https://www.jec.senate.gov/public/_cache/files/2f5ca5c1-44c9-4e23-944e-8008293856f7/sfr-gregory-heeb.fbi.pdf.

48. The cryptocurrency ecosystem is used by criminals not only to receive victim money but also to launder it quickly, anonymously, and at scale. Like traditional money laundering, laundering money through cryptocurrency shares the same three stages of placement, layering, and integration, with different techniques applied within each:

a. **Placement** – Criminals use non-custodial, or "private" wallets to initially receive victim funds. This is because such wallets are unattributable to law enforcement by blockchain analysis alone, are simple to create, and can accept large transaction amounts without additional scrutiny.

b. **Layering** – Next, criminals will have victim funds transverse numerous private wallets, consolidate with other illegitimate and sometimes legitimate funds, and be subjected to other more cryptocurrency-specific processes to obfuscate both the origin of, and the ultimate destination for, the victim funds.

c. **Integration** – Finally, by using a diffuse network of "brokers," who agree to exchange cryptocurrency for fiat using various means, criminals render their proceeds liquid and fully integrated with the legitimate financial system.

B. Background on Guarantee Services

49. According to publicly available reporting, guarantee networks are commonly used by criminal groups in Southeast Asia to facilitate financial transactions with other criminal groups. Investigative journalists reporting on cyber-scam compound operators in Southeast Asia have noted that stories of money launderers "running away with the money" had often circulated on Chinese-language social media in Cambodia. [6] To prevent such occurrences, cyber-scam

[6] Chen, Yanyu. "Moving Bricks: Money-Laundering Practices in the Online Scam Industry," *Global China Pulse*, September 24, 2024. https://globalchinapulse.net/moving-bricks-money-laundering-practices-in-the-online-scam-industry/.

companies and money mule networks sought out guarantors or arbitrators to guarantee their transactions. These guarantee networks eliminate the risk of the other criminal group simply stealing the money sent to them, rather than actually performing the service requested or fulfilling a sale of goods or equipment.

50. According to the Royal United Services Institute, these guarantee networks can act as both online marketplaces and escrow services for their merchants, which range in legitimacy[7]. These vendors, often advertising their services on encrypted communications applications such as Telegram, can offer a wide variety of services to include money laundering or the sales of equipment or data used to support scam center operations.[8]

51. According to TRM Labs, these vendors interact with prospective clients within Telegram "rooms," overseen by a representative from the guarantee network. Because the transaction is essentially guaranteed by the network, clients are able to send funds to the vendor with the knowledge the vendor's "security deposit" will be drawn upon if the service is not delivered, eliminating the risk for the cybercriminal actor interacting with the vendor. Many of these clients also use a cryptocurrency wallet provided by the guarantee network, complicating tracing by law enforcement[9].

---

[7] Robinson, Tom. "Multi-Billion Dollar Guarantee Marketplaces Exploit Stablecoins for Scams." *Royal United Services Institute*, May 19, 2026. https://www.rusi.org/explore-our-research/publications/commentary/multi-billion-dollar-guarantee-marketplaces-exploit-stablecoins-scams.

[8] Elliptic Research, "Xinbi: The $8 Billion Colorado-Incorporated Marketplace for Pig-Butchering Scammers and North Korean Hackers" (May 12, 2025), *available at* https://www.elliptic.co/blog/xinbi-guarantee.

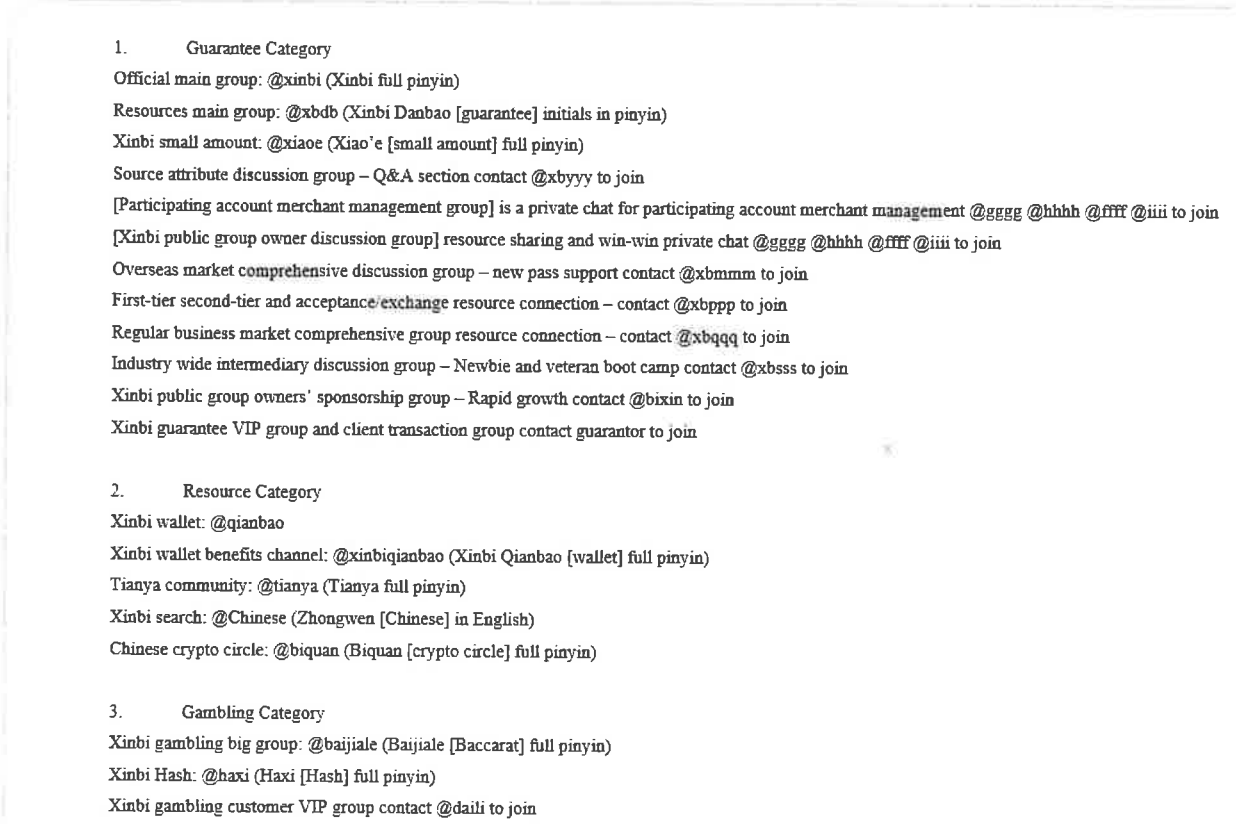
[9] TRM Team. "Xinbi Marketplace Remains Active with USD 17.9 Billion in Total Volume Despite Enforcement Actions," TRM Labs, February 6, 2026. https://www.trmlabs.com/resources/blog/xinbi-marketplace-remains-active-with-usd-17-9-billion-in-total-volume-despite-enforcement-actions.

C. Xinbi Guarantee

Background

52. Xinbi Guarantee (Xinbi) is a Chinese-language Telegram-based marketplace that also acts as a guarantee network for its vendors. Affiant [redacted] personally reviewed Telegram channels associated with Xinbi, as well as exports of multiple Xinbi-affiliated Telegram groups. Xinbi purports to act as a neutral third-party that holds funds in escrow while services are rendered. Vendors, or "merchants," register with Xinbi and also post a deposit of required collateral, the amount which can vary based on the service offered.[10] Once allowed on the Xinbi platform (i.e., the Telegram page), these merchants can market their goods and services and engage securely with prospective buyers. The screenshot below shows how Xinbi advertises its use of Telegram and the Telegram pages:

[10] See supra note 7 and accompanying text.



New official groups

1. Guarantee Category

Official main group: @xinbi (Xinbi full pinyin)

Resources main group: @xbdb (Xinbi Danbao [guarantee] initials in pinyin)

Xinbi small amount: @xiaoe (Xiao'e [small amount] full pinyin)

Source attribute discussion group – Q&A section contact @xbyyy to join

[Participating account merchant management group] is a private chat for participating account merchant management @gggg @hhhh @ffff @iiii to join

[Xinbi public group owner discussion group] resource sharing and win-win private chat @gggg @hhhh @ffff @iiii to join

Overseas market comprehensive discussion group – new pass support contact @xbmmm to join

First-tier second-tier and acceptance/exchange resource connection – contact @xbppp to join

Regular business market comprehensive group resource connection – contact @xbqqq to join

Industry wide intermediary discussion group – Newbie and veteran boot camp contact @xbsss to join

Xinbi public group owners' sponsorship group – Rapid growth contact @bixin to join

Xinbi guarantee VIP group and client transaction group contact guarantor to join

2. Resource Category

Xinbi wallet: @qianbao

Xinbi wallet benefits channel: @xinbiqianbao (Xinbi Qianbao [wallet] full pinyin)

Tianya community: @tianya (Tianya full pinyin)

Xinbi search: @Chinese (Zhongwen [Chinese] in English)

Chinese crypto circle: @biquan (Biquan [crypto circle] full pinyin)

3. Gambling Category

Xinbi gambling big group: @baijiale (Baijiale [Baccarat] full pinyin)

Xinbi Hash: @haxi (Haxi [Hash] full pinyin)

Xinbi gambling customer VIP group contact @daili to join

Fig. 1 – Screenshot of the Xinbi website on February 16, 2025, machine translated and reviewed by an FBI linguist.[11]

[11] This and the following screenshots were taken on July 21, 2026 from the Wayback Machine (which archives internet content) at https://web.archive.org/web/20250216000552/https://www.xinbi.com/. The date of the Wayback Machine historical snapshot was February 16, 2025. For all the webpages contained herein, your Affiant used a machine translation service and then had the results reviewed by an FBI Chinese linguist.

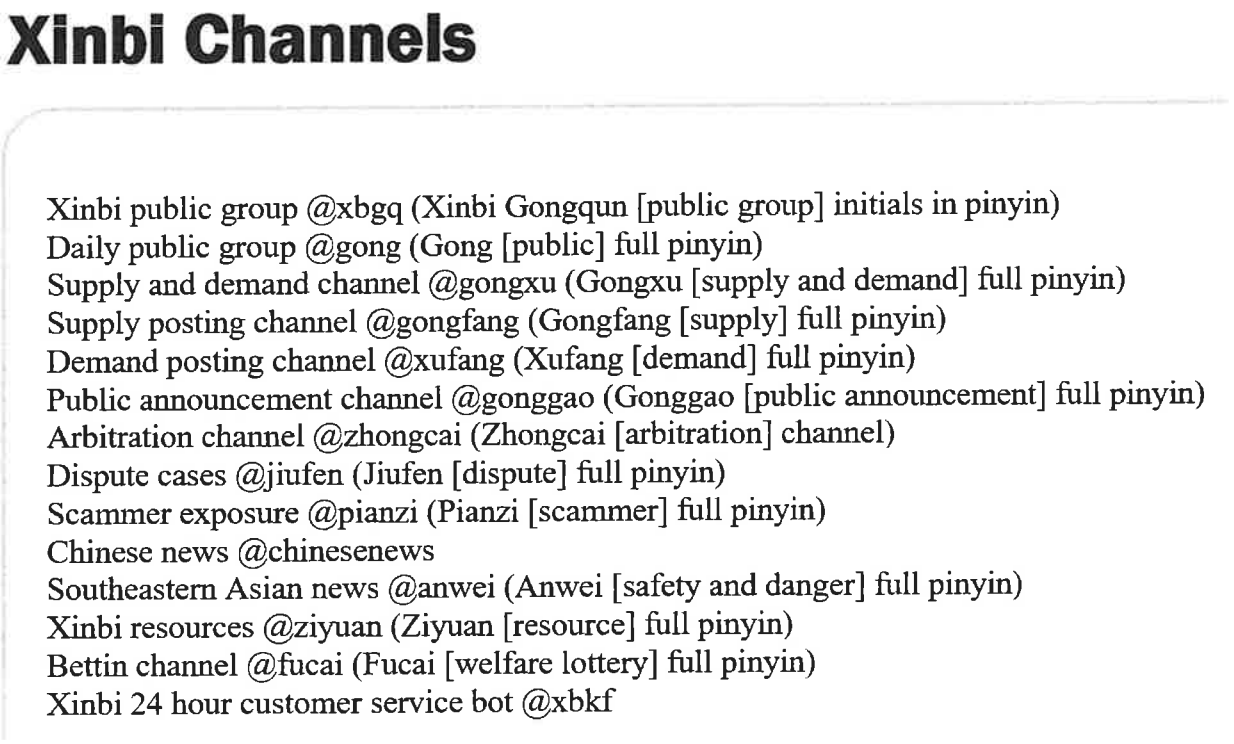


Fig. 2 – Screenshot of the Xinbi website on February 16, 2025, showing use of Telegram Channels.

53. Information on the Xinbi Telegram Channel and on Xinbi's website (www.xinbi.com) shows that Xinbi will guarantee financial transaction conducted within their groups up to the merchant's deposit limit. Xinbi's own website states, "The current business scope guaranteed by Xinbi includes but is not limited to: Providing guarantees for all regions around the world (except for Mainland China) for virtual currency transactions, asset transactions, motor vehicle transactions, and network technology talent, aspiring to ensure the security of funds for users." (This quote was from an August 6, 2026 screenshot of the Xinbi website, which was later translated by an FBI linguist.) A separate August 6, 2026 screenshot of a Xinbi Telegram channel post stated, "We [Xinbi] only guarantee transactions within the public group, not the group owner's personal reputation." (This post was also translated by an FBI linguist.) The below screenshot shows how Xinbi advertises its guarantee services:

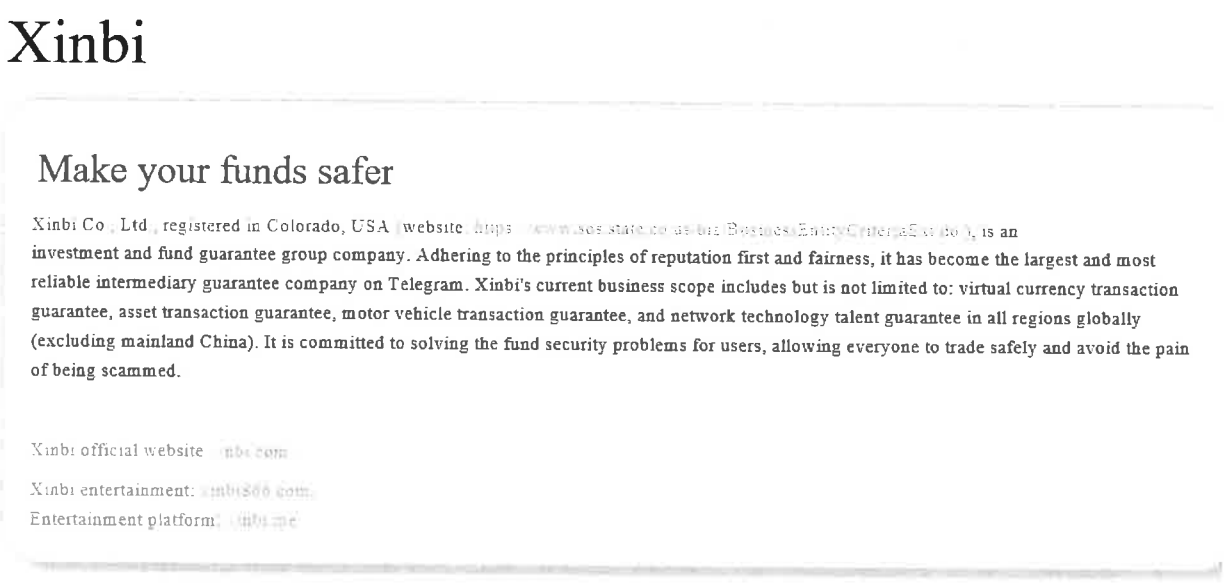


Fig. 3 – Screenshot of the Xinbi website on February 16, 2025, showing description of guarantee services.

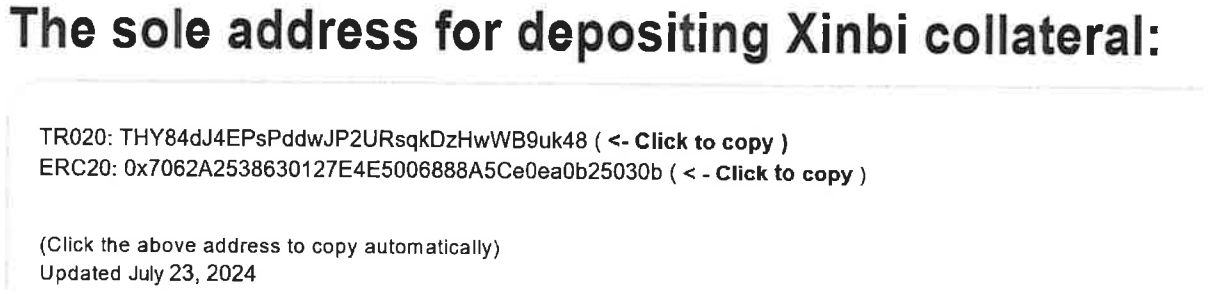


Fig. 4 – Screenshot of the Xinbi website on February 16, 2025, showing description of guarantee wallets.[12]

54. As seen in the screenshots above from Xinbi's website, Xinbi's escrow, or "collateral" wallet (referred to further herein as an "Onboarding Address") is publicized, so its merchants and their clients can have certainty regarding where to send funds while using the

[12] Although the above collateral address is shown to have been last updated July 23, 2024. It is Affiant [redacted] understanding that Xinbi now changes consolidation wallets much more frequently. Affiant [redacted] has reviewed additional screen captures from later in 2025, which appear to show an update within the prior 24 hours, as opposed to 7 months. Affiant [redacted] has also reviewed a screen capture from May 15, 2025, which indicated it was last updated May 10, 2025.

network. Based on my training and experience, this public wallet display assures the merchants and the clients that, because Xinbi will guarantee the transaction, they cannot be defrauded by other criminal actors convincing them to send funds to a non-Xinbi wallet.[13]

55. Based on our review of the Telegram pages, expert reports, and cryptocurrency block chain, Xinbi's marketplace operates as follows:

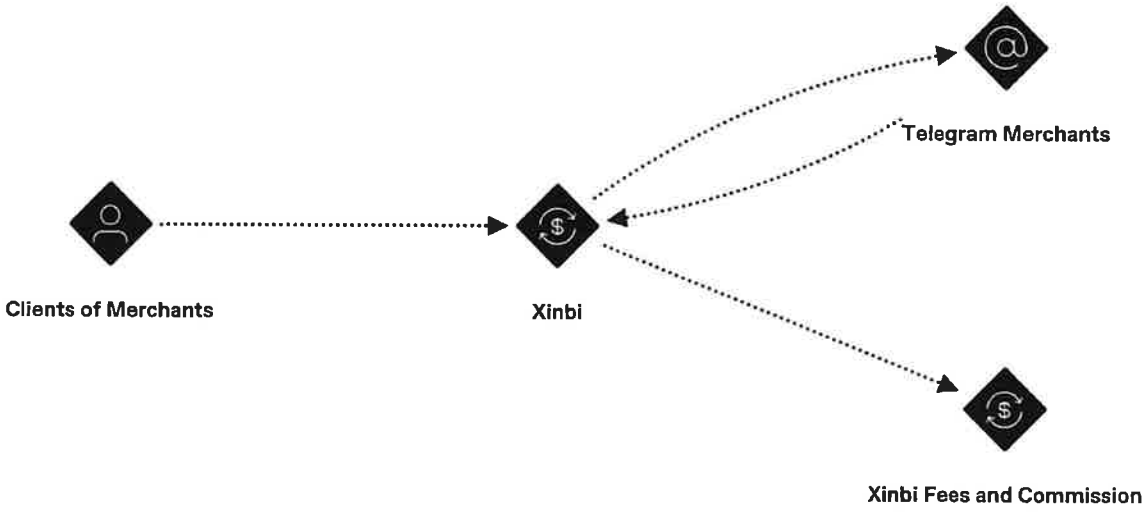
a. Clients pay cryptocurrency directly to merchants. When the merchants receive payment, they provide the client with the requested service. The merchants pay fees into the Xinbi cryptocurrency address as payment for using the Xinbi platform. Xinbi keeps these fees as profit.

Demonstrative 1: Interaction Between Clients, Merchants, and Xinbi on the Xinbi Marketplace

b. According to Export Report 2, described later in this affidavit, oftentimes, clients and merchants will require Xinbi to act as a guarantee service. Certain Telegram groups are configured to facilitate these transactions. Xinbi still charges similar fees as the above structure from the merchants; in addition, Xinbi will take a commission, often 3%, of each transaction processed through Xinbi. In these scenarios, clients will deposit funds directly into Xinbi's cryptocurrency address. Xinbi will consolidate the

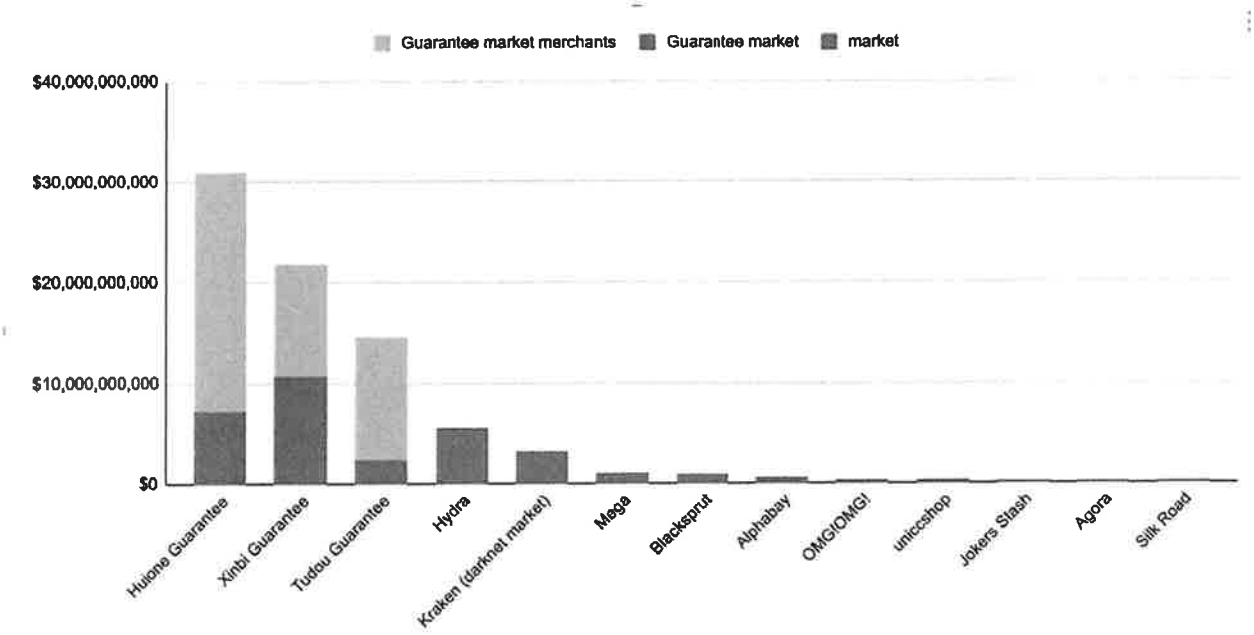
[13] As described further herein, information reported to me by multiple sources shows that Xinbi changes this wallet address with regularity, approximately every two weeks. See infra Pt. D.

funds and, upon verification from the client and merchant that the contract has been satisfied, release the funds to the merchant. Xinbi will keep its percentage as commission.



Demonstrative 2: Interaction Between Clients and Merchants using the Xinbi Guarantee

56. Based on blockchain analysis, further described in this affidavit, investigators estimate that, since its inception in 2022, Xinbi has received a total inflow of funds exceeding 11 billion US Dollars. Elliptic, a private blockchain analysis firm, estimates that the thousands of merchants who utilize Xinbi's Telegram channels and guarantee infrastructure have also received a total inflow of funds exceeding 11 billion US Dollars. Figure 3, provided by Company 2, illustrates the amount of funds flowing through Xinbi and its merchants compared to other marketplaces.



Demonstrative 3: Total flow of Funds into Guarantees and Darknet Markets

Sanctions and Regulation

57. According to chats in Xinbi telegram groups, @biquan/@xinbi, Xinbi staff advertised the launch of a physical Xinbi storefront within Yatai New City, a large compound of scam centers in Shwe Kokko, Myanmar. Yatai New City was sanctioned by the United States in violation of human rights abuses and facilitating cyberfraud against American citizens.[14] The buildings which surrounded the storefront were identified as scam centers[15]. This storefront directly contradicts Xinbi's operating terms associated with avoiding human trafficking and US scam funds. Figure 5, a photo posted by Xinbi staff, shows the Xinbi storefront between the Hongtu scam center towers with xinbi[.]com visible on the signage.[16]

---

[14] U.S. Dept. of the Treasury, Treasury Sanctions Southeast Asian Networks Targeting Americans with Cyber Scams (Sept. 8, 2025), *available at* https://home.treasury.gov/news/press-releases/sb0237

[15] BBC News, Inside the brand new city 'built on scams' on the Myanmar-Thai border (Youtube, Feb 7, 2025), *available at* https://www.youtube.com/watch?v=dRbYZZa1UX4.

[16] Post on the @biquan Telegram channel, https://t.me/biquan/71(June 13, 2025).

Fig. 5 - Xinbi Storefront in Yatai New City

58. On March 26, 2026, Xinbi Guarantee was designated by the United Kingdom's Foreign, Commonwealth and Development Office (FCDO), describing it as "a Chinese-language online marketplace that enables the operation of scam centres in Southeast Asia by offering cryptocurrency-based services. It is one of the largest such marketplaces and has facilitated the laundering of stolen crypto assets by North Korea."[17] The United Kingdom Secretary of State considered there were,

[17] "UK crackdown on vile scam centres steps up with sanctions on illicit crypto network," March 26, 2026, *available at* https://www.gov.uk/government/news/uk-crackdown-on-vile-scam-centres-steps-up-with-sanctions-on-illicit-crypto-network.

> reasonable grounds to suspect that "Xinbi Company Limited ("Xinbi") is an involved person within the meaning of the Global Human Rights Sanctions Regulations 2020 on the basis of the following grounds: (1) Xinbi is or has been involved in providing financial services or making available funds, economic resources, goods or technology, knowing or having reasonable cause to suspect that those financial services or funds will or may contribute to human rights abuses, and; (2) Xinbi is or has been involved in profiting financially or otherwise obtaining a benefit from human rights abuses. Xinbi has enabled and profited from the operation of scam centres in Southeast Asia. The treatment of individuals in these scam centres amounts to a serious abuse of the right not to be subjected to cruel, inhumane, or degrading treatment or punishment, and of the right to be free from slavery, not to be held in servitude or required to perform forced or compulsory labour.[18]

59. According to public reports by two blockchain analytics firms that have studied Xinbi Guarantee (TRM Labs and Elliptic), Xinbi appears to be a hub of highly sophisticated money laundering networks. According to these blockchain firms' analyses, Xinbi knowingly supports cybercriminals and the scam economy in Southeast Asia by running illicit Telegram-based marketplaces that serve cybercriminals who run cyber-enabled fraud schemes.[19,20]

60. [redacted]

61. A query of the publicly-available Kingdom of Cambodia business registrations for "Xinbi" and "XinbiPay" revealed that XinbiPay Trading Co., Ltd. was registered in June of 2025. The listed business activity for the company is "computer programming, consultancy, and related services." Based on the information reviewed by the investigators, along with blockchain analysis

---

[18] "Xinbi Company Limited," UK Sanctions List, March 26, 2026, *available at* https://search-uk-sanctions-list.service.gov.uk/designations/GHR0190/Entity.

[19] Guarantee Marketplace Profile Xinbi Guarantee, TRM Labs, March 26, 2026. https://www.trmlabs.com/resources/intel-library/xinbi-guarantee.

[20] Elliptic Research, "Xinbi: The $8 Billion Colorado-Incorporated Marketplace for Pig-Butchering Scammers and North Korean Hackers," *available at* https://www.elliptic.co/insights/xinbi-guarantee/ (last visited Sept. 3, 2026).

between addresses attributed to Xinbi and XinbiPay, investigators believe the two companies are affiliated organizations based in Southeast Asia.

62. According to information from the Colorado Secretary of State's Office, Xinbi Co., Ltd was registered as a business entity in Colorado in or around August 2022. Xinbi's website (www.xinbi[.]com) advertised this specific registration at least as late as February 16, 2025.

63. According to a publicly-filed lawsuit, on or around May 20, 2026, the Colorado Attorney General's Office filed a suit to dissolve the "fraudulently formed and operated business entity" Xinbi Co., Ltd. The lawsuit alleges Xinbi fraudulently filed its articles of incorporation with the Colorado Secretary of State by using a commercial address not connected to the company as the company's principal office address and registered agent address and Xinbi did not have consent or authorization to use the address it used in its Secretary of State filings to register itself as a corporation.[21,22]

Use of Telegram

64. According to TRM Labs, Xinbi has been previously banned from operating on Telegram in or around May 2025,[23] but, as seen below from the information obtained by the FBI, continues to operate on the platform on a number of channels. Xinbi manages the Telegram channels, resolves disputes, and advertises merchants to prospective clients. Xinbi is compensated by the merchants for allowing the merchant to operate within its Telegram structure. For example,

---

[21] "Attorney General Weiser launches crackdown on fraudulent Colorado businesses tied to national and international scam networks," Office of the Colorado Attorney General, May 21, 2026, *available at* https://coag.gov/press-releases/weiser-launches-crackdown-on-fraudulent-colorado-businesses/.

[22] https://coag.gov/app/uploads/2026/05/2026CV031373-Xinbi.pdf

[23] TRM Labs, "Huione Guarantee and Xinbi Still Operating on Telegram Despite Ban, Underscoring Illicit Actors' Persistence," May 30, 2025, *available at* https://www.trmlabs.com/resources/blog/huione-guarantee-and-xinbi-still-operating-on-telegram-despite-ban-underscoring-illicit-actors-persistence.

according to Expert Report 2, described later in this affidavit, Xinbi charges a 200 USDT one-time group opening fee, a recurring monthly fee of 600 USDT, and a fee per post on the Xinbi advertising Telegram channel of 200 USDT. These fees vary based on the type of Telegram group, with some merchants being charged as much as 30,000 USDT to open a group.[24]

65. Based on a combination of research from expert analytics firms (as discussed further herein), the Xinbi website itself, and reporting from a confidential human source[25] with access, Xinbi Guarantee operates (at least)[26] the following affiliated Telegram channels along with their listed descriptions:

No.	Telegram Channel	Description
i.	@gqdh (Target Site 1)	Public Group Channel
ii.	@xbdh (Target Site 2)	Public Group Backup Channel
iii.	@gonggao	Announcement Channel
iv.	@gong	Newly Opened Public Groups
v.	@abcd	Supply & Demand Channel
vi.	@kashang	Card Merchant Categories Channel
vii.	@xufang	Demand Channel
viii.	@gongfang	Supplier Channel
ix.	@pianzi	Scammer Exposure Channel
x.	@zhongcai	Arbitration Channel
xi.	@jiufen	Dispute Channel
xii.	@fucai	Lottery/Gambling Channel

[24] See footnote 11.

[25] The CHS has provided information regarding Xinbi Guarantee as well as other networks of criminals operating in Southeast Asia and committing mass wire fraud against U.S. victims and through the use of U.S. wires. The CHS has received no money from the FBI. The CHS's information about Xinbi has been verified by other sources, as described herein.

[26] Public information appears to associate additional Telegram Channels with Xinbi.

xiii.	@gaoshou	Expert Tips Channel
xiv.	@xinbei	Investment Promotion Channel
xv.	@xbgx	Supply & Demand Backup Channel
xvi.	@xincai	Premier Entertainment Channel
xvii.	@zhuanqunxb	Specialized Group Process Channel

66. Xinbi's primary Telegram channel for its merchant groups is @gqdh (Target Site 1). Affiant [redacted] reviewed the contents of this Telegram Channel as supplied by the CHS, who is a member of the Channel and provided an export of it to the FBI. On the @gqdh channel, Xinbi posts a directory of its merchants. The channel, which currently has over 650,000 subscribers, serves as the landing page for new users of Xinbi.

67. The @xbdh channel (Target Cite 2) is openly being advertised by Xinbi as the backup channel to the @gqdh channel, and it contains a completely identical directory post, complete with the same hyperlinks. Affiant [redacted] reviewed the @xbdh channel and saw it had the same style of posts listing out groups similar to the @gqdh channel.

68. Additionally, in reviewing the @gqdh channel, the Affiants reviewed and relied upon two expert reports, each of which describes the content of the Xinbi Telegram Channels.

a. Expert Report 1 was written by a blockchain-intelligence company (Company 1) that analyzes crypto transactions. Expert Report 1 was commissioned by the U.S. government pursuant to an expert contract at Company 1's standard hourly rates. Expert Report 1 also included a listing of more than 430 wallets that Company 1 identified as on the Xinbi network between October 30, 2023, and August 8, 2026. This included approximately 111 wallets identified by Company 1 as "deposit collection wallets," i.e., the wallets listed as the "sole address for depositing Xinbi collateral" (see,

e.g., the screenshot displayed Fig. 4, supra), between the period of November 2, 2024, and August 8, 2026. The U.S. government has used the services of Company 1 in numerous other cases.

b. Expert Report 2 was written and produced by a blockchain analytics firm pursuant to a government contract. Expert Report 2 was commissioned by the U.S. government pursuant to an expert contract at Company 2's standard hourly rates. Expert Report 2 included reviews of the Telegram Channels used by Xinbi, which included review of multiple merchants listings within the Telegram Channels. The U.S. government has used the services of Company 2 in numerous other cases.

69. The @gqdh channel contains a post that lists eleven categories of services provided by merchants, which includes hyperlinks to other posts within the Channel. These hyperlinked posts contain lists of merchant groups, which have also been hyperlinked.

70. As seen in the screenshots below, the @gqdh channel serves as the main directory for the eleven categories (noted below with numbers 1-11) of groups within the Xinbi Telegram network.

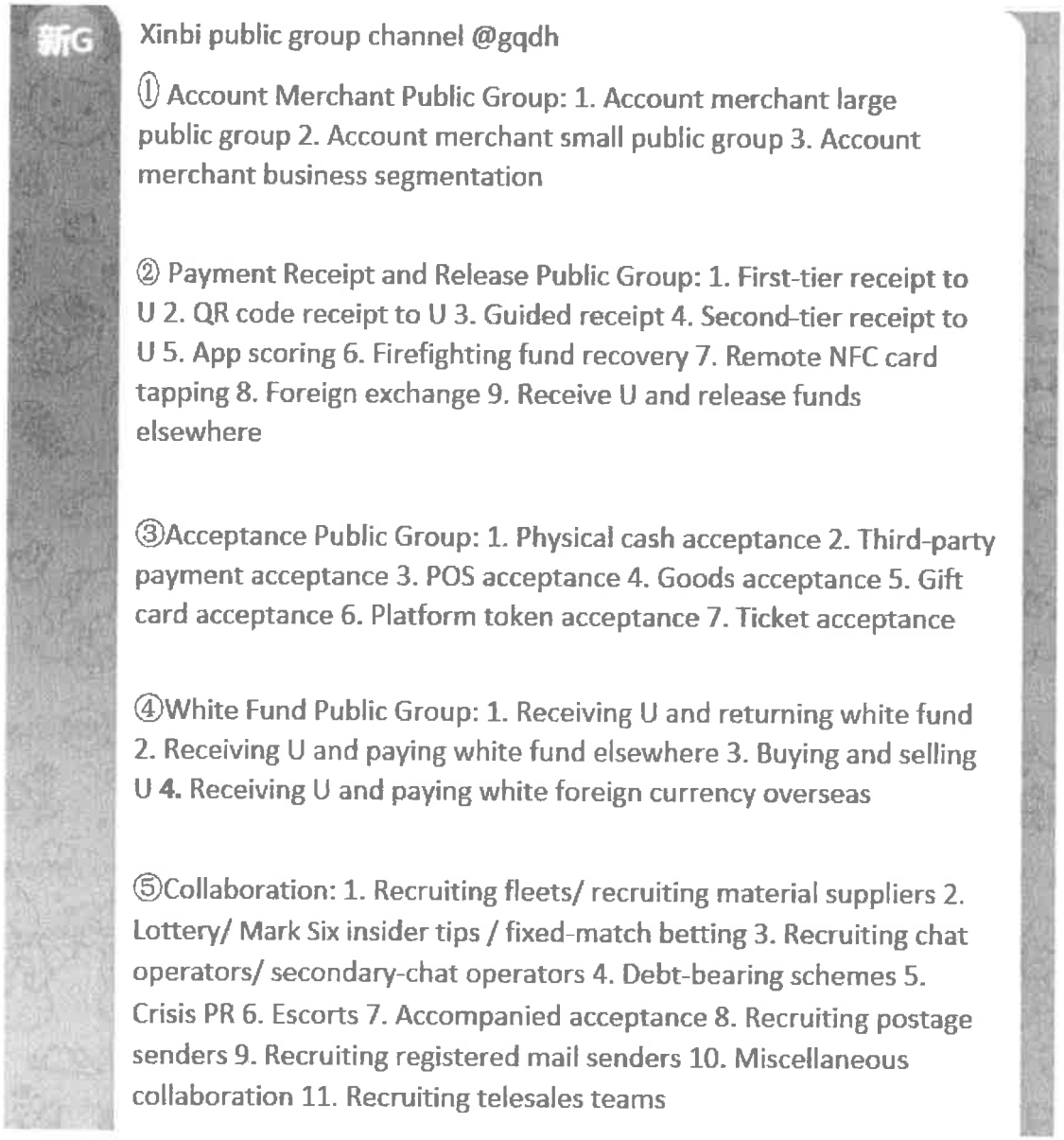


Fig. 6 – August 7, 2026 screenshot of the Xinbi @gqdh Telegram channel directory post.

⑥Service category: 1. Tianyancha [data look-up] 2. Ticket payment service 3. Social media account rental 4. Graphic design 5. SMS verification-code services 6. Account/exchange unfreezing 7. Errands and call services 8. High-end escorts 9. [Apple] ID loans 10. AI face swapping tools 11. Other services

⑦ Infrastructure category: 1. Platform design 2. Robots 3. Servers 4. Retrieval plugins 5. Remote control 6. Domain names 7. Custom IPs 8. [App] signing and app store listings

⑧Cryptocurrency related: 1. *NewPay* 2. Spot and futures trading 3. Coin mixing and cross-chain swaps 4. TRX & energy rental

⑨Goods buying and selling category: 1. Various accounts 2. SIM cards 3. 888 anonymous number NFTs 4. Tobacco and alcohol 5. Health supplements / luxury goods 6. Telegram accounts/memberships 7. Gold-plated tungsten/high-quality replica mobile phones 8. Other trading

Fig. 7 – August 7, 2026 screenshot (cont.) of the Xinbi @gqdh Telegram channel directory post.

⑩Gambling public groups: 1. PC 2.0 / PC high stakes/ PC cloud storage 2. Dice 3. Comprehensive betting/electronic [games] 4. Baccarat 5. Sports [betting] 6. Mark six 7. Texas hold'em 8. Red Envelope 9. Other games

Fig. 8 – August 7, 2026 screenshot (cont.) of the Xinbi @gqdh Telegram channel directory post.

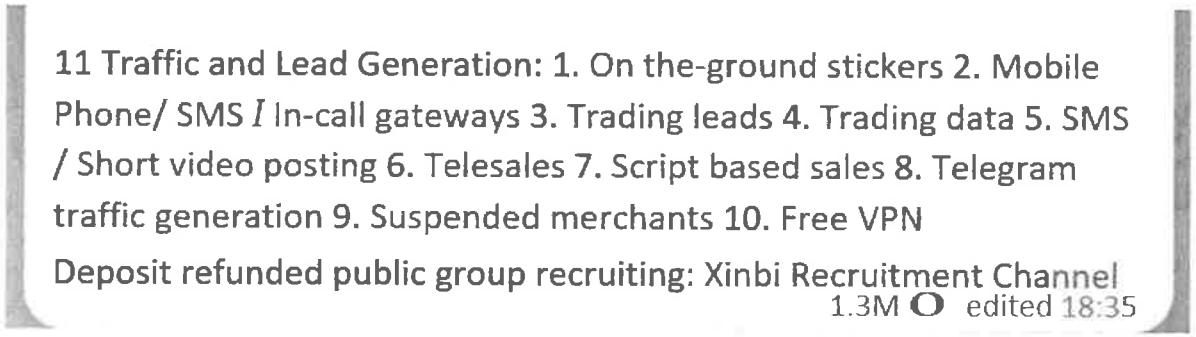


Fig. 9 – August 7, 2026 screenshot (cont.) of the Xinbi @gqdh Telegram channel directory post.

71. Each of the blue hyperlinks in the directory above directed the viewer to a specific post within the @gqdh channel, a separate Xinbi-affiliated Telegram channel, or to xinbipay.com.[27] The hyperlinked posts generally list specific Telegram groups, as further discussed below. Certain of these eleven categories appear to advertise potential money laundering services, the sales of potential cybercriminal infrastructure/tools, and other possibly illicit services and recruitment opportunities, which are discussed further herein (specifically, Category Nos. 1, 2, 3, 4, 5, 6, 7, 8, 11).

Category 1 - Account Merchant Public Group

72. The first category (No. 1) is the "Account Merchant Public Group." According to Expert Report 2, this category of groups includes merchants who buy, sell, and rent bank accounts, Alipay, and WeChat Pay accounts, possibly in the names of money mules.

Fig. 10 – An August 7, 2026 screenshot of the first category within the @gqdh Telegram channel.

[27] As of this writing, Category 8, no longer includes the hyperlink to xinbipay[.]com.

73. Based on a review of the postings within Category 1, performed by Company 2, the first two subcategories appear to be split into the amount of collateral that is placed into the marketplace, i.e., "large" and "small." The third subcategory groups merchants by their characteristics and the geographical region that relate to their sales.

Category 2 – Payment Receipt and Release Group

74. The second category is the " Payment Receipt and Release Group." According to Expert Report 2, this is the largest category on the marketplace, with 1,565 merchants.

> ② Payment Receipt and Release Public Group: 1. First-tier receipt to U 2. QR code receipt to U 3. Guided receipt 4. Second-tier receipt to U 5. App scoring 6. Firefighting fund recovery 7. Remote NFC card tapping 8. Foreign exchange 9. Receive U and release funds elsewhere

Fig. 11 – An August 7, 2026 screenshot of the second category within the @gqdh Telegram channel directory post.

75. According to Expert Report 2, most offerings relate to the receipt of funds directly, or nearly directly, from victims. Most subcategories (2.1, 2.2, 2.3, 2.4, 2.7) primarily receive fiat and release USDT; one subcategory (2.9) receives USDT and releases fiat.

76. Based on my discussions with Company 2 analysts who studied the Xinbi network and reviewed the postings within Category 2, Affiant [redacted] understands "First-tier" and "Second-tier" card receipts to be in reference to the degrees of separation between the merchant and the victim of a fraud. "First-tier" card receipt means this merchant is willing to accept the most risk and receive funds directly from a fraud victim. "Second-tier" indicates the merchant is willing to receive funds from a "first-tier" account. This section of the @gqdh Telegram channel appears to advertise posts listing groups willing to receive the proceeds of fraud.

77. Per Company 2, offerings are differentiated by three characteristics:

a. **Tier:** First-tier ("一道") merchants (e.g., Subcategory 2.1: " 一道 卡 接 回 U") receive the victim's money directly and are the most exposed to victim reporting and law enforcement attention. Second-tier ("二道") merchants (e.g., Subcategory 2.4: " 二道 卡 接 回 U") receive from a first-tier account (controlled by a cyberscam operation or another launderer), adding a layer of separation.

b. **Receipt method:** How the funds are received. Funds can be paid into bank accounts (e.g. Subcategory 2.1, 2.4), received when the victim scans a QR code connected to a non-bank payments app (Subcategory 2.2: 码 接 回 U), or received via cryptocurrency (Subcategory 2.9: 收 U 放 料). Definitions for each subcategory are provided in Appendix A.

c. **Toxicity:** Funds are graded by "toxicity" (the level of risk attached to their source). Merchants commonly specify which types they will accept. Three example toxicity grades are provided in Table 1.

Category 3 – Acceptance Public Group

78. The third category translates to "Acceptance Public Group". Based on reports from expert analysts as well as my training and experience, this this category appears to contain merchants who "accept" (receive) value and return USDT. Unlike Category 2 merchants, who primarily deal in funds held in freezable bank and payment accounts, these merchants appear to handle less traceable, harder-to-freeze forms, such as cash, gold or gift cards. The merchants ensure the funds take these harder-to-freeze forms (either on initial receipt or by their own conversion), returning USDT in exchange.

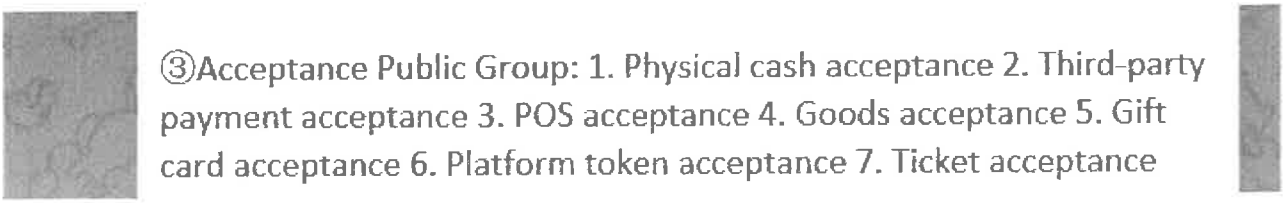
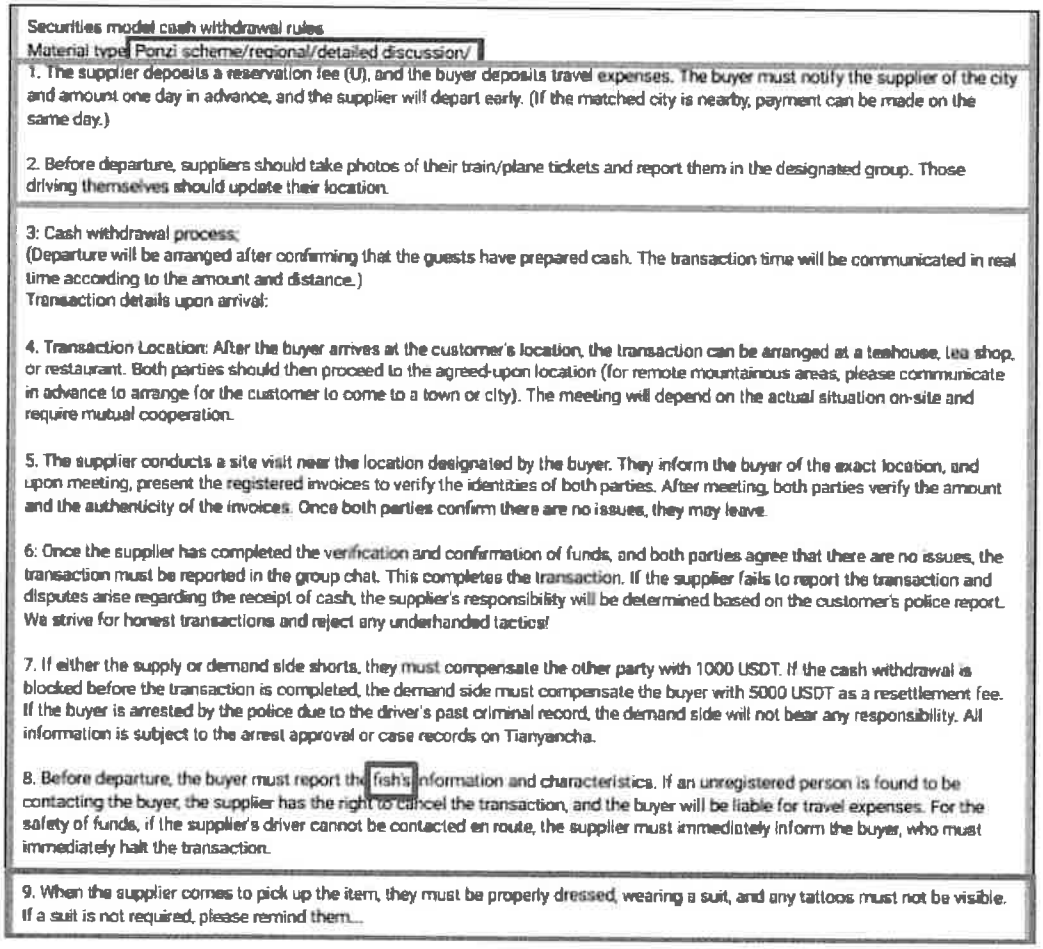


Fig. 12 – An August 7, 2026 screenshot of the third category within the @gqdh Telegram channel directory post.

79. The largest subcategory (Subcategory 3.1: 现 金 业 务) centers on physical cash collection. In rare cases, this involves merchants/mules physically collecting cash from scam victims according to Expert Report 2. The screenshot below, provided to me by Company 2, shows in-person collection rules being outlined within one merchant's group (focused on China). The boxes highlight key parts: the red box lists the types of funds that can be received, including "Ponzi scheme" and "detailed discussion" (pig butchering) funds; the orange box discusses travel to the collection point; the purple box highlights a reference to the victim (鱼; "fish"); the blue box shows that the collector is required to wear a suit by default.


Securities model cash withdrawal rules
Material type: Ponzi scheme/regional/detailed discussion/

1. The supplier deposits a reservation fee (U), and the buyer deposits travel expenses. The buyer must notify the supplier of the city and amount one day in advance, and the supplier will depart early. (If the matched city is nearby, payment can be made on the same day.)

2. Before departure, suppliers should take photos of their train/plane tickets and report them in the designated group. Those driving themselves should update their location.

3: Cash withdrawal process:
(Departure will be arranged after confirming that the guests have prepared cash. The transaction time will be communicated in real time according to the amount and distance.)
Transaction details upon arrival:

4. Transaction Location: After the buyer arrives at the customer's location, the transaction can be arranged at a teahouse, tea shop, or restaurant. Both parties should then proceed to the agreed-upon location (for remote mountainous areas, please communicate in advance to arrange for the customer to come to a town or city). The meeting will depend on the actual situation on-site and require mutual cooperation.

5. The supplier conducts a site visit near the location designated by the buyer. They inform the buyer of the exact location, and upon meeting, present the registered invoices to verify the identities of both parties. After meeting, both parties verify the amount and the authenticity of the invoices. Once both parties confirm there are no issues, they may leave.

6: Once the supplier has completed the verification and confirmation of funds, and both parties agree that there are no issues, the transaction must be reported in the group chat. This completes the transaction. If the supplier fails to report the transaction and disputes arise regarding the receipt of cash, the supplier's responsibility will be determined based on the customer's police report. We strive for honest transactions and reject any underhanded tactics!

7. If either the supply or demand side shorts, they must compensate the other party with 1000 USDT. If the cash withdrawal is blocked before the transaction is completed, the demand side must compensate the buyer with 5000 USDT as a resettlement fee. If the buyer is arrested by the police due to the driver's past criminal record, the demand side will not bear any responsibility. All information is subject to the arrest approval or case records on Tianyancha.

8. Before departure, the buyer must report the fish's information and characteristics. If an unregistered person is found to be contacting the buyer, the supplier has the right to cancel the transaction, and the buyer will be liable for travel expenses. For the safety of funds, if the supplier's driver cannot be contacted en route, the supplier must immediately inform the buyer, who must immediately halt the transaction.

9. When the supplier comes to pick up the item, they must be properly dressed, wearing a suit, and any tattoos must not be visible. If a suit is not required, please remind them...

Fig. 13 - A rules post in merchant T:285's group outlining physical collection procedures (supplier = person collecting the cash; buyer = scammer; fish = victim) (posted July 5 2026).

80. Merchants in a similar subcategory (Subcategory 3.4: 实物承兑, "Goods acceptance") appear willing to receive a variety of high-value physical goods and convert them to USDT based on the report from Company 2. Merchant K:4444 illustrates this, inviting 盘总, "Pan Zong" to "cooperate" and offers "direct access to securities brokers" as well as "cash pickup service nationwide."

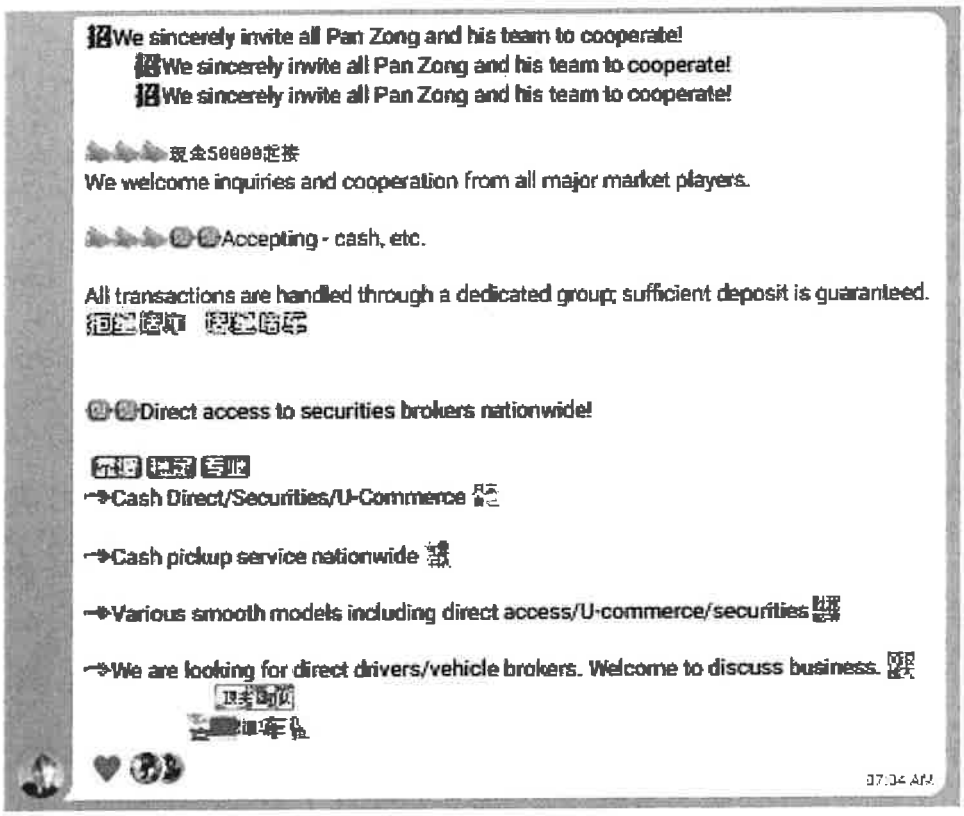


Fig. 14 - Merchant K:4444 inviting all "Pan Zong" to cooperate.

81. Merchant K:4444 also makes an isolated reference to "us 车 队" which translates to "U.S. motorcade" (Figure 15). Motorcades refer to teams who specialize in moving funds.[28]

[28] Amerhauser, Kristina, et al., Global Initiative Against Transnational Organized Crime, The Business of Exploitation (Aug. 2025), *available at* https://globalinitiative.net/wp-content/uploads/2025/08/Kristina-Amerhauser-Audrey-Thill-The-business-of-exploitation-The-economics-of-cyber-scam-operations-in-Southeast-Asia-GI-TOC-July-2025-2MR-11-Aug-CJ.pdf

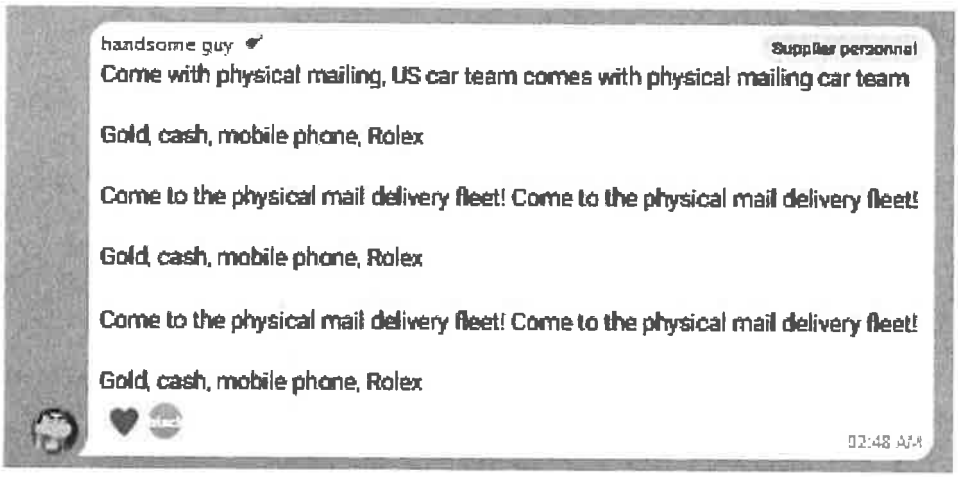


Fig. 15 - Merchant K:4444 mentions a U.S. motorcade/car team ("us 车队").

Category 4 – White Fund Public Group

82. The fourth category translates to "White Fund Public Group". Based on my discussions with Company 2 analysts, who reviewed the content of the category, as well as my training and experience, this "white capital" refers to funds that will not draw attention from law enforcement or be subject to seizure. Cybercriminal actors with fraud proceeds are able to send the USDT to these Xinbi merchants and will receive "white fund" currency from the merchant, guaranteed by Xinbi.

④White Fund Public Group: 1. Receiving U and returning white fund 2. Receiving U and paying white fund elsewhere 3. Buying and selling U 4. Receiving U and paying white foreign currency overseas

Fig. 16 – An August 7, 2026 screenshot of the fourth category within the @gqdh Telegram channel directory post.

83. The below screenshot, provided to me by Company 2, shows an example, Merchant F:225, discussing providing "clean" funds in Chinese Yuan (RMB).

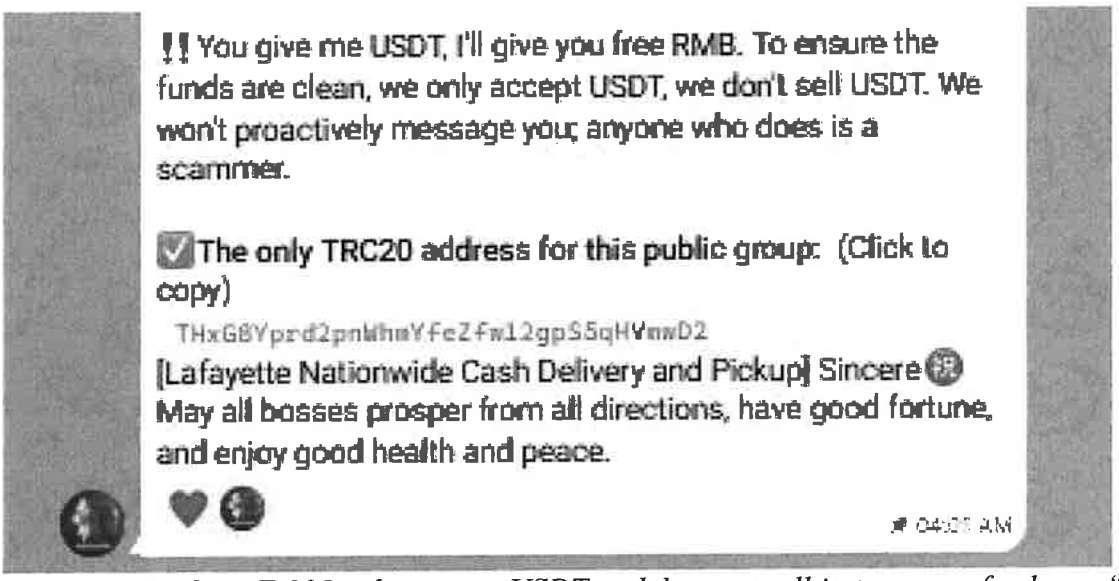


Fig. 17 - Merchant F:225 only accepts USDT and does not sell it, to ensure funds are "clean".

84. Subcategory 1 further contains information about receiving funds and returning clean funds. Within that subcategory, multiple listings show merchants who are willing to make exchanges, as seen in the screenshot below. Groups appear to be advertising services exchanging "white fund" for USDT, shortened to "U."

Xinbi public group channel @gqdh

Receiving U and returning white fund:

All account, address, and screenshot information must be shared within the group. Information involving personal privacy can be partially replaced with asterisks, and the complete information sent via private message. Xinbi guarantees only cover transactions within the current trading group. Transactions conducted privately or elsewhere are at your own risk. Do not trust any private messages, as they may be from scammers. In case of disputes, screenshots of private messages cannot be used as evidence. To prevent scammers from exploiting loopholes, all white fund group owners must, starting today: all existing white fund balances must be reported in the group. Do not simply send a private message.

Customer reporting format:
XX Bank Last 5 digits of your bank account number
Current balance: **XXXX** yuan

Group owner will reply with confirmation. Then, retain video recordings, receipts, and other evidence.

This implementation is crucial. There have been several recent cases where scammers have exploited loopholes.

Note: Groups not listed in this guide are fake public groups. This list is updated in real time !

Related public groups: ① Receiving U and returning white fund ② Receiving U and paying white fund elsewhere ③ Buying and selling U ④ Receiving U and paying white foreign currency overseas

Receiving U and returning white fund real-time ranking page 1

i: 666 deposit up to 600,000 U Tangren receiving U and returning white fund nationwide cash delivery public group

Fig. 18 - July 20, 2026 screenshot of the "Receiving U and returning white fund" post within the @gqdh Telegram channel, listing out various Xinbi Telegram groups. Based on my discussions with expert analysts who work for Company 2 that have studied the Xinbi Telegram network, Affiant [redacted] understands the letter before each group to notate which representative is the administrator of the group. Groups next to the letter F are administered by the F staffer. Groups next to the letter N are administered by the N Xinbi staffer, and so on.

F: 556 deposit up to 580,000 U Tonghui receiving U and returning white fund public group

F: 916 deposit up to 528,888 U Ajian receiving U and returning white fund/global cash delivery public group

F: 476 deposit up to 400,000 U Ruifeng large single transaction Receiving U and returning white fund Cash delivery public group

N: 1008 deposit up to 300,000 U Shaba receiving U and returning white fund (nationwide cash delivery) public group

F: 225 deposit up to 266,666 U Laofoye receiving U and returning white fund /nationwide cash delivery public group

I: 1549 deposit up to 238,888 U Yonglihui all-day receiving U and returning pure white fund public group

G: **444** deposit up to 210,000 U Daxiang Shanghang receiving U and returning white fund (nationwide cash delivery) public group

T: 9999 deposit up to 170,000 U Huaxia receiving U and returning white fund with permanent guarantee (open all day) public group

H: 999 deposit up to 158,888 U Mayi Shanghang receiving U and returning white fund open all day public group

N: 5555 deposit up to 141,333 U Huaren receiving U and returning white fund nationwide cash delivery public group

I:4544 deposit up to 120,889 U Beijing-Tianjin-Hebei-Shandong-Shanxi receiving U and returning white fund nationwide cash delivery public group

Fig. 19 - July 20, 2026 screenshot (cont.) of the "Receiving U and returning white fund" post within the @gqdh Telegram channel, listing out various Xinbi Telegram groups.

Fig. 20 - July 20, 2026 screenshot (cont.) of the "Receiving U and returning white fund" post within the @gqdh Telegram channel, listing out various Xinbi Telegram groups.

85. Subcategory 4 is related to paying "white foreign currency overseas." Within that subcategory, multiple listings show merchant groups who are willing to make exchanges, as seen in the screenshot below. These merchants appear to include payments to be made to Europe, China, and India.

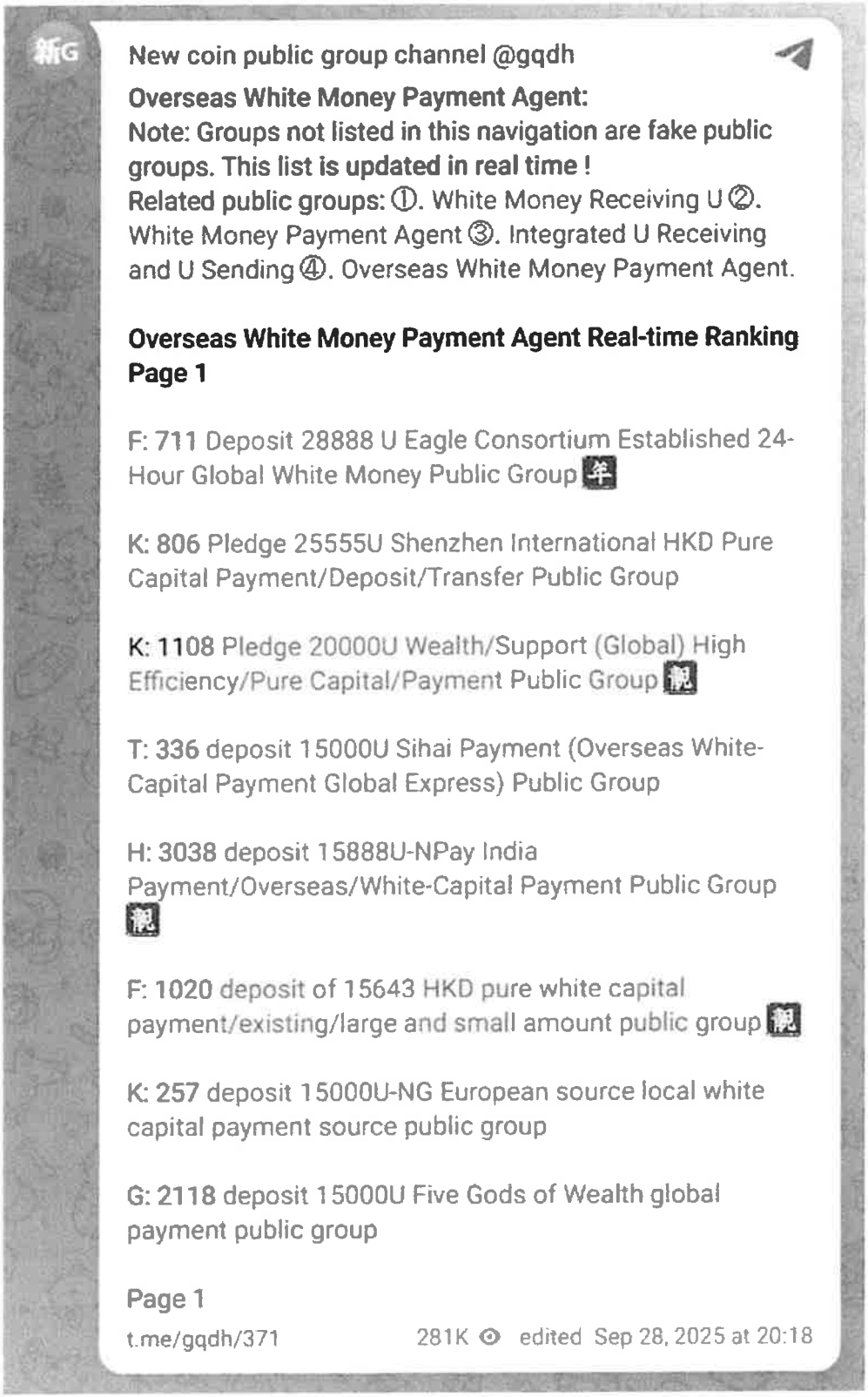


Fig. 21 - July 20, 2026 screenshot of the "Receiving U and returning white fund" post within the @gqdh Telegram channel, listing out various Xinbi Telegram groups.

Category 5 – Collaboration

86. The fifth category within the @gqdh channel translates to "Collaboration." Within this category, there appear to be lists of Telegram groups of what appear to be merchants openly describing what they are seeking or what they can provide. Based on a report from Company 2, the details of any engagement are then arranged privately, away from the public Telegram groups. This category discusses similar services seen elsewhere on the marketplace, just from a different perspective.

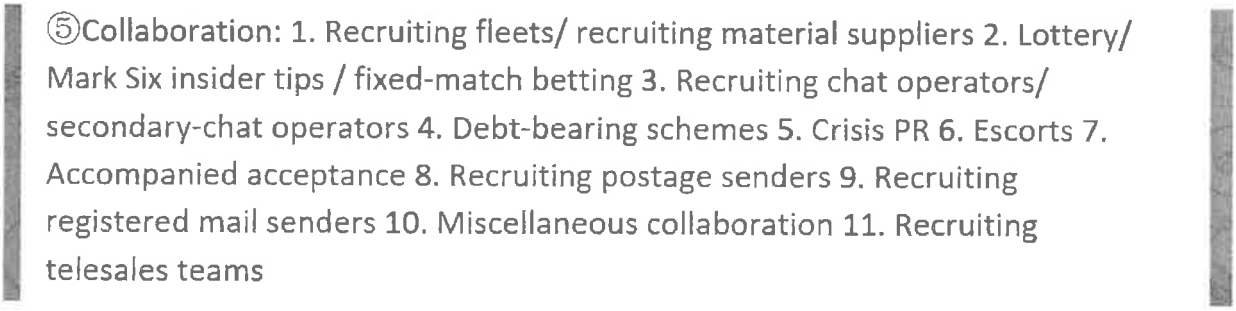


Fig. 22 – An August 7, 2026 screenshot of the fifth category within the @gqdh Telegram channel directory post.

87. Subcategory 1 contains information on merchants "Recruiting fleets." Based on my discussions with expert analysts as well as public reporting[29], vehicles, fleets, motorcades, or cars are often code-words for bank accounts used to launder illicit funds through money mules, sometimes referred to as "drivers." Chat operators are commonly used in scam centers to contact victims, who are enticed to send funds overseas to cybercriminal groups. Within this "recruiting fleets" subcategory, the list of groups repeatedly reference fleets, which Affiant [redacted] understands to reference bank accounts. Of note, multiple hyperlinked posts refer to "cash withdrawal fleet[s]," which Affiant [redacted] understands to mean money-mule account.

[29] See footnote 7.

Additionally, the groups repeatedly reference scams and "chat operators," which is consistent with scam center operations, as seen below.

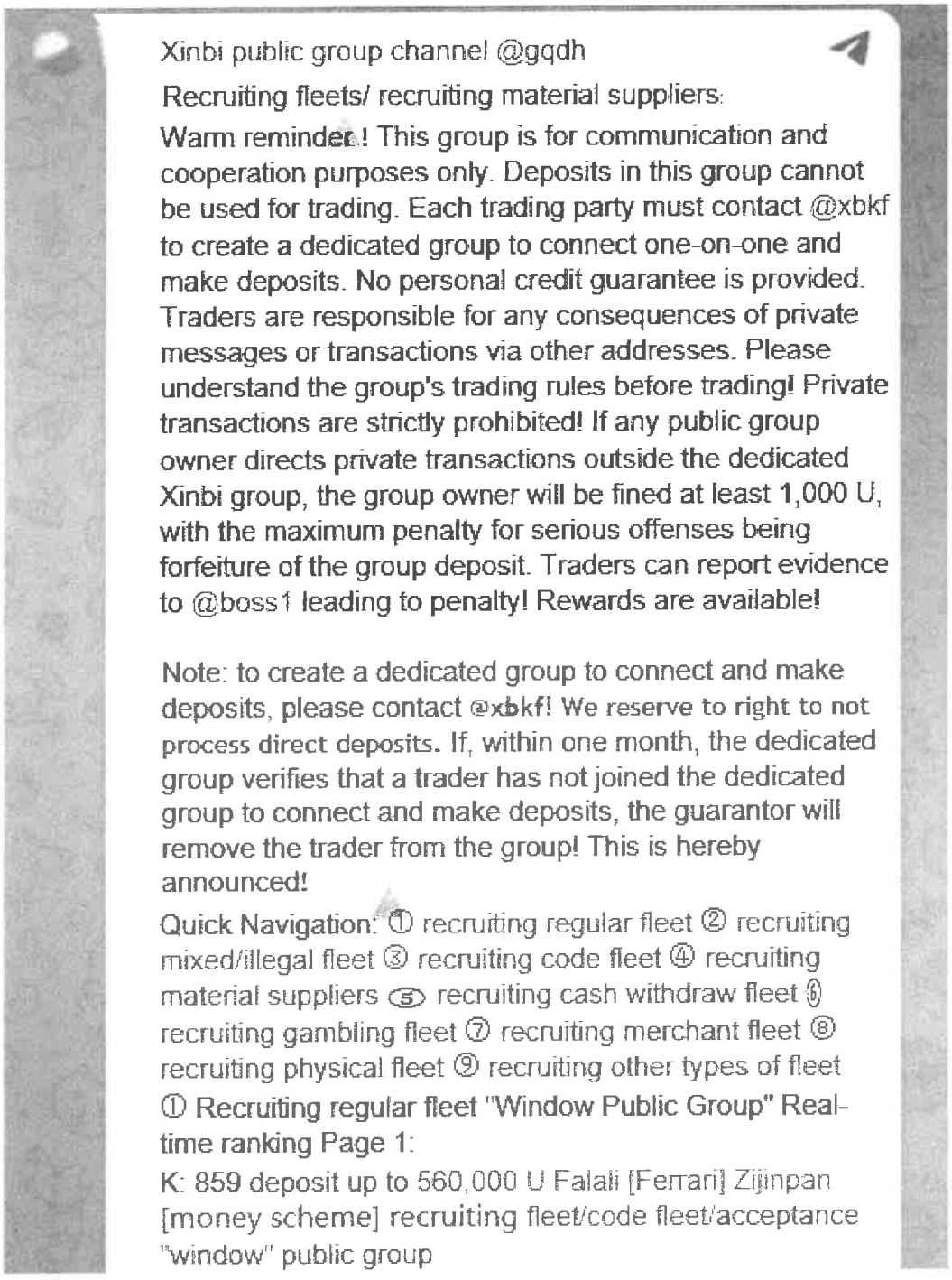


Fig. 23 – A July 2026 screenshot of the hyperlinked post labeled "Recruiting fleet drivers."

F: 22222 deposit up to 118,888 U Huojian [rocket] Zijinpan recruiting white fleet/code fleet/cash withdraw fleet "window" public group

K: 8886 deposit up to 70,000 U Yefan Zhifu [payment]/recruiting Alipay various seamless codes/fleet "window" public group

K: 381 deposit up to 68,088 U Changjiu [long-term] Zijinpan recruiting cash withdrawal fleet "window" public group

N: 352 deposit up to 38,899 U Bamin Dianshangjituan [e-commerce group] recruiting code/cash withdrawal/physical goods/gift cards "window" public group

G: 2164 deposit up to 38,888 U Taiqing Zijinpan recruiting fleet/code fleet "window" public group

K: 2207 deposit up to 38,288 U recruiting various seamless payment fleet "window" public group

H: 2805 deposit up to 31,999 U Haisheng Zhipan [direct currency pairs] recruiting Regular color material Premium chat operators Code fleet Regular fleet "window" public group

H: 1017 deposit up to 30,000 U recruiting in-person honey pot/first and second tier receipt/online loan repayment "window" public group

G: 2270 deposit up to 28,888U Huifeng [HSBC] first-tier premium chat operators standard long term team code fleet "window" public group

H: 3167 deposit up to 25,888 U Dimaxi honey-pot fleet "window" public group

Fig. 24 – A July 2026 screenshot (cont.) of the hyperlinked post labeled "Recruiting fleet drivers."

88. Subcategory 3 contains information on merchants offering "chat operators." Based on my training and experience, Affiant [redacted] knows that "chat operators" typically refers to individuals in scam centers used to contact victims, who are enticed to send funds overseas to cybercriminal groups. Within this subcategory, multiple merchants offer services (listed with the alphabet letter). The listings include recruiting for "sex scam" operators.

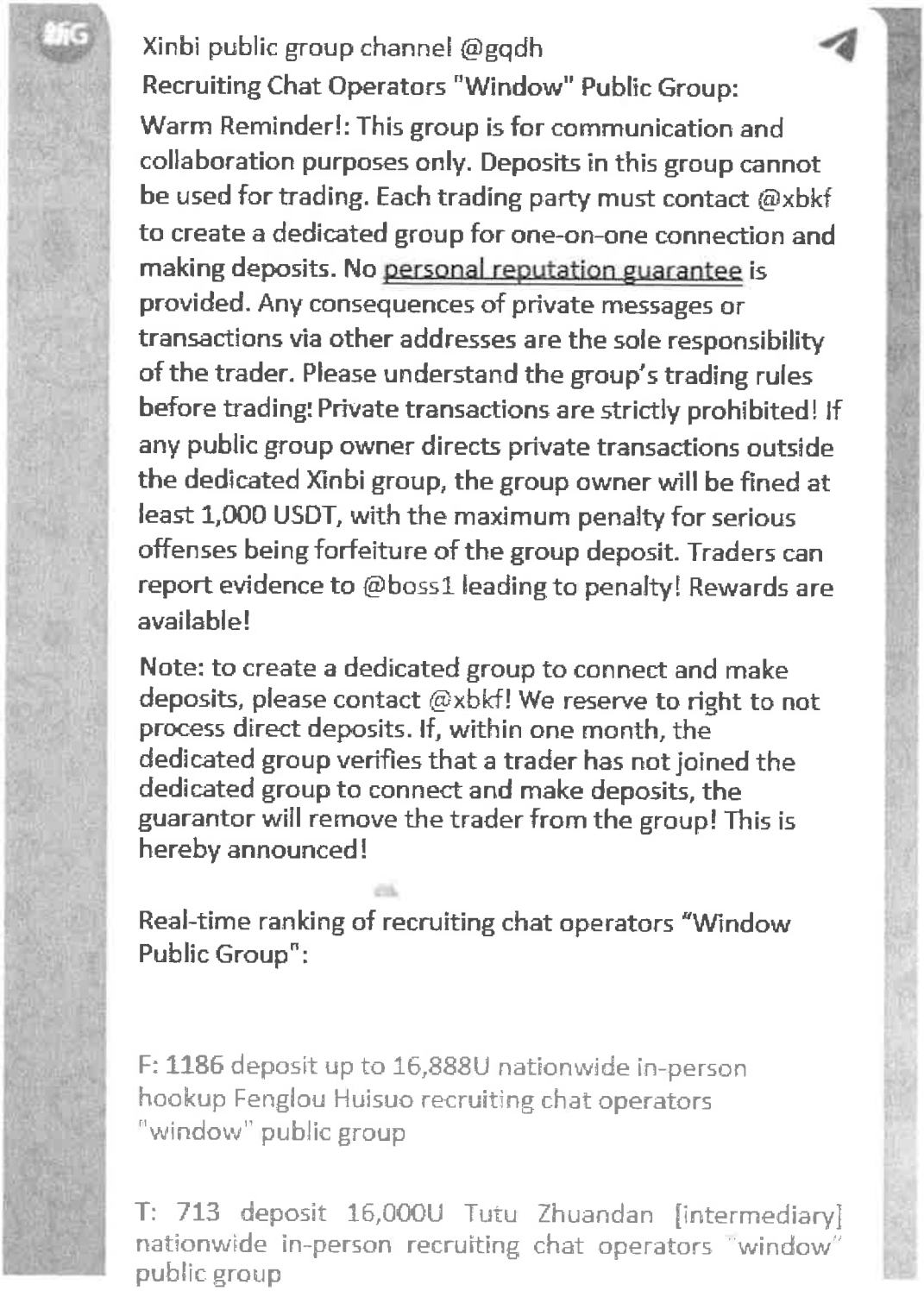


Fig. 25 – A July 2026 screenshot of the hyperlinked post labeled "Recruiting chat operators."

G: 755 deposit up to 8,888 U recruiting overseas premium WeChat Douyin chat operator team/individual "window" public group

T: 939 deposit up to 6,666 U Chengcheng Zhuandan nationwide in-person hookup recruiting chat operators "window" public group

T: 1 52 deposit up to 6,666 U Xiaren [Open-claw] Quanguozhuandan real in-person hookup recruiting chat operators "window" public group

i: 1876 deposit up to 6,266 U Dabai nationwide real in-person recruiting chat operators "window" public group

T: 719 deposit up to 3,888U Aying gaming proxy in-person one-stop shop recruiting sex chat operators "window" public group

T: 322 deposit up to 3,888 U recruiting sex chat operators/naked female live-streamer "window" public group

i: 2207 deposit up to 3,400 U Yuguo recruiting offline staff "window" public group

F: 960 deposit up to 3,000 U Guangtouqiang recruiting in-person hookup/escort chat operators "window" public group

N: 976 deposit up to 3,001 U Dabiaoge [big cousin] Zhuandan nationwide in-person recruiting chat operators "window" public group

K: 795 deposit up to 3,000 U Shuangying [win-win] Group direct recruiting *BC* promoters fast settlement "window" public group

Fig. 26 – A July 2026 screenshot (cont.) of the hyperlinked post labeled "Recruiting chat operators."

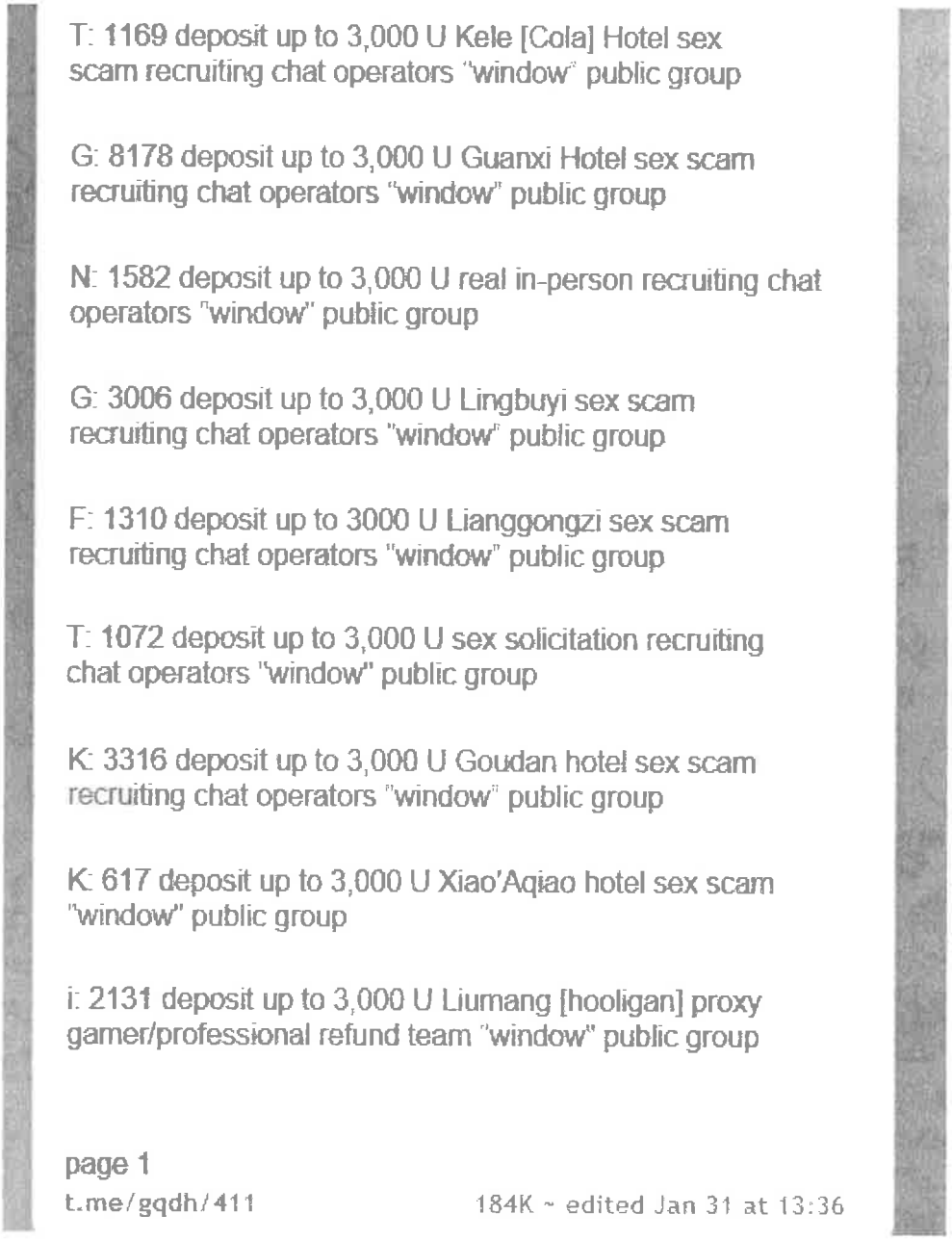


Fig. 27 – A July 2026 screenshot (cont.) of the hyperlinked post labeled "Recruiting chat operators."

89. Below, screenshots, provided to me by Company 2, show merchant listings for "chat operators," from merchants advertising services within subcategory 3.

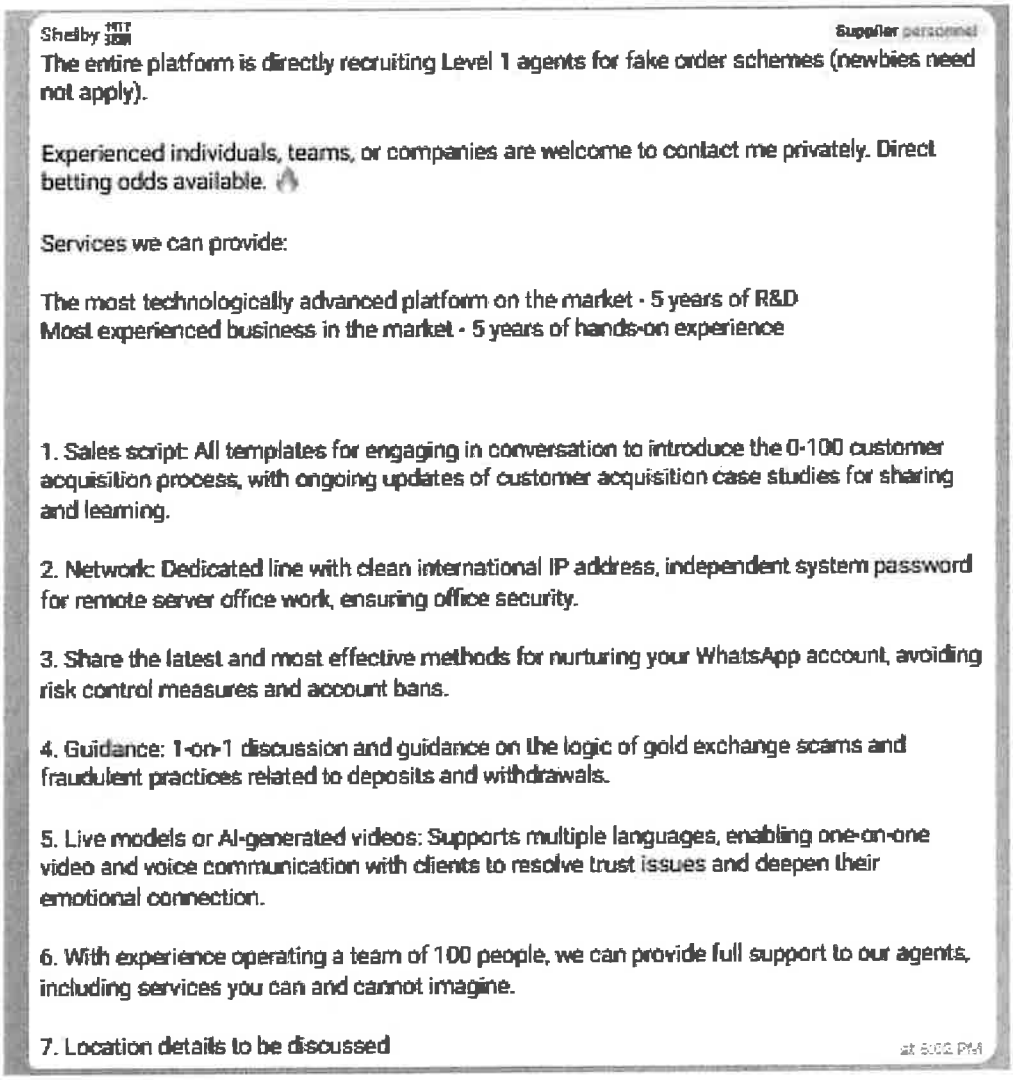


Fig. 28 – Merchant F:927 recruits chat operators.

Category 6 – Service Category

90. As seen below, the sixth category within the @gqdh Telegram channel, "Service," include notable hyperlinks labeled "Tianyancha," "Social media account rental," and "AI face swapping tools." Tianyancha refers to a large business database platform in China.

⑥Service category: 1. Tianyancha [data look-up] 2. Ticket payment service 3. Social media account rental 4. Graphic design 5. SMS verification-code services 6. Account/exchange unfreezing 7. Errands and call services 8. High-end escorts 9. [Apple] ID loans 10. AI face swapping tools 11. Other services

Fig. 29– An August 7, 2026 screenshot of the sixth category within the @gqdh Telegram channel directory post.

91. Based on training and experience, Affiant [redacted] knows that renting social media accounts and AI face swap services can be used by cybercriminals in fraud schemes. For instance, within subcategory 10 (AI face swapping tools), the following merchants listed their services.

T: 768 deposit up to 10,000 U Qianxun [Spirit AI] *chatgpt* various AI agents public group

T: 509 deposit up to 9,999 U Xuanwukeji [Xuanwu AI] AI face swap public group

G: 3086 deposit up to 3,994 U - *GodAi* face swap/ AI customer service/ AI premium chat public group

N: 1123 deposit up to 3,374 U Xiaomi Keji [technology] AI real-time face swap and voice changer public group

G: 3243 deposit up to 3,000 U Moshushi [magician] Mote [model] proxy gamer video/ AI face swap software public group

T: 1288 deposit up to 3,000 U - AI generated WeChat Douyin Alipay facial recognition unlocking public group

Page 1

t.me/gqdh/452 180K ~ edited Jan 31 at 13:36

Fig. 30 – An August 8, 2026 screenshot of the post hyperlinked under the "AI face swapping tools" label. This screenshot includes a sampling of the groups on the post.

92. From my training and experience, cybercriminal actors will utilize AI tools to disguise their face and their voice, which is consistent with what is being advertised within the Xinbi channel, according to a report from Company 2. One merchant, shown below, advertised face-swapping, as well as voice cloning and guidance on replies for "detailed chat" (i.e., pig butchering) scams. Requests for specific tasks are also posted to the group: the screenshot on the bottom right shows a request for a selfie with a person holding a written note containing a specified name, likely done to build trust with a victim.

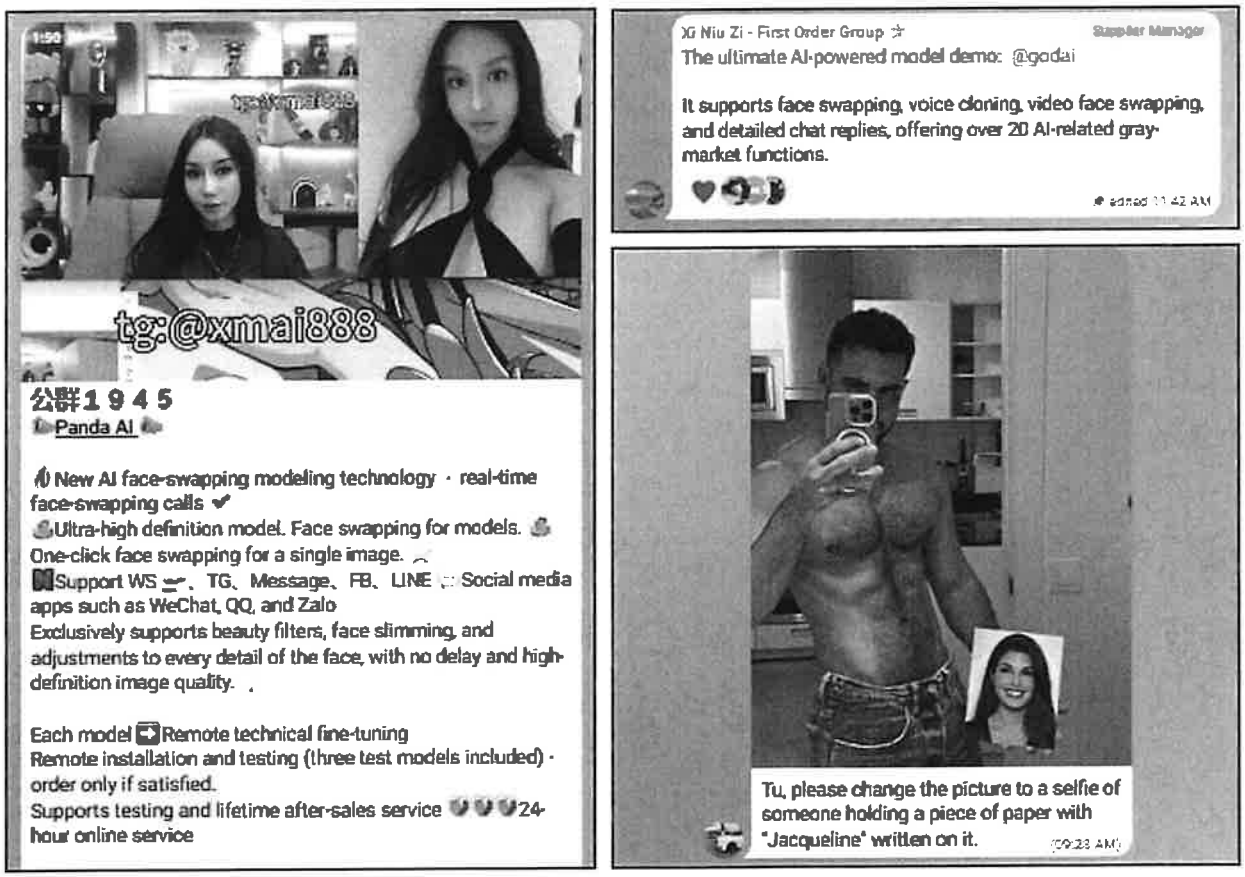


Fig. 31 – Merchant i:1945 advertises face swapping for chat applications, provided by Company 2.

Category 7 – Infrastructure Category

93. The seventh category within @gqdh Telegram channel, "Infrastructure category," appears to advertise website/app development services, domain registrations, and IP/VPN services. All of these services can be used to support scam center and general cyber-enabled fraud infrastructure. A sampling of some of the groups listed under the posts is provided below:

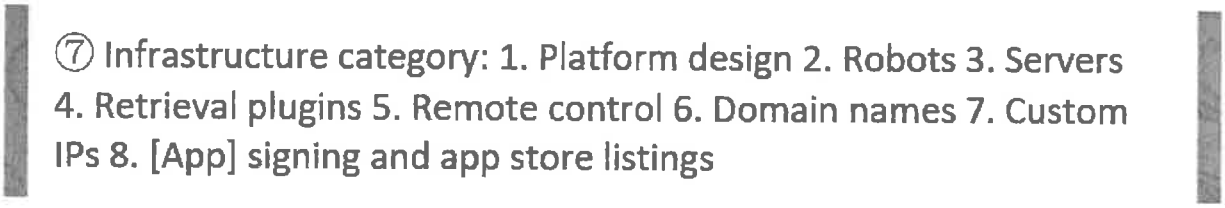


Fig. 32 – An August 7, 2026 screenshot of the seventh category within the @gqdh Telegram channel directory post.

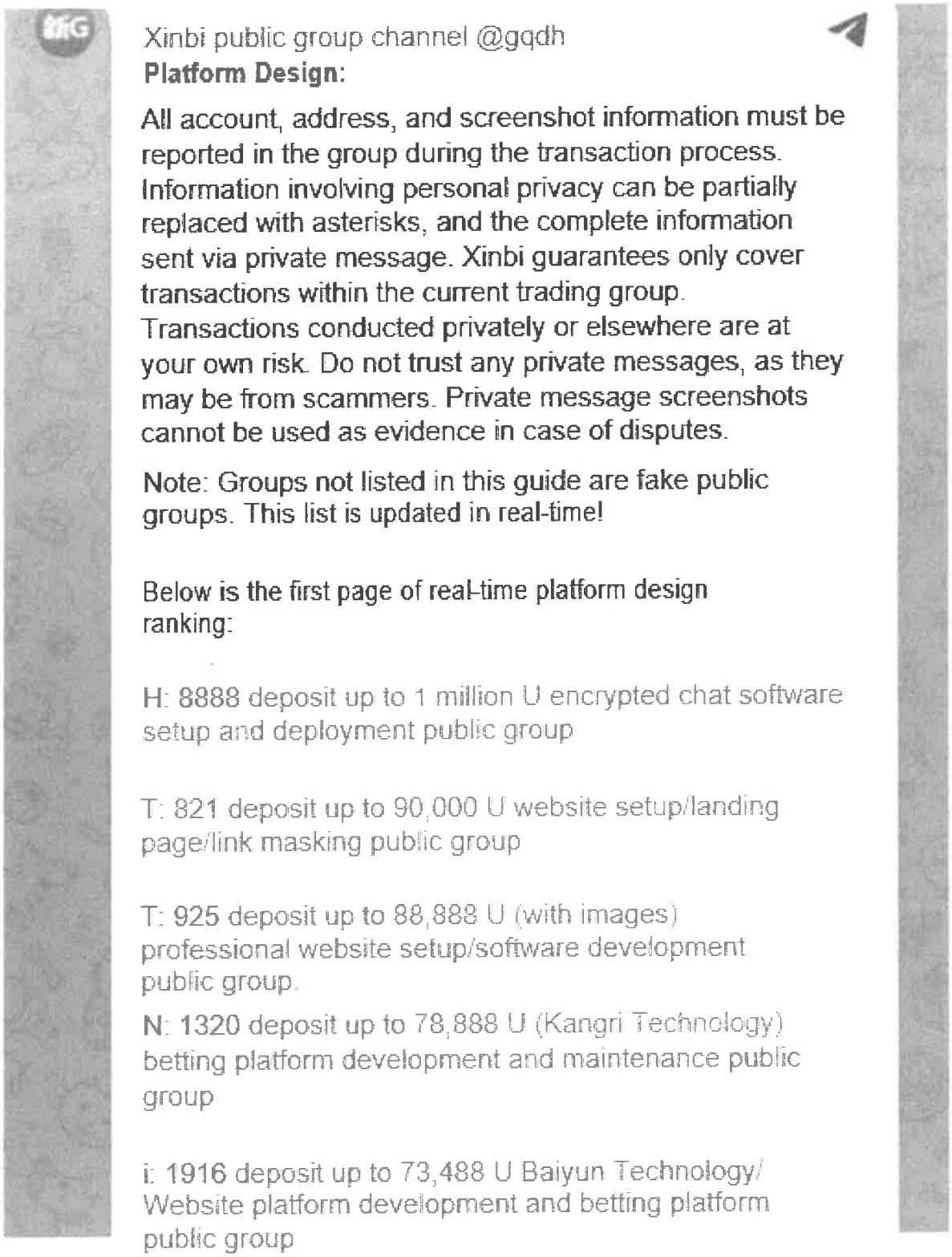


Fig. 33 – A July 28, 2026 screenshot of the hyperlinked post under the "Platform Design" label.

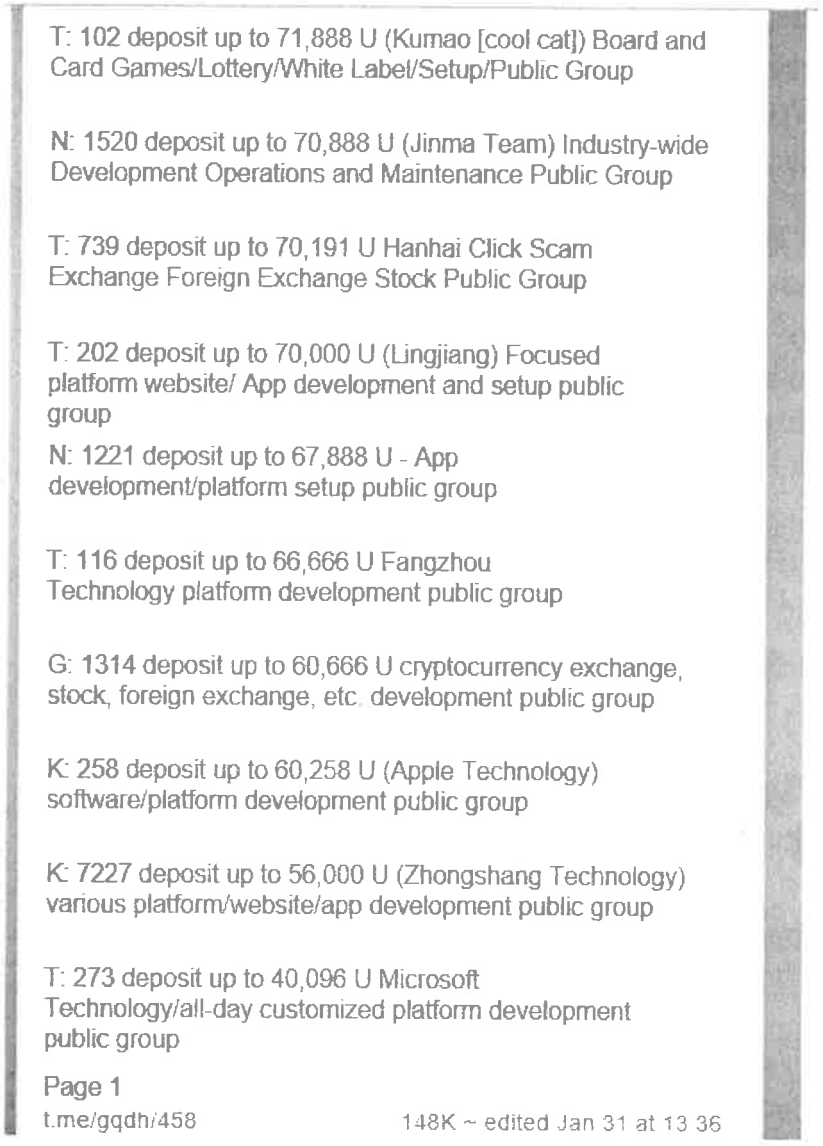


Fig. 34 – A July 28, 2026 screenshot (cont.) of the hyperlinked post under the "Platform Design" label.

94. The above groups appear to be advertising platform development that could be used by scam centers. Of note, "link masking" and "Scam Exchange" are openly advertised by the Xinbi merchant groups.

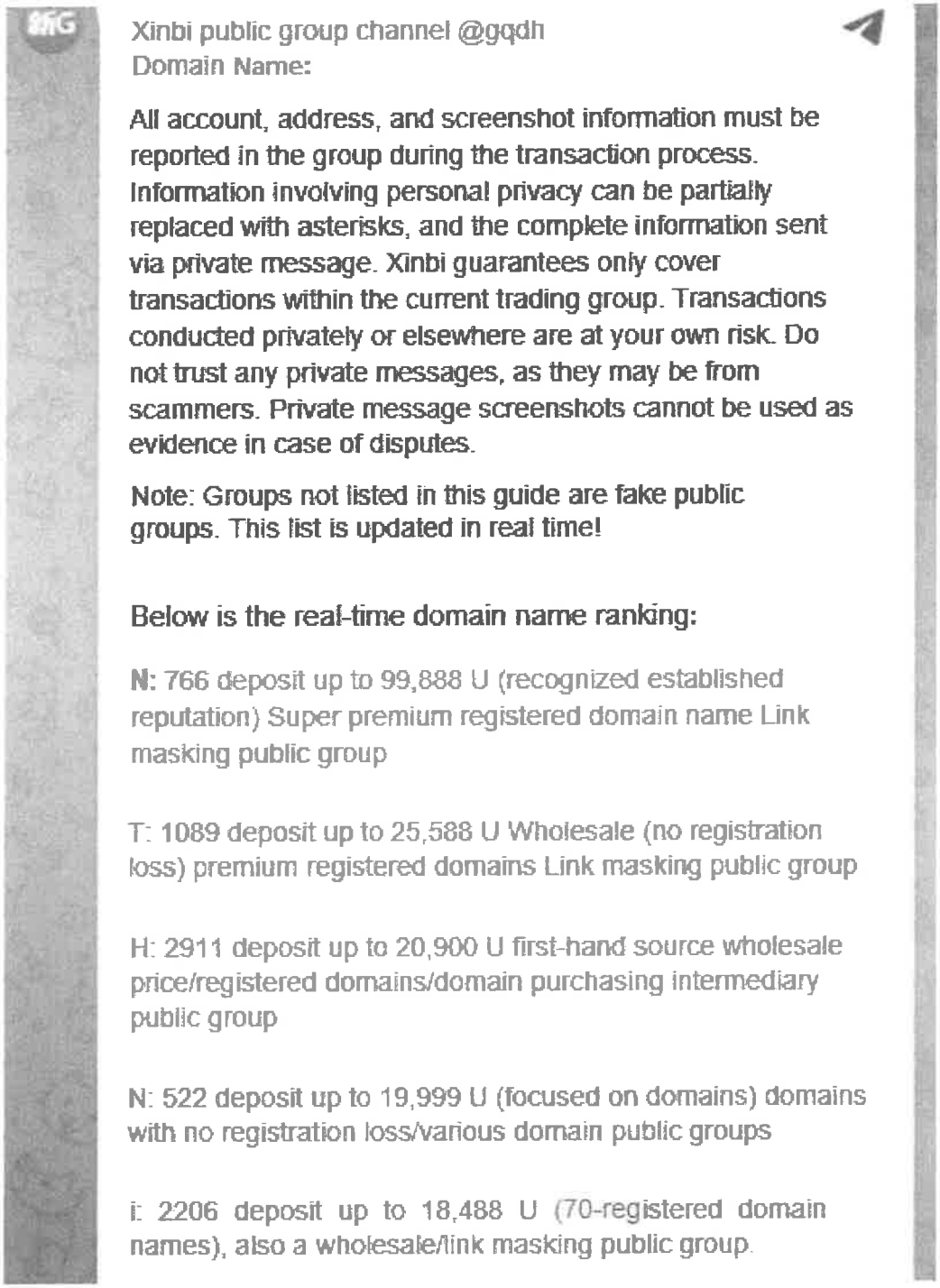


Fig. 35 – A July 28, 2026 screenshot of the hyperlinked post under the "Domain names" label.

K: 695 deposit up to 12000 U (Wukong) domain name anti-blocking/no-loss registration/domain name purchase public group

T: 1185 deposit up to 9,333 U (first-hand domain) premium domain name wholesale/SSL certificate public group

H: 3118 deposit up to 9,188 U (Yunjie) domain name/SSL certificate/domain name purchasing public group

F: 926 deposit up to 6,888 U (permanent domain) no-loss domain registration wholesale public group

N: 329 deposit up to 5,888 U (professional and stable) domain registration wholesale/SSL certificate public group

T: 328 deposit up to 5,008 U permanent domain name wholesale/link masking/first-hand source public group

G: 1746 deposit up to 3,888 U (domain king) domain name registration/no-loss domain registration/domain name public group;

T: 194 deposit up to 3,500 U long shelf life (regardless of source) domain name registration public group

i: 1918 deposit up to 3,400 U permanent domain name wholesale public group

Fig. 36 – A July 28, 2026 screenshot (cont.) of the hyperlinked post under the "Domain names" label.

95. The reselling of domain names is possibly an attempt to disguise the ownership of fraudulent websites by cybercriminal actors.

Category 8 – Cryptocurrency related

96. Category 8 is titled "cryptocurrency-related." Viewers were directed to xinbipay[.]com and also advertised coin-mixing groups. Based on my training and experience, coin-mixing is a tactic used by cryptocurrency fraudsters to launder funds obtained through fraud, frustrating law enforcement efforts to effective trace and seize funds for victims.[30]

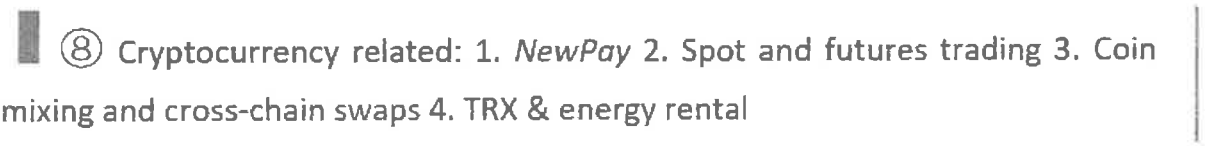


Fig. 37 – An August 7, 2026 screenshot of the eighth category within the @gqdh Telegram channel directory post.

97. One subcategory (Subcategory 8.3: 混 币 与 跨 链 兑 换) appears to provide cryptocurrency laundering and mixing services. The offerings in this subcategory differ from those elsewhere on the marketplace, according to a report from Company 2,in that both the input and the output are cryptocurrency, whereas the other money laundering categories involve fiat currency on one side.

[30] As of August 25, 2026, it appears Xinbipay has been removed as a link on this page.

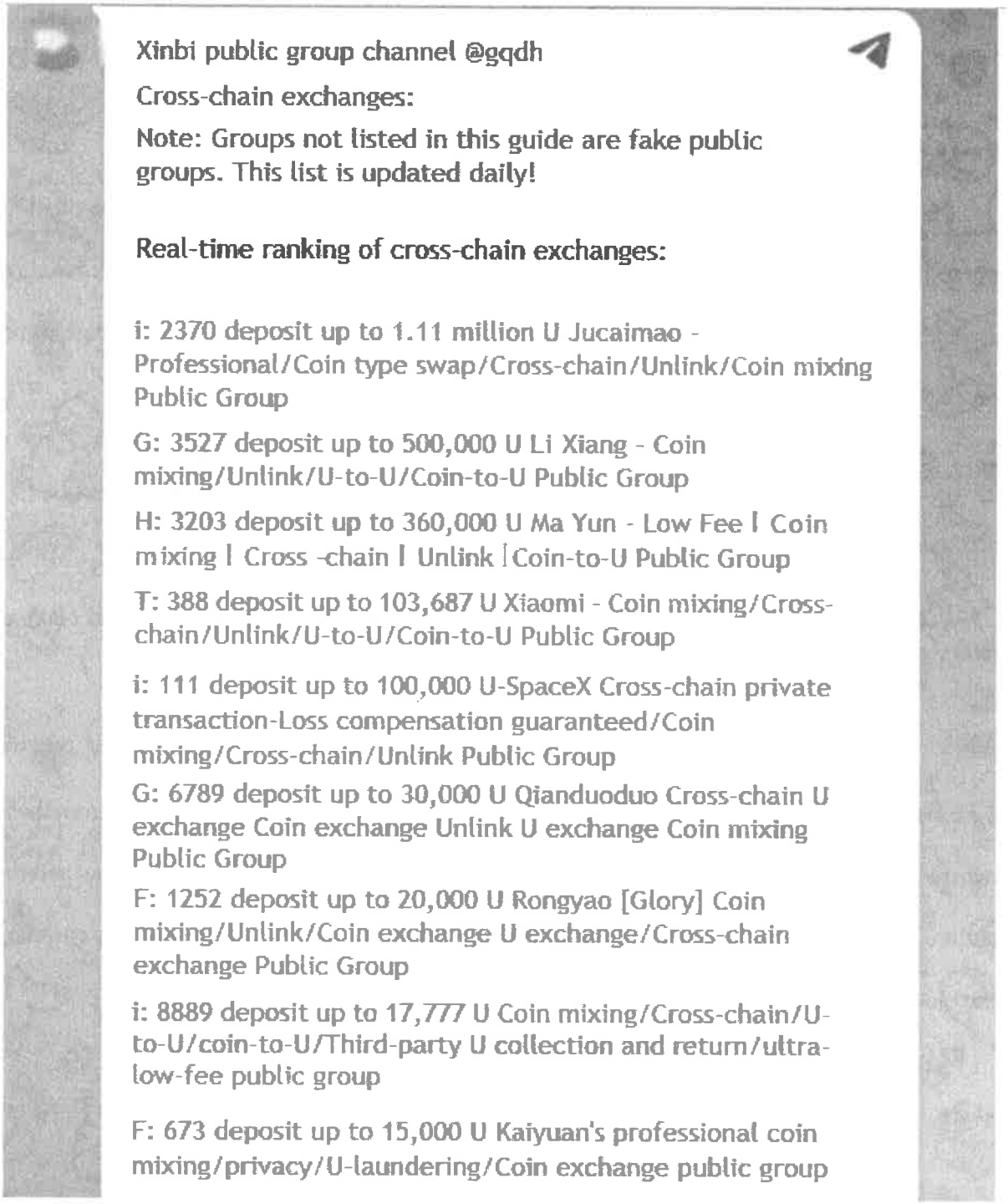


Fig. 38 – An August 2026 screenshot of the post hyperlinked from the "Coin mixing and cross chain swaps" label.

98. Within subcategory 3, merchants appear to advertise their ability to launder and mix cryptocurrency. Below are two example merchants provided to me by Company 2; the

merchant on the right refers to serving users concerned about "freezing" (Tether freezes) or "marking" (addresses being flagged by blockchain-analytics tools).

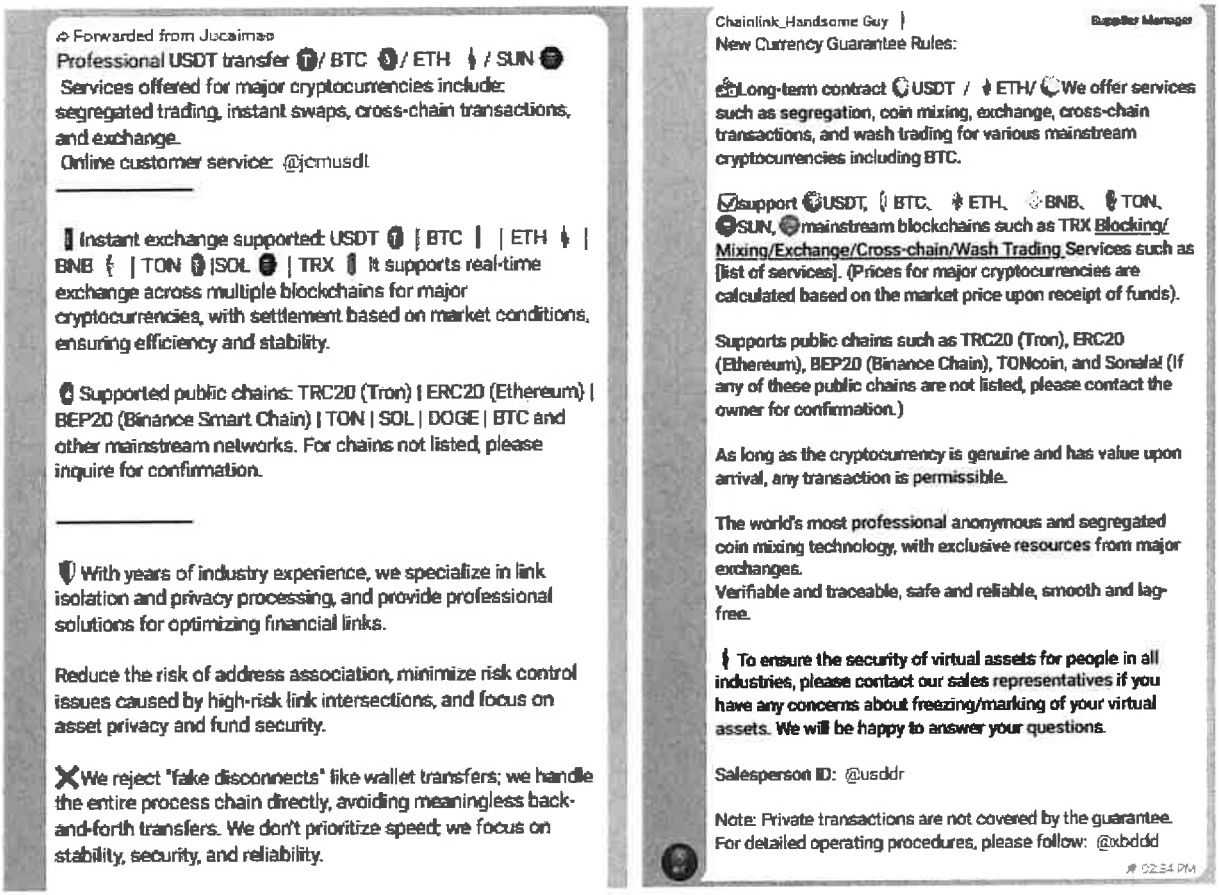


Fig. 39 – (Left) Merchant i:2370 offers to "minimize risk control issues".
(Right) Merchant i:8889 looks to serve those who have "concerns about freezing/marking"

Category 11 – Traffic and Lead Generation

99. Category 11 is titled "Traffic and Lead Generation." This category appears to cover initial promotion and the sourcing of new "leads" (victims).

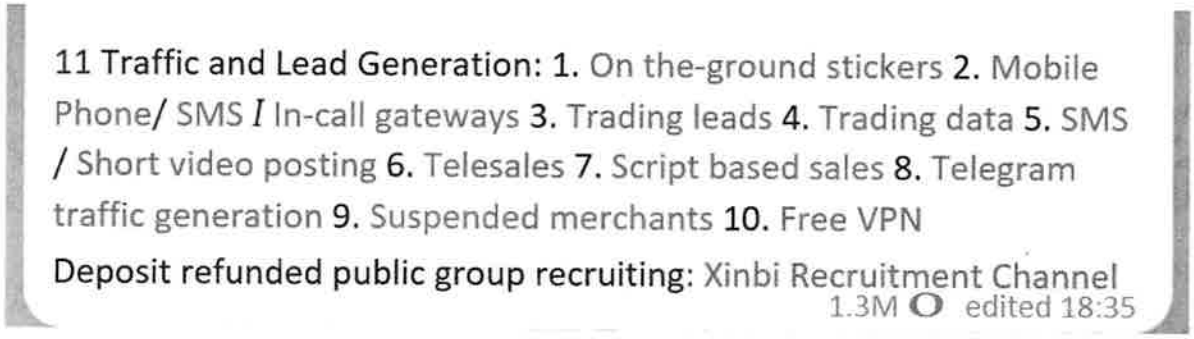


Fig. 40 – August 7, 2026 screenshot of the Xinbi @gqdh Telegram channel directory post.

100. One subcategory (Subcategory 11.3: 出 粉) provides lead-generation services directly according to Company 2. Figure 41 shows two adverts from merchants in this subcategory, provided to me by Company 2. For instance, Merchant N:905 advertises leads for "dating" (romance scams) and part-time jobs (task scams), as well as investment and cryptocurrency scams. It states that leads can be generated through SMS and group chats, and that the merchant "welcome[s] Mr. Pan to cooperate". Merchant T:853 (right) provides messaging services focused on WhatsApp according to Company 2.

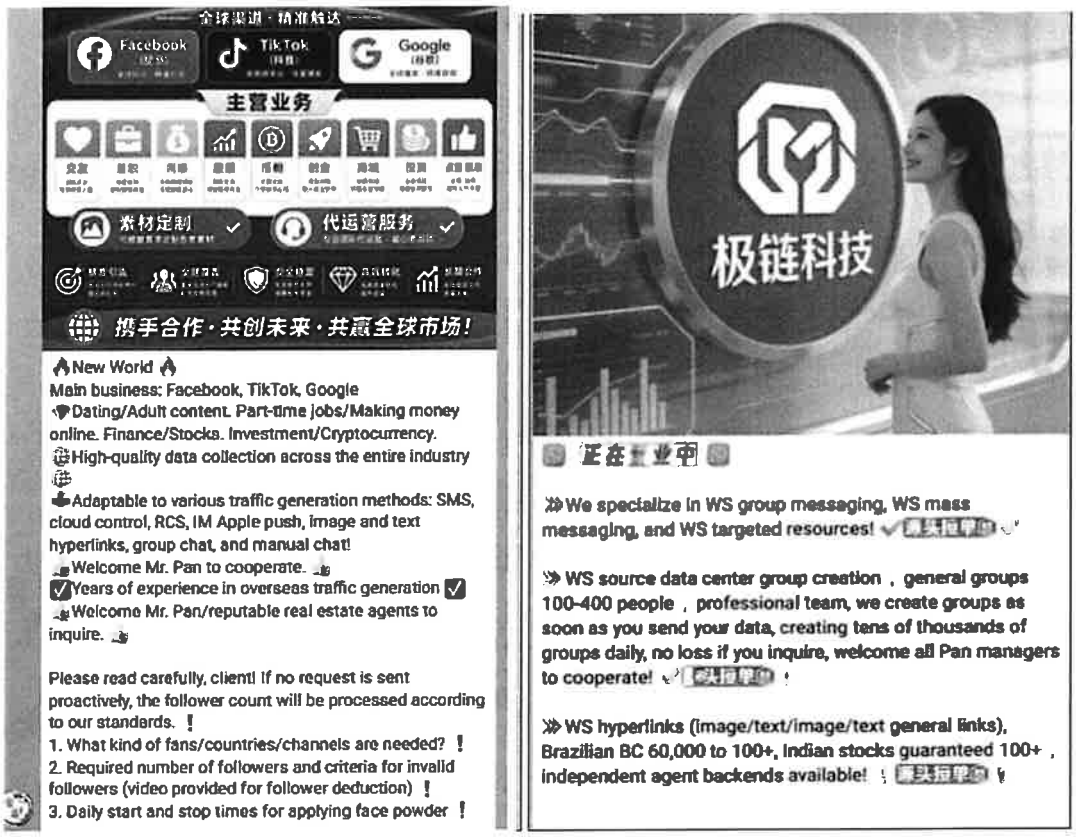


Fig. 41 – Merchant N:905 (left) offers lead-generation services to "Mr. Pan". Merchant T:853 (right) provides messaging services focused on WhatsApp

Xinbi's Control of the Telegram Channels

101. Based on the information obtained through Xinbi Guarantee's Telegram channels as well as the merchant Telegram channel, more than merely being present in merchant channels, Xinbi staff appear to actively provide moderation services between merchants and their clients. Xinbi posts results of adjudicated disputes on the Telegram channel [redacted] It would be impossible for Xinbi staff to resolve these issues without knowing the details of each specific interaction, including the origin of the funds in question.

102. One example from August of 2025 shows Xinbi staff resolving a dispute between a client and a merchant. The client, a scammer, needed a clean bank account through which to launder funds from a victim. The client purchased a bank account from the merchant.

When the client transferred victim funds into the bank account, the account was closed by the bank. The merchant alleged that the client had lied about the volume and dirtiness of funds he intended to launder. The large flow of funds which were traceable to fraud proceeds caused the account to be closed.

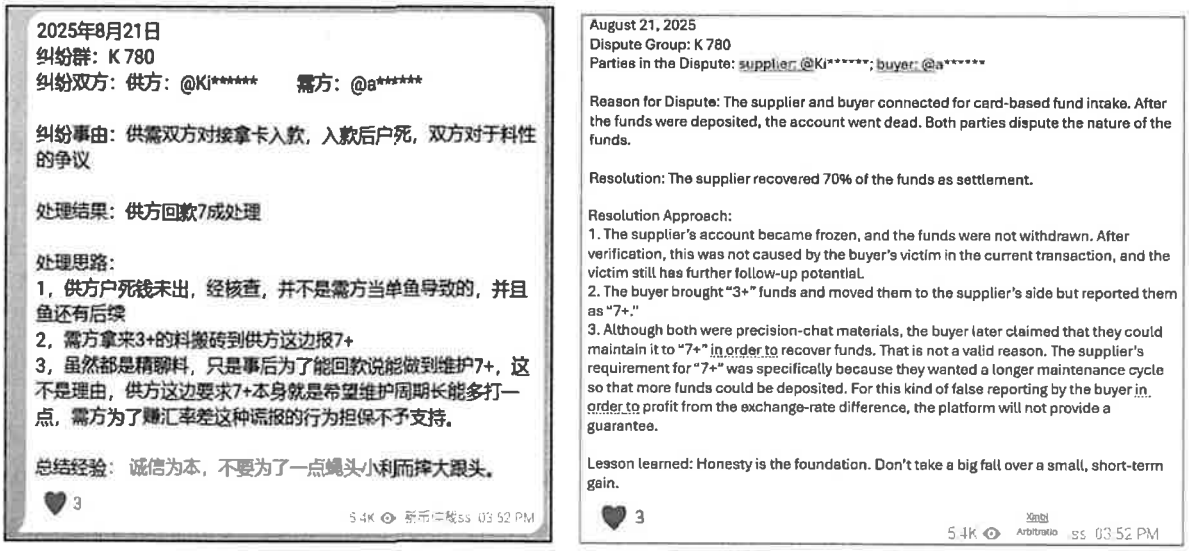


Fig. 42 – Xinbi Staff Adjudicating Merchant Dispute[31]

103. Based on the information obtained through Xinbi Guarantee's Telegram channels as well as the merchant Telegram channels, Xinbi not only has visibility into the merchant groups but acts as the arbiter between Xinbi merchants and their clients. Xinbi has visibility to see the merchants' cryptocurrency addresses. Xinbi sees the merchant's addresses from the merchants' Telegram posts, when the guarantee network receives cryptocurrency from the merchants, and when it transfers cryptocurrency to merchants when the escrow is settled. Therefore, Xinbi is reasonably aware of the nature of the activity surrounding the merchants' cryptocurrency addresses.

[31] Translated by USSS linguist.

D. Identification of Wallets from the Xinbi Guarantee Telegram Channel

104. Company 2 compiled a list of 58 total Onboarding Addresses which have been used by Xinbi Guarantee since July of 2022. These addresses were identified because they are the public addresses which Xinbi posts on its Telegram channel and website and are therefore publicly advertised. These addresses are the rotating addresses into which merchants pay fees and clients deposit escrow. Since July of 2022, these Onboarding Addresses have had an incoming total volume of over $11 billion.

105. Company 1 estimates that there are approximately 10,700 Xinbi addresses based on analysis conducted by following the flow of funds from the Onboarding Addresses (measured August 4, 2026). This number includes Intermediary, Final Intermediary, Consolidation, merchant, and other associated addresses. Company 2 estimates that there are at least 2,000 merchant cryptocurrency addresses (measured August 11, 2026), as Company 2 has queried all merchant Telegram channels accessible to them and retained the cryptocurrency addresses it has found in each.

E. Connection of Xinbi Telegram Channels (The Target Sites) to Specific Instances of Laundering

106. Investigators reviewed multiple instances in which they identified money laundering activity within the eleven Telegram channel categories, discussed above. Five specific examples follow.

Example 1: Category 4.2, Public Group, Section G, No. 2129

107. Public Group, Section G, No. 2129, is one of the Xinbi merchants identified by investigators, and is contained within the Category 4.2 . A review of the blockchain shows that, since September 2025, its cryptocurrency address,

[redacted], has received over $29 million of cryptocurrency. Its Telegram group, visible to Xinbi for moderation, published the merchant's rules.

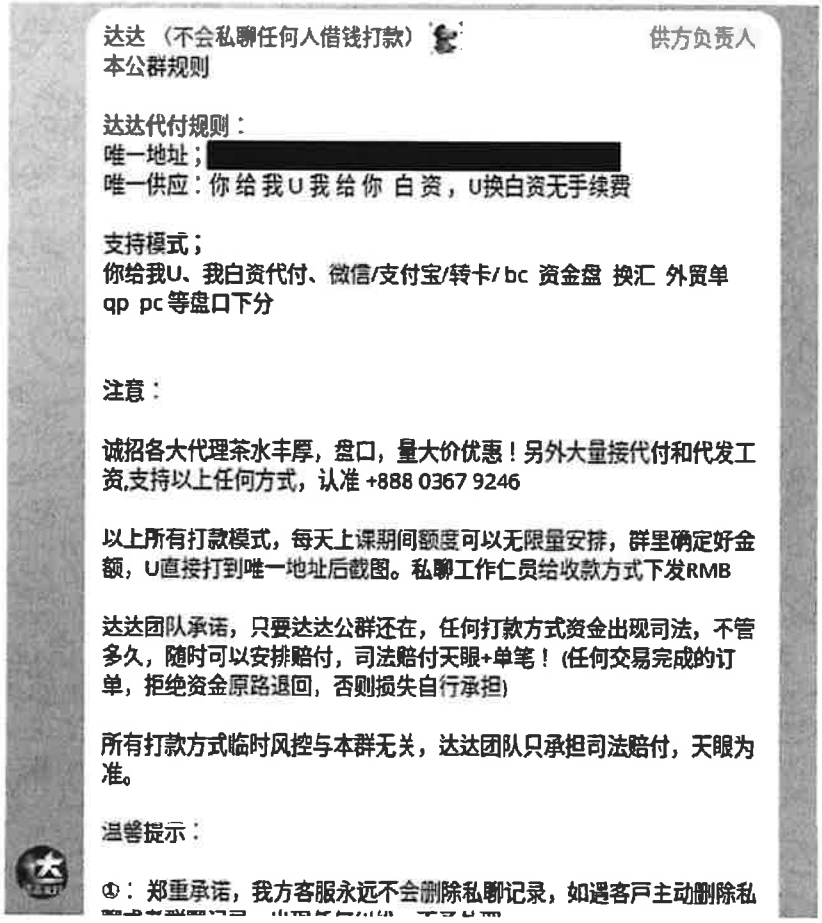


Fig. 43 - Public Group, Section G, No. 2129 Rules

108. As translated, the Rules state: "You give me USDT, I disburse clean funds on your behalf, via WeChat / Alipay / card-to-card transfer / bc [online gambling] / investment-scheme pools / currency exchange / foreign-trade orders / qp [card-and-board gambling] / pc [gambling game], and other downstream settlement to gambling-platform accounts."

109. Based on information archived from the Telegram chat by Company 2, Public Group, Section G, No. 2129, offers servicing for funds from illegal gambling and fraud, "pig butchering," schemes. Users send USDT to the merchant cryptocurrency address and receive

"clean" RMB[32] suggesting users of this merchant are located in China or prefer to use Chinese currency.

110. Law enforcement traced proceeds from a known CIF U.S. victim into this merchant and to addresses associated with Xinbi.

a. In December of 2025, "**Victim-EG**" from Virginia contacted the USSS Washington Field Office to report being a victim of cryptocurrency investment fraud ("CIF") scheme in which he lost approximately $800,000 between September and December of 2025. **Victim-EG** was contacted on Facebook, a U.S. social networking platform, by an individual who advertised a purported investment opportunity. The victim subsequently messaged the individual on WhatsApp, a U.S. social networking messaging applicatoin. **Victim-EG** transferred cryptocurrency from his accounts at Crypto.com and Coinbase, both U.S. based cryptocurrency exchanges, to cryptocurrency addresses at the direction of the scammer. The victim now realizes this "investment opportunity" was a scam.

b. A transaction on October 16, 2025, of 3,600 USDT into the cryptocurrency address listed in Public Group, Section G, No. 2129, included approximately 2,564 USDT of **Victim-EG**'s funds.

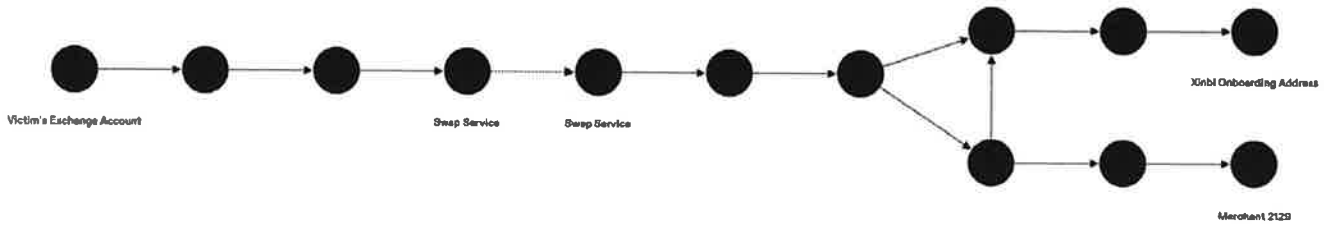
c. **Victim-EG's** funds also entered into the Xinbi ecosystem on at least two other occasions.

    i. On October 18, 2025, approximately 2,203 USDT of **Victim-EG**'s funds included in a 15,000 USDT transaction were deposited into a Xinbi Onboarding Address, [redacted].

[32] RMB, Renminbi, is the currency for the People's Republic of China of which CNY is the base unit.

ii. Again, on December 13, 2025, approximately 213 USDT of **Victim-EG**'s funds included in a 15,000 USDT transaction were deposited into a Xinbi Onboarding Address, [redacted].

iii. **Victim-EG**'s funds were processed through a cryptocurrency swap, a service that swaps funds between blockchains with no know-your-customer information needed to be provided. The flow of **Victim-EG**'s funds is illustrated in Demonstrative 4, below.

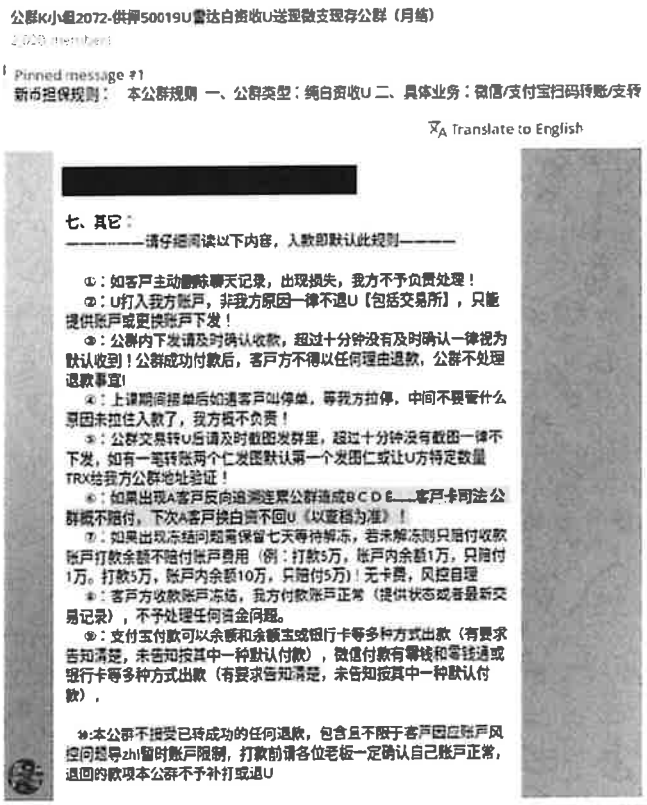


Demonstrative 4: Flow of Victim-EG's funds into Xinbi Public Group, K-Team 2072

Example 2: Category 4.2, Public Group, K-Team 2072

111. Public Group, K-Team 2072 is a Xinbi Merchant Telegram Channel identified by the investigators, and is contained within the Category 4.2. A review of the blockchain shows that, since May of 2025, the merchant has had a total incoming volume greater than $330 million into its cryptocurrency address, [redacted].

112. Information provided by Company 2, which observed the chats on this channel, described the group as a one-way cryptocurrency cash-out desk. Clients deposit USDT into the merchant's cryptocurrency address and receive "clean funds" – as advertised by the merchant – in RMB through bank transfer, bank cash deposit, or cash transfer. Its Telegram group published the merchant's rules, below in Fig. 44.


公群K小组2072-供押50019U雷达白资收U送亚微支理存公群（月结）

2,020 members

Pinned message #1

新币担保规则： 本公群规则 一、公群类型：纯白资收U 二、具体业务：微信/支付宝扫码转账/支转

Translate to English

[redacted]

七、其它：

————请仔细阅读以下内容，入款即默认此规则————

①：如客戶主动删除聊天记录，出现损失，我方不予负责处理！

②：U打入我方账戶，非我方原因一律不退U【包括交易所】，只能提供账戶或更换账戶下发！

③：公群内下发请及时确认收款，超过十分钟没有及时确认一律视为默认收到！公群成功付款后，客戶方不得以任何理由退款，公群不处理退款事宜！

④：上课期间接单后如遇客戶叫停单，等我方拉停，中间不管管什么原因未拉住入款了，我方概不负责！

⑤：公群交易转U后请及时截图发群里，超过十分钟没有截图一律不下发，如有一笔转账两个仁发图默认第一个发图仁或让U方特定数量TRX给我方公群地址验证！

⑥：如果出现A客戶反向追溯连累公群造成BCDE……客戶卡同法公群概不赔付，下次A客戶换白资不回U《以查稽为准》！

⑦：如果出现冻结问题需保留七天等待解冻，若未解冻则只赔付收款账戶打款余额不赔付账戶费用（例：打款5万，账戶内余额1万，只赔付1万。打款5万，账戶内余额10万，只赔付5万）！无卡费，风控自理

⑧：客戶方收款账戶冻结，我方付款账戶正常（提供状态或者最新交易记录），不予处理任何资金问题。

⑨：支付宝付款可以余额和余额宝或银行卡等多种方式出款（有要求告知清楚，未告知按其中一种默认付款），微信付款有零钱和零钱通或银行卡等多种方式出款（有要求告知清楚，未告知按其中一种默认付款），

※:本公群不接受已转成功的任何退款，包含且不限于客戶因应账戶风控问题导zhi留时账戶限制，打款前请各位老板一定确认自己账戶正常，退回的款项本公群不予补打或退U

Fig. 44 - Public Group, K-Team 2072 Rules

113. As translated, the Rules state, "If client A's reverse traceback implicates the public group and causes clients B, C, D, E... to have their cards subject to judicial action, the public group will not provide compensation. The next time, when client A tries to exchange for clean funds, they will not be allowed to convert it back into USDT. Subject to file review."

114. Based on the training and experience of the investigators, the investigators believe this rule is a form of admission that criminal funds are commonly processed by this merchant. Further, investigators believe that this merchant rule likely originates from the experience of the merchant who has previously seen law enforcement freeze cryptocurrency addresses due to association with illicit funds.

115. Law enforcement traced proceeds from a known CIF U.S. victim into this merchant and to addresses associated with Xinbi.

a. In May of 2025, "**Victim-LL**" of Florida filed an IC3 complaint reporting a $246,000 loss in a CIF scheme in or around April of 2025. **Victim-LL** met an apparent wealthy businesswoman on the Canadian dating application Plenty of Fish and subsequently communicated with the individual on WhatsApp. According to **Victim-LL**, he deposited funds from his Crypto.com and Coinbase accounts into cryptocurrency addresses at the direction of the scammer. **Victim-LL** believed he was depositing into a legitimate investment platform, x-onchain[.]com. Based on the training and experience of the investigators, CIF investment platforms often use ".com" websites, in order to project legitimacy to fraud victims. The top-level domain registrar for all .com websites is VeriSign, Inc., a U.S. company, which manages all ".com" domains.[33]

b. When **Victim-LL** attempted to withdraw his funds from the purported investment platform, he was instructed to deposit an additional $20,000 as fees into the cryptocurrency address [redacted].[34]

c. Approximately 120,000 USDT has flown from [redacted], an identified scam address, into [redacted], the merchant address for the Public Group, K-Team 2072.

---

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

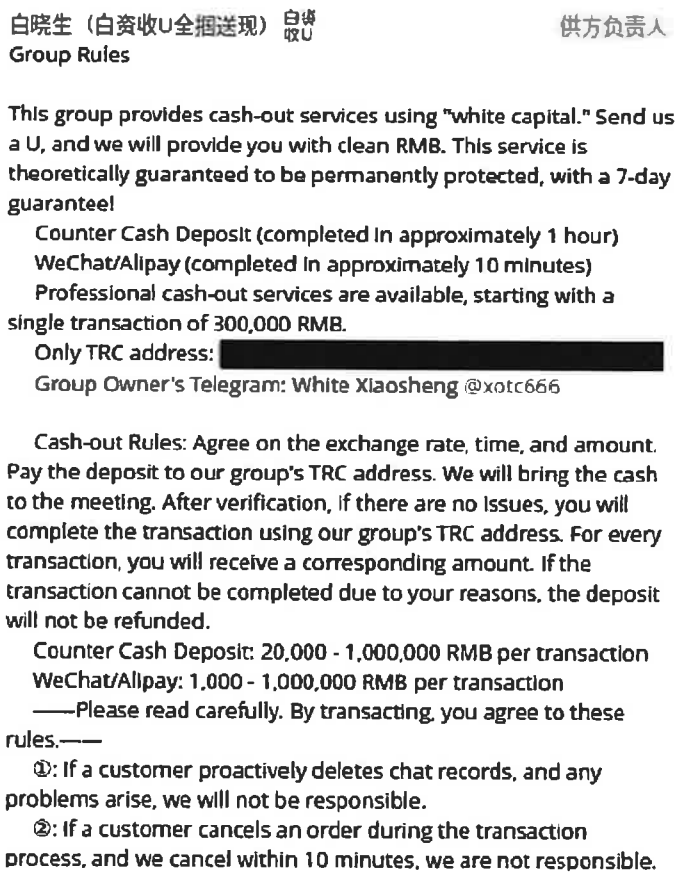
[34] Based on the experience of the investigators with working CIF cases, perpetrators of cryptocurrency investment fraud schemes commonly ask victims to pay "withdrawal fees" to retrieve what victims believe to be investment profits. Perpetrators of these schemes typically continue to request additional deposits until the victim is unable to continue making payments or becomes overtly suspicious of the perpetrators. Typically, in this type of scheme, there is no legitimate method for a victim to withdraw his funds.

116. Even if a victim's funds are not traced directly into Xinbi, the merchant's known use of Xinbi indicates other victim funds may have been laundered through Xinbi or other funds not identified by the investigators likely used Xinbi services.

Example 3: Category 4.1, Public Group, H Sub-Team 369

117. Public Group, H Sub-Team 369 is a Xinbi Merchant Telegram Channel identified by the investigators and is contained within the Category 4.1. A review of the blockchain shows that, since July of 2025, the merchant has had an incoming total volume greater than $44 million into its cryptocurrency address, [redacted].

118. This merchant advertises cash-out services from USDT to RMB. It further claims to be "theoretically guaranteed to be permanently protected," offering protection from law enforcement action by promising reimbursement. Based on the training and experience of the investigators, offering a guarantee and reimbursement from law enforcement action is a form of admission that criminal funds are commonly processed by this merchant.



白晓生（白资收U全捆送现） 白资收U 供方负责人

Group Rules

This group provides cash-out services using "white capital." Send us a U, and we will provide you with clean RMB. This service is theoretically guaranteed to be permanently protected, with a 7-day guarantee!

Counter Cash Deposit (completed in approximately 1 hour)

WeChat/Alipay (completed in approximately 10 minutes)

Professional cash-out services are available, starting with a single transaction of 300,000 RMB.

Only TRC address: [redacted]

Group Owner's Telegram: White Xiaosheng @xotc666

Cash-out Rules: Agree on the exchange rate, time, and amount. Pay the deposit to our group's TRC address. We will bring the cash to the meeting. After verification, if there are no issues, you will complete the transaction using our group's TRC address. For every transaction, you will receive a corresponding amount. If the transaction cannot be completed due to your reasons, the deposit will not be refunded.

Counter Cash Deposit: 20,000 - 1,000,000 RMB per transaction

WeChat/Alipay: 1,000 - 1,000,000 RMB per transaction

——Please read carefully. By transacting, you agree to these rules.——

①: If a customer proactively deletes chat records, and any problems arise, we will not be responsible.

②: If a customer cancels an order during the transaction process, and we cancel within 10 minutes, we are not responsible.

Fig. 45 – Translation of Public Group, H Sub-Team 369 Rules[35]

119. Law enforcement traced proceeds from a known wire fraud victim into this merchant and to addresses associated with Xinbi.

a. In August of 2026, the USSS interviewed "**Victim-KM**" of California who reported a loss amount of over $1.6 million in a CIF scheme in August 2025.

b. In August of 2025, **Victim-KM** was contacted by an unknown individual on the LinkedIn, a U.S. based social networking platform. **Victim-KM** was eventually convinced by the scammer to transfer funds from her IRA and 401k held at a U.S. bank into a Coinbase account and eventually into cryptocurrency addresses associated with a purported

[35] Based on the training and experience of the investigators, "white" is a common term for clean funds, and "U" in the screenshot references USDT. "TRC address" is a cryptocurrency address on the TRON Blockchain.

investment website, Zgtcx.com. As stated previously, the top-level domain registrar for all .com websites is VeriSign, Inc., a U.S. company.

c. In May of 2026, **Victim-KM** attempted to withdraw her funds, but the platform "required" a "fee" of approximately $365,000 to process any withdrawals. **Victim-KM** was unwilling to sell her condo to pay the fee at which time the scammers ceased all contact with her.

d. Of the $1.6 million of **Victim-KM**'s loss, approximately 400,000 USDT was deposited to [redacted]. Approximately 120,000 USDT from [redacted], an identified scam address, has flown into the merchant cryptocurrency address, [redacted].

Example 4: Category 4.1, Public Group. F-Group No. 1193

120. Public Group. F-Group No. 1193 is a Xinbi Merchant Telegram channel identified by the investigators, and is contained within the Category 4.1. A review of the blockchain shows that, since April of 2025, the merchant has had an incoming total volume greater than $102 million into its cryptocurrency address, [redacted].

121. Information provided Company 2, which reviewed the Telegram Channel, identifies the group as a one-way cryptocurrency cash-out desk (similar to Example 2). Clients deposit USDT into the merchant's cryptocurrency address and receive "clean funds" – as advertised by the merchant – in RMB through bank transfer, bank cash deposit, or cash transfer. The merchant includes checks to identify freezes, a waiting period for freeze, and compensation for accounts frozen by law enforcement. Based on the training and experience of the investigators, offering a guarantee and reimbursement from law enforcement action is a form of admission that criminal funds are commonly processed by this merchant.

122. Law enforcement traced proceeds from a known CIF victim into this merchant and to addresses associated with Xinbi.

a. In October of 2025, **"Victim-HL"** of Arizona filed an IC3 complaint reporting a loss amount of over $600,000 in a CIF scheme between July and August of 2025.

b. **Victim-HL** communicated with an unknown individual on WhatsApp and was subsequently convinced to deposit cryptocurrency from his Coinbase account into a purported investment platform, xenonstore.com. As stated previously, the top-level domain registrar for all .com websites is VeriSign, Inc., a U.S. company. The purported investment platform showed high yields, with the victim's approximate 600,000 USDT deposit growing to over 2.9 million USDT.

c. When **Victim-HL** attempted to withdraw funds to his cryptocurrency exchange account, the funds never were transferred, and the victim was told by the scammers that the funds had been "hacked." In order to recover the funds, the scammers told **Victim-HL** that he would need to pay "fees" in excess of $300,000 to recover the funds. When **Victim-HL** told the scammers that he believed this was a scam, the subjects ceased all communication with the victim.

d. During the course of the scheme, **Victim-HL** deposited over 400,000 USDT into cryptocurrency address [redacted]. Funds from this identified scam address were laundered through cross-chain swaps and numerous intermediary addresses. Funds from [redacted] are included in transfers to a network of addresses which deposits into [redacted], the Public Group. F-Group No. 1193 cryptocurrency address.

Example 5: Category 4.1 Public Group, F Section, No. 1181

123. Public Group, F Section, No. 1181 is a Xinbi Merchant Telegram Channel identified by the investigators, and is contained within the Category 4.1. A review of the

blockchain shows that, since April of 2026, the merchant has had an incoming total volume greater than $43 million into its cryptocurrency address, [redacted].

124. Information provided by Company 2, which reviewed the Telegram Channel, identified the group as a one-way cryptocurrency cash-out desk. (similar to Examples 2 and 4). Clients deposit USDT into the merchant's cryptocurrency address and receive RMB through bank transfer or cash transfer, including physical cash couriered in China.

125. The merchant guarantees clean, "white funds" and compensation if law enforcement freezes funds. Based on the training and experience of the investigators, offering a guarantee and reimbursement from law enforcement action is a form of admission that criminal funds are commonly processed by this merchant.

126. While U.S. victim funds have been identified as interacting with the Xinbi network throughout the investigation, these merchants provide laundering services for funds fraudulently obtained across the world. Even in cases when non-U.S. persons are scammed, scammers depositing funds into the Xinbi network utilize U.S. infrastructure to commit their CIF schemes.

127. Law enforcement traced proceeds from a known CIF victim into this merchant and to addresses associated with Xinbi.

a. In August of 2026, the USSS interviewed "**Victim-SQ**," a resident of France, who reported falling victim to a cryptocurrency romance and confidence scam in which she lost over $70,000 in [date].

b. **Victim-SQ** was contacted by an unknown individual on Tantan, a Chinese-based dating application. After gaining the victim's trust, the individual convinced **Victim-SQ** to deposit

funds and open a "shop" on a purported drop shipping platform, LavishLocs Inc.[36] The platform used the website, lavishlocs.com. According to a WHOIS[37] domain name registration, the Website Registrar for lavislocs.com is NameBright.com, a U.S. based web registrar.

i. The scammer and the fraudulent website advertised LavishLocs Inc. as a registered corporation in the State of Colorado. LavishLocs Inc. is listed as a corporation in good standing with the Colorado Secretary of State website as of August 9, 2026. As described previously in this affidavit, Xinbi itself had been fraudulently registered as a corporation in Colorado. Based on the experience of the investigators with working cryptocurrency crime, fictitious investment platforms, exchanges, and corporations commonly register specifically with a U.S. Secretary of State in order to prove apparent legitimacy to victims.

c. The scammer had **Victim-SQ** deposit more and more funds, making her believe that she was running a store on the platform and that she would see profits. Throughout the duration of the scam, **Victim-SQ** deposited approximately 40,000 USDC into the platform, utilizing the Ethereum blockchain.

d. In January of 2026, **Victim-SQ** was contacted by another "shop owner" who stated that the platform was a scam. In total, four victims, **Victim-SQ**; a victim from Australia; a victim from Hong Kong; and a victim from Taiwan, communicated with each other after

[36] Drop shipping is the process of advertising and selling products when the store itself does not hold any inventory.

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

realizing they have been scammed, all via the same investment website, hosted in the United Sates.

e. One of the other victims stated to **Victim-SQ** that because the victim had alerted other victims on the platform, the scammer communicating with her stated he was being physically beaten by his supervisors. This information, and the fact that the scammers were communicating in a Chinese language, suggests that this particular scam, and thus the funds flowing from it to the merchant, originated from a facility such as a scam compound in Southeast Asia.

f. The website, lavishlocs.com, advertised two TRON blockchain wallet addresses, [redacted] and [redacted]. Funds from these two addresses flow into the Public Group, F Section, No. 1181 cryptocurrency address, [redacted].

F. Laundering Activity Involving the Target Xinbi Addresses (The Target Funds)

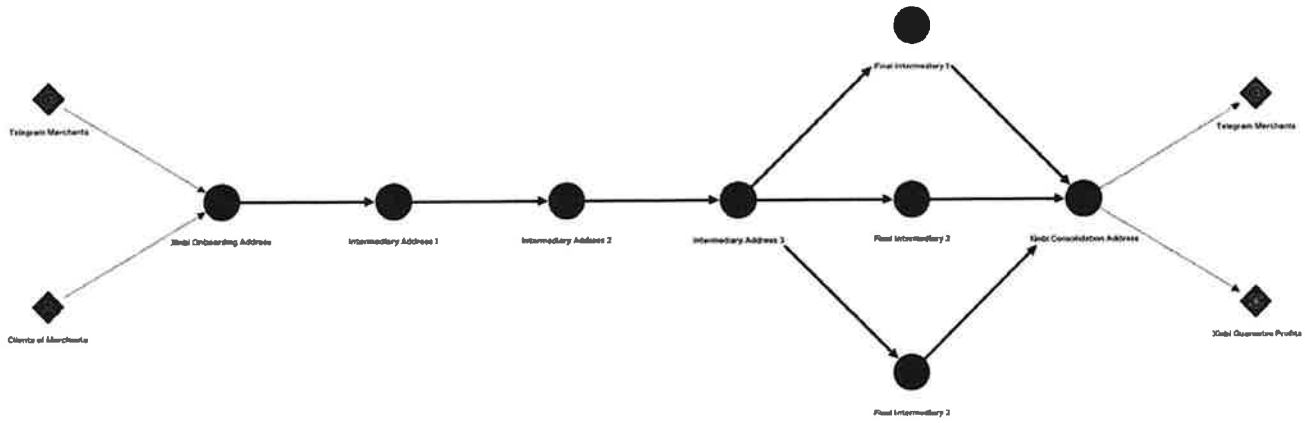
128. Investigators determined, based on blockchain analysis and information posted in Telegram channels, that Xinbi Guarantee [redacted] While the addresses themselves change, the structure of the laundering process remains the same. Scam victim funds move through a series of unhosted cryptocurrency wallets and/or cross chain swaps before arriving into an attributed Xinbi wallet address. These transactions occur rapidly within a short timeframe which have no legitimate financial purpose other than to obfuscate fund movement and avoid seizure by law enforcement. Investigators know that moving victim funds in such a manner is how criminals regularly launder cryptocurrency on blockchains.

129. Due to the length of time in which these cryptocurrency addresses are active, often only two weeks, and the rapid rate through which the funds flow, it is unviable for law enforcement to fully attribute the funds held in Xinbi controlled cryptocurrency addresses to victim funds or other specified unlawful activity. The commingling of fees, payments for services, and disbursements, make it difficult for law enforcement to develop enough attribution to seize a given cryptocurrency address and impact the operations of Xinbi prior to Xinbi turning over to new cryptocurrency addresses. Based on the training and experience of the investigators, this is believed to be a feature of design by Xinbi to obfuscate its operation and make it difficult for law enforcement to take action against its infrastructure. By analyzing the current and previous framework by which Xinbi operates and applying it to future addresses, investigators can determine the role of a new cryptocurrency address immediately when it is first used in the network.

130. Specific target addresses are described later in this affidavit, and listed in Attachment A-1. These cryptocurrency addresses have been identified through the below methods and analysis.

131. [redacted]

[redacted]



Demonstrative 5: Xinbi Guarantee's Laundering Structure

132. Funds initially flow into the [redacted] When the [redacted]

[redacted]

133. Based on the experience of the investigators, criminals will often conduct multiple otherwise unnecessary transactions that incur transaction costs to layer ill-gotten funds. This is done intentionally to ultimately conceal or disguise the nature, location, source, ownership, or control of those proceeds. These quick transfers between addresses attributed to Xinbi is a strong indication that the movement of funds is meant to conceal or disguise the nature, location, source, ownership, or control the funds.

134. [redacted]

135. [redacted]

136. [redacted]

137. [redacted]

138. [redacted]

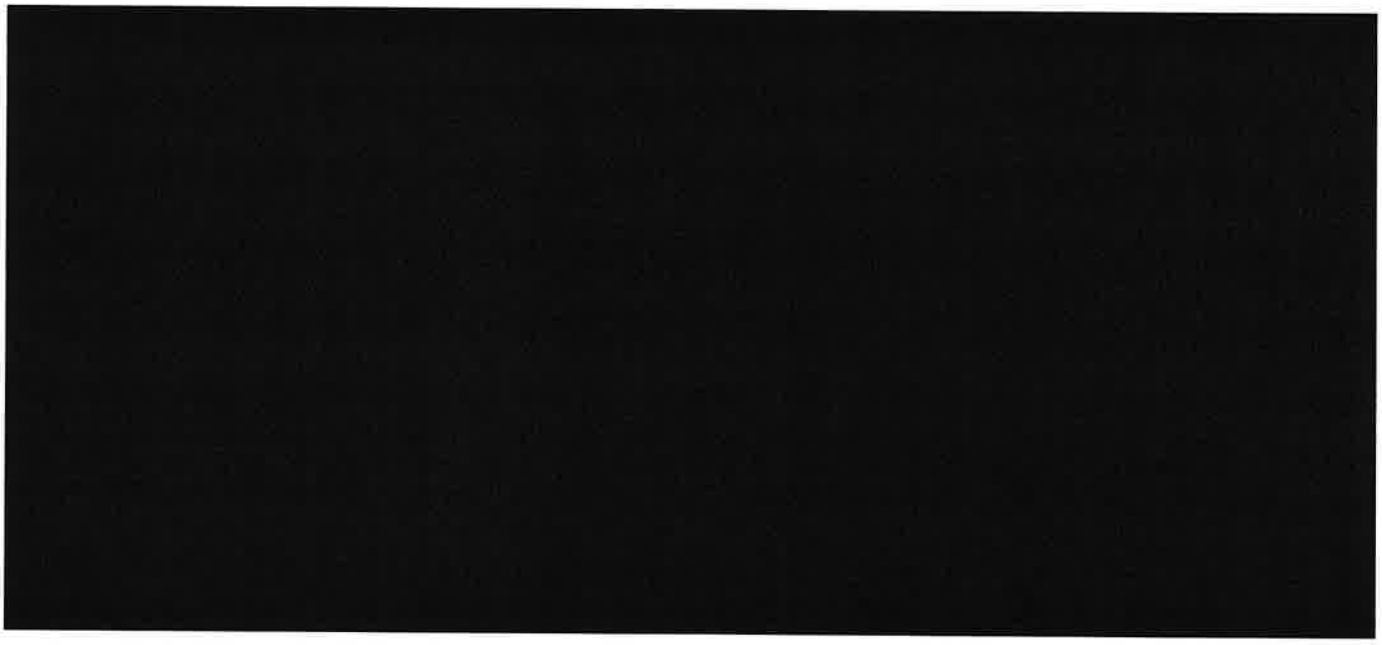
[redacted]

38 [redacted]

39 [redacted]

139. [redacted]

140. [redacted]



141. [redacted]

142. [redacted]

143. [redacted]

	Onboarding Address	Date of First Transfer	Date of Last Transfer	Incoming Volume (USD)
a.	TCuSMYxiPKLq4u5g8hj74qmrg61vSXYF9n	07/07/2022	03/29/2024	$220,498,358.67
b.	TDCm3Puu5Ry3Nwv3xpLWHaPufLyf341Bny	07/07/2022	08/23/2023	$199,173,342.12
c.	TNANMFXnTZ5UBsHx4Hk7ViTgXu8KgwPfdh	07/07/2022	05/20/2026	$316,308,082.18
d.	TPy6nXLR1MXaXbUBGTXsHKmXxd6rkicm7	07/07/2022	10/01/2023	$233,712,502.38
e.	TR9gwkMdd7KgvALqawrbp6fySsBAf4pEj2	07/07/2022	05/13/2024	$227,539,126.23
f.	0x3E5f12F0F7f99415dE966f0F3c30d2D4e5106D01	07/12/2022	10/16/2023	$304,960.05
g.	0x73C45AF516F1B64A904e230B16CC133eda4c40c1	07/12/2022	07/13/2024	$159,741.49
h.	0xd08EF8d3467EfCE45CE00bEe02415bF738Ee8626	07/27/2022	08/12/2023	$52,575.29
i.	0x2d5d3B617BD8C596bB17995aEEd31a8Ea10445eF	08/17/2022	08/12/2023	$55,118.75
j.	0xd3d16885B31Fa2EA6F719c6637a36AA882FA3306	09/16/2022	08/12/2023	$145,341.07
k.	TDAeQJ2VVCMnYesmpAQR251D3vo7kuGNut	12/30/2022	05/22/2024	$50,509,825.49
l.	0x71ebA2e9CD5b71b76736A8186Bf8588fDc247F3a	01/09/2023	08/12/2023	$49,691.70
m.	TAYaFmVWqXZWcLSEuyWMNjxt861MRbxqJy	02/12/2023	05/13/2025	$35,001,186.45
n.	0xf03dC0C4d1b9086399180FF031cE591068e1492b	02/17/2023	08/12/2023	$58,950.59
o.	TXco6CeJFBY1qz946bpvi2pgWuq7xV49uf	08/07/2023	05/23/2026	$984,586,922.80
p.	0x41e211e7f400ba3a61adbe869f7887810be06c00	08/10/2023	02/19/2025	$7,610,620.42
q.	THY84dJ4EPsPddwJP2URsqkDzHwVB9uk48	07/22/2024	05/12/2026	$1,317,059,505.37

r.	0x7062a25a86a0f27e4e5006868a5ce0ea0b2b030b	07/31/2024	04/05/2025	$2,060,965.62
s.	TKiGdnr3U8UkG5rBcAfscag68gJGvryNdv	04/05/2025	01/18/2026	$355,645,431.60
t.	0x3df41d385dc036bbc8adfa94729c171bb33b2cad	04/07/2025	05/09/2025	$105,736.91
u.	TV6Bj9HbSexcYRcLHqwJvPTMFagQ9RgphH	05/09/2025	02/16/2026	$344,149,924.48
v.	0x3c0b33f4bea6c5c08f9d1815fc6191a733ecf0e6	05/12/2025	08/30/2025	$38,011.68
w.	TAtgkTdvTAcK74dRmxJ1zb4vQNjoqefFin	05/31/2025	04/08/2026	$423,632,772.73
x.	0x9e937cdd8ded66c65aabf95142d591e69682e206	06/01/2025	09/20/2025	$176,534.71
y.	0x9E1fa5B32f5414Ce8d7568EDe0853DB86f0feB7d	07/01/2025	09/20/2025	$125,945.24
z.	TAB2kKwPYiXq1qNxaQHhrxvFNPZ51hSzmR	07/01/2025	07/25/2026	$388,338,973.23
aa.	TW5tokvhEfrb77z98Rc8HqbkzQJ6sxYtGX	07/31/2025	04/23/2026	$422,700,657.50
bb.	0xd11a1e86b7a1349228079b248e5b690ced91689d	08/01/2025	10/15/2025	$448,280.35
cc.	TG6mCSLxNCc8NUAmygwMMy4Ma6cGouaanW	08/30/2025	07/16/2026	$486,093,877.82
dd.	0x048bcbce6168750e5ccdAc7B3328D66D5500c6Bc	08/31/2025	10/15/2025	$600,060.83
ee.	TFfYgfg6SRgMXQNFu1iY75S8n664gSXYRo	09/30/2025	02/05/2026	$203,974,878.87
ff.	0x56e11e016818996008018B07D4B6c720F57E65ff	10/03/2025	12/06/2025	$38,176.23
gg.	TPN6bWLcTY6We2eKajRx18peJEhkxQG78y	10/15/2025	03/31/2026	$299,616,999.96
hh.	TDxQY8axwyTEWXiixVzVBG6Q46zKLU9fjb	10/31/2025	06/27/2026	$450,283,795.88
ii.	0x9FC718B137A1B11E086EbBAfbcdf4d398678A953	11/01/2025	12/07/2025	$56,997.22
jj.	TGFWLzVvyDdwnrN3XKKGsqthFf61nTX155	11/25/2025	06/19/2026	$358,796,699.99
kk.	TPC9By4t2rzCCMe1MnugRLtCSPbeiBe4wJ	12/12/2025	07/07/2026	$391,119,278.68
ll.	0xaaB14c8DddcADAE1AB364C595D7955dDE3Cf32dc	12/19/2025	02/03/2026	$14,153.92
mm	TL5EciS2Eg58W5HUY3w48D1xsmo7vJws8m	12/31/2025	05/31/2026	$135,503,440.14
nn.	0x5c48D56696F1DDe3Bdd5CB78c6100ce5cf452BE2	01/05/2026	03/31/2026	$50,243.13
oo.	TT66hhnGtCietkCNd4izkuUEiRFmSygqLD	01/07/2026	06/19/2026	$500,189,302.78
pp.	TTgSvGT4ncQje6pLvCaMKGiCnVZZcVhj61	02/01/2026	07/19/2026	$196,545,923.46
qq.	0x4FbF87f9FcE0ff225bc278916f7De3348Af79dB2	02/03/2026	03/31/2026	$111,650.20
rr.	0x63c7A120F5E891ccA78E30cb48bD6447810cb02a	02/25/2026	03/31/2026	$41,922.26
ss.	TFyUaAFASzRExZcEkov1sPqRdo2H6iruHc	02/25/2026	07/23/2026	$163,844,269.79
tt.	TPxubKsyAPtqgxXAoDmYg9zbYvULZeNGBS	03/02/2026	03/31/2026	$11,071,134.05
uu.	0x8f2fB423A0188C86313cD9FD60B4B29d216407a0	03/09/2026	07/02/2026	$1,542.82
vv.	TYiXvj2vsE8D9QANBSPxtCrqbADHjhmBPK	03/30/2026	06/19/2026	$350,546,566.78
ww	TL9FowVPhqALcZwScxECpXcXry65XQSJGx	04/01/2026	05/20/2026	$136,913,460.54
xx.	0x0c7469d0a4995410719788cecf68d008cf641342	04/07/2026	07/23/2026	$202.08
yy.	TTyc4iwhiU6KZwQ3757JizRHvCVUjNZ92v	04/17/2026	07/24/2026	$197,338,878.57
zz.	TY8rbQc4GbnmqXwtoLPsmvJJBeThvZdX6H	04/30/2026	07/11/2026	$235,309,856.49
aaa.	THVBx81sjRxHqCxPt7JKcfe4k1ShnPVY1k	04/30/2026	07/11/2026	$162,933,487.88
bbb	TGoUxuDmr6T9Vov1GSJzt5JjpisBaJvCbk	05/11/2026	07/18/2026	$283,663,657.75
ccc.	TAhvsFPGf6TyPEZknYkCyDfS96gnebPhkz	05/27/2026	08/03/2026	$570,097,326.77
ddd	TWqcMjV7Wq2RHe2CSiKQHpkn6A7B2AWUPe	06/30/2026	08/05/2026	$544,603,876.70
eee.	TG83Fk56S2mycAUMYHZyZp9wMg6DCf4bUn	07/31/2026	Present	$543,979,369.48
fff.	TWPma8xH48AEN93x2krdukV9e1j6sPsBeS	08/31/2026	Present	$35,627,488.61