CYBER
THREAT
ANALYSIS

Recorded Future®

Insikt Group®

September 15, 2026

Inside Tajin Group's Phishing and Money Laundering Network

Tajin Group detailed its operational challenges and announced key plans and changes, showcasing its ability to adapt and evolve to conduct payment card theft and money laundering activities.

Operators and third-party vendors of Chinese-language Guarantee Marketplaces are using Fragment Marketplace to purchase Telegram usernames and anonymous phone numbers for fraud-related purposes.

The ever-increasing number of guarantee marketplaces means that third-party vendors are able to pivot to rival guarantee marketplaces, signifying that this ecosystem is becoming more competitive.

Executive Summary

This report provides insights and analysis to better understand the role of third-party vendors and guarantee marketplaces from the perspective of Tajin Group, a third-party vendor that advertises and provides services on two Telegram-based Chinese-language guarantee marketplaces, Dabai Guarantee and Xinbi Guarantee. This includes operational challenges, perspectives regarding the competition from other threat groups, and how Tajin Group adapts to changes in its operating environment.

Additionally, we identified that Chinese-language guarantee marketplace users and third-party vendors are increasingly using third-party services to purchase and sell Telegram usernames and anonymous virtual numbers. Through these services, Chinese-speaking criminals can link multiple Telegram usernames and an anonymous virtual number (in lieu of SIM cards) to a single Telegram account. This activity indicates a continued evolution and adaptability among these threat actors, who are strengthening their operational security (OPSEC) measures through tactics such as using anonymous virtual numbers to create Telegram accounts to avoid detection and reach a wider audience.

The phishing, payment card theft, and money laundering activities of Tajin Group, guarantee marketplaces, and their third-party vendors can negatively impact banks, fund transfer services providers, cryptocurrency exchanges, and individuals vulnerable to scam and fraud-related campaigns. As Tajin Group is a single third-party vendor, the potential financial gains in the global payment industry are likely to incentivize other threat groups operating on Chinese-language guarantee marketplaces to conduct campaigns by replicating Tajin Group's tactics, techniques, and procedures (TTPs) on a global scale.

Key Findings

- Tajin Group is mainly involved in phishing, payment card theft, and money laundering. The group actively targeted mainland Chinese citizens and Chinese banks and demonstrated a nuanced understanding of the prerequisites required to transfer funds overseas or use other payment cards remotely.
- Tajin Group conducts extensive testing involving payment cards belonging to multiple countries on the financial platforms CCAvenue and Geidea. They are well-versed in financial crimes and have listed multiple Bank Identification Numbers (BINs) for payment cards from twelve countries.
- Tajin Group constantly seeks cooperation with other threat groups to use direct payment channels that accept UnionPay, VISA, Mastercard, JCB, and Apple Pay; exploit 2D, 3D, and other payment gateways; and UAE Dirhams and electronic gift cards for their financial theft and money-laundering operations.
- Tajin Group has pivoted from Dabai Guarantee to Xinbi Guarantee, showcasing that third-party vendors do not necessarily stay loyal to a single guarantee marketplace platform. The threat group also detailed their operational challenges, intense competition from competitors, and trust issues with their previous payment card suppliers.
- Operators of Tajin Group have sold and bought at least 100 Telegram usernames and multiple phone numbers from Fragment Market, a platform that facilitates the buying and selling of virtual, anonymous phone numbers and Telegram usernames, further anonymizing their operations.

Table of Contents

Background

Guarantee marketplaces have become increasingly popular among Chinese cybercriminals as viable alternatives to Chinese-language dark web marketplaces since Huione Guarantee and its business model gained prominence around 2021. Based on our research and previous reports, we have observed that multiple third-party vendors who are usually involved in advertising the sale of malware, databases, phishing kits, and money laundering services on dark web marketplaces have also begun to use Telegram-based guarantee marketplaces to advertise their services or seek cooperation on these platforms. These marketplaces act as a powerful force multiplier to strengthen cooperation among Chinese-speaking threat groups in recruitment, crowdsourcing information, sharing resources, and deploying personnel to commit crimes that require in-person interactions. For additional insights, see our previous report "Evolution of Chinese-Language Guarantee Telegram Marketplaces".
We noted that these Chinese-language guarantee marketplaces typically consist of hundreds to thousands of third-party vendors, each operated by different Chinese-speaking threat actors (some syndicates) across the globe. To better understand how third-party vendors operate on these guarantee marketplaces and how they contribute to cybercriminal activities, Insikt Group analyzed the activities of Tajin Group, a threat group that conducts phishing campaigns, payment fraud, money laundering, carding, and exploits 3D and 2D payment gateways, among others. Chinese-language guarantee marketplaces typically follow a strict rule requiring that third-party vendors use only one guarantee marketplace at any given time, and we identified that Tajin Group complied with this rule by ceasing activities on Dabai Guarantee before pivoting to Xinbi Guarantee. Tajin Group observed Chinese etiquette and showed respect for the Chinese-language guarantee marketplace ecosystem, demonstrating that there is likely a common understanding between the operators of these guarantee marketplaces by having a system where no third-party vendors are allowed to make use of multiple platforms to advertise and conduct their campaigns.

Overview of Tajin Group

Tajin Group (踏金集团;踏金 [Tajin] translates to "stepping on gold" in Mandarin) is a Chinese-speaking threat group that focuses on phishing, carding, financial fraud, and money laundering. Insikt Group observed that Tajin Group used to be a third-party vendor operating on Dabai Guarantee from May 2025 to April 2026, but pivoted to Xinbi Guarantee around May 2026. Dabai and Xinbi guarantee marketplaces are known to be populated with third-party vendors that provide various services that facilitate cybercriminal activities, including money-laundering methods and services, the sale of compromised social media and e-commerce accounts, SIM cards, data containing personally identifiable information (PII), malware-as-a-service (MaaS), deepfake technology, know-your-customer (KYC) bypass services, and other illegal activities.

As guarantee marketplaces typically require their vendors to stake cryptocurrency as deposits, Tajin Group claimed to have deposited 208,848 in Tether (USDT) on Xinbi Guarantee. The deposit amount often indicates vendors' scale of operations, where larger deposit amounts reflect larger-scale operations. By comparison, most vendors on Chinese-language Telegram guarantee marketplaces

typically deposit only a few hundred to a thousand USDT. As shown in **Figure 1**, the deposit amount of 208,848 USDT is significantly larger than that of most other third-party vendors.[1]

Figure 1: *Tajin Group's channel @ttjt claimed that the group is a vendor on Xinbi Guarantee with the corresponding channel @xb8848, and that the group has deposited 208,848 USDT into Xinbi Guarantee Marketplace (Source: Telegram)*

The following are some observed illegal activities that members of Tajin Group have been involved in since March 2026:

- Financial fraud services involving point-of-sale (POS) machines, QR codes, apps, and gift card websites across various countries (see **Table 3**), as well as professional hacking services
- Fund transfer services involving ATMs and bank transfers belonging to multiple countries
- Ghost-tapping and contactless ATM withdrawal operations involving near-field communication (NFC) relay techniques
- Buying and selling compromised payment card information, including card verification values (CVVs)
- Currency swaps involving major currencies such as USD, Singapore dollar, Korean won, Japanese yen, UAE Dirham, and more

The following lists official Tajin Group Telegram channels:

- 踏金集团（交流群💧广告每日限制一条）**(@tjjt):** Main Tajin Group channel; 3,282 members as of writing

[1] Insikt Group is unable to verify Tajin Group's claim regarding the deposit amount on Xinbi Guarantee.

- 踏金集团💧供需频道 **(@xb8848):** Dedicated Xinbi Guarantee Public Group channel for Tajin Group; 2,193 subscribers as of writing
- 踏金集团💧供需（外料）**(@tjjt_gx):** Tajin Supply and Demand channel; 290 subscribers as of writing
- 公群**8848**已押**888U**长期招境外银联、自建站渠道 **(@dbtm898):** Tajin's Public Group channel on Dabai Guarantee; 141 members as of writing; however, this channel's activities ceased on April 10, 2026, as Tajin Group pivoted to Xinbi Guarantee
- 卡扣渠道**/**技术交流群（广告每日限制一条**) (@tjjt_liaotianqun):** Withholding/technical channel; 463 members as of writing; 卡扣渠道 (withholding channels) are financial channels through which funds are transferred from consumers' bank accounts to merchants
- 踏金集团 外料 **(@tjjt_wailiao):** Channel to transfer funds or cryptocurrency using Tajin Group's transfer services; 315 members as of writing; this channel is only for threat groups involved in carding activities (payment card information with CVV, unauthorized use of payment cards, and more)

***Figure 2**: Tajin Group's known channel, @dtb898, when it was operating as a third-party vendor on Dabai Guarantee, with a known deposit amount of 888 USDT; the channel has been inactive since April 10, 2026 (Source: Telegram)*

Insikt Group has observed that, apart from Tajin Group, multiple Chinese-speaking threat groups, including guarantee marketplace owners and third-party vendors, have been obtaining and using Telegram collectible usernames. Telegram collectible usernames are secure, tradable digital assets on the TON blockchain through the use of Toncoins (TON). They grant full ownership to the buyer, who can then also sell or lease them. **Figure 3** shows that Tajin Group acquired the Telegram username @tjjt_gx for 88 fragments (approximately $149.48 USD) on the Fragment Market.

Fragment Market is the official decentralized marketplace integrated with Telegram, designed for buying and selling virtual anonymous phone numbers, premium digital usernames, Telegram Stars, ad placements, and premium subscriptions. It is powered by the TON blockchain and provides users with

income by enabling the secure, anonymous trading of unique usernames and numbers. Through Fragment Market, individuals can purchase multiple collectible usernames as NFTs on the TON blockchain and link all usernames to a single Telegram account. According to Bitget Wallet, key features of Fragment Market include:

- **Virtual Numbers and Usernames:** Individuals can purchase anonymous numbers (which allow them to register Telegram accounts without a physical SIM card) and secure rare or "OG" short usernames that are minted as NFTs
- **Telegram Stars & Ads:** The platform enables individuals to buy Telegram Stars (in-app currency for mini-apps) often at a discount, or purchase ad placements to promote channels
- **Decentralized Auctions:** Users can bid on high-value usernames using TON, with smart contracts automating ownership transfer instantly upon auction closure

Chinese threat actors looking to expand or scale down their operations can buy or sell Telegram usernames. Insikt Group assesses that in the event Tajin Group's operators wished to sell their business to another threat group, they could use Fragment Market to automate the transfer of ownership via smart contracts. Additionally, because Fragment Market allows individuals to purchase anonymous numbers to register private Telegram accounts, this would enable Chinese-speaking threat groups to strengthen their OPSEC by further anonymizing their operations, making detection and tracking by law enforcement agencies more difficult.

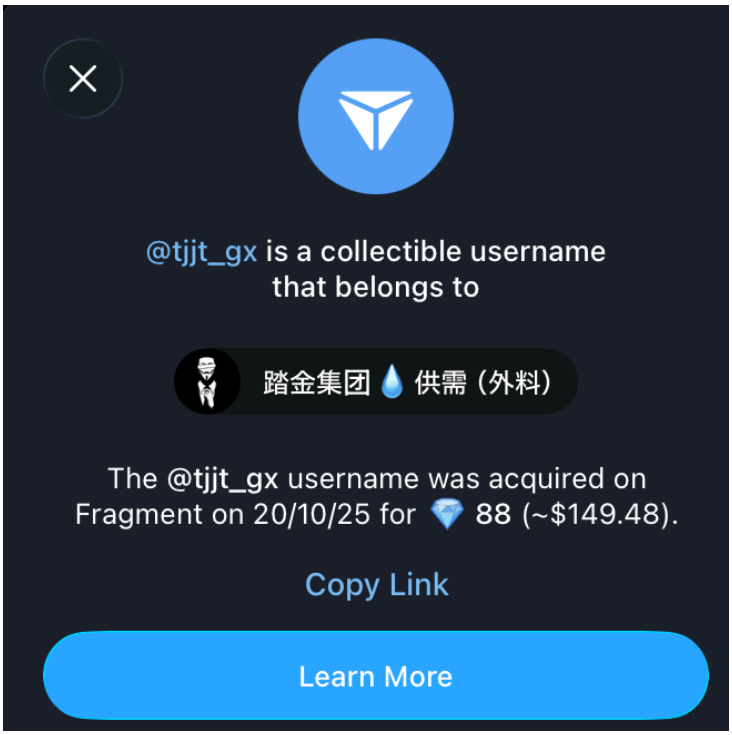

Figure 3: *Tajin Group's money laundering channel @tjjt_gx was acquired with 88 Toncoins (worth approximately $149.48) on Fragment Market on October 20, 2025 (Source: Fragment Market)*

By analyzing the TON wallet address belonging to the current owner using the TON blockchain, **Figure 4** showcases that the current owner of the Telegram username @tjjt_gx has two TON addresses, UQAXN4aCAbJ_1GK1jA38eOpG-py3MYP3RhAuChCG4HE7oX1S (Transaction History) and UQCOe_qYf9xsaQFWbq5Jg-Q0BRP_RwwHYIY1ErS9enJrjgoW (Transaction History), where part of their funds have been frozen and labeled "SCAM". As shown in **Figure 5**, the TON address has multiple suspicious transactions flagged by the TON blockchain.

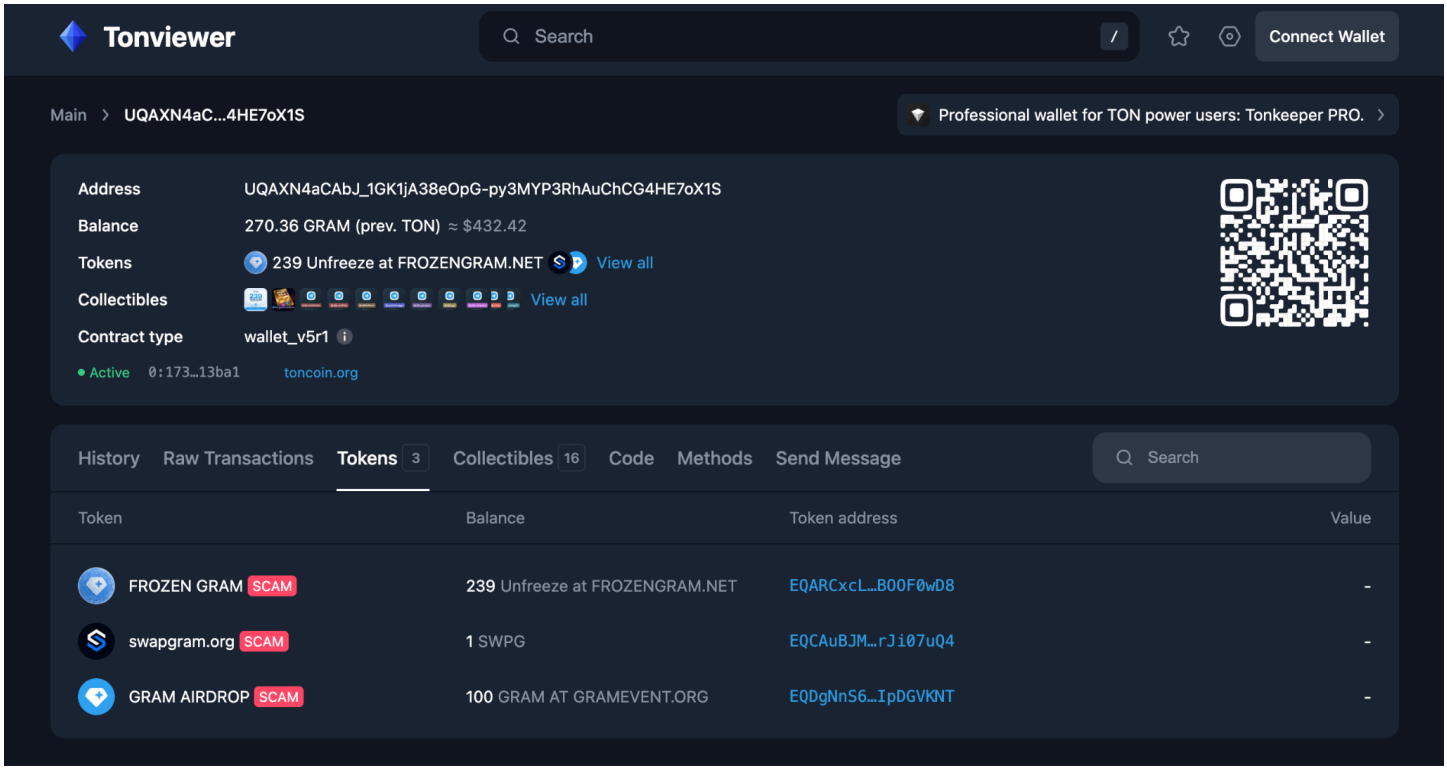

Figure 4: *Current owner of money laundering channel @tjjt_gx; TON tokens were frozen and labeled "SCAM" (Source: TON)*

By analyzing both TON address transaction histories, we identified that this group sold and purchased more than 100 Telegram usernames and multiple phone numbers, some of which were likely used in transactions with other criminal groups. For more information regarding the monikers of Telegram usernames and phone numbers being bought and sold by Tajin Group on Fragment Market, please refer to the transaction histories (1, 2). The transaction histories also open the potential for future investigations into the dealings of Tajin Group within and outside their group, and identify additional Indicators of Compromise (IoCs), such as private Telegram handles and channels, belonging to this threat group.

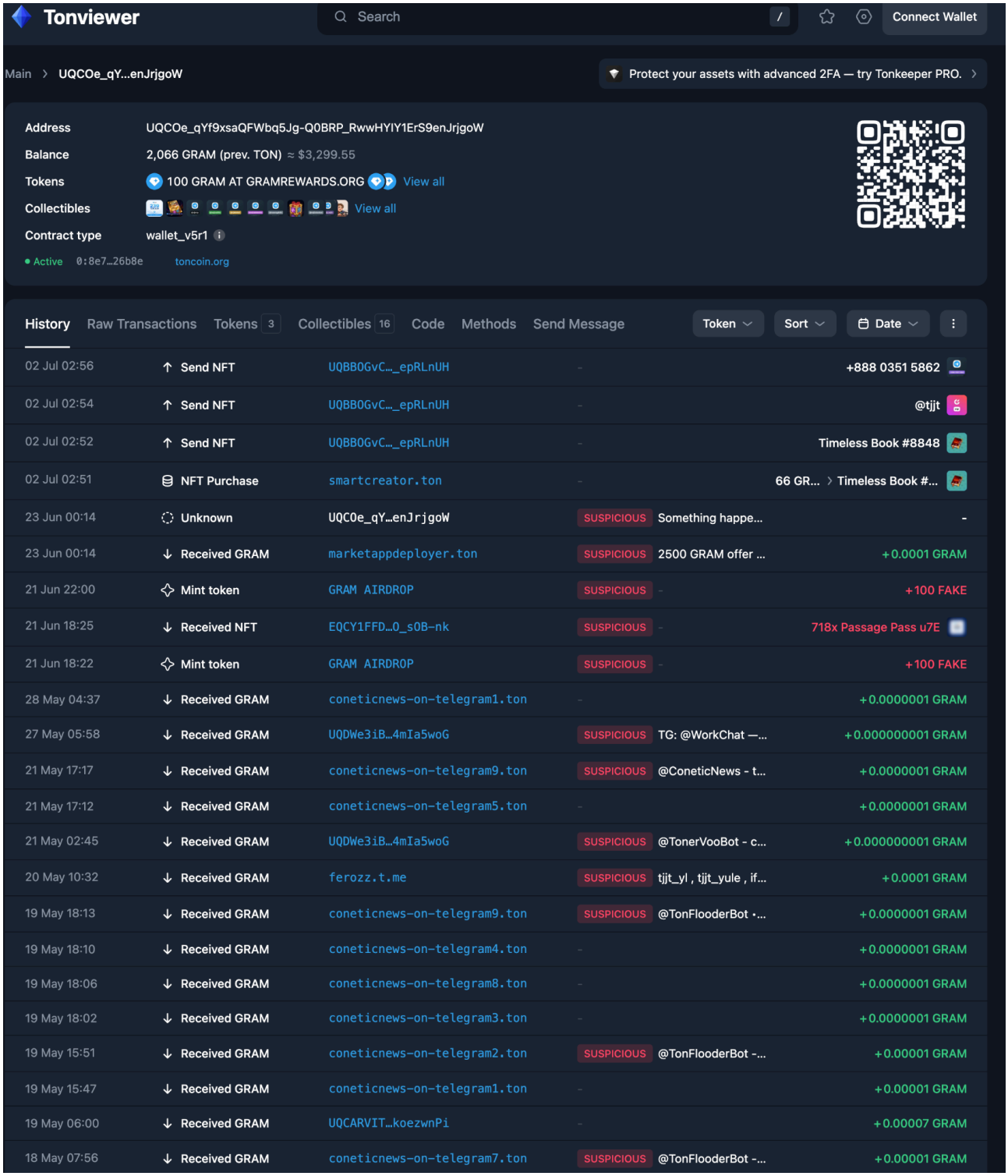

Figure 5: *Transaction history of the TON address UQAXN4aCAbJ_1GK1jA38eOpG-py3MYP3RhAuChCG4HE7oX1S, where operators of Tajin Group bought and sold Telegram usernames and phone numbers (Source: TON)*

Scamming and Hacking Activities

Exploiting Payment Channels and Methods Involving 2D and 3D Payment Gateways

踏金集团💧六六（未及时回复请弹语音）(@tjjt66), an administrator of Tajin Group, stated on their Telegram information page that Tajin Group is always looking for first-hand channels for UnionPay, Visa, Mastercard, JCB, and Apple Pay. In this context, "first-hand channel" refers to compromised payment cards stolen by another threat actor that have yet to be sold to another threat actor. This means that Tajin Group is looking to work with professional hackers or database brokers who can obtain payment card details and may also possess proprietary knowledge to exploit Apple Pay.

@tjjt66 stated that Tajin Group is open to discussing various setups, including self-hosted online stores using 3D and 2D payment gateways. A 2D gateway processes a transaction only involving the conventional card-not-present (CNP) e-commerce authorization layer. Meanwhile, a 3D gateway employs the 3D Secure protocol (3DS), which adds an authentication layer to the conventional authorization layer of CNP e-commerce transactions. 3DS facilitates the transfer of a richer set of data that allows the issuer (banks) to attempt to authenticate the cardholder. This is done either through the richer data itself or, if doubt remains, step-up authentication that requires the customer to complete an extra authentication step, such as a one-time password (OTP), biometric confirmation, or approval through their banking app, which makes it more difficult for threat actors such as Tajin Group to complete unauthorized transactions.

Tajin Group claims to have professional operators available and is capable of handling high volumes of transactions. The threat group also promised compensation to their customers for any downtime and will only accept serious inquiries (potential customers must be able to post an unspecified security deposit). The Telegram biography page also states that if @tjjt66 does not respond on time, the customer should initiate a voice call to the phone number +888 0353 0246, which is a collectible phone number that Tajin Group acquired for 1,899 Toncoins ($3,053.52) on Fragment Market on December 18, 2025. This collectible number can be used to create a Telegram account that is not tied to any SIM card. More information regarding the transaction details of this anonymous phone number can be found on the Fragment website.

We note that, unlike typical Chinese-speaking threat groups, which prefer to buy burner SIM cards in bulk from other threat groups or mules to conduct fraud or scam-related operations, Tajin Group is paying a relatively large sum for anonymous phone numbers via Fragment Market for OPSEC reasons. In most countries, the purchase of SIM cards typically involves at least some form of official documentation, such as passports, driving licenses, and identity cards, which include real names and identities that serve as investigation starting points. By purchasing anonymous phone numbers through Fragment Market, Tajin Group is masquerading its activities, making it harder for law enforcement agencies to identify its operators.

Additionally, Telegram usernames @jingwaikakou, @tjjtyw, and @tjjt_yewu were also purchased by Tajin Group on Fragment Market, with the usernames leading back to the threat actor when searched on Telegram.

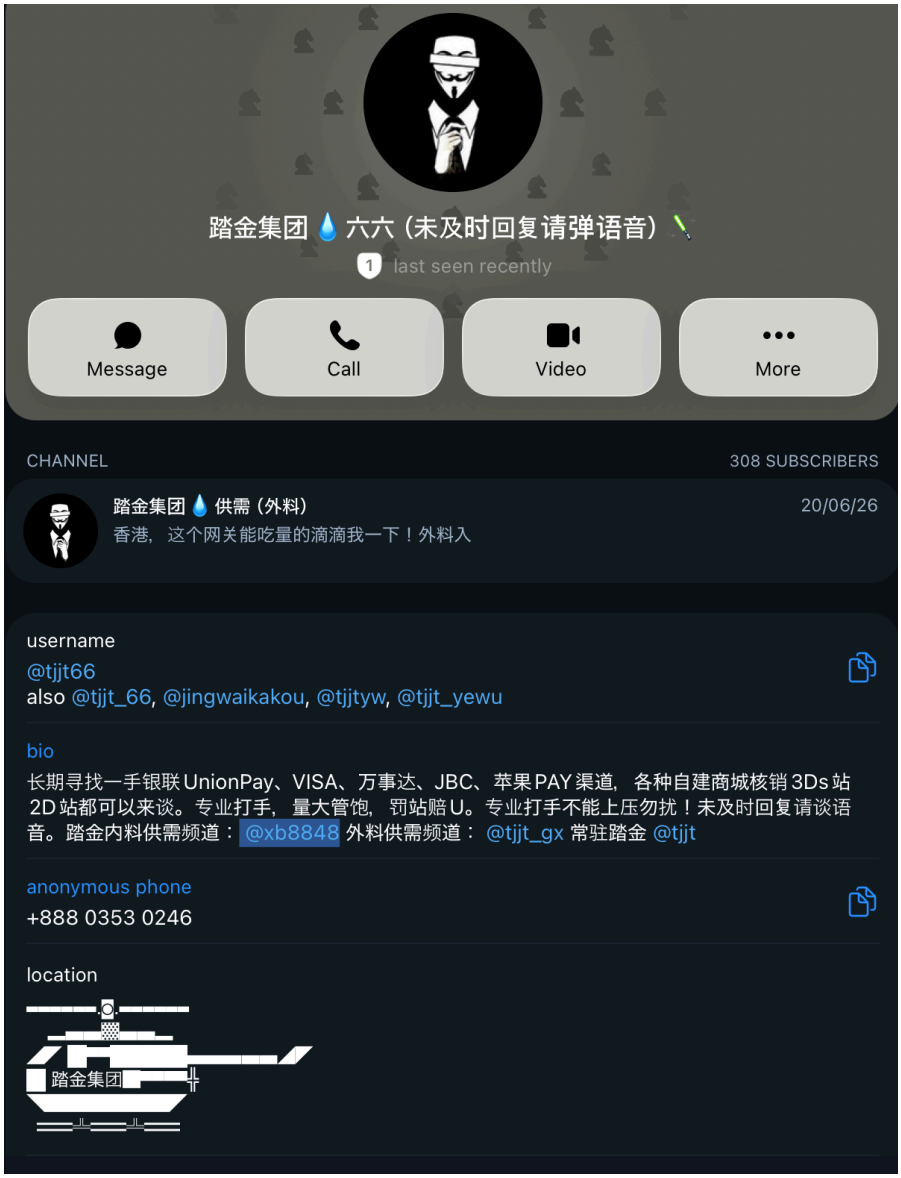

Figure 6: *@tjjt66's Telegram biography page (Source: Telegram)*

Insikt Group identified a Tajin Group announcement posted on April 16, 2026, on its Xinbi Guarantee-linked Telegram channel @xb8848 about six major updates and developments concerning the threat group's activities. The updates (translated in **Table 1**, with the original post in **Figure 7**) highlight the operational challenges the group faced and the intense competition among Chinese-speaking threat groups involved in carding, financial crime, and money laundering that forced Tajin Group to undergo changes.

Point	Announcement
1	Tajin Group will no longer accept overseas card-processing orders from industry peers (primarily due to recent strict overseas restrictions and conflicts between many channels and overseas operations). Tajin Group is also unable to verify the prior use history of the payment cards. **Insikt Group Analysis:** This section highlights the operational challenges Tajin Group previously faced, likely stemming from stricter banking regulations and competition from rivals. Tajin Group also noted that it was unable to verify the prior use history of the payment cards, which suggests that the threat actors who supplied the stolen payment card information are not reliable.
2	Comprehensive withdrawal channels provided for customer; main channels include: 1. Large-amount overnight hold ICBC & Lanzhou: no PIN/password required; others: physical card + withdrawal required; Agricultural Bank & Rural Credit Cooperatives not accepted). 2. Overseas card cash out (limit: 50,000 RMB ($7,382.26) per QR code scan; ICBC & Lanzhou: no PIN/password required; others: physical card + withdrawal required; Agricultural Bank & Rural Credit Cooperatives not accepted). 3. AI Card Transfer: Supports CCB, ABC, Rural Credit Cooperatives, Rural Commercial Banks, and local/village banks; physical card + withdrawal required for all except CCB. 4. ICBC E-Payment: ICBC savings card has a withdrawal limit of 10,000 RMB ($1,476.45); ICBC credit card allows the maximum withdrawal up to the card limit (no CVV required for credit cards). 5. High-speed rail station card swipe/debit. 6. 24-hour card-to-USDT conversion service. **Note:** ICBC: Industrial and Commercial Bank of China (*icbc.com[.]cn*) Lanzhou: Bank of Lanzhou (*lzbank[.]com*) ABC/Agricultural Bank: Agricultural Bank of China (*abchina[.]com*) CCB: China Construction Bank (*ccb[.]com*) Rural Credit Cooperatives: a cooperative or credit union sanctioned by the People's Bank of China to provide credit in the rural areas of China. Rural Commercial Banks: China's Rural Commercial Banks (RCBs) are regional financial institutions primarily formed through the restructuring of local Rural Credit Cooperatives.

Point	Announcement
	There are currently over 1,500 of these institutions operating nationwide, serving local agriculture, small businesses, and individuals. AI Card Transfer: Insikt Group believes this term likely refers to AI-themed payment cards being rolled out in large numbers in China. These cards offer benefits such as AI token credits, cloud computing services, AI memberships, and developer-focused awards. For more information, please refer to this page. **Insikt Group Analysis:** This section showcases that Tajin Group conducted many tests to conduct financial theft by abusing stolen payment card information belonging to Chinese banks. They have a clear understanding of cash-out limits, and whether the payment card PIN, CVV, and physical card are required. The mention of physical payment cards in this section also indicates that Tajin Group is involved in purchasing physical payment cards that are obtained through unspecified and illegal means.
3	Primary Cash-Out Methods: 1. If a "fish" card (target account) is found to have funds, first check if the target holds accounts with ICBC or Lanzhou Bank. If they do, funds can be transferred remotely to the ICBC card without requiring the PIN for overseas transfers; large amounts can be held overnight. 2. If the target holds an account with the Bank of China (BOC) but the PIN is unknown, funds can be remotely moved to a BOC transfer card. If the PIN is known, the funds can be transferred out directly. For amounts under 200,000 RMB ($29,529.02), the BOC AI system can be used to transfer funds to other cards without requiring an SMS verification code. 3. CCB cards with PINs can be directly used for CCB AI card-swapping services. **Insikt Group Analysis:** This section provides unique insights into how Tajin Group targets mainland Chinese citizens and its understanding of the prerequisites and fund transfer thresholds required to transfer funds overseas or use other payment cards remotely. Tajin Group also mentioned the use of AI systems belonging to the BOC and China Construction Bank to conduct card-swapping to steal funds from victims.
4	Regarding "Overnight Cards": 1. Going forward, do not submit any "**overnight cards**" that do not support transfers/forwarding. 2. Recently, many ICBC card BINs have had overseas transaction capabilities disabled; small-amount test withdrawals are performed during the control-bypass process - please notify us in advance in the event that withdrawals fail. 3. Please also notify us in advance if the card has been used via other channels; otherwise,

Point	Announcement
	any funds successfully withdrawn during the control-bypass process will not be credited to the account. 4. Once the control-bypass process is complete, do not arbitrarily use the card on other channels; you are solely responsible for any issues where funds cannot be withdrawn as an "overnight" transaction due to such actions. 5. Please declare in advance if funds are being moved via "Cloud Transfer" (Yun Nuo Qian) or if the card has been used for other operations. 6. For cards being brought over from other control-bypass providers: we will attempt only one transaction; if it goes through, great - if not, please look elsewhere. 7. Additionally, a new "password-free" limit has recently been introduced for transit-related transactions; the daily spending limit for transit is capped at 50,000 RMB ($7,382.26). **Note:** “Notify us”: notify Tajin Group “Other channels”: Typically refers to transfer and withdrawal services provided by other threat actors “Overnight Card”: Typically refers to extremely time-sensitive user data, such as online shopping order details, personal private information, and payment card information **Insikt Group Analysis:** This section highlights the operational challenges Tajin Group faced and its commitment to providing reliable fund transfer and withdrawal services without overpromising its customers. This section also showcases that Tajin Group is skeptical of stolen payment card details bought from other threat actors, and wants its clients to be upfront about whether the cards have been tried and tested on other channels.
5	Comprehensive customer support - cloud-based fund transfers, exclusive card and balance checks, exclusive retrieval of full card details (including expiry dates), and a free Telegram account. **Insikt Group Analysis:** This section highlights Tajin Group’s commitment to its customers by offering services that include most, if not all, details of stolen payment card information. Tajin Group will assist its clients (other threat actors) to shift funds that are misappropriated or stolen from victims using cloud deduction (云扣) or cloud services (云服务) methods. Cloud deduction/services typically refers to victims who suffered online fraud, such as unauthorized charges caused by malware and phishing pages.
6	Our team has currently opened external distribution channels for external projects; operators managing "sync panels," overseas remote control services, or conference call

Point	Announcement
	platforms are welcome to connect with us! Currently supported countries and regions include: the Philippines, Sri Lanka, Vietnam, South Africa, Colombia, the UK, Switzerland, Canada, Germany, Türkiye, Denmark, Greece, Taiwan, Chile, Ireland, Ecuador, Kenya, Portugal, Sweden, Romania, Mexico, Estonia, Ukraine, Morocco, Peru, Cyprus, Botswana, El Salvador, the Czech Republic, Mauritius, Ghana, Puerto Rico, Mozambique, Guatemala, and others. **Note:** “Overseas remote control services”: Refers to stealing data and payment card information remotely, likely through malware or social engineering tactics “Sync panels”: Refers to schemes involving stealing sensitive information through cloud-based storage platforms such as OneDrive and Dropbox “Conference call platforms”: Refers to hackers exploiting employees' trust in "meeting materials," "meeting notifications," or "corporate cloud storage" to gain an entry point for planting trojan horses or stealing sensitive information **Insikt Group Analysis:** This section highlights that Tajin Group desires to cooperate with threat groups that have been involved in card-related fraud.

Table 1: *Translation of Figure 7 (Source: Telegram)*

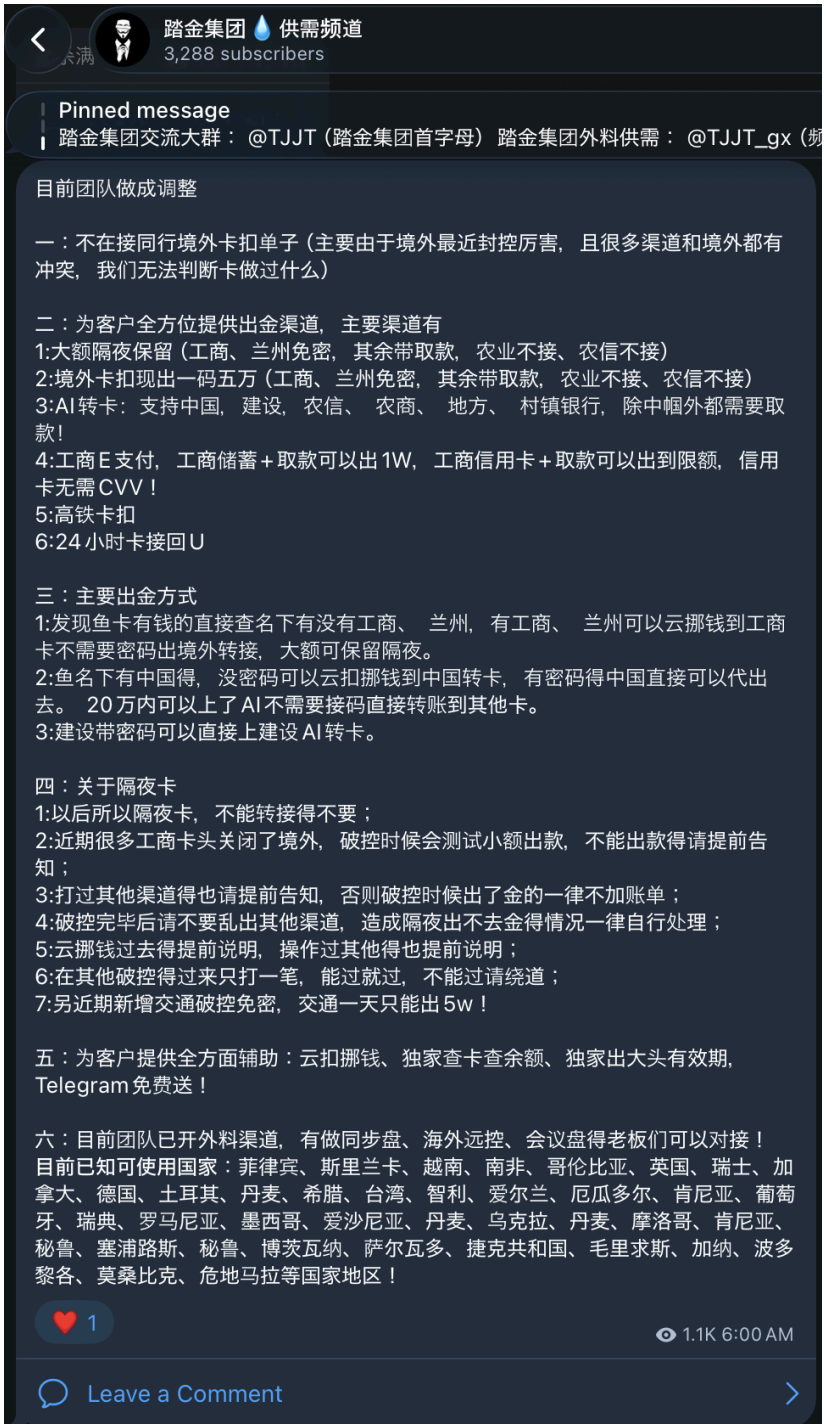

Figure 7: *Tajin Guarantee's April 16, 2026, announcement including their latest update and developments (Source: Telegram)*

Financial Theft and Money Laundering Avenues

Tajin Group's money laundering service Telegram channel @tjjt_gx 踏金集团💧供需(外料) has 290 subscribers as of writing. The channel advertises multiple methods to launder money, including three payment gateway systems: CCAvenue UAE, gift cards, and Paypage.

CCAvenue UAE

CCavenue UAE (*ccavenue[.]ae*) is the UAE branch of CCAvenue, a large and well-established Indian payment gateway and merchant account provider in the Middle East. It enables businesses to accept payments across websites, apps, phones, and social media. The payment links advertised by Tajin Group are unique payment links its customers can use to make payments. Tajin Group operates two such merchants on CCAvenue and will generate unique payment links for other threat actors to input stolen payment card information. The generated unique payment links follow the format *hxxps://payae[.]cc/* (unique characters) and will redirect customers to their merchant page. The following two unique links lead us to discovering two merchant accounts Tajin Group operates on CCAvenue:

- *hxxps://payae[.]cc/QTTb209*: Visiting this URL led us to a link belonging to CCAvenue (*ccavenue[.]ae*), and a CCAvenue merchant account named MOON ENTERPRISE TRADING LLC is listed as the merchant. See **Figure 9** for more information.
- *hxxps://payae[.]cc/Qwpf734*: Visiting this URL led us to a link belonging to CCAvenue (*ccavenue[.]ae*), and a CCAvenue merchant account named SUNWEL ENTERPRISE TRADING LLC is listed as the merchant. See **Figure 15** in **Appendix D** for more information.

A unique order ID is generated each time a user visits the page. Users have the option to input the amount they wish to transfer, and input their mobile number, name, and description. CCAvenue UAE only accepts United Arab Emirates Dirham (AED) for all transactions. After entering all required information, the user has the option to pay by credit card or UnionPay (*unionpayintl[.]com*), a Chinese state-owned financial services corporation headquartered in Shanghai, China.

We did not find any company named MOON ENTERPRISE TRADING LLC or SUNWEL ENTERPRISE TRADING LLC. Instead, we found two registered UAE entities with very similar names:

- MOON TRADING LLC (*moon-pack[.]com*), a Dubai-based firm that specializes in packaging materials and complete packing solutions
- Sunwell Trading Co. LLC, a Dubai-based supplier specializing in industrial hardware, primarily dealing in nuts, bolts, screws, and fasteners; there is no website available, but the business registration information can be found here.

Due to similarities in the names of entities listed on CCAvenue UAE's unique payment pages, it is possible that operators of Tajin Group are impersonating legitimate UAE businesses to mask their money laundering activities.

Tajin's Group's operational instructions for their fraudulent card-processing scheme include guidance on processing stolen or illicitly obtained payment cards. These cards are used to make transfer payments through the CCavenue UAE payment gateway in Dubai. The instructions also include which card BIN to avoid to evade detection, transaction limits (likely to stay under fraud monitoring thresholds), and rules for submitting stolen card data. This is consistent with carding fraud and money laundering activity of the type commonly associated with Chinese-language cybercrime networks operating in Southeast Asia and the Middle East. The TTPs are similar to the Chinese-language money laundering group named "Dream of Red Chamber Global Access" (红楼梦全球通道).

All cards from the Middle East, the US, Pakistan, India, Thailand, Hong Kong, Japan, and Egypt are banned. **Table 2** lists countries, the banks operating in those jurisdictions, and their banned BIN prefixes. Tajin Group also mentioned that when new banned BIN prefixes appear, notifications will be sent to the channel immediately. Banned BIN prefixes announced in the channel take effect after 30 minutes; anyone who posts a banned prefix after 30 minutes of the prefix being banned will not receive a response, nor will the prefix be checked.

Country	Bank/Financial Institution Name	Banned BIN Prefixes
Sri Lanka	Hatton National Bank (*hnb[.]lk*)	488910
The Philippines	Bank of China@Manila (*bankofchina.com[.]ph*)	528557
The Philippines	BDO Unibank (*bdo[.]com[.]ph*)	512571 524301 548095
The Philippines	BANCO DE ORO UNIBANK (*bdo[.]com[.]ph*)	418359
South Africa	INVESTEC BANK (*investec[.]com*)	402167
South Africa	Discovery Bank (*discovery[.]co[.]za*)	430938 423240 430864
South Africa	FirstRand Bank (*firstrand[.]co[.]za*)	412752 405769

Country	Bank/Financial Institution Name	Banned BIN Prefixes
		490115 410588 523982 5520578 (Note: This BIN has seven digits instead of the traditional six) 491050 479012 457896 400738
South Africa	Standard Bank (*standardbank[.]co[.]za*)	522250 532657
Vietnam	Vietcombank (*vietcombank[.]com[.]vn*)	438103 452404 546285
Vietnam	Techcombank (*techcombank[.]com*)	510164 483931
Malaysia	United Overseas Bank Malaysia (*uob[.]com[.]my*)	459914 414170
Malaysia	Maybank (*maybank2u[.]com[.]my*)	463225 542124

Country	Bank/Financial Institution Name	Banned BIN Prefixes
United Kingdom	Bank of Scotland (*bankofscotland[.]co[.]uk*)	446291 476223 528683 446278
United Kingdom	Lloyds Bank (*lloydsbank[.]com*)	492181 446274 492182 446272 552157 492182 446259 467062 492182
United Kingdom	TransactPay(*transactpay[.]com*)	430864
United Kingdom	National Westminster Bank (*natwest[.]com*)	537410
Romania	ING Bank Romania (*ing[.]com*)	466286 425603 425602
Romania	CEC Bank (*cec[.]ro*)	424382 423463
Pakistan	JS Bank Pakistan (*jsbl[.]com*)	522545

Country	Bank/Financial Institution Name	Banned BIN Prefixes
Pakistan	Habib Bank (*hbl[.]com*)	490286 490287
Pakistan	Standard Chartered Bank Pakistan (*sc[.]com/pk*)	557572
Pakistan	Allied Bank (*abl[.]com*)	407572
Bangladesh	Bank of East Asia (*hkbea[.]com*)	413401
Bangladesh	Eastern Bank (*ebl[.]com[.]bd*)	423800
Bangladesh	BRAC Bank (*bracbank[.]com*)	528652 548895
Bangladesh	Jamuna Bank (*jamunabankbd[.]com*)	412788
Bangladesh	Mutual Trust Bank (*mutualtrustbank[.]com*)	498851 536310
Czech Republic	MONETA Money Bank (*moneta[.]cz*)	464461 478553
Greece	Piraeus Bank (*piraeusbank[.]gr*)	441029
Belgium	WISE EUROPE SA/NV (*wise[.]com*)	456933

***Table 2**: List of BIN prefix numbers that cannot work with Tajin Group's financial fraud scheme involving CCAvenue UAE (Source: Telegram)*

Known payment cards belonging to countries that can work for the CCAvenue scheme according to Tajin Group include the Philippines, Sri Lanka, Vietnam, South Africa, Colombia, the UK, Switzerland, Canada, Malaysia, Germany, Türkiye, Denmark, Greece, Taiwan, Chile, Ireland, Ecuador, Kenya, Portugal, Sweden, Romania, Mexico, Estonia, Denmark, Ukraine,, Morocco, Kenya,, Cyprus, Peru, Botswana, El Salvador, the Czech Republic, Mauritius, Ghana, Puerto Rico, Mozambique, and Guatemala.

The use of CCavenue UAE is limited to a maximum of two transactions per card. If the same card is used for three transactions, none of the transactions will go through. Screenshots showing proof of

success are valid for 24 hours, and Tajin Group will not check or respond to screenshots older than 24 hours. The countdown starts the moment the screenshot is sent to Tajin Group.

Additionally, customers are advised not to conduct transaction testing for transaction amounts ranging from 100 to 20,000 AED. Tajin Group also encourages its clients to avoid identical amounts for both transactions and advises clients to use random values with decimal points. Based on Tajin Group's recommended transaction amount, Insikt Group assessed that typical transaction amounts would be 1591.93 Dirhams and 17539.19 Dirhams. (Please note that numbers are only for illustration purposes based on Tajin Group's advice.)

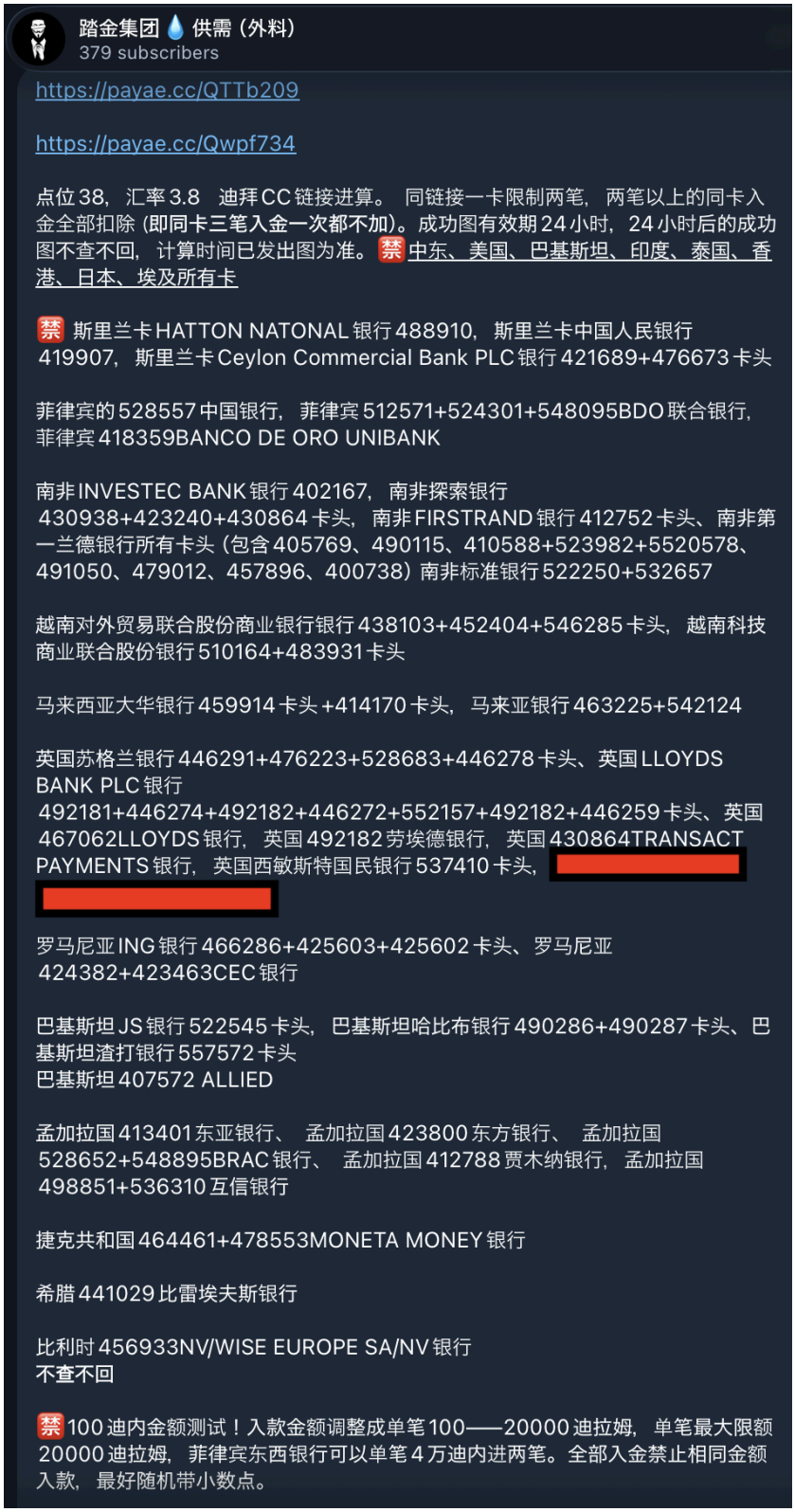

***Figure 8**: CCAvenue UAE unique links are listed in this posting, and the names of multiple banks across multiple countries are also listed (Source: Telegram)*

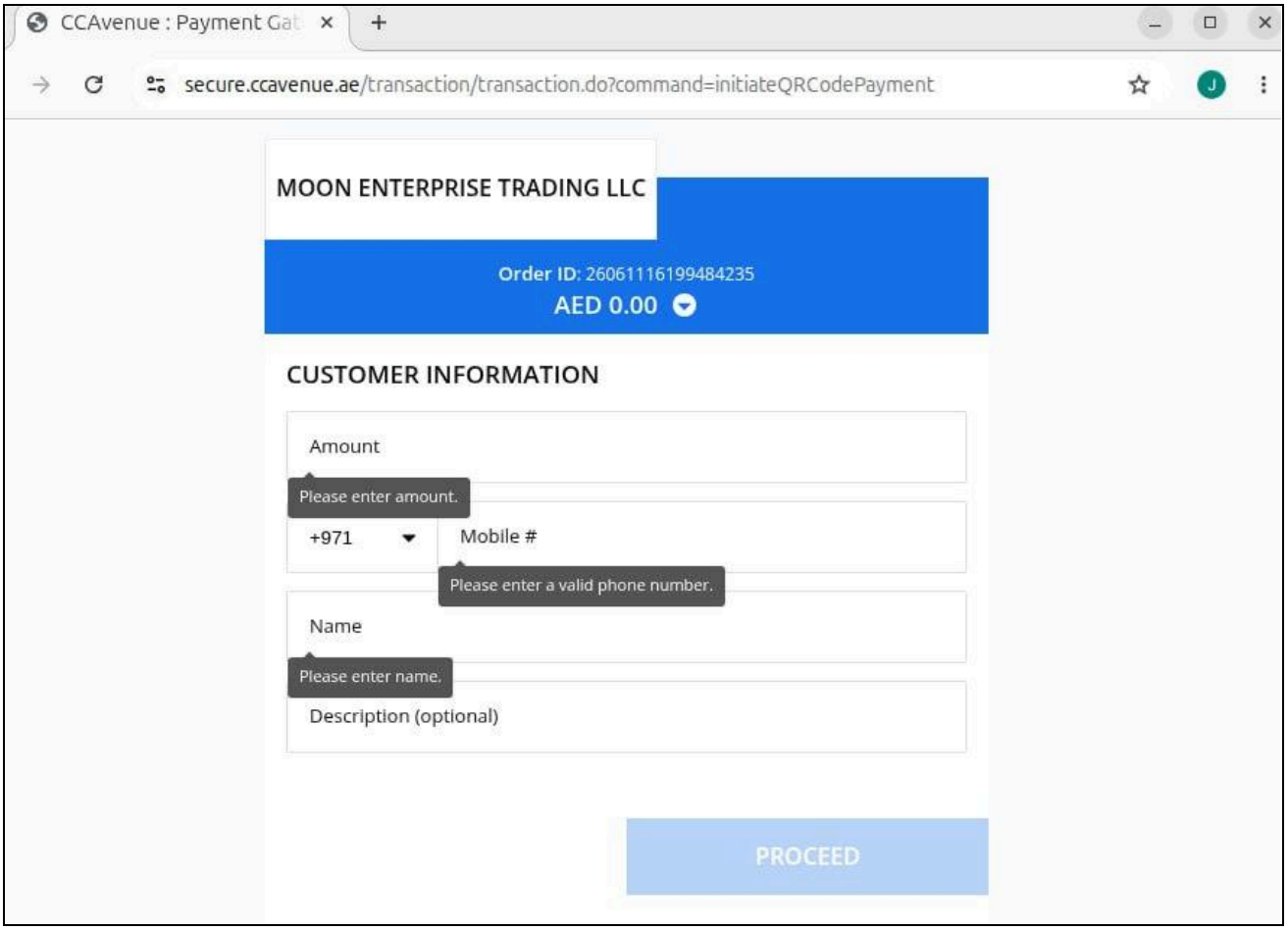

Figure 9: *Visiting the URL payae[.]cc/QTTb209 led us to a link belonging to CCAvenue (ccavenue[.]ae), a company named MOON ENTERPRISE TRADING LLC is listed as the merchant (Source: Recorded Future Proprietary Data)*

Analysis of the BIN Prefixes Banned by Tajin Group

A review of the banned BIN prefixes against Payment Fraud Intelligence BIN Review data (552 card-checker records from November 2023 to July 2026, roughly 405 unique) indicates that the ban list is driven more by 3DS enforcement than by issuer fraud designations. Of the 65 prefixes, 46 appear in the data, with consumer debit and entry-tier products (mostly Visa Classic) dominating. Among 195 observations with a 3DS result, 141 failed authentication, while only 54 processed without 3DS. Authentications typically fail if the issuer detects signs of unauthorized activity or the purchaser fails a step-up challenge (such as an OTP or in-app approval).

Threat actor commentary corroborates this and adds that the prefixes are inconsistent: Many are described as “50/50” on 3DS and as clearing only below issuer step-up thresholds (for example, small-value purchases). This is consistent with Tajin Group’s guidance to avoid amounts of 100 to 20,000 AED and to use small, randomized values, likely to keep charges below issuer authentication triggers.

Tajin Group does not disclose why the BINs on this list are banned; however, Insikt Group assesses that the most likely explanation is that threat actor-initiated unauthorized transactions involving the banned BINs and Tajin Group's CCAvenue UAE merchant accounts are declined at a high rate. A high decline rate, especially if the declines are accompanied by an issuer-side fraud reason code, would expose Tajin Group's merchants to discovery by card networks and acquirers, resulting in merchant account closure. While the fact that the banned BINs are primarily 3DS-enabled debit cards would explain a higher decline rate for unauthorized transactions, it remains unclear why the ban list is limited to only a subset of all 3DS-enabled debit cards.

Financial Theft by Using Geidea UAE, Selfridges, and N-Genius

In addition to CCAvenue, Tajin Group is also making use of the following three other services for their money laundering operations: Geidea UAE (*geidea[.]net*), N-Genius (*network[.]ae*), and Selfridges & Co (*giftcards.selfridges[.]com*). For Geidea, Tajin Group is making use of Geidea's UAE-specific domain. Geidea's UAE payment API environment runs on *api[.]geidea[.]ae*, and their UAE consumer/merchant website address is *geidea[.]net/uae/en*.

The biggest difference between CCAvenue and these three other services is that CCAvenue's unique payment links can be reused and do not expire immediately, whereas threat groups can use CCAvenue's platform to enter large quantities of stolen payment card details. Meanwhile, Geidea and Network International's payment gateway (N-Genius) allow merchants to generate unique and secure payment links via email, SMS, or social media platforms such as WhatsApp, Facebook, and Instagram, without needing an e-commerce website. **Figures 10** and **12** illustrate the unique payment links sent by Tajin Group for their clients to make fund transfers using Geidea and N-Genius.

Company Name and URL	Country of Origin	Unique Payment Link Examples
Geidea (*geidea[.]net*)	Saudi Arabia	*payments.geidea[.]ae/payByLink/SUNWORLDWorkshopEquipmentMachinerySpareParts/l1f-fa8-mn8-uf4*
Network International (*network[.]ae*)	UAE	*paypage.ngenius-payments.com/invoices/invoice/3aeb04ff-8025-451a-9259-5df661503a62/payment*
Selfridges (*giftcards.selfridges[.]com*)	UK	No unique payment link *giftcards[.]selfridges[.]com* is the link that can be used by threat actors to misuse payment cards to purchase electronic gift cards.

***Table 3**: Companies Tajin Group is using for their financial theft and money laundering activities (Source: Telegram)*

In **Figure 10**, Tajin Group mentions that only 3DS payments are accepted for Geidea (Dubai). Verification requires a screenshot of the successful payment plus the four key transaction details (cardholder name, card number, expiry date, and CVV/CVC). There is also a limit of one transaction per card. All payment

cards are from Middle Eastern countries, and digital wallet payment methods are prohibited. Additionally, Tajin Group posted unique payment links and instructed their customers to send a certain amount of AED for each unique Geidea payment URL. For example, for the unique Geidea payment link (see **Table 3**), the client is supposed to send 1467.9 AED ($399.70).

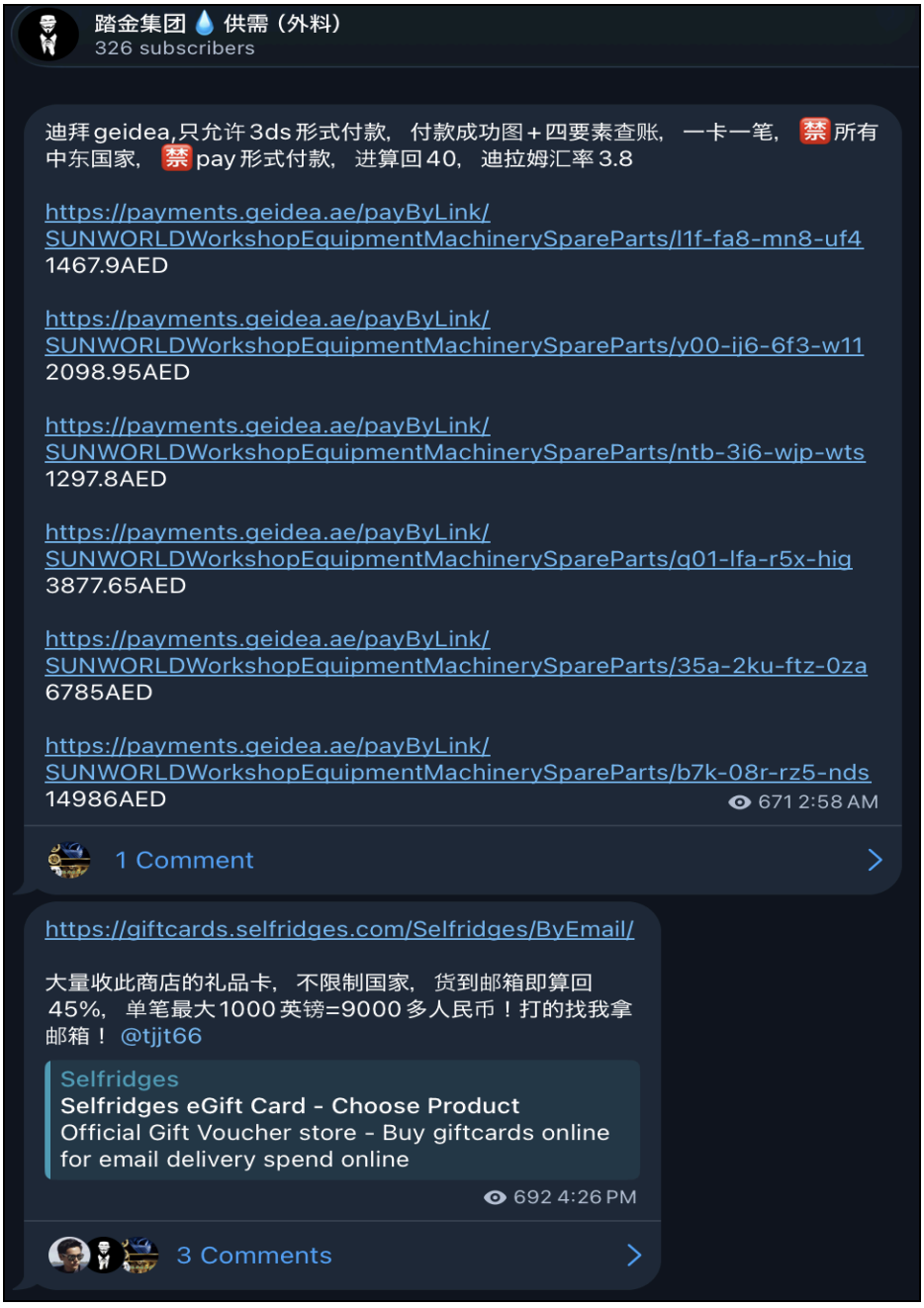

Figure 10: *Unique payment links belonging to Geidea, and the official Selfridges URL to launder money (Source: Telegram)*

In **Figure 10,** Tajin Group announces it is buying large quantities of Selfridges gift cards. It claims there are no country restrictions, meaning payment cards from any country can be used to purchase the gift cards. The administrator announced that the seller will get a 45% payout as soon as the cards arrive in

Tajin Group's email inbox. The maximum single transaction is £1,000 ($1,337.38), and the seller must contact the private Telegram handle @tjjt66 to get the email address. **Figure 11** demonstrates that Selfridges allows individuals to send eGift cards to others immediately. Upon attempting a checkout, we found that payment options include Visa, Mastercard, American Express, Maestro, and Google Pay.

It is very likely that Tajin Group is working with other Chinese-speaking criminals who use stolen payment card information to purchase Selfridges eGift cards and then send them directly to email addresses provided by Tajin Group. As Tajin Group only pays a 45% share to the sellers, we assess that Tajin Group can resell the gift cards to other criminal groups to make a profit, highlighting that Chinese-speaking criminals are also making use of traditional methods such as committing fraud and laundering money through gift cards, which have been used by other threat actors for decades to cash out illegal proceeds.

In January 2025, Yahoo News reported that there were 198 cases of fraud escalated to the UK's scams reporting service, with losses amounting to £2.8m ($3.743 million). The article reported that fraudsters stole a victim's ICBC credit card and spent £7,130 ($9,531.56) across four transactions in 15 minutes. The same article also stated that, unlike most UK credit cards, many Chinese cards can be verified with a signature rather than a PIN; the victim also mentioned that Chinese credit cards are "really easy to use," as there is no PIN. Similarly, the first row in **Table 1** shows Tajin Group mentioning that no PIN/password is required for ICBC cards, and that the overseas card cash-out limit is 50,000 RMB ($7,382.26). The information provided in the case study strongly corroborates Tajin Group's announcement, and we assessed that Tajin Group is knowledgeable about the Chinese banking industry. The victim's unauthorized transaction of approximately $9,531.56 is close to Tajin Group's overseas cash-out limit of $7,382.26. We assess that Tajin Group believes that unauthorized transactions of 50,000 RMB ($7,382.26) are likely to be processed successfully rather than flagged by ICBC's fraud detection systems.

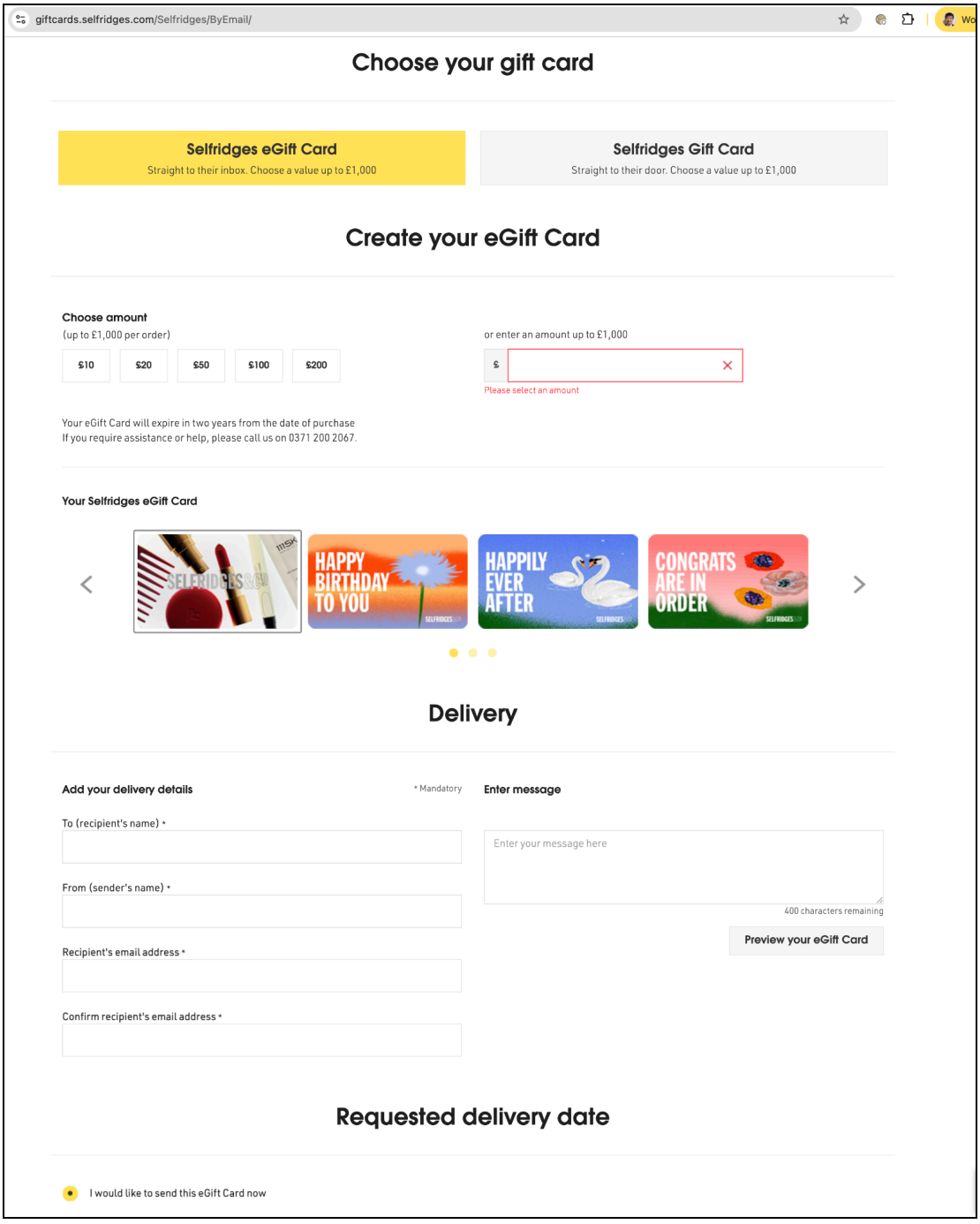

Figure 11: *Selfridges allows individuals to send eGift cards to other individuals (Source: Selfridges)*

Figure 12 shows Tajin Group mentioned that clients should only use UnionPay on the N-Genius platform, deposit the specified amount to activate the payment link, and bypass the fraud detection mechanism by using small-sum transactions. Insikt Group noted that apart from UnionPay, N-Genius supports a wide number of payment methods.

Tajin Group typically includes a specific amount in Dirhams to be sent for each unique payment link it generates. For example, in **Figure 12**, the unique payment link is supposed to be used to send 49 AED ($13.34).

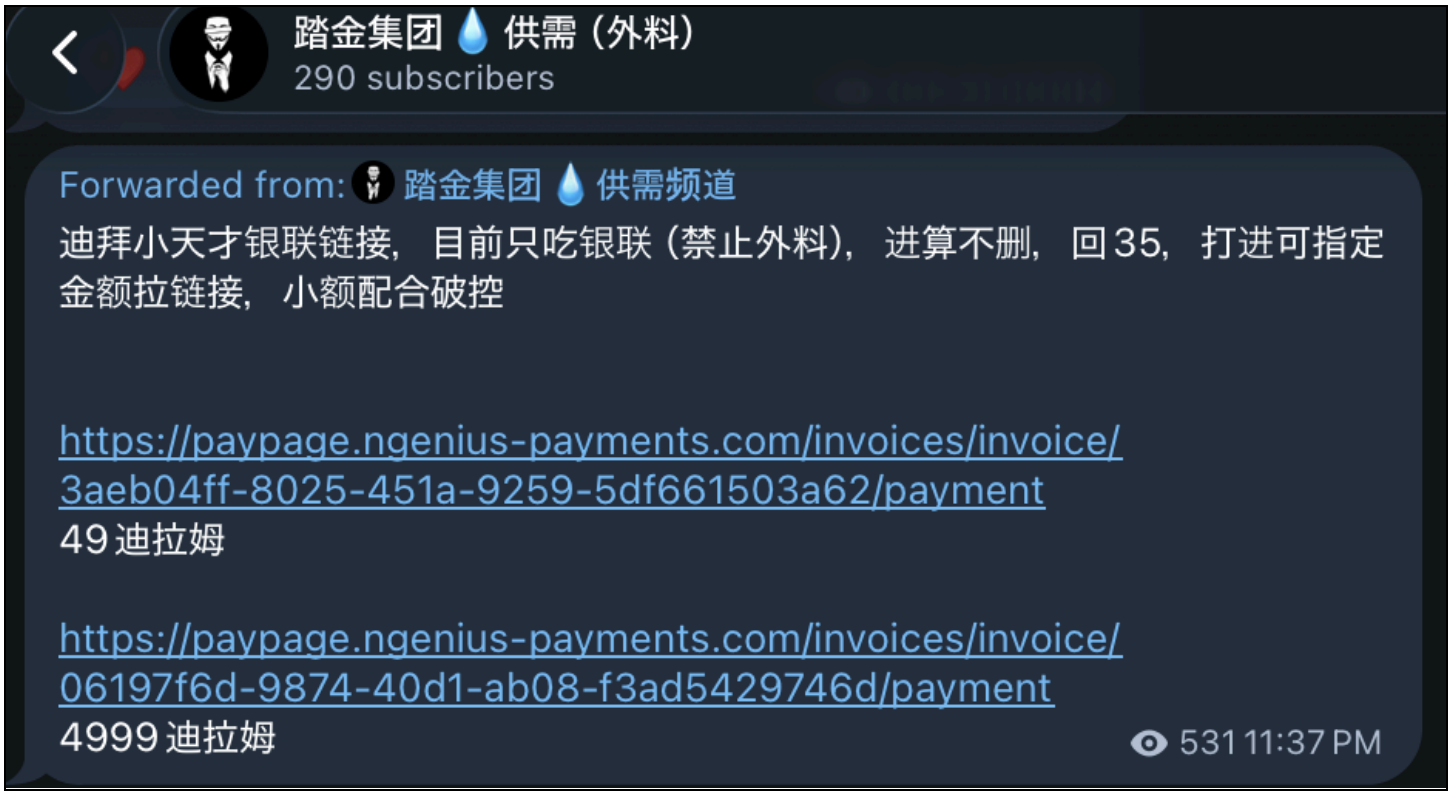

Figure 12: *Unique payment links sent by Tajin Group (using N-Genius) to launder money (Source: Telegram)*

Figure 13 shows Tajin Group congratulating clients who successfully deposited (transferred) Dirhams. The first customer deposited 4,888.88 AED ($1331.21), and the second customer deposited 50,000 RMB ($7,389.84). Tajin Group also claimed that the second customer successfully deposited the funds into a bank account belonging to the Agricultural Bank of China. The screenshots show successful transactions involving Dirhams and a private Telegram chat channel with 21 members, in which their customer monikers have been censored by Tajin Group's administrators to preserve their anonymity. Such screenshots prove that Tajin Group does create multiple private Telegram chat rooms to facilitate fund transfer services for their customers.

***Figure 13**: Screenshot showing Tajin Group's Telegram administrator congratulating two anonymous customers for successfully depositing 4,888.88 AED ($1331.21) and 50,000 RMB ($7,389.84) (Source: Telegram)*

Skimming and Unauthorized Transactions Involving China Eastern Airlines and Hong Kong Jewelry Business

Figure 14 showcases five screenshots posted by Tajin Group showing transaction records of Chinese payment cards belonging to Postal Savings Bank of China, China Construction Bank (CCB), and ICBC

that were allegedly used to make payments to Chow Tai Fook Jewellery Hong Kong (*chowtaifook[.]com*), a Hong Kong-based jewelry business.

Tajin Group mentioned that this is an airline ticket card-skimming scheme that is guaranteed to work. The scheme requires the victim to cooperate with a facial scan, and Tajin Group is willing to provide guidance to people interested in participating. There are two key sets of instructions:

1. Instruct the victim to download the China Eastern Airlines application, register an account using the victim's phone number, and complete the facial scan and real-name verification. Next, bind a payment card with money to the account, and set the payment password to 147258.
2. Send the SMS verification code to log in to the account, and inform Tajin Group about the card balance.

Insikt Group is unable to confirm whether the China Eastern Airlines application mentioned by the threat group is the official application owned by the legitimate China Eastern Airlines or whether it is a fake application that is designed by Tajin Group to steal card payment information belonging to victims. It is also possible that the China Eastern Airlines application could be real, and Tajin Group's scheme involves binding payment cards to the China Eastern Airlines account to check the payment card's remaining credit balance, which will provide Tajin Group with the exact information they need for their next step — using the stolen cards to make payment for jewelry.

However, the screenshots showcasing payments using stolen card payment information to Chow Tai Fook Jewellery Hong Kong show that this is likely Tajin Group's method to cash out by purchasing high-value items such as jewelry, which are also small in size, easy to transport, and have considerable resale value. Chow Tai Fook provides official documentation for its jewelry, including physical certificates of authenticity, third-party lab grading reports like GIA, and digital blockchain-backed certificates for specific lines like T Mark diamonds.

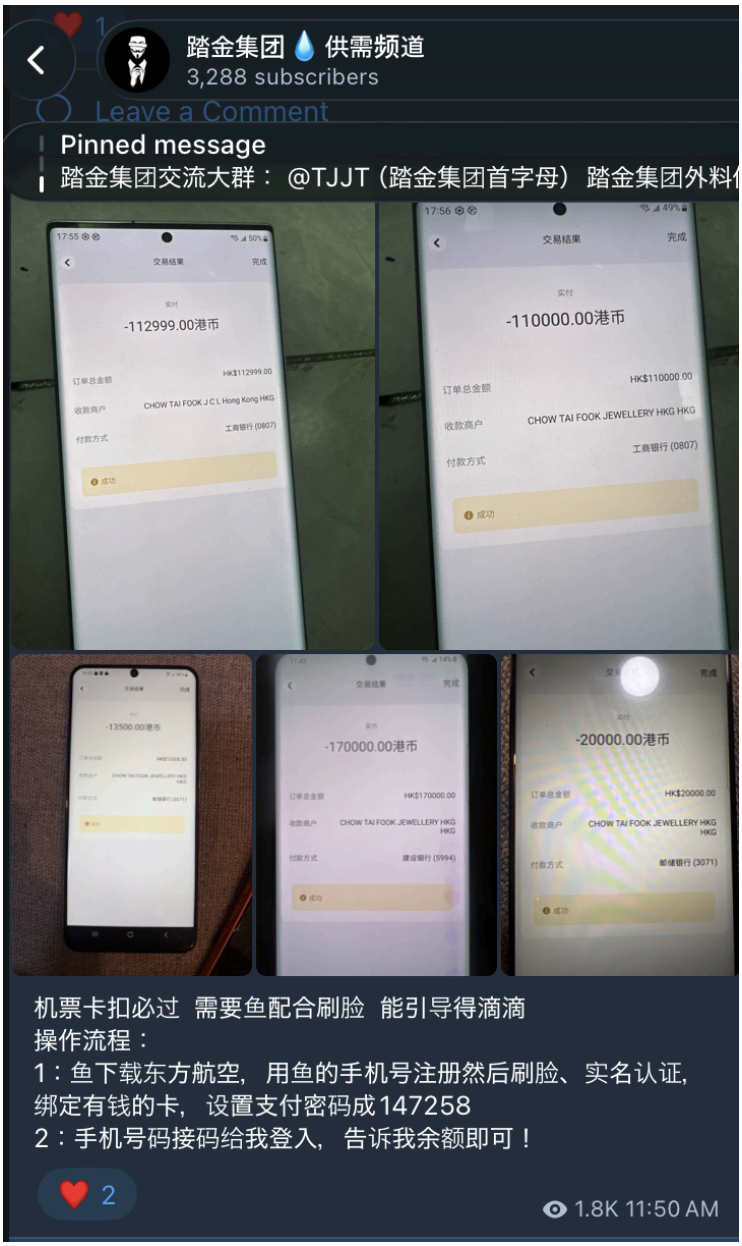

Figure 14: *Screenshots posted by Tajin Group showcasing them conducting unauthorized payments to Chow Tai Fook Jewellery Hong Kong using Hong Kong dollars (Source: Telegram)*

Outlook

As Chinese-language guarantee marketplaces continue to grow in popularity, third-party vendors such as Tajin Group will likely continue to adapt and evolve in ways that strengthen their OPSEC. Having more guarantee marketplaces would also give them greater flexibility to move to another guarantee marketplace and negotiate better terms, such as revenue sharing with guarantee marketplace operators. More options would mean increased competition, forcing operators of guarantee marketplaces to constantly innovate, improve customer satisfaction, and reliability to retain third-party

vendors, some of which may grow large enough, like Tajin Group, to become a seasoned and reliable vendor to attract more threat groups to operate under a guarantee marketplace's ecosystem.

There is always the risk of guarantee marketplaces being sanctioned and shutting down operations abruptly, such as in the case of Huione Guarantee being shut down in mid-2025, where existing third-party vendors that once operated on Huione Guarantee had to pivot to other dark web marketplaces and Telegram-based guarantee marketplaces to continue operations. And just as Tajin Group switched from Dabai Guarantee to Xinbi Guarantee, other third-party vendors will likely do the same to promote their services. We also note that Xinbi Guarantee was sanctioned by the UK government in March 2026, and should they disband, Tajin Group will likely move to another guarantee marketplace. We assessed that Tajin Group is currently focused on building its own brand name and reputation within the Chinese cybercriminal space and aims to reduce reliance on guarantee marketplaces. From the activities we observed, Tajin Group also appears to be dealing with customers directly as much as possible to avoid unspecified middleman fees and regulations imposed by the administrators of guarantee marketplaces.

Fragment Market is likely going to become increasingly popular among Chinese-speaking criminal groups, and we assess that operators of Chinese-language guarantee groups and third-party vendors will purchase more anonymous phone numbers and Telegram monikers using cryptocurrencies or cash. The ease of swapping major cryptocurrencies for Toncoins will also simplify the process and complicate tracking by law enforcement and security researchers. More Telegram monikers created by Chinese-speaking threat actors without real SIM cards will likely result in more opportunities for new attack vectors and scam operations.

As observed from Tajin Group's April 16, 2026 announcement (detailed in **Table 1**), Tajin Group has faced operational challenges due to evolving security protocols and competition from other threat groups offering similar services. Trust issues remain prevalent within the Chinese cybercrime ecosystem, and Tajin Group will likely have to break off existing partnerships that do not work well for them. Tajin Group is likely to continue exploring new exploitation methods and introducing new avenues to launder funds, similar to CCAvenue, Geidea, N-Genius, and Selfridges eGift card services, for existing and future customers, and to facilitate illicit transactions using stolen payment card information.

Lastly, Tajin Group will likely continue to find cash-out methods by obtaining physical goods that are high in value and easy to transport within and beyond borders, which is the reason why their scheme involved jewelry retailers like Chow Tai Fook Jewellery Hong Kong. We assess that Tajin Group will likely coordinate with other Chinese-speaking groups using the Chinese-language guarantee marketplaces to conduct such campaigns across many countries, in a manner similar to retail fraud campaigns involving ghost-tapping techniques that we covered in "Evolution of Chinese-Language Guarantee Telegram Marketplace."

Appendix A: List of Mandarin Terminologies and Translation

Chinese Term	English Term	Context
一手	First hand	Refers to compromised payment cards or databases that are breached by the threat actor, usually by compromising the internal network system of entities, if the stolen payment card information or database has never been sold to another threat actor.
专业打手	Professional enforcer	Someone who makes sure that operations are carried out smoothly. They can include malware developers, individuals proficient at creating phishing pages, pentesters, and more.
迪拉姆	Dirham	The Emirati Dirham is the official currency of the UAE, one of the main currencies exploited by Tajin Group to conduct money laundering and other financial crimes.
连刷	Continuously swipe	Refers to threat actors using Tajin Group's online payment portals to "swipe cards," likely involving stolen payment card credentials.
隔夜卡	Overnight card	Typically refers to extremely time-sensitive user data, such as online shopping order details, personal private information, and payment card information.
云扣挪钱	Cloud-based fund transfers	Tajin Group will assist their clients (other threat actors) in shifting misappropriated or stolen funds from victims using cloud deduction (云扣) or cloud service (云服务) methods. Cloud deduction/services typically refers to victims of online fraud, such as unauthorized charges caused by malware and phishing pages.
破控	Break control	Bypassing risk controls or the banks' transfer security protocols.
小额出款	Withdrawing small amounts	Usually conducted by Chinese threat groups to test withdrawal limits and whether their transaction attempts will be stopped or flagged by the financial institutions.
卡头	Card BIN	BIN of payment card details stolen by other threat actors.

Appendix B: Tajin Group's April 16, 2026, Announcement in Mandarin

目前团队做成调整
一:不在接同行境外卡扣单子(主要由于境外最近封控厉害,且很多渠道和境外都有冲突,我们无法判断卡做过什么)
二:为客户全方位提供出金渠道,主要渠道有
1:大额隔夜保留(工商、兰州免密,其余带取款,农业不接、农信不接)
2:境外卡扣现出一码五万(工商、兰州免密,其余带取款,农业不接、农信不接)
3:AI转卡:支持中国,建设,农信、农商、地方、村镇银行,除中帼外都需要取款!
4:工商E支付,工商储蓄+取款可以出1W,工商信用卡+取款可以出到限额,信用卡无需CVV!
5:高铁卡扣
6:24小时卡接回U
三:主要出金方式
1:发现鱼卡有钱的直接查名下有没有工商、兰州,有工商、兰州可以云挪钱到工商卡不需要密码出境外转接,大额可保留隔夜。
2:鱼名下有中国得,没密码可以云扣挪钱到中国转卡,有密码得中国直接可以代出去。20万内可以上了AI不需要接码直接转账到其他卡。
3:建设带密码可以直接上建设AI转卡。
四:关于隔夜卡
1:以后所以隔夜卡,不能转接得不要;
2:近期很多工商卡头关闭了境外,破控时候会测试小额出款,不能出款得请提前告知;
3:打过其他渠道得也请提前告知,否则破控时候出了金的一律不加账单;
4:破控完毕后请不要乱出其他渠道,造成隔夜出不去金得情况一律自行处理;
5:云挪钱过去得提前说明,操作过其他得也提前说明;
6:在其他破控得过来只打一笔,能过就过,不能过请绕道;
7:另近期新增交通破控免密,交通一天只能出5w!
五:为客户提供全方面辅助:云扣挪钱、独家查卡查余额、独家出大头有效期,Telegram免费送!
六:目前团队已开外料渠道,有做同步盘、海外远控、会议盘得老板们可以对接!
目前已知可使用国家:菲律宾、斯里兰卡、越南、南非、哥伦比亚、英国、瑞士、加拿大、德国、土耳其、丹麦、希腊、台湾、智利、爱尔兰、厄瓜多尔、肯尼亚、葡萄牙、瑞典、罗马尼亚、墨西哥、爱沙尼亚、丹麦、乌克拉、丹麦、摩洛哥、肯尼亚、秘鲁、塞浦路斯、秘鲁、博茨瓦纳、萨尔瓦多、捷克共和国、毛里求斯、加纳、波多黎各、莫桑比克、危地马拉等国家地区!

Appendix C: Tajin Group's List of BINs Belonging to Several Banks Shown in Figure 8

hxxps://payae[.]cc/QTTb209
hxxps://payae[.]cc/Qwpf734

点位38，汇率3.8　迪拜CC链接进算。同链接一卡限制两笔，两笔以上的同卡入金全部扣除（即同卡三笔入金一次都不加）。成功图有效期24小时，24小时后的成功图不查不回，计算时间已发出图为准。禁中东、美国、巴基斯坦、印度、泰国、香港、日本、埃及所有卡
禁 斯里兰卡HATTON NATONAL银行488910，斯里兰卡中国人民银行419907，斯里兰卡Ceylon Commercial Bank PLC银行421689+476673卡头
菲律宾的528557中国银行，菲律宾512571+524301+548095BDO联合银行，菲律宾418359BANCO DE ORO UNIBANK
南非INVESTEC BANK银行402167，南非探索银行430938+423240+430864卡头，南非FIRSTRAND银行412752卡头、南非第一兰德银行所有卡头（包含405769、490115、410588+523982+5520578、491050、479012、457896、400738）南非标准银行522250+532657
越南对外贸易联合股份商业银行银行438103+452404+546285卡头，越南科技商业联合股份银行510164+483931卡头
马来西亚大华银行459914卡头+414170卡头，马来亚银行463225+542124
英国苏格兰银行446291+476223+528683+446278卡头、英国LLOYDS BANK PLC银行492181+446274+492182+446272+552157+492182+446259卡头、英国467062LLOYDS银行，英国492182劳埃德银行，英国430864TRANSACT PAYMENTS银行，英国西敏斯特国民银行537410卡头，英国罗马尼亚ING银行466286+425603+425602卡头、罗马尼亚424382+423463CEC银行
巴基斯坦JS银行522545卡头，巴基斯坦哈比布银行490286+490287卡头、巴基斯坦渣打银行557572卡头巴基斯坦407572 ALLIED
孟加拉国413401东亚银行、孟加拉国423800东方银行、孟加拉国528652+548895BRAC银行、孟加拉国412788贾木纳银行，孟加拉国498851+536310互信银行
捷克共和国464461+478553MONETA MONEY银行
希腊441029比雷埃夫斯银行
比利时456933NV/WISE EUROPE SA/NV银行

不查不回
禁100迪内金额测试！入款金额调整成单笔100——20000迪拉姆，单笔最大限额20000迪拉姆，菲律宾东西银行可以单笔4万迪内进两笔。全部入金禁止相同金额入款，最好随机带小数点。
目前已知可使用国家：菲律宾、斯里兰卡、越南、南非、哥伦比亚、英国、瑞士、加拿大、马来西亚、德国、土耳其、丹麦、希腊、台湾、智利、爱尔兰、厄瓜多尔、肯尼亚、葡萄牙、瑞典、罗马尼亚、墨西哥、爱沙尼亚、丹麦、乌克拉、丹麦、摩洛哥、肯尼亚、秘鲁、塞浦路斯、秘鲁、博茨瓦纳、萨尔瓦多、捷克共和国、毛里求斯、加纳、波多黎各、莫桑比克、危地马拉
群内图+卡信息，格式整理工整，卡号之间不要有空格，禁止出现给假卡号现象。对接请关注踏金外料供需频道@tjjt_gx 出现新禁止卡头会第一时间发频道通知，频道发出禁止卡头已30分钟为准，30分后的禁止卡头一律不查不回！

Appendix D: Tajin Group's Financial Theft Scheme Involving CCAvenue

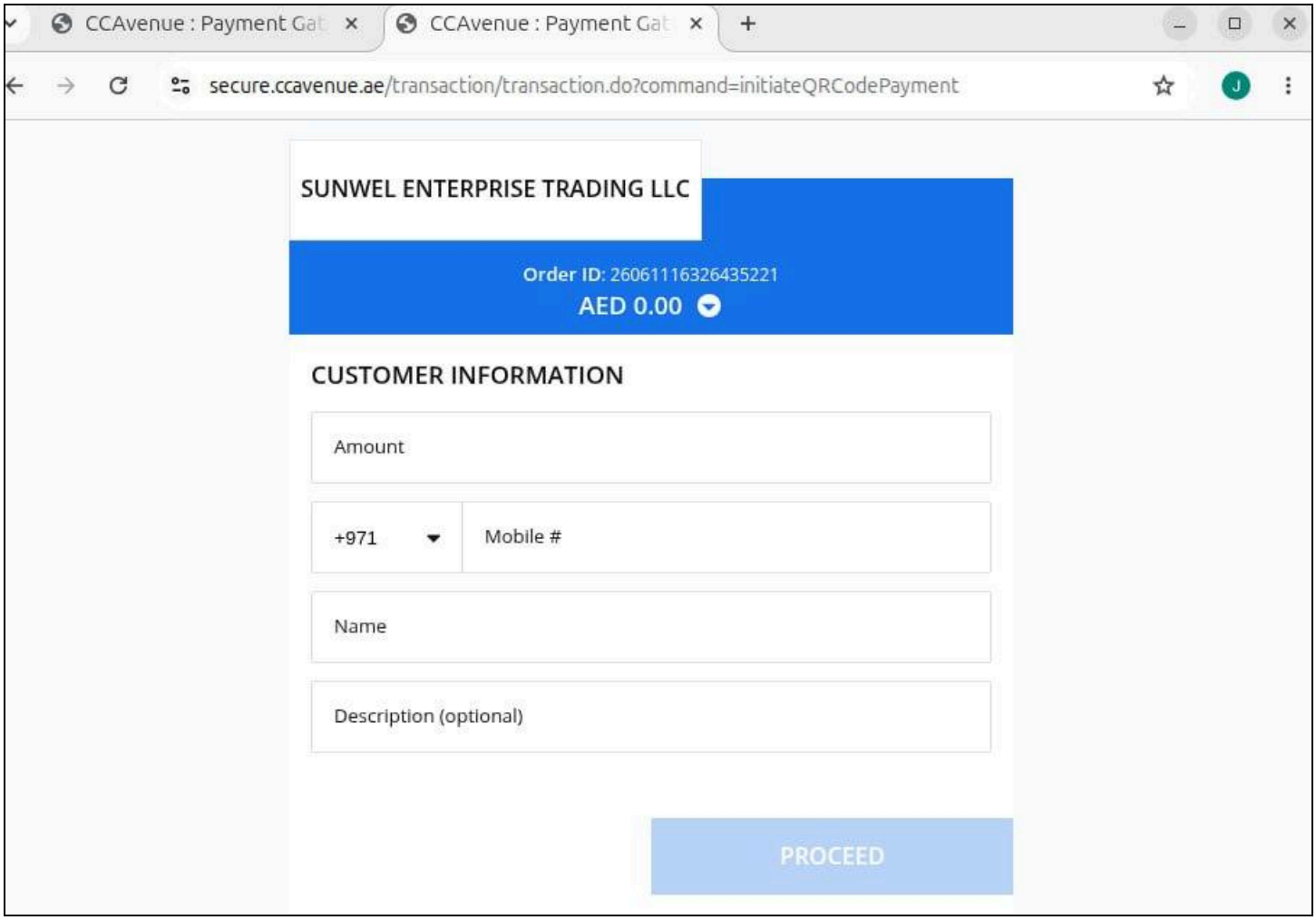

Figure 15: *Visiting the URL hxxps://payae[.]cc/Qwpf734 led us to a link belonging to CCAvenue (ccavenue[.]ae), a company named SUNWEL ENTERPRISE TRADING LLC is listed as the merchant (Source: Recorded Future Proprietary Data)*

Recorded Future reporting contains expressions of likelihood or probability consistent with US Intelligence Community Directive (ICD) 203: Analytic Standards (published January 2, 2015). Recorded Future reporting also uses confidence level standards employed by the US Intelligence Community to assess the quality and quantity of the source information supporting our analytic judgments.

About Insikt Group®

Recorded Future's Insikt Group, the company's threat research division, comprises analysts and security researchers with deep government, law enforcement, military, and intelligence agency experience. Their mission is to produce intelligence that reduces risk for customers, enables tangible outcomes, and prevents business disruption.

About Recorded Future®

Recorded Future is the world's largest intelligence company. The Recorded Future Intelligence Operations Platform provides the most complete coverage across adversaries, infrastructure, and targets. By combining precise, AI-driven analytics with the Intelligence Graph® populated by specialized threat data, Recorded Future enables cyber teams to see the complete picture, act with confidence, and get ahead of threats that matter before they impact your business. Headquartered in Boston with offices around the world, Recorded Future works with more than 1,900 businesses and government organizations across 80 countries.

Learn more at recordedfuture.com