THREAT HUNTER RESEARCH

Fraud Risks in China's Consumer Subsidy Program

A focused investigation into merchant abuse and transaction manipulation targeting China's consumer subsidy program.

Original publication: 2025-05-22
Research team: Threat Hunter Research Team
Source report: 19 pages

Original report text

This text version is reconstructed based on the 19-page original PDF, retaining the report narrative, chapters and research scope; the cover, duplicate table of contents and purely decorative pages are not repeated. Localized figures are placed in context throughout this web edition, with the original PDF retained for reference.

About Threat Hunter

Threat Hunter was founded in 2017 and helps organizations identify and respond to business fraud, external digital risk, and API security threats. Its work combines cybercrime intelligence, risk data, product platforms, and specialist services.

The company provides mature and diverse products and services focusing on risk scenarios such as business fraud, data leakage, phishing and counterfeiting, and API attacks that different industries face in the process of digital development. It has been selected as a representative vendor in Gartner's technology maturity curve report and IDC's threat intelligence field for many times.

Headquartered in Shenzhen, Threat Hunter also operates offices in Beijing, Shanghai, and Chongqing, with Digital Risk Response Centers in Shenzhen and Chongqing. The company supports customers in China, Europe, the United States, South America, and Southeast Asia.

01The cybercrime ecosystem chain under the supervision of “state subsidies”

02. Various roles in the national subsidy industry chain exploit the advantages of national subsidy

Benefit method analysis and case presentation

03. Conclusion

Directory

Preface

Starting from 2024, the national subsidy policy for the trade-in of consumer goods, hereinafter referred to as the "national subsidy" policy, will be fully implemented in the three major fields of automobiles, digital products, and home appliances to promote consumption upgrades, energy conservation, and emission reduction. The activity subsidies are significant, such as a 20,000 yuan subsidy for new energy vehicles and a 15% subsidy for digital products, covering multiple online e-commerce platforms and physical brand stores.

Behind the policy dividends, there are also behaviors of profiteering from subsidies; in order to prevent cybercrime ecosystem from taking profits from subsidies, the state and participating platforms (e-commerce, express delivery) have simultaneously launched a number of anti-scalper measures, including users needing to meet real-name purchase, purchase limit of 1 item, personal signature activation and other conditions, and through technical means such as qualification code binding, order invoice matching, SN code verification and signature, restricting cybercrime ecosystem and illegal users from obtaining off-site subsidy qualifications, and increasing their resale profit costs.

Despite this, some cybercrime ecosystem still bypass supervision and implement arbitrage through fine division of labor and role collaboration, forming a mature industrial chain, invading the preferential rights and interests of normal consumers on major platforms, and seriously damaging the fair ecology of the platform.

Threat Hunter is based on long-term investigations and research on the "consumer subsidy" industry chain, combined with relevant data, and strives to accurately and objectively demonstrate the current malicious activity status and behavior patterns of cybercriminal groups use of the "consumer subsidy" industry chain.

01The cybercrime ecosystem chain under the supervision of “state subsidies”

1.1 Overview of the industrial chain

Under the supervision of the "state-approved" policy, the Threat Hunter intelligence platform still detected cybercrime ecosystem profiting from state-approved vulnerabilities. cybercriminal groups use various methods such as illegal acceptance of joint couriers, resale of qualifications, illegal verification operations, counterfeit recycling orders for arbitrage, recruiting individuals to recycle national subsidy, and other methods to obtain the preferential state subsidy.

These techniques involve multiple roles, including cybercrime ecosystem, merchants and individual users, specifically involving fraud users, resale qualified users, merchants, agents, scalpers, couriers, etc. These roles cooperate with each other to bypass national subsidy areas and user supervision through purchasing, forwarding, activation, etc., forming a complex chain of interests.

The points and methods of profit-making through multi-role collaboration are as follows:

Group	Core technique	Profit point
Scalpers	Recruit individuals to sell their subsidy eligibility, "harvest" subsidized goods in bulk and resell them	Pocket and resell subsidies
Fraudulent merchants	Without the user visiting the store, fake device verification with remote QR scans to complete subsidy redemption	Earn merchant subsidies and boost sales
Resellers	Stack several discounts for arbitrage and lure buyers with low-priced bundles to defraud subsidy funds	Earn merchant subsidies and boost sales
Individual users	Sell their own subsidy eligibility and help buyers activate devices	Errand fees and eligibility fees
Couriers	Help fake sign-offs and, for a fee, forward parcels for fraudulent users	Small commissions

Roles in the consumer-subsidy fraud chain: core techniques and how each profits

Source: Threat Hunter original report, page 5. Table re-typeset in English from the original.

1.2 Digital home appliances have become the hardest hit area for sales of state-subsidized goods

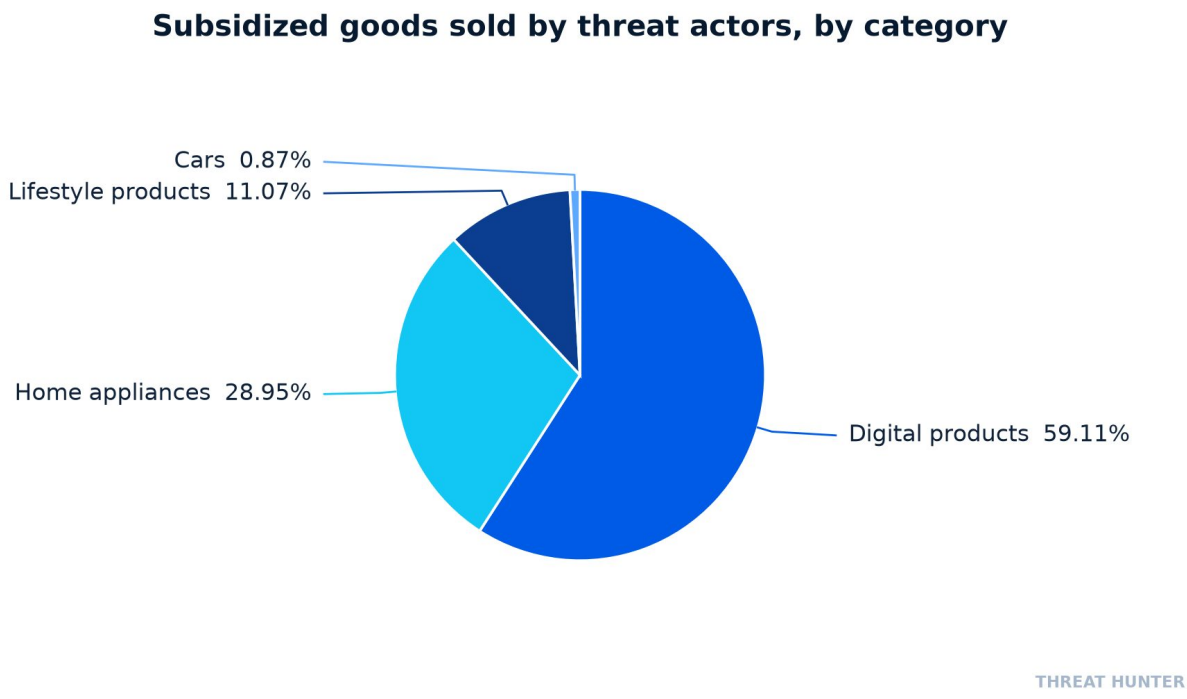
Threat Hunter has compiled statistics on the types of products related to China's national consumer subsidy program sold in the cybercrime ecosystem trading market. The top product categories with the highest transaction popularity are: digital products, home appliances, and lifestyle products. Accounting for 59.11%, 28.95% and 11.07% respectively.

Category	Typical products
Digital products	Phones, tablets, smartwatches, earphones and other electronic devices
Home appliances	Fridges, TVs, washing machines, air conditioners, dishwashers and other large appliances
Lifestyle products	Hair dryers, water flossers, hair-removal devices, computer peripherals, etc.
Cars	Cars and car accessories

Categories of subsidized goods resold by threat actors

Source: Threat Hunter original report, page 6. Table re-typeset in English from the original.

Digital and home appliance products have become the main target of cybercrime ecosystem reselling for profit due to their high unit prices and strong subsidies (the maximum subsidy is 1,000 yuan for digital products and 2,000 yuan for home appliances). In contrast, lifestyle products have little profit potential, and it is difficult to resell cars. At the same time, the demand for digital and home appliances is highly elastic and price-sensitive. National subsidies stimulate demand, and cybercriminal groups use low-price discounts and multiple discount qualifications to attract consumers to make profits.



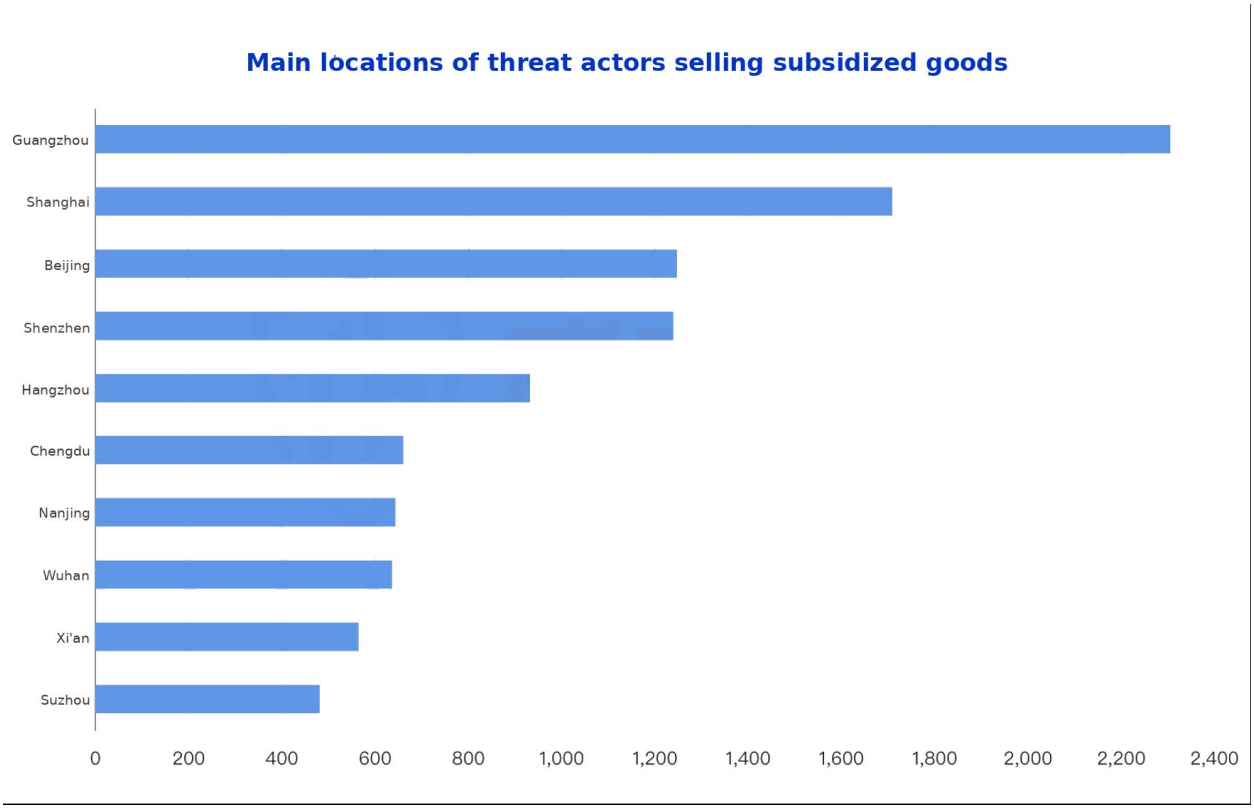
Subsidized goods sold by threat actors, by category: digital products 59.11%, home appliances 28.95%

Source: Threat Hunter original report, page 6. Redrawn in English from the original figure.

These factors work together to make digital and home appliances the hardest hit areas for cybercrime ecosystem arbitrage.

1.3 Main distribution areas of cybercrime ecosystem selling consumer subsidy products top 3: Guangzhou, Shanghai, Beijing

Threat Hunter researchers analyzed the registration locations of individual cybercrime ecosystem stores selling consumer subsidy products on major trading platforms and found that cybercrime ecosystem stores selling consumer subsidy products are mainly distributed in Guangzhou, Shanghai, Beijing, Shenzhen and other areas.

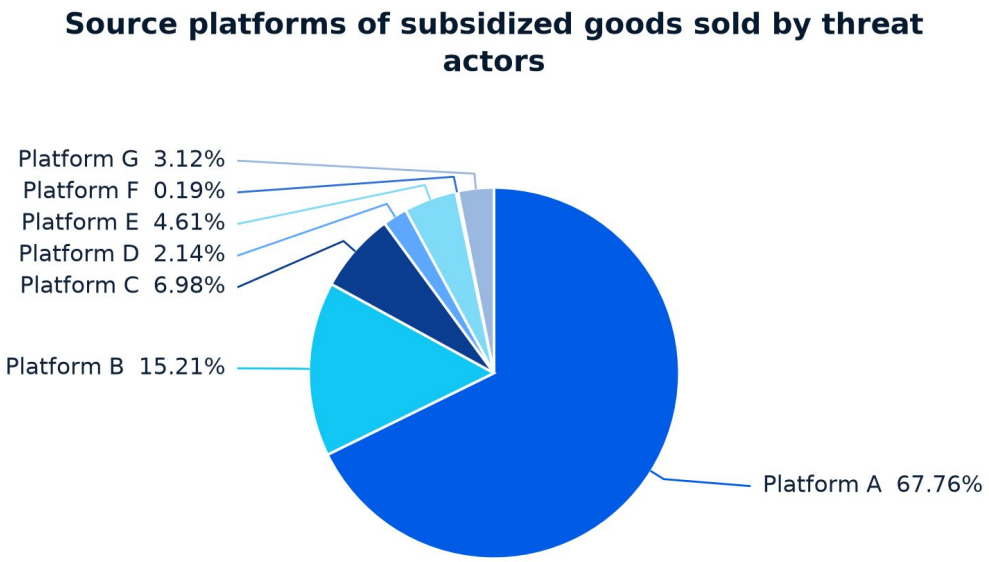


Main locations of threat actors selling subsidized goods: Guangzhou, Shanghai and Beijing lead

Source: Threat Hunter original report, page 7. Original figure with Chinese text replaced by English.

1.4 The main source channels for selling consumer subsidy products are the two leading domestic e-commerce platforms.

Note: The content of the following report has been desensitized (relevant e-commerce platforms are designated by A, B, C, etc.), and the "internal publication" version will be synchronized for customers who have cooperated. Threat Hunter collects statistics on the source and channel information of the consumer subsidy products sold by cybercrime ecosystem from the capture cycle sample data. Among them, 82.93% of the consumer subsidy products come from the two leading domestic e-commerce platforms.

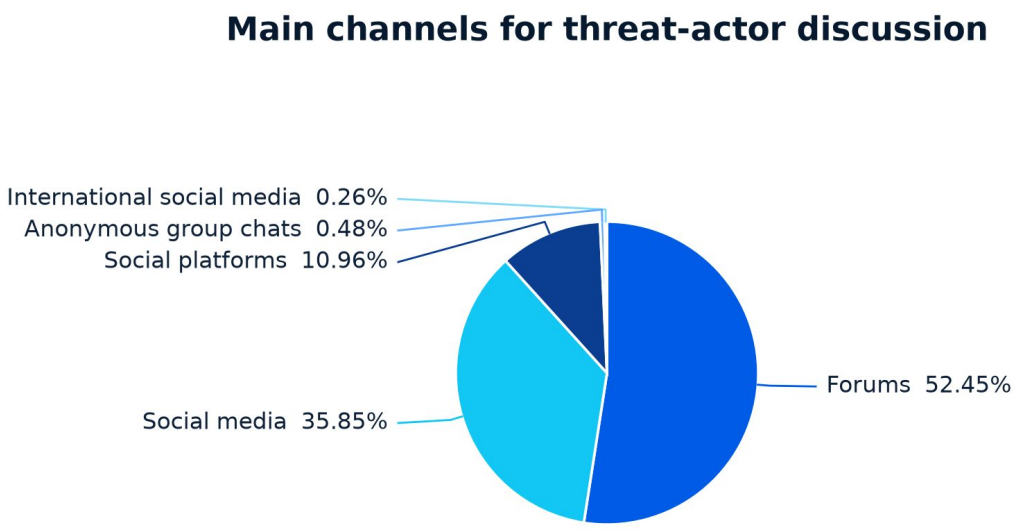


Source platforms of subsidized goods sold by threat actors (platforms masked as A to G)

Source: Threat Hunter original report, page 7. Redrawn in English from the original figure.

1.5 cybercriminal groups publishes advertisements in forums and social media and then diverts traffic to the private domain to complete transactions

Threat Hunter monitored the discussion channels surrounding the risks related to “purchasing, forwarding, cashback, and recycling” of state subsidies. Forums and social media were the main active channels for threat actors; forum channels accounted for 52.45%, and social media channels accounted for 35.85%.



Main channels where threat actors discuss subsidy arbitrage: forums 52.45%, social media 35.85%

Source: Threat Hunter original report, page 8. Redrawn in English from the original figure.

cybercriminal groups publishes advertisements in forums or social media, directing users to private domains for detailed exchanges and transactions.

Threat Hunter researchers further analyzed and found that the main reasons why forums and social media are the main active channels for cybercriminal groups are:

The portraits of users using forums and social media are highly overlapped with the target group of consumer subsidy products, and the form of information release is flexible and concealed, such as disguising it as a 'money-saving guide' or diverting traffic to private domains through QR codes, which can effectively avoid platform review.

At the same time, the forum’s old accounts, hot posts, and social media’s algorithm recommendations and the ‘big V’ effect also provide trust endorsement and dissemination convenience for these illegal information, greatly reducing the cost of cybercriminal groups' traffic and improving the recruitment success rate.

02 Analysis and case studies on the methods used by various actors in the state subsidy industry chain to obtain preferential state subsidy. Under such strict policy supervision, cybercriminal groups can still exploit the "loopholes" of state subsidy. How do the various actors cooperate with each other to bypass the state subsidy supervision and successfully obtain state subsidy?

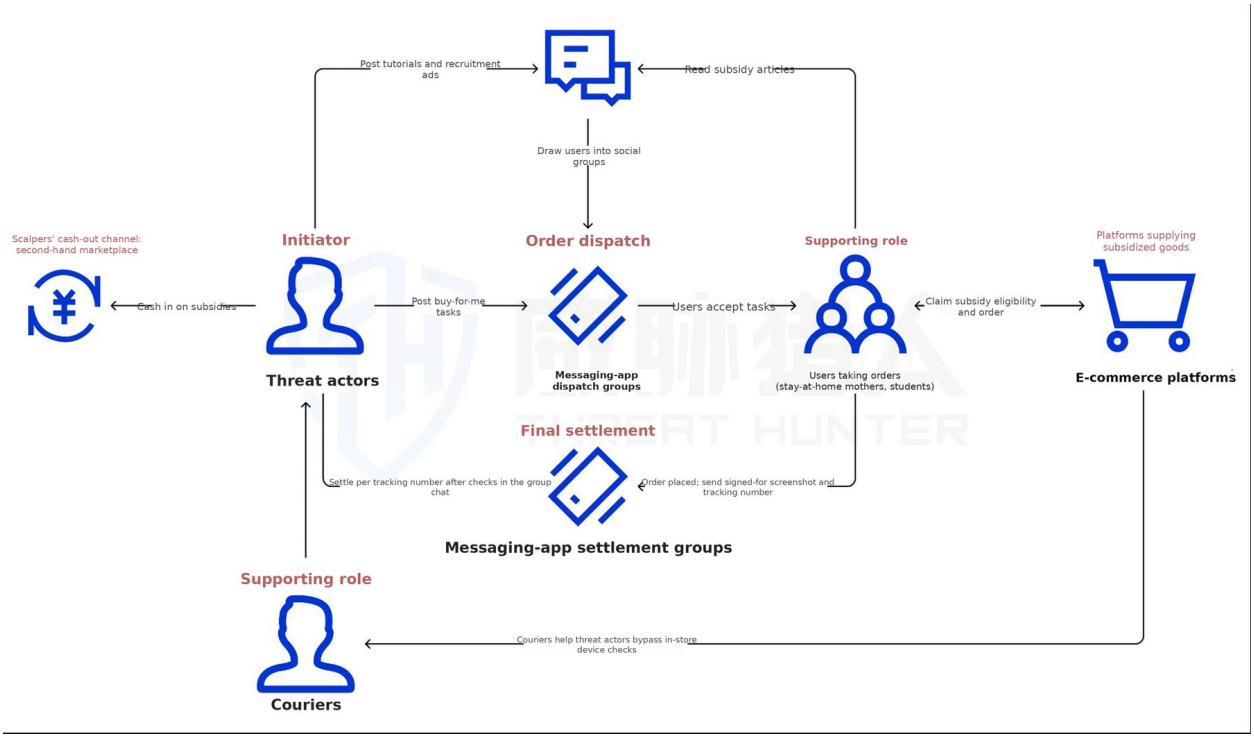
The following are typical behavior patterns of each role

2.1 Analysis of scalper group techniques

Threat Hunter research found that scalpers use social media to recruit users who are qualified to sell state subsidies, recycle the state subsidies, and allow couriers to collaborate to bypass supervision. They mainly use the following characteristics:

- Diversion and recruitment: cross-regional collaboration and supervision are difficult

- Cash on delivery: collaborative courier supervision is bypassed
- Temporary dispatch of orders to group chat and group settlement: high concealment



How scalpers profit from the subsidy: recruiting order-takers through group chats, with couriers helping to bypass checks

Source: Threat Hunter original report, page 9. Original figure with Chinese text replaced by English.

2.1.1 Scalpers summon users to collect China's national consumer subsidy programary products to share cases

Scalpers convene "trading national subsidy-qualified users" on social media, forums and other social platforms, divert traffic to a temporary messaging-app group, and fill in the real names and phone numbers of the selling-qualified users in accordance with the scalpers' requirements. The delivery address is selected from the address database provided by the scalpers, and orders are placed via cash on delivery.



A scalper briefs order-takers: cash on delivery, real names and phone numbers, and a list of delivery addresses

Source: Threat Hunter original report, page 10. Original image retained; numbered translations added by Threat Hunter.

Figure guide

1	Choose cash on delivery; anything under 4,000 is fine to order
2	Is this the one I just sent, to order after binding?
3	Name and phone must be your own real ones and reachable
4	Image of an electronic product
5	Final price ¥4,999.00
6	List of Beijing delivery addresses (partly masked)
7	The same three instructions, sent again

On the surface, this is a commonly used recycling method, but in fact, scalpers team up with the "consignee" - that is, the courier to illegally inspect and accept the equipment for express delivery, bypassing policy supervision and recycling the national subsidy. In order to avoid monitoring, scalpers divide order dispatch and settlement into groups, disbanding old groups within 1 to 2 days and reopening new groups to continue placing orders, which increases the difficulty of supervision.

After the scalper signs for the receipt, the order-receiving user enters the scalper-specific statement group chat and provides a screenshot of the signed receipt and the courier order number for settlement.



Order-takers are told to join a separate pay group and post proof of delivery to be settled

Source: Threat Hunter original report, page 11. Original image retained; numbered translations added by Threat Hunter.

Figure guide

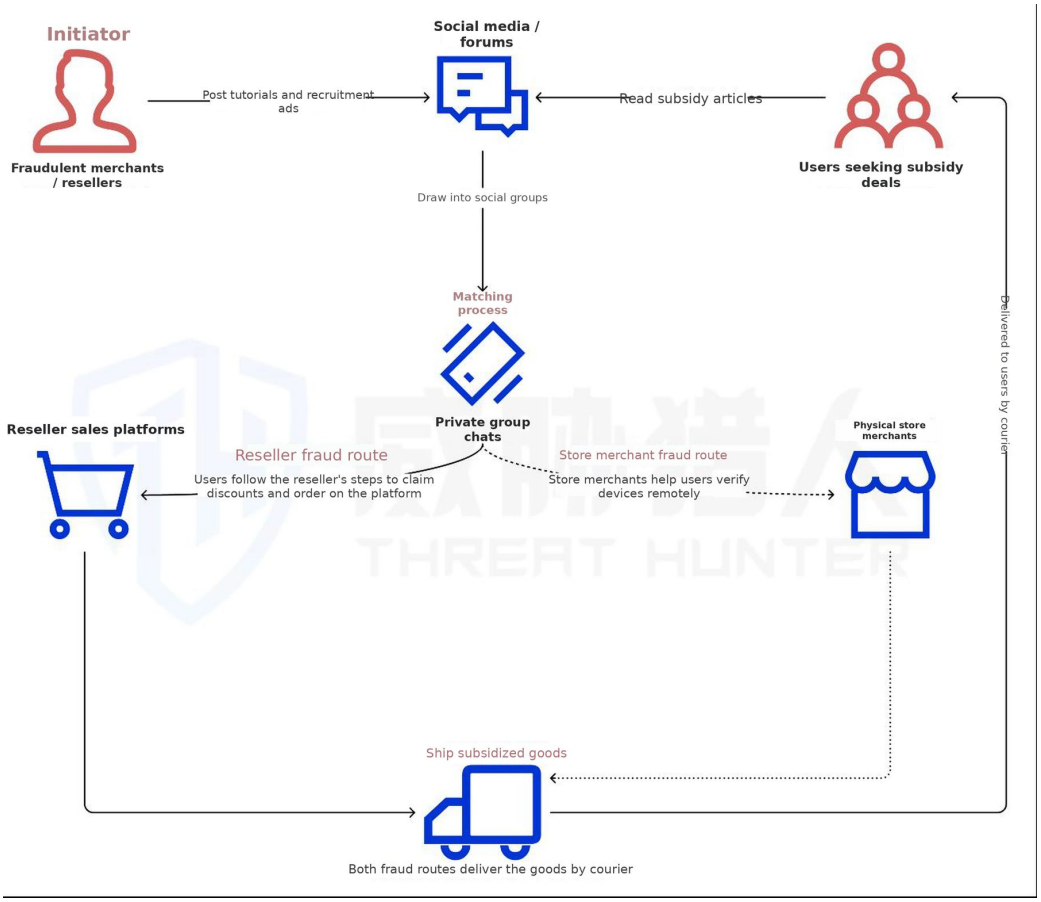
1	Everyone whose order has been signed for: join the pay group and post the signed-for screenshot and tracking number
2	Make sure it shows as signed before joining the group

2.2 Analysis of merchant fraud techniques

Threat Hunter research found that under the national subsidy regulatory policy, some merchants will still cooperate with consumers to implement arbitrage even though they are aware of the violations. Merchants mainly profit from the following characteristics:

- Remote verification/false trade-in: taking advantage of policy loopholes to avoid supervision
- Social media traffic: hashtag topic group traffic, high consumption rate, merchants assist fraud methods, generally divided into two situations: physical-store merchants and online dealers:

1) Physical merchants remotely activate someone other than themselves to increase product sales
2) Online dealers and agents fabricate the trade-in process to defraud double subsidies

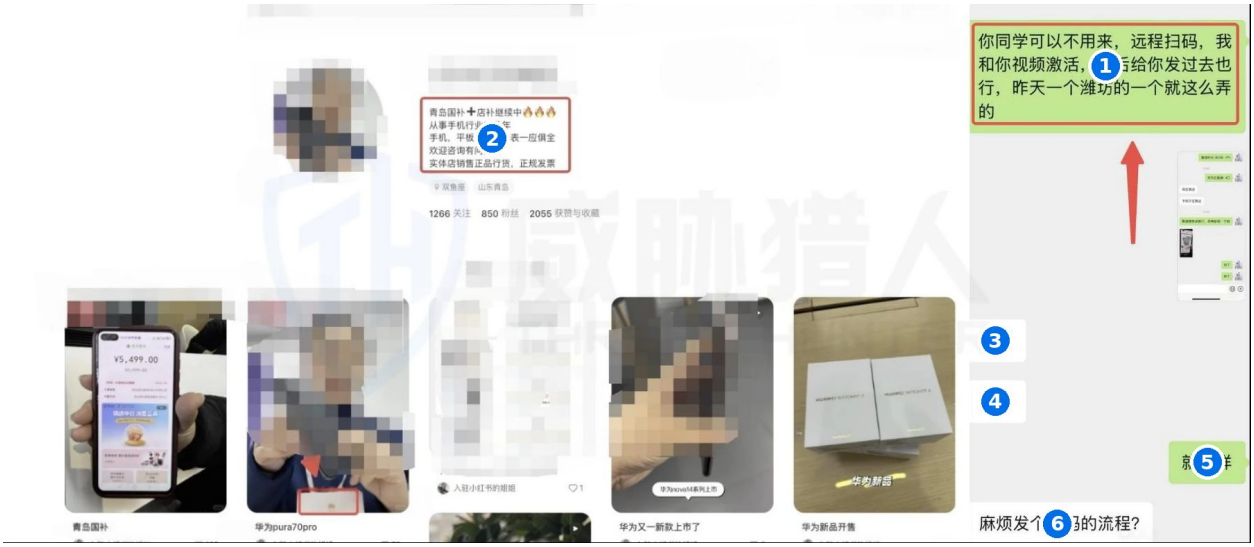


Two merchant fraud routes: resellers stacking discounts online, and stores verifying devices remotely

Source: Threat Hunter original report, page 12. Original figure with Chinese text replaced by English.

2.2.1 Case sharing of merchants assisting users in fraud to obtain nationally supplemented products 1) Remote activation by merchants not in person

In accordance with the national subsidy supervision policy, the normal process of purchasing national subsidy in physical stores requires the purchaser to be present with his or her ID card information, and the store merchant will verify that the identity is consistent and the machine will be inspected and activated on the spot. However, some merchants remotely allow buyers to scan codes to activate the device through messaging-app video calls, and then deliver it to the purchasing user's address by express delivery. to bypass regulation



A phone store advertises subsidized devices on social media and offers remote activation over a video call

Source: Threat Hunter original report, page 12. Original image retained; numbered translations added by Threat Hunter.

Figure guide

1	Your classmate doesn't need to come: scan the code remotely and I'll activate it over a video call, then ship it. Did one for someone in Weifang yesterday
2	Seller profile: Qingdao subsidy plus store subsidy; 10+ years in the phone trade; phones, tablets and smartwatches; genuine goods from a physical store with official invoices
3	Wow
4	Great
5	That's how
6	Could you send the scanning steps?

2) Agents take advantage of the triple discount of national subsidies. According to research, some online dealers use the "triple discount" to sell national subsidy products at low prices to increase sales and obtain double profits.

The "triple discount" for distributors includes:

1. Normal state subsidies for individual users

2. National subsidy trade-in subsidy discount

3. Agents provide platform coupons

In addition, some dealers cheat in the "trade-in" process and falsely recycle old products, allowing users to enjoy the subsidy without providing any old product recycling certificate when choosing the "trade-in" subsidy.



A dealer explains that a "trade-in" order needs no old device

Source: Threat Hunter original report, page 13. Original image retained; numbered translations added by Threat Hunter.

Figure guide

1	I see it's a trade-in, but I have no old one
2	No old device needed
3	I'll let you know the price
4	Oh, so I just pick a trade-in option and need not provide an old item?
5	Since Chinese New Year I've sold this many TVs with the general agent; with prices up this much I would rather not have people order
6	Not worth it

In addition, agents revealed that if users need to purchase products with national subsidy in other places, they can find "gunners" (i.e. users in remote areas with national subsidy and whose qualifications for national subsidy are idle) to place orders on their behalf, thereby bypassing the restriction of national subsidy IP regions. Users only need to click this operation and then complete the transaction through the agent channel.



An agent explains how out-of-area buyers use local "gunners" to place subsidized orders

Source: Threat Hunter original report, page 14. Original image retained; numbered translations added by Threat Hunter.

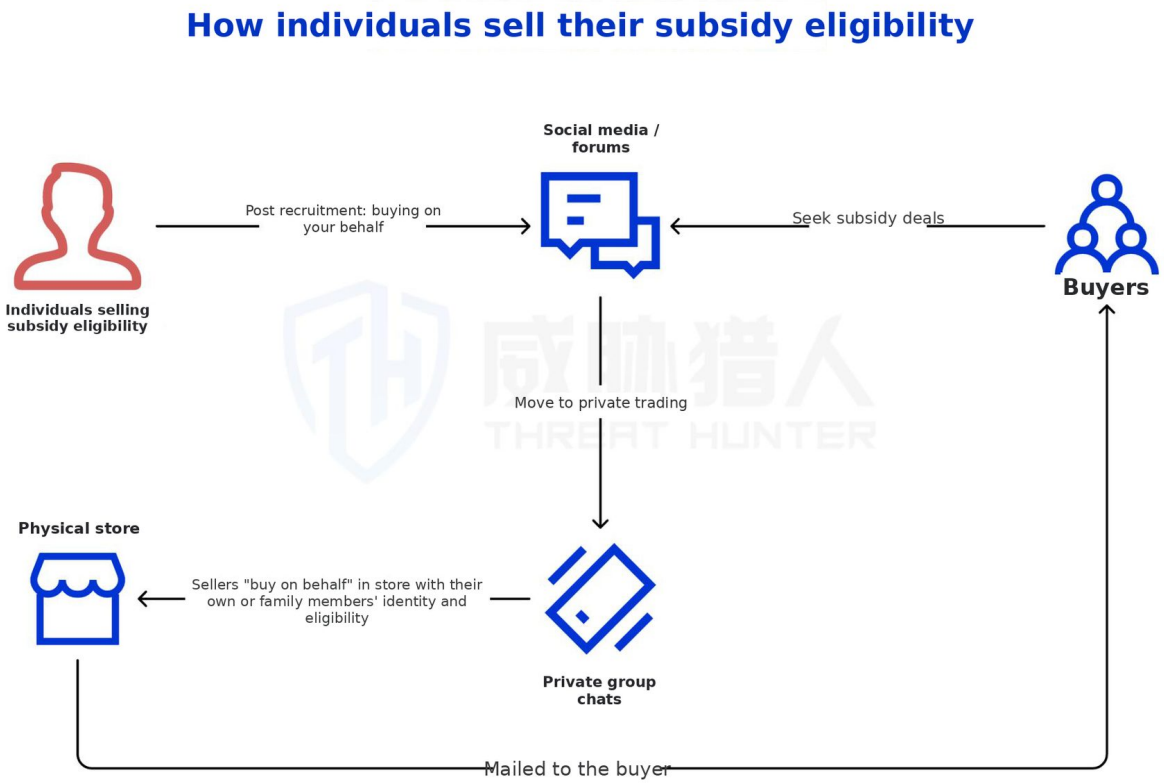
Figure guide

1	Only family members can buy it
2	So only my family in Chongqing can help me buy it?
3	In theory, yes. Before, some people who sold goods on an e-commerce platform found "gunners" in Chongqing to place the orders
4	"Gunners"?
5	Yes. People in Chongqing who aren't using the subsidy have little else to do with it
6	Pay someone to place the order

2.3 Analysis of individual users’ violation methods

Research by Threat Hunter intelligence staff found. In the scenario of "consumer subsidy fraud", more and more real users are making malicious profits by studying and using the "legitimate" rules of platform business. Among them, the following characteristics are mainly used to make profits:

- Couriers collaborate to “forward”: taking advantage of policy loopholes to avoid supervision
- Personal information purchasing on behalf of individuals: supervision is difficult

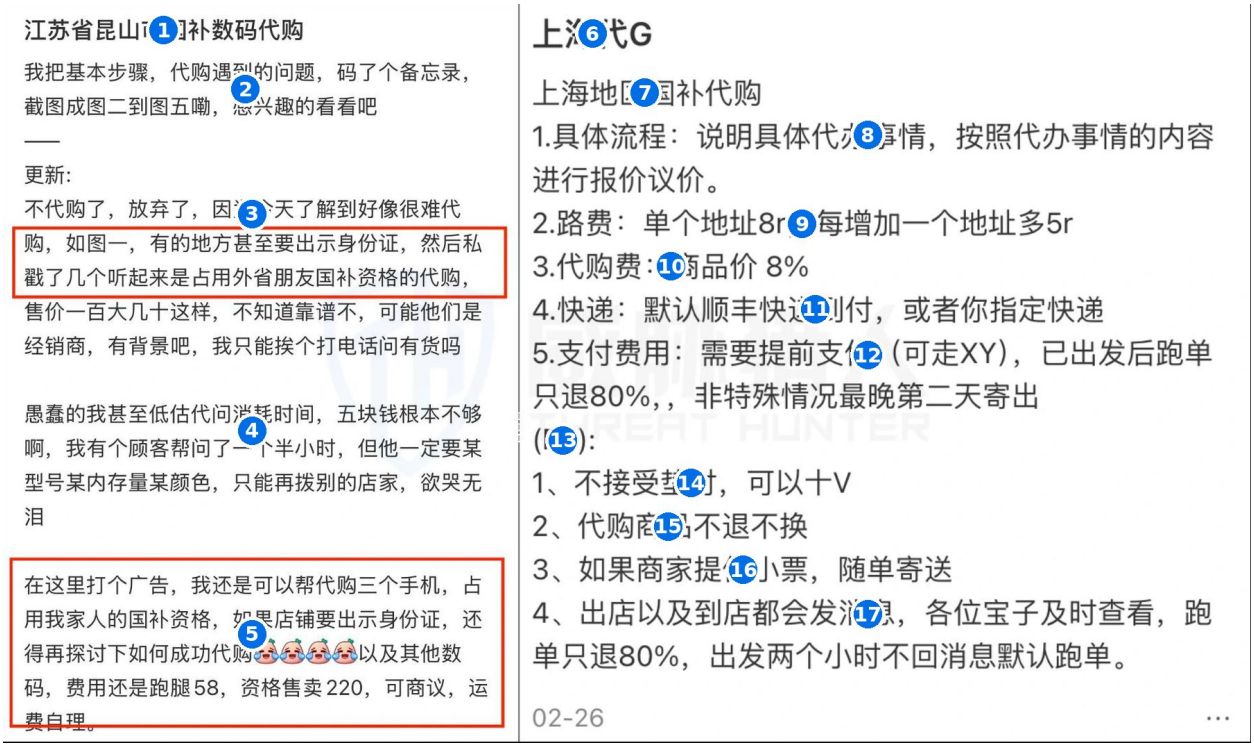


How individuals sell their subsidy eligibility: recruiting buyers online and buying in store on their behalf

Source: Threat Hunter original report, page 15. Original figure with Chinese text replaced by English.

2.3.1 Case sharing of individual users selling/fraud to obtain national subsidy products 1) Users make profits by selling personal national subsidy qualifications

Some individual users publish recruitment information through active social platforms and resell their or their family members' qualifications for national subsidy in physical stores, placing orders for national subsidy equipment and verification equipment as themselves or their family members, and finally delivering them to the address of the person in need by mail. This will charge a certain qualification fee and legwork fees.



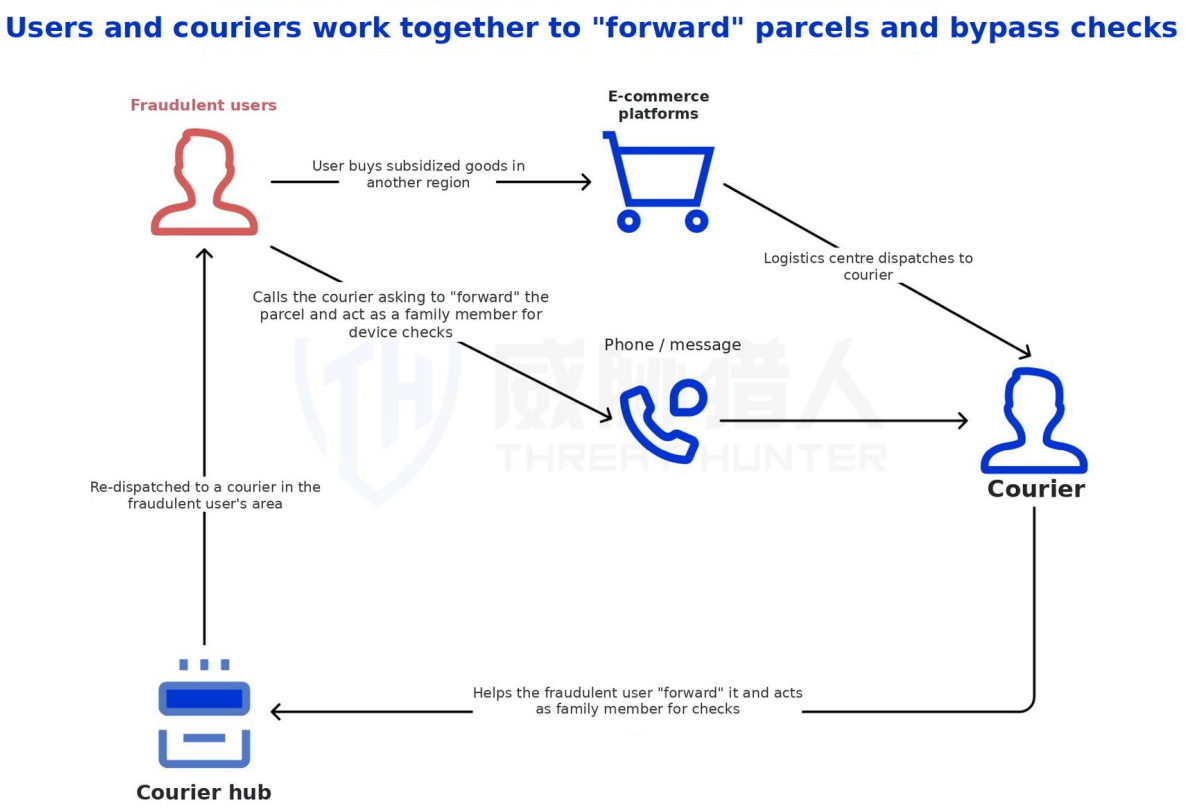
Individuals advertise buying subsidized goods for others with their own or family members' eligibility, with fee schedules

Source: Threat Hunter original report, page 16. Original image retained; numbered translations added by Threat Hunter.

Figure guide

1	Kunshan, Jiangsu: subsidized digital goods bought for you
2	I wrote the basic steps and problems up in a memo; see images 2 to 5
3	Update: I've given up, it seems hard to do; some stores even ask for ID. I messaged a few sellers who use out-of-province friends' eligibility, at about 170 to 190; not sure they are reliable, maybe dealers with connections
4	I underestimated the time: 5 yuan is nowhere near enough. One customer had me ask around for an hour and a half for a specific model, storage size and colour
5	Ad: I can still buy three phones with my family's eligibility; if the store asks for ID we'll work it out. Errand fee 58, eligibility 220, negotiable, plus shipping
6	Shanghai buying agent
7	Subsidized purchases for you, Shanghai
8	1. Process: tell us what you need; we quote and negotiate
9	2. Travel fee: 8 per address, plus 5 for each extra address
10	3. Agent fee: 8% of the item price
11	4. Delivery: courier, paid on delivery by default, or a courier of your choice
12	5. Payment in advance (a second-hand marketplace is OK); cancel after we set out and 80% is refunded; shipped by the next day at the latest
13	Notes
14	1. No advance payments; add us on a messaging app
15	2. No returns or exchanges
16	3. Receipts shipped with the order if the store provides one
17	4. We message when leaving and arriving; no reply for 2 hours after we set out counts as a cancellation (80% refunded)

2) Users cooperate with couriers to "forward" to bypass supervision. In addition, in order to obtain multiple national subsidy discounts, some users actively participate in off-site subsidy arbitrage and provide identity information to cooperate with verification. They also communicated with the courier and forwarded the goods to bypass the country's regional restrictions on subsidy. Some users deliberately look for courier companies that can forward their shipments, and then use forwarding to bypass regional restrictions.



Fraudulent users work with couriers to forward subsidized goods bought in another region

Source: Threat Hunter original report, page 15. Original figure with Chinese text replaced by English.

There is also a special participant in the industry chain of swindling state subsidies - the couriers in the area. As mentioned above, they play a key role in bypassing the regional restrictions on state subsidies. They are responsible for helping users activate products and assist users in forwarding, and finally deliver the goods to the real owner's address.



Users share how to get couriers to forward subsidized goods and act as family members, tipping them with a red envelope

Source: Threat Hunter original report, page 17. Original image retained; numbered translations added by Threat Hunter.

Figure guide

1	Change the delivery address to any parcel locker there; when the courier calls, tell them to forward it, or place an order on a logistics app
2	If the courier says it must be activated before signing, ask if they can help sign for it (it needs activation; I refused)
3	I placed an order and had the courier act as my family member to sign, then forward it to me
4	Hubei subsidy
5	Fill in any address; when the courier delivers, just tell them to forward it. Add a tip and they will happily do it fast
6	Greeting message
7	Contact added; you can start chatting
8	Is this the one?
9	Red envelope: good luck and prosperity
10	Thanks for the trouble, have a drink on me
11	OK
12	Yes

03 Conclusion During the implementation of the consumer subsidy policy, although the state and platforms have taken a number of anti-scalper measures, the cybercrime ecosystem still exploits loopholes to obtain subsidies through refined division of labor and collaboration, seriously damaging the fair market ecology.

Faced with this problem, all parties need to continue to update their understanding of cybercrime ecosystem malicious activity, and continuously strengthen supervision and technical means to better maintain a fair market environment and ensure that subsidy policies truly benefit consumers.

Company official website: www.threathunter.cn Cooperation email: Marketing@threathunter.cn