

“国补”政策下的 黑色产业链分析报告



关于威胁猎人

威胁猎人 Threat Hunter（深圳永安在线科技有限公司）成立于 2017 年，以黑灰产情报能力和反欺诈技术为核心，专注于及时、精准、有效的业务欺诈风险的发现和响应。

公司围绕不同行业在数字化发展过程中面临的业务欺诈、数据泄露、钓鱼仿冒、API 攻击等风险场景，提供成熟多样的产品与服务，并多次入选 Gartner 技术成熟度曲线报告、IDC 威胁情报领域代表厂商。

公司总部在深圳，在北京、上海、重庆、新加坡等地设有分公司，并在深圳和重庆两地建立数字风险应急响应中心（DRRC），为客户提供 7*24 小时全天候数字风险应急响应和及时、优质的服务支持。截至目前，公司已为金融、政务、物流、互联网、科技、零售等行业的 300 多家客户提供安全服务，覆盖 85% 头部互联网企业，每年帮助客户减少数十亿资金损失。

目录

01 “国补” 监管下的黑灰产产业链

02、国补产业链各类角色套取国补优惠手法分析及案例展现

03、结语

前言

2024 年起，消费品以旧换新的国家补贴政策，下文简称“国补”政策，在汽车、数码、家电三大领域全面推行，以推动消费升级、节能减排等。活动补贴力度显著，如新能源车补贴 2 万元，数码产品补贴 15%，覆盖多个电商线上平台及线下品牌门店。

在政策红利背后，也存在套取补贴获利的行为；为防止黑灰产套取补贴获利，国家及参与平台（电商、快递）同步推出多项防黄牛措施，包括用户需满足实名购买、限购 1 件、本人签收激活等条件，以及通过资格码绑定、订单发票匹配、SN 码核验签收等技术手段，限制黑灰产及违规用户薅取异地补贴资格，并增加其转卖获利成本。

尽管如此，部分黑灰产仍通过精细分工和角色协作，绕开监管实施套利，形成一条成熟的产业链，侵占了各大平台正常消费者的优惠权益，严重破坏了平台的公平生态。

威胁猎人基于长期对“国补”产业链的调查和研究，结合相关数据，力求准确、客观展现当前利用“国补”代下/套补产业链黑灰产的作恶现状和行为模式。

01 “国补” 监管下的黑灰产产业链

1.1 产业链概述

在“国补”政策监管下，威胁猎人情报平台仍监测到黑灰产利用国补漏洞获利。黑灰产通过联合快递员违规验收、资格转卖、违规核验操作、伪造回收刷单套利、招募个人回收国补等多种手法套取国补优惠。

这些手法涉及多个角色，包括黑灰产、商家和个人用户，具体涉及作弊用户、转卖资格用户、商家、代销商、黄牛、快递员等。这些角色相互配合，通过代买、转寄、代激活等方式绕过国补地区 and 用户监管，形成了一个复杂的利益链条。

多角色协同牟利点及手段如下：

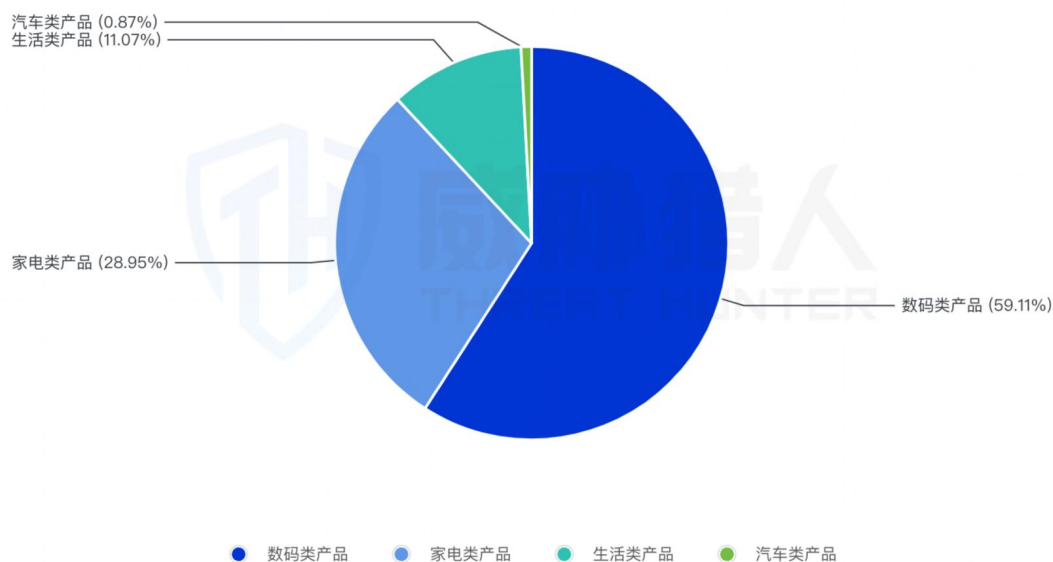
主要群体	核心手段	牟利点
黄牛	招募散户回收国补资格，大量“撸取”国补商品并进行二次转卖	套取补贴倒卖
作弊商家	在用户未实际到店的情况下，通过远程扫码伪造设备违规核验，完成国补核销。	获得商户补贴、提升销量
代销商	利用多重优惠组合套利、包装产品低价引流，骗取补贴资金。	获得商户补贴、提升销量
个人用户	贩卖个人国补资格并协助购买者激活	赚取跑腿费及贩卖资格费用
快递员	协助伪造签收、收取一定好处费协助违规用户转寄	赚取小额佣金

1.2 数码家电产品成为国补商品贩卖重灾区

威胁猎人对交易市场黑灰产贩卖国补相关商品的种类数据进行统计，交易热度 TOP 的商品类别分别为：数码类产品、家电类产品、以及生活类产品。分别占比 59.11%、28.95%和 11.07%。

数码类产品	手机、平板电脑、智能手表、耳机等产品，以电子设备为主
家电类产品	冰箱、电视机、洗衣机、空调、洗碗机等大型电器类
生活类产品	吹风机、冲牙器、脱毛仪、电脑外设等
汽车	汽车，汽车用品类

黑灰产贩卖国补相关商品类别分布

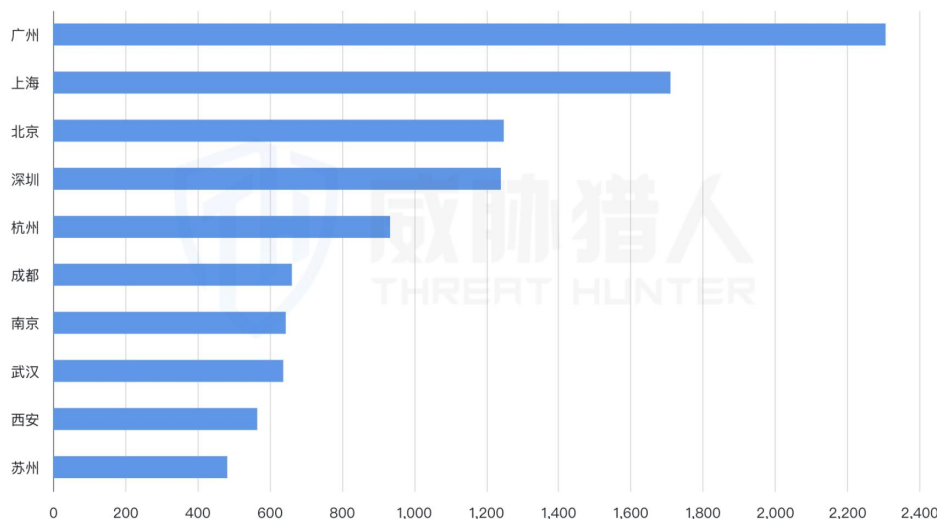


数码和家电类产品因单价高、补贴力度大（数码最高补 1000 元，家电最高补 2000 元），成为黑灰产倒卖获利的主要目标。相比之下，生活类产品获利空间小，汽车倒卖难度大。同时，数码和家电需求弹性大、价格敏感，国补刺激需求，黑灰产利用低价优惠和多优惠资格吸引消费者获利。这些因素共同作用，使数码和家电成为黑灰产套利的重灾区。

1.3 售卖国补商品的黑灰产主要分布地区 TOP3：广州市、上海市、北京市

威胁猎人研究人员根据监测到的各大交易平台中贩卖国补商品的个体黑灰产店铺注册地分析发现，
售卖国补商品的黑灰产主要分布在广州、上海、北京、深圳等地区。

售卖国补商品的黑灰产主要分布地区

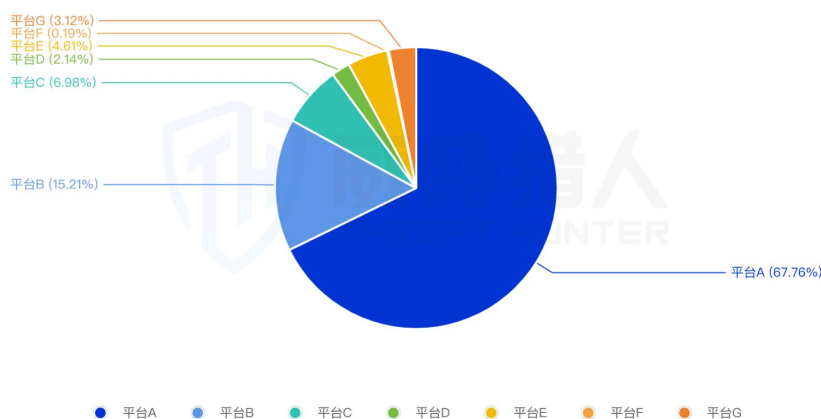


1.4 售卖国补产品来源渠道主要来源国内两大头部电商平台

注：以下报告内容已做脱敏处理（相关电商平台用 A、B、C 等代称），对已合作客户会同步“内刊”版本

威胁猎人从捕获周期样本数据中对黑灰产售卖的国补产品来源渠道信息进行统计，其中 82.93% 的国补产品来源国内两大头部电商平台

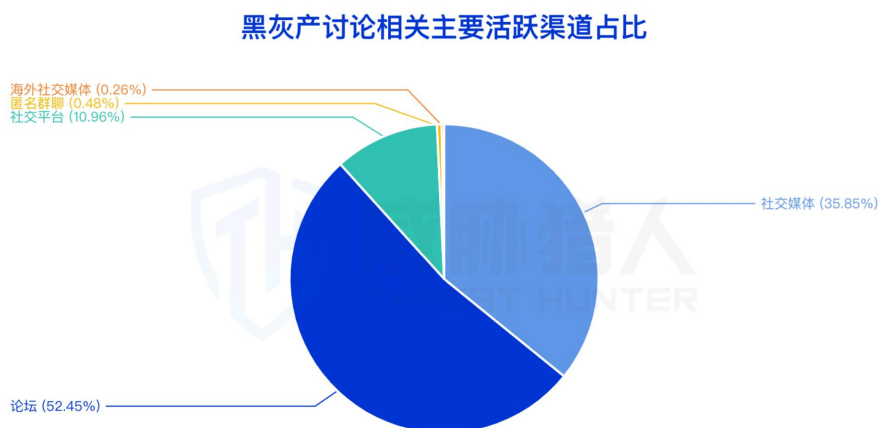
黑灰产售卖“国补”商品来源渠道分布



1.5 黑灰产在论坛和社媒进行广告发布后引流到私域完成交易

威胁猎人监测到围绕国补“代购、转寄、返现、回收”相关的风险的讨论渠道中，论坛与社交社媒为黑产的主要活跃渠道;论坛渠道占比高达 52.45%，社交媒体渠道占比 35.85%。

黑灰产在论坛或社媒发布广告，将用户引流到私域继而进行细节交流和交易。



威胁猎人研究人员进一步分析发现，论坛和社交媒体作为黑灰产主要活跃渠道的主要原因在于：

使用论坛以及社交媒体的用户画像与国补商品目标人群高度重合，信息发布形式灵活隐蔽，例如伪装成‘省钱攻略’或通过二维码引流至私域，能有效规避平台审核。

同时，论坛的老账号、热帖以及社交媒体的算法推荐和‘大V’效应，也为这些非法信息提供了信任背书和传播便利，大大降低了黑灰产的引流成本并提高了招募成功率。

02 国补产业链各类角色套取国补优惠手法分析及案例展现

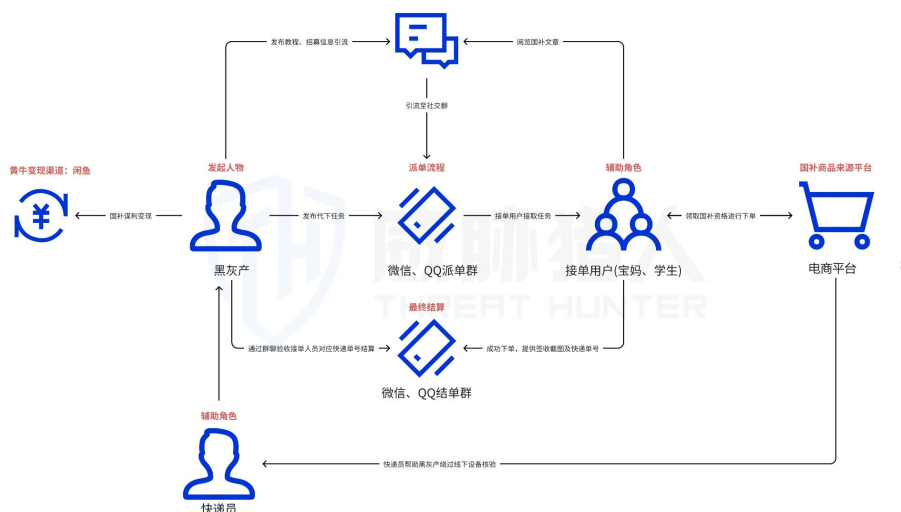
在如此严格的政策监管下，黑灰产仍然能够钻到国补“漏洞”，各角色是如何相互配合绕过国补监管成功薅取国补的呢？

以下是各角色典型行为模式

2.1 黄牛群体手法分析

威胁猎人研究发现黄牛利用社媒招募贩卖国补资格用户，回收国补，让快递员协同绕过监管，主要利用以下特点：

- **引流招募**：跨地域协作监管难度高
- **货到付款**：协同快递员监管绕过
- **临时派单群聊、分群结算**：隐蔽性高



2.1.1 黄牛召集用户薅取国补商品案例分享

黄牛在社媒、论坛等社交平台召集“贩卖国补资格用户”，引流至临时微信群，按照黄牛要求填写贩卖资格用户真实姓名及电话号码，而收货地址从黄牛所提供地址库选取，以货到付款下单。

表面上看，这是惯用的回收手段，但实际上，黄牛联合“收货人”——即快递员违规验收设备快递，绕过政策监管回收国补。为规避监测，黄牛将派单与结算分群处理，1 - 2 天解散旧群、重开新群继续做单，增加了监管难度。



待黄牛签收后，接单用户进入黄牛专用结单群聊提供已签收截图和快递单号进行结算



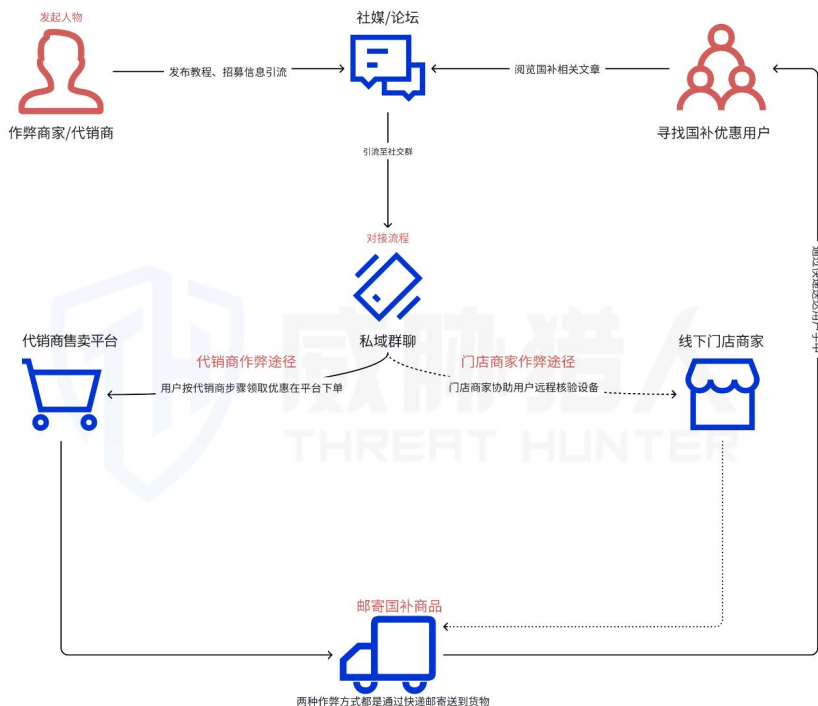
2.2 商家端作弊手法分析

威胁猎人研究发现，在国补监管政策下，有部分商家在明知违规的情况下，仍然会协同消费者实施套利。商家主要利用以下特点获利：

- **远程核验/虚假以旧换新：**利用政策漏洞规避监管
- **社媒引流：**标签话题群体引流，消费率高

商家端协助作弊手法上，一般分为线下门店商家以及线上经销商两种情况：

- 1) 实体商家远程非本人异地代激活，提高产品销量
- 2) 线上经销商代经销商虚构以旧换新流程，骗取双重补贴



2.2.1 商家端协助用户作弊薅取国补商品案例分析

1) 商家远程非本人异地代激活

按照国补监管政策，线下门店购买国补正常流程需购买者本人携身份证信息到场，门店商家核验身份一致并当场验机激活。但部分商家却通过微信视频远程让购买者扫码激活设备，然后以快递配送至购买用户地址。以此绕过监管



2) 代销商利用三重叠加优惠的国补

据调研，某些线上经销商以“三重优惠”低价贩卖国补商品，以此提高销量获取双倍收益。

代销商“三重优惠”包含：

1、个人用户正常国补补贴优惠

2、国补以旧换新补贴优惠

3、代销商提供平台优惠券

除此外某些代销商在“以旧换新”环节时作弊，以虚假回收旧品方式，让用户在选择“以旧换新”补贴时无需提供任何旧品回收凭证，也可享受该补贴。



另外代销商透露：若用户需购买异地国补商品，可寻找“枪手”（即异地国补地区、国补资格闲置的用户）代为下单，以此绕过国补 IP 地区限制。用户只需按此操作，再通过代销商渠道完成交易即可。

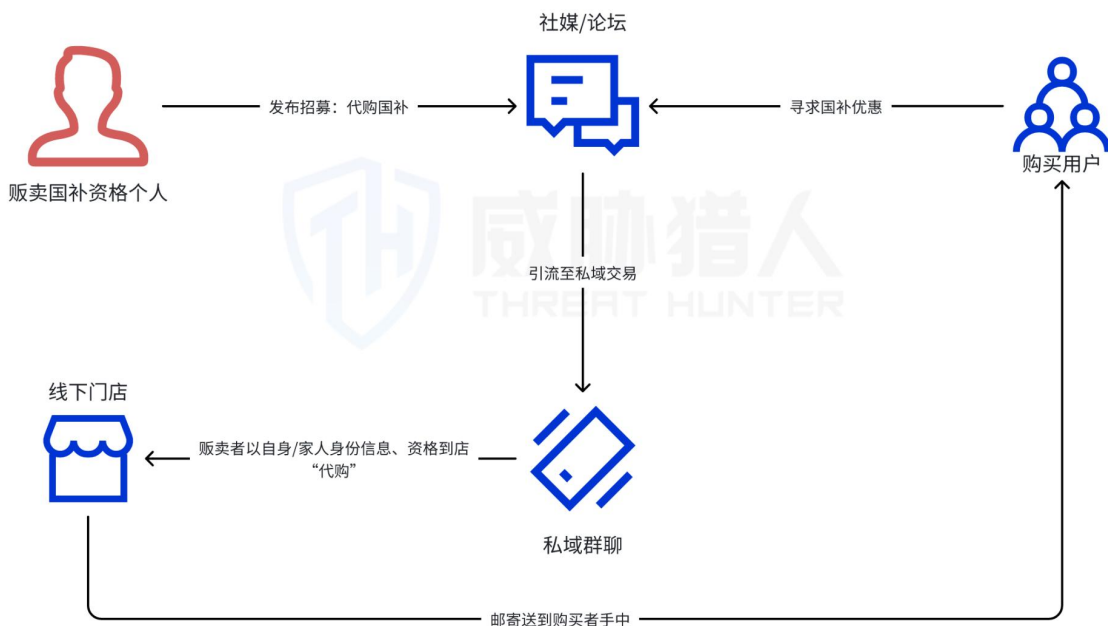


2.3 个人用户违规手法分析

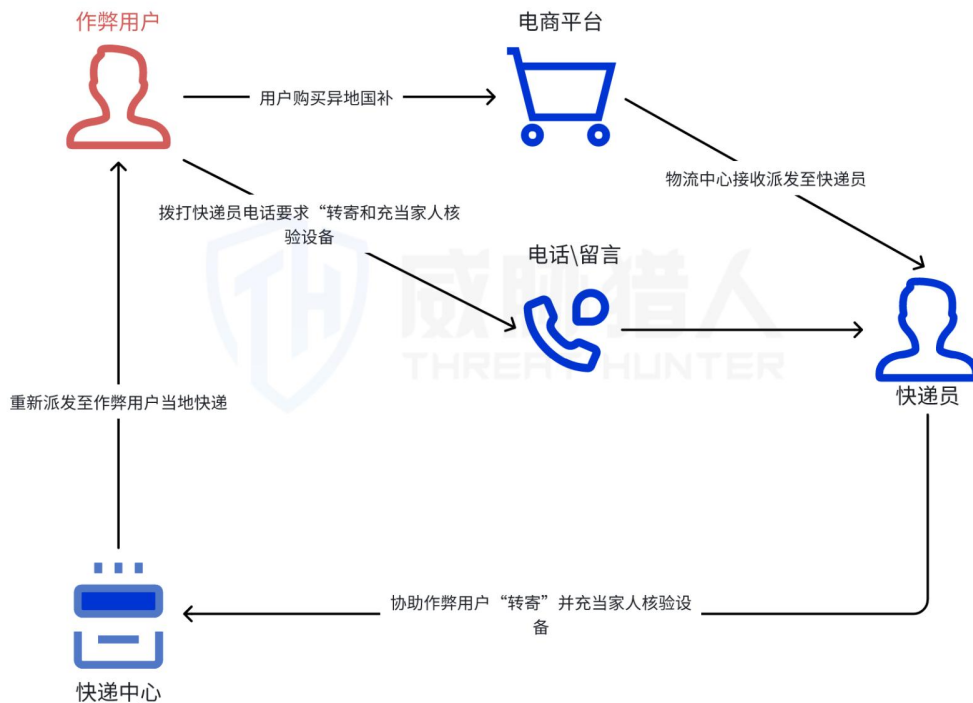
威胁猎人情报人员研究发现。在“国补作弊”的场景中，越来越多的真人用户通过研究和利用平台业务的“正当”规则进行恶意牟利。其中主要利用以下特点获利：

- **快递员协同“转寄”**：利用政策漏洞规避监管
- **个人自身信息代购**：监管难度高

个人贩卖国补资格流程图



用户伙同快递员协同“转寄”绕过监管



2.3.1 个人用户贩卖/作弊骗取国补商品案例分享

1) 用户以贩卖个人国补资格进行牟利

部分个人用户通过主动社交平台发布招募信息，转卖自身或家人的国补资格在线下门店以本人或家人身份下单购买国补设备、核验设备，最终以邮寄方式送达至需求者地址。以此收取一定的资格费用以及跑腿费。

江苏省昆山市国补数码代购

我把基本步骤，代购遇到的问题，码了个备忘录，截图成图二到图五嘞，感兴趣的看看吧

更新:

不代购了，放弃了，因为今天了解到好像很难代购，如图一，有的地方甚至要出示身份证，然后私戳了几个听起来是占用外省朋友国补资格的代购，售价一百大几十这样，不知道靠谱不，可能他们是经销商，有背景吧，我只能挨个打电话问有货吗

愚蠢的我甚至低估代问消耗时间，五块钱根本不够啊，我有个顾客帮问了一个半小时，但他一定要某型号某内存容量颜色，只能再拨别的店家，欲哭无泪

在这里打个广告，我还是可以帮代购三个手机，占用我家人的国补资格，如果店铺要出示身份证，还得再探讨下如何成功代购🤔🤔🤔以及其他数码，费用还是跑腿58，资格售卖220，可商议，运费自理。

上海代G

上海地区国补代购

1.具体流程：说明具体代办事情，按照代办事情的内容进行报价议价。

2.路费：单个地址8r，每增加一个地址多5r

3.代购费：商品价 8%

4.快递：默认顺丰快递到付，或者你指定快递

5.支付费用：需要提前支付（可走XY），已出发后跑单只退80%，，非特殊情况最晚第二天寄出

(PS):

1、不接受垫付，可以十V

2、代购商品不退不换

3、如果商家提供小票，随单寄送

4、出店以及到店都会发消息，各位宝子及时查看，跑单只退80%，出发两个小时不回消息默认跑单。

02-26

...

2) 用户联合快递员协同“转寄”绕过监管

此外，部分用户为了获取多个国补优惠，主动参与异地补贴套利，提供身份信息配合验证。他们还通过与快递员沟通转寄，绕过国补地区限制规则。部分用户刻意寻找可以转寄的快递公司，继而利用转寄完成绕过地区限制的操作。



在套取国补产业链条中还有一个特别的参与者——片区的快递员，在前文提到绕过国补地区限制规则中，他们是起着关键作用的一环，负责帮助用户激活产品并协助用户转寄，最终将货物送到真实的货主地址处。

03 结语

在消费补贴政策的实施过程中，虽然国家和平台已采取多项防黄牛措施，但黑灰产仍通过精细化分工和协作，利用漏洞套取补贴，严重破坏了市场公平生态。

面对这一问题，各方需持续更新对黑灰产作恶的认知，不断强化监管和技术手段，以更好地维护公平的市场环境，确保补贴政策真正惠及广大消费者。



关注“威胁猎人”

公司官网: www.threathunter.cn

合作邮箱: Marketing@threathunter.cn