30岁的林某之前在上海从事快递工作，离职后自主经营一家快递驿站。期间，他发现快递系统存在漏洞：客户下单寄件，公司会给快递员一个单号，但若客户取消寄件，单号却不会被收回。该单号既未被使用，又已经形成，成为特殊的虚拟号。

2021年2月起，林某便想办法利用这个漏洞钻空子。他从上家以0.2~0.4元每单的价格购买大量此类未使用的快递面单，随后以0.9元每单的价格转卖给下家，赚取差价。快递员杨某某和严某则通过购买这类面单以骗取公司每单1.2元的派件费和0.7元的返利。

9月16日，上海市青浦区人民检察院以涉嫌诈骗罪对林某等三人提起公诉。据悉，截至案发林某等人共计使用快递公司非售卖的单号500万余单，致使快递公司损失人民币1200万余元。

“面单”黑产在快递行业并不是新鲜的事情。通常，快递包裹上都贴有一张“快递面单”，主要用来记录发件人、收件人以及货物种类等相关信息，其中还包含收件人的姓名、电话、家庭住址等隐私信息。未使用的面单可能被用于刷单，而已经使用面单则包含大量个人信息，一旦被盗取或被诈骗团伙利用。

第一财经记者从业内了解到，今年6月，余姚市公安局破获了全国首例利用木马软件盗取快递始发云仓快递面单信息案，抓获嫌疑人35名，涉案金额达3000余万元。

在这条新型侵犯公民个人信息的黑灰产业链中，快递面单信息被称为“料”。负责去各个快递始发云仓非法安装木马软件的被称为“马仔”，“马仔”一般会通过临时应聘的方式渗透进各地的快递始发云仓，或者利用一些快递始发云仓的防盗漏洞偷偷潜入，对这些快递始发云仓的电脑下手，安装特定的木马程序。在组织中，还有专门的技术人员，他们则为这些木马程序提供技术支持和保障。

当那些电脑被植入特定的木马程序后，只要经过它们处理的快递面单信息就会全部传输到“分包商”手中。最终，这些经过整理的公民信息就会经过“料商”转卖给诈骗团伙。

平均下来，一般一张快递面单，“马仔”会以1至2元的价格卖出，然后上家会层层加价，最后以5.5至7元的价格卖到境外“料商”手中。

除了盗取用户信息，空包刷单也是常见的快递黑产链条。在2020年，无锡警方破获了一起网络贩卖快递单号案件，两名犯罪嫌疑人在两年时间里，贩卖了约6亿条快递单号。空包通常用在网店刷交易量时使用。在没有商品交接的情况下，完成网购的流程，也就是俗称的刷单。此外警方约谈了涉及此案的9家快递公司相关负责人

，要求他们加强内部管理，禁止再销售空保单号。

对此，浙江大学国际联合商学院数字经济与金融创新研究中心联席主任、研究员盘和林对第一财经记者表示，快递黑产有些是围绕快递物流的用户信息将用户信息转卖获利，有些是通过快递物流信息来刷单，比如有些网店利用虚假交易的快递单号来伪造交易。当前电商平台都有物流追溯，所以空包刷单依然存在，也有快递员和商家联合弄虚作假，还有些人通过快递刷单这个由头来欺骗普通人，想要刷单赚钱最后反而下单被骗钱。

盘和林表示，案例中利用快递企业系统漏洞的黑产其实并不普遍，因为管理较好的快递公司一般不会出现这种情况，快递公司系统识别出是真实交易还是虚假交易，只要通过用户款项实际到账就能够确认，且物流系统普遍是可以对快递路径进行精准追踪，所以规范的快递公司很少会出现这类系统漏洞。这些漏洞的形成或是因为部分快递公司自身IT系统建设存在欠缺。

对于黑产链条中空包、制作假物流路径等方式实现刷单的情况，盘和林表示只要将物流订单的流程里将用户支付款项纳入到流程当中，总部统一收款，按照单个订单各个环节精准结算，就不会出现快递员刷单的问题。