要求『别发货』却已被『签收』出口商邮箱被黑未收到货款

法院：承运人应承担赔偿责任

□ 见习记者 王葳然 通讯员 姜圣芃

黑客入侵电子邮箱，欺骗收货人向错误的账户支付货款。意识到上当受骗后，托运人多次要求承运人不要放货，防止损失进一步扩大，但货物早在运抵目的港后就进行了交付……

近日，上海海事法院审结一起因伪造电邮方式跨境实施对国内贸易出口商欺诈而引发的无单放货纠纷案。

案件回顾>>>

2023年9月，一科技公司委托一国际运输公司的宁波分公司，从中国宁波向西班牙巴塞罗那海运出口一批货物。收货人西班牙某公司与科技公司之间存有长期货物出口销售贸易业务往来。

国际运输公司作为运输公司的签单代理，签发已装船正本提单承运这批货物。一式三份全套正本提单由科技公司持有。

2023年8月底至9月初，科技公司销售部经理发现自己的办公电脑出现故障无法开机，于是联系外包服务商进行维修。不久后，西班牙某公司收到该销售部经理的邮箱地址发来的电子邮件，该邮件发送了涉案货物全套资料，并称收款银行更改为境外某银行，要求根据所附账户支付货款。

同年9月中旬，西班牙某公司根据邮件所附银行账户汇付货款，后因存在疑虑暂停转账，但为时已晚，最终仅有少量资金被追回。科技公司于10月28日告知西班牙某公司，前述收款银行信息不正确，且其电脑及所属邮箱已遭黑客攻击。后经报警调查发现，该邮箱在涉案期间曾多次于新加坡、瑞士、英国、美国等IP地址进行异常登录。

因为没有收到西班牙某公司的货款，自同年10月29日起，科技公司多次要求不要放货并催促安排货物退运船期。然而，10月22日承运船舶驶抵巴塞罗那后，涉案集装箱货物于10月25日重箱离场并于10月30日空箱返回。科技公司发现涉案货物在目的港已被放行及提取，西班牙某公司已收到涉案货物但因邮箱遭黑客入侵事件而拒绝支付货款。

科技公司于是将国际运输公司、国际运输公司宁波分公司、运输公司一并诉至法院，要求三被告赔偿货款损失。

法院经审理认为，承运人依法应当凭正本提单放行货物，或是在电放操作模式下凭托运人电放指示、通知或保函放行货物。该案中，原告科技公司因黑客入侵事件不能收悉货款，其一再向被告运输公司强调不得放行货物。被告运输公司没有按原告要求不得放行货物，且在已向原告出具并交付涉案正本提单的情形下，在目的港仍向收货人整箱交付涉案货物，由此导致原告丧失涉案货物控制权。因此，原告作为托运人可以要求被告运输公司作为承运人承担由此造成货款损失的赔偿责任。其他两名被告（国际运输公司及其宁波分公司）作为签单代理和货运代理，无证据证明在签单及订舱事务中存有过错而导致货款损失，法院对科技公司主张两名被告连带赔偿涉案货款损失不予支持。

综合案件查明事实后，上海海事法院判决被告运输公司作为承运人承担涉案货款28万余元的赔偿责任。本案判决现已生效。

说法>>>

承运人应当依法履行凭正本提单或电放指示、通知和保函放行货物之义务，但在近年来的国际贸易中，网络欺诈事件时有发生，而直接“黑化邮箱”是实施手段中的一类。本案中，黑客通过直接入侵企业邮箱掌握交易进度及往来文件资料以寻找可乘之机，并另行通过“黑化邮箱”更改或设立账户诱导汇付货款。

● 出具提单承运货物的承运人有义务按照合同约定及法律规定交付货物

提单是证明海上货物运输合同和货物已由承运人接收装船及保证据以交付的单证。出具提单承运货物的承运人有义务按照合同约定及法律规定将货物在目的港凭提单，或凭托运人指示、通知和保函等交付货物。

承运人若有违前述义务造成托运人或提单持有人货款损失的，应按照货物装船时的价值加运费和保险费加以赔偿。

● “黑化邮箱”的可信度更高、欺骗性更强

较之以往“高仿邮箱”“相似账户”等欺诈手段，“黑化邮箱”的欺骗性更强。国际贸易网络欺诈事件的行为实施地、更改或设立账户所在地等，往往都位于境外，有时处于多个不同国家和地区。一旦发生类似事件，无论基于贸易合同还是运输合同，都将给外贸企业维权和追款造成一定困难。

● 外贸企业应加强网络安全管理，增强自我风险防范意识和能力

外贸企业应加强网络安全管理，定期检查网络安全状况，强化业务内部管理，完备货款支付条款，细化资金审批流程。特别是在款项结算过程中，若需更改收款账户信息的，应通过书面形式予以明确指示，并通过微信、邮件、电话等多重方式进行确认货款结算事宜，切记不得过分依赖网络或惯例。外贸企业在平时也应多关注反诈宣传，对此类行为提高警惕，增强自我风险防范意识和能力。

14万元赃款经套路 “秒变”燕窝订购款

警方火速拦截成功阻止诈骗赃款洗白

□ 记者 季张颖

受害人手机黑屏后被“客服”隔空转走14万元，赃款转至一经销商账户后竟成为了“燕窝订购款”。近日，上海崇明警方成功阻断一起诈骗分子骗钱、洗钱的电信网络诈骗案件，为受害人追回被骗款的同时，及时阻止燕窝经销商发货，避免其沦为洗钱帮凶。

误开通直播会员？客服来电协助取消

5月29日上午，崇明区长兴镇居民张女士接到自称“某视频网站官方客服”的来电，对方声称其“误开通”了价值9600元/年的直播会员服务。为增加可信度，“客服”诱导张女士访问仿冒的该网站官网，在线“客服”随即发来盖有“公章”的电子账单。

“看到白纸黑字的扣费协议，我整个人都慌了。”张女士回忆，对方趁其慌乱时，要求下载“服务通”APP，便于帮助她“远程协助取消”。正当张女士下载完该软件并打开读取权限，准备询问下一步操作时，手机竟然黑屏了，任凭她怎么操作都无法打开手机画面。此时，张女士意识到自己可能被骗，急忙向派出所电话求助。

民警在电话里让张女士停止操作，并立即拔除电话卡，待赶到后查询发现，张女士的手机银行已被转出14万元。经反诈中心调查，该笔资金已经流向外省某燕窝专卖店对公账户，随即启动警银联动机制，将该笔资金冻结。

燕窝大额订单背后竟是洗白的赃款

民警当即联系到燕窝专卖店店主陈先生。陈先生电话里表示，一周前的确有一陌生客户联系过他，说要订购一批燕窝，两人谈妥价格后互加了微信，对方问他要了银行账号，并给了他一个地址，说是过几天会有一笔钱打到他的账户上，让陈先生收到钱后准备好等价的燕窝向这个地址发货。

陈先生虽然做生意心切，但在接到民警电话后立即停止了发货。发现账上的货款被冻结后，陈先生当时还通过电话、微信询问客户原因，客户却一直没有回复他。

5月30日，民警赶到该燕窝专卖店，向陈先生当面询问情况。陈先生出示的聊天记录显示，诈骗分子使用企业微信与其沟通，提供的营业执照、身份证均为伪造，送货地址也只是一个物流集散地。“对方给的采购价高于市场价10%。本以为接到一笔大单，没想到这笔钱是诈骗分子骗来的赃款。”陈先生说。

民警向陈先生解释，诈骗分子为了隐蔽诈骗钱款来源，会专门物色销售高价值、易变现货物的商户，然后将诈骗来的钱款直接转入商户经营者的账户内充当货款，拿到货物后再以低于市场价快速卖出，达到快速洗白赃款的目的，而商户经营者无意中成为了诈骗分子利用的洗钱工具。所幸，该案中该批货物尚未发货，14万元也成功冻结追回。

据办案民警介绍，该类诈骗团伙形成完整犯罪链条：话务组负责钓鱼骗钱、技术组开发“木马”、物流组负责销赃洗钱。这次如果不是商户尚未发货，资金极可能通过燕窝变现流失。目前，该案件正在进一步侦办中。

警方提示：市民切勿点击安装陌生人提供的APP链接，遇到手机异常黑屏，应立即断网并报警。商户经营者对“不见面的大额订单”要保持警惕，核实对方经营资质，收到陌生账户转账时，应确认资金来源的合法性。

责任编辑/徐荔 E-mail:fzb_zhoukanbu@163.com