利用分期付虚假交易帮人套现925万

男子犯非法经营罪被判刑

现代快报讯（通讯员 李星 吴云 记者 庄剑翔）如今，“月付”“分付”等互联网消费信贷产品广泛普及，为群众日常消费提供了便利。虽然此类信用额度仅限真实合规消费场景使用，严禁虚假交易、违规变现。但仍然有人钻空子，非法为他人套现。近日，仪征市检察院依法办理一起利用空包刷单、虚构交易套取网络消费贷的非法经营案件，被告人童某某因犯非法经营罪被判刑。

在走上违法犯罪道路之前，童某某就在做套现生意。一开始，他帮人用购买实体商品的方式套出钱款，从中收取手续费。2021年起，他发现不用发生实质性交易就能套出分期付中的钱，于是动起了歪心思。童某某组建了专门的团队，在网上开设了一家“皮包店铺”。

有套现需求的顾客在其店铺中用分期付下单购买根本不会发货的“商品”。整个交易全程无真实商品流转，商铺仅做虚假发货处理，客户随即点击确认收货，平台信贷额度自动划转至涉案店铺账户。店铺扣除双方约定的手续费后，剩余资金经童某某流转返还至客户手中，从中赚取虚假交易额3%左右的差价利润。这一操作，其实就是将POS机套现的手段用在了线上。

经查明，2023年2月至2024年3月期间，童某某团队通过上述虚假交易模式，累计套现网络消费信贷资金高达925万余元，非法获利4万余元，长期违规从事资金支付结算业务，严重扰乱金融市场秩序。

检察机关审查认为，被告人童某某未经国家金融监管部门批准，伙同他人以虚构交易、虚假刷单、空单回款等方式，为不特定对象套取网络消费信贷资金，变相从事非法资金支付结算业务，情节严重，其行为已构成非法经营罪。结合其犯罪数额、认罪悔罪态度、退赃退赔等情节，检察机关依法精准提出量刑建议，最终被法院全部采纳。

近日，童某某因犯非法经营罪，被法院判处有期徒刑一年三个月，缓刑一年六个月，并处罚金十万元。

伪装高收入群体，3人租宝马行窃落网

5月21日，据海峡导报，“五一”假期前夜，一辆藏青色宝马车上，孙某与两名同乡谈笑风生，三人带着在省外流窜作案牟取的财物现金，来到厦门挥霍消遣。

5月1日，经历整日的高额挥霍，囊中见底的孙某一行决定在厦门找个地方再次下手。孙某认为位处西北部同安老城，街巷交错、地形蜿蜒，恰恰方便掩人耳目、下手作案。遂于2日凌晨，几经兜兜逛逛后瞄上了一个目标。孙某三人分工明确，两人行窃作案，一人外围望风。在寻找下手目标过程中，孙某等全程刻意埋首低头企图逃避。孙某再一度凭借自己拿手的“钩门”绝技，飞速破开街边一辆宝马车门，一举盗空车辆中控台上的两千元红包现金。

得手后，孙某将被盗宝马“恢复如初”，直接弃置了案前租借的宝马，三人连夜分头逃离厦门。直到2日晚间，车主郑先生外出用车才发现钱财失窃。“因为车里放了钱，我反复回忆，确定我把车锁得好好的，这帮贼太猖狂了！”接警后，同安分局祥平派出所民警连夜启动研判，迅速理清线索链条。那台自认高明的宝马车，反而成了“贼喊捉贼”最显眼的标签。

自5月3日起，祥平派出所联合分局刑侦大队展开跨市追缉。从行动当日傍晚到次日凌晨，分三路逃窜的孙某等三人，相继落网。据孙某到案后供述，“租宝马”这一招，是他们自认整个作案过程最高明的一环。伪装高收入人群，以干扰警方侦查视线。孙某等三人到案后，退返郑先生全额损失。目前，该案件正在进一步依法侦办中。

据九派新闻

电梯装醉拖时间，同伙偷装摄像头

三人合伙潜入女子家装偷拍设备

坐电梯遇上醉汉耍酒疯，原以为是偶遇，不料居然是一场精心设计的“偷拍局”。近日，深圳市人民检察院公布了一起三人合伙，潜入女子家安装偷拍设备的案件。

事情还得从2025年4月的一个晚上说起，被害人宋女士像往常一样下楼扔垃圾。返回时，她看到两名陌生的醉酒男子在电梯口耍酒疯，手舞足蹈并乱按电梯，其他邻居也都无法进出电梯。

混乱持续了几分钟，这两名男子才貌似突然意识到自己走错了单元楼，相互搀扶着蹒跚离开，宋女士这才得以顺利坐上电梯回到家中。正嘀咕着这次奇怪的“电梯酒疯子”事件时，宋女士竟然无意间在家中置物架上的盒子中发现了一个隐蔽的摄像头，不禁大惊失色。

回忆起自己刚才出门时，想着短短几分钟时间就能回到家里，所以只是虚掩上房门。想到这里，警觉的宋女士立即联想到方才电梯口两名陌生男子的异常行为。“这两者之间会不会有联系？”宋女士立即找到小区物业管理公司帮助调出监控，果然发现端倪。监控显示，那两名男子貌似醉酒蹒跚地离开小区大门后，迅速恢复正常人行走姿态离去，根本没有醉酒。

深感居住安全被侵犯的宋女士立刻报警，涉案的“醉酒”男子甲某（化名）及其同伙乙某（化名）、丙某（另案处理）很快落网。经查，甲某此次受人委托私下调查宋女士。在前期掌握了宋女士基本外出规律后，案发当日他发现宋女士临时离家未锁门，于是就立即安排同伙乙某潜入宋女士家中安装监控摄像头，自己则拉上司机丙某自导自演了一场“电梯醉酒戏”，拖延宋女士的回家时间，以便让乙某安全脱身，未曾想这么快就被宋女士识破。福田区检察院经审查后认定，甲某及其同伙无视公民合法权益，未经同意私自进入他人住宅并安装摄像头进行偷拍，已严重侵犯他人居住安宁，构成非法侵入住宅罪，依法对甲某、乙某提起公诉。法院经审理，以非法侵入住宅罪分别判处甲某、乙某有期徒刑六个月。

据深圳市人民检察院公众号

协助企业将超标电动车卖给骑手从中牟利

深圳5名外卖站站长及负责人被刑拘

广州交警近日披露广州首例即时配送站点负责人因涉嫌重大责任事故罪被依法刑事拘留的案情，引起外界关注。

记者查询发现，因协助违法企业将超标电动车销售给骑手并从中牟利，深圳5名外卖站站长及相关负责人涉嫌销售伪劣产品罪被刑拘。

据微信公众号“深圳交警”5月19日消息，近日，深圳龙岗交警在查处某企业售卖不合格电动自行车案件中深挖溯源，查实多家外卖平台站点向该企业采购超标车辆并售卖给骑手，且已有多名骑手驾驶该类违法车辆上路配送，并相继引发道路交通事故。

涉案外卖站点站长、负责人明知车辆不合规，仍受利益驱使，协助违法企业将超标电动车销售给骑手并从中牟利，其行为已涉嫌销售伪劣产品罪。目前，龙岗交警已依法对涉案五名站点站长及相关负责人采取刑事拘留强制措施。

消息称，伴随行业快速发展，部分骑手出现闯红灯、逆行、超速等违法行为，部分平台站点更是漠视安全，默许甚至要求骑手使用非法改装电动车、三轮车。针对此类情况，深圳交警强化专项管控，压实平台及站点主体责任，对涉外卖、快递的交通事故，严格溯源倒查，严肃追究主体责任。

自4月4日开展涉快递、外卖等行业“斩源”专项行动以来，深圳交警已依法刑事拘留5人、行政拘留37人，完成事故溯源定责43宗，关停违规站点2个，有力整治行业交通乱象，进一步规范电动车通行秩序，筑牢道路交通安全防线。

据澎湃新闻

酒驾撞车听朋友劝，掏10万私了

原来朋友和对方司机是一伙，涉嫌敲诈罪已被起诉

“还是私了吧，酒驾是要‘进去’的……”听着高某的劝说，秦先生无奈同意花10万元“平事”。但事后回想，这场酒局和交通事故都透着蹊跷，秦先生于是决定报警，最终查明这是一场连环诈骗。近日，北京海淀检察院通报了该案。

秦先生和高某在网络相识。去年11月的一天，二人相约在烧烤店聚餐。饭桌上，高某频频劝酒，热情至极，秦先生碍于情面，难以推辞，接连饮下数杯。酒足饭饱后，秦先生原本打算呼叫代驾，前往附近宾馆休息，可高某百般阻挠，以“路程极短”“代驾麻烦”为借口，极力怂恿秦先生自行驾车。在高某持续鼓动与劝说下，秦先生心存侥幸，最终坐上了驾驶座。

谁料车辆刚驶出约100米，后方一辆轿车突然强行并道、违规超车，与秦先生的车辆发生剐蹭。对方车主马某与同行男子下车后，先是赔礼道歉，可察觉到秦先生身上散发着酒气后，立刻变了脸色，一口咬定秦先生酒后驾车，更扬言要立即报警处理。此时，同行的高某故作“好心”，提醒秦先生酒后驾车可能面临拘留处罚，顺势提议私下解决。在几人一唱一和、步步紧逼之下，秦先生瞬间陷入恐慌。

协商过程中，高某与马某还故意上演“争执”戏码，刻意将事态“升级”，进一步施压秦先生。走投无路的秦先生，最终被迫同意“私了”，向对方赔偿10万元并签订“交通事故调解书”，高某甚至“假仗义”地帮秦先生承担了7000元。

示意图 视觉中国供图

可事后，秦先生越想越觉得疑点重重，随即向警方报案。警方侦查后，真相浮出水面：这并非一起普通的交通事故，而是高某与马某等人精心策划的“碰瓷”局——高某负责劝酒，诱导秦先生酒驾，马某负责制造事故、言语威胁，几人利用秦先生酒驾后不敢报警的心理，联手实施犯罪。

检察机关认定，高某等人构成敲诈勒索罪，且数额巨大。目前，该案已由海淀检察院依法向海淀法院提起公诉，案件正在进一步办理中。

检察官警示，一旦触碰酒后驾车的红线，不仅会面临严厉的法律处罚，更会沦为犯罪分子瞄准的“猎物”。坚守“酒后不开车”的底线，既是守护自己与他人的生命安全，也能从根源上斩断不法分子的黑手。

同时，检察官建议，对待网络相识的“新朋友”，务必保持清醒认知与高度警惕，真正的挚友会为你的安全保驾护航；虚假“热情”的背后，往往暗藏精心设计的陷阱。如果不慎落入陷阱，检察官提醒，要保持冷静，第一时间拨打报警电话，如实说明情况，勇敢维护自身合法权益，同时在确保自身安全的前提下，可对协商过程、对方威胁言论进行录音录像，固定关键证据。

据北京晚报

“银狐”木马出新变种，陌生文件要小心

5月21日，国家计算机病毒应急处理中心和计算机病毒防治技术国家工程实验室依托国家计算机病毒协同分析平台，捕获多款以“内部调查结果”“违纪名单”“裁员补偿”等为文件名的恶意程序，这类程序伪装成各类常用文件，实为针对Windows用户的远程控制木马，均是针对我国用户的“银狐”木马最新变种。用户一旦不慎点开运行，设备便会遭不法分子远程操控、信息被窃取，还极易被不法分子当作实施电信网络诈骗的作案跳板。

本次发现的木马病毒新变种继续采用钓鱼欺诈手段，大量采用人事业务相关的诱导性文件名，文件名以“××季度违纪名单”“通报人员信息”“裁员名单”“补偿方案”等为主，并将图标伪装成文件夹、快捷方式、回收站等，并添加“pdf”后缀迷惑用户。木马病毒运行后，会在“C:\Program Files\Internet Explorer\”文件夹下投放下一步所需的载荷文件。其中关键文件log.dll为下一步运行的加载器，该dll文件通过白文件installer.exe进行加载。

“银狐”系列木马病毒攻击活动与电信网络诈骗活动联系密切，长期将我国用户作为攻击目标，具有变种速度快、隐蔽性强等特点。本次发现的病毒木马攻击活动的攻击目标较为广泛，重点针对具有一定规模的组织机构工作人员，特别是人事相关业务工作人员，主要目的仍然是通过木马病毒控制大量受害者主机，窃取受害企业敏感数据和公民个人信息，进而实施勒索或欺诈。建议采取以下综合防范措施。在使用即时通信工具或电子邮件处理工作事务期间，警惕新增临时工作群组和电子邮件中传播的“违纪”“裁员”等相关主题文件，拒绝点击陌生人发送的文件，对本单位或外单位同事发送的相关文件应与其本人或正式渠道核实。用户可将可疑的文档文件、可执行文件、压缩包文件或解压后的可疑文件先行上传至国家计算机病毒协同分析平台（https://virus.cverc.org.cn）进行安全检测。一旦发现本人即时通信工具或电子邮件发生被盗用现象，应立即停止使用可能感染病毒的计算机设备，将其断开网络连接，对相关计算机设备进行杀毒和安全检查。

据央视新闻