

长宁检察院发布《“互联网+生活性服务业”常见刑事法律风险防控提示》

27项风险提示直击互联网服务业“痛点”

现状：

涉互联网企业
刑案大幅增长

据《风险提示》显示，2016 年 1 月至 2019 年 9 月，长宁检察院共办理涉互联网企业刑事案件 212 件 321 人。检察官分析，由于互联网犯罪成本低、隐蔽性强、辐射面广，成为一些不法分子的犯罪新渠道，新型互联网犯罪案件逐年攀升并呈现一些新特点。

自 2016 年以来，涉互联网企业刑事案件数量大幅增长，涉案人数明显上升，共同犯罪情形突出。其中，2016 年 13 件 20 人，2017 年 30 件 52 人，2018 年 75 件 135 人，2019 年 1 月至 9 月 94 件 114 人。

其次，侵财类刑事案件占比高。盗窃、诈骗等传统侵犯财产类案件最为常见，占 72.6%。

此外，作案人员呈现低龄化趋势，学生群体涉案比例偏高。在所有涉案人员中，共有未成年人 15 名，多为近两年内发案，罪名以诈骗为主；学生群体涉案比例较高，达 51

人，主要为大中专院校学生。以上群体存在较高接触网络不良信息与犯罪手法后产生投机心理而违法犯罪的风险。

企业员工内外勾结作案情况较为常见。诈骗类、侵犯公民个人信息等案件中，企业员工利用职务便利与他人里应外合进行作案的情况时有发生。

除了上述特征，还有一些涉互联网企业的新类型案件也不容忽视。长宁检察院就办理了全市首例职业索赔人敲诈勒索案，不法分子抓住企业害怕被投诉、“花钱买太平”等心理，以反复“举报、投诉”为手段向超市、亲子教育机构等多家被害单位施压，进而索要“顾问费” 5.6 万余元。该案反映出企业经营不规范，被抓住把柄后又急于“私了”，而职业索赔人利用了这一点进行非法牟利，与正常的消费者维权存在本质区别。

新型欺诈：

利用“闪退”
申请退款诈骗

近年来，“无人收款”或“自助缴费”模式逐渐被商家和消费者所接受，但也有不法分子通过多种手段“钻空子”。

2018 年 11 月至 2019 年 5 月期间，蔡某某等人通过“未扫描商品条码”“夹带”“扫描商品再取消”等方式，谋取利益。经检察机关起诉，被法院判处盗窃罪。检察官建议企业要不断创新安防科技手段、对消费者引入“征信评级”、提升员工安防责任意识等。

还有不法分子利用电商平台推出的便利消费者相关服务来实施诈骗等违法犯罪行为。

2018 年 9 月间，应某利用某平台“闪退”功能申请退款，得款后未将商品退回商家，骗取物品。

经检察机关起诉，应某被法院以诈骗罪定罪量刑。检察官认为电商平台应该加强用户信用体系建设，同时建立预警机制，利用大数据技术及时发现异常订单与账号，减少损失。目前，此类案件呈高发态势，该院在办案件有 21 件 24 人，案值最高的达 30 余万元。

不法分子的作案手法“五花八门”。2016 年 12 月，徐某编写了一款名为“小白改机”的软件，该款软件具有篡改手机设备信息的功能，使平台无法识别是否是新号码注册，从而使得用户可以无限次享受该平台每次 10 至 20 元不等的首次下单优惠，造成企业蒙受损失。

检察机关对徐某以提供侵入、非法控制计算机信息系统程序、工具罪起诉，获法院判决支持。检察官分析，互联网企业应加大研发力度，堵住技术安全漏洞，建立异常行为的发现和处理机制，与公安、司法机关以及相关部门加强配合，共筑网络安全生态。

利用技术漏洞：

网约车平台成
“生财之道”

据检察机关披露，随着互联网产业蓬勃发展，一些不法分子利用互联网企业平台管理漏洞实施犯罪的案件也随之逐年上升，并出现了职业化倾向，已然形成黑色产业链条。

在一起非法获取公民个人信息、敲诈勒索案中，刘某利用被害公司员工无意中泄露的邮箱密码，采用黑客技术手段非法侵入某公司计算机信息系统，窃取大量客户信息，后又以出售信息为要挟勒索公司钱财。目前，检察机关已对刘某提起公诉。检察官提醒，公司应提升员工的保密意识和网络安全风险意识，建立有效的网络安全监测和通报预警系统，采取严格的页面和数据加密措施，提高对网络攻击的溯源能力。

一些“网约车”平台成了某些不法分子的“生财之道”。2018 年 3 月至 7 月期间，余某某通过微信接单，为乘客提供代

打车服务并收取低于实际的打车费用，其后不支付网约车平台车费。经检察机关起诉，余某某被法院以诈骗罪判刑。对此，检察官建议企业优化平台系统，建立预警机制，提升反作弊能力，对于交易异常情形存在违法犯罪嫌疑的，应立即向公安机关报案。

另外一起案例中，潘某在 2016 年 1 月至 5 月间使用境外银行信用卡在网络平台上预订机票，随后通过改签的方式换票或退票，之后向银行提出交易异议，拒付机票费用。检察机关以诈骗罪起诉潘某，获法院判决支持。检察官提出建议，企业一方面应提高异常数据的检测能力、分析能力，降低恶意拒付风险；另一方面要引进高效的信用卡安全服务商，缩短对欺诈交易的调查及反应时间。

“监守自盗”：

互联网企业
内部人员“钻空子”

检察官在办案中还发现，互联网企业内部也存在管理风险。比如员工伪造证件，利用职权便利泄露企业数据信息等，通过资源倾斜获取非法利益，破坏公平竞争环境等。

长宁检察院之前受理过不少此类案件。2017 年 6 月至 2018 年 4 月间，何某为完成公司业绩考核以及获取额外收入，伙同外部人员先后伪造、变造 42 份工商

营业执照后上传到其公司平台，公司未尽到对材料真实性、有效性的严格审核义务，导致 10 余家没有合法证照的商户在平台上线。何某等人被追究伪造、变造国家机关证件罪的刑事责任。

还有一些外卖员因使用外挂软件在外卖平台上频繁抢单被平台封号后，伪造身份证件，再次注册账号成为该平台外卖员，并接单进行跑腿业务，被法院判处伪造身份证件罪。针对此类案件，检察官建议网络订餐平台应尽到调查入网经营者的地址及证件真实性等义务，确认相关信息真实有效，同时紧抓在岗人员的培训，确保操作规范。

除此之外，有些网购平台员工还利用职务之便收受贿赂，被法院判处受贿罪。比如黄某某在 2015 年 11 月至 2016 年 7 月期间，利用职务之便，非法收受商户贿赂共计 20 余万元；2016 年 6 月至 2017 年 11 月间，邹某利用职务之便，非法收受他人给予的好处费 49 万余元。

检察官对企业提出相关防控建议，一方面要在员工入职培训和在岗培训中强化法治教育；另一方面要加强内部安全稽查、风险控制等监督制约机制建设，建立企业与司法机关的“亲”“清”关系，实现良性互动。

11 月 21 日，记者从上海警方获悉，警方成功捣毁一特大电信网络诈骗团伙，抓获犯罪嫌疑人 101 名，查冻涉案资金 1400 余万元，涉案金额 3500 余万元。警方表示，该案系今年以来本市涉案金额最大的一起电信网络诈骗案件。

市公安局 供图

