

“互联网+生活性服务业”  
常见刑事法律风险防控提示  
(案例版)

长宁区人民检察院

2019年11月

# 前 言

在全球新一轮科技革命和产业变革中，互联网与各领域的融合发展已成为不可阻挡的时代潮流。自上海市首个“互联网+生活性服务业”创新试验区落户长宁以来，经过两年多的实践，区域“互联网+生活性服务业”发展驶入了“快车道”，长宁区正逐步成为上海“互联网+生活性服务业”企业集聚地、互联网新兴行业的制度创新策源地、风险投资遴选项目高地和成熟“互联网+”企业和 TMT（科技、媒体、通信融合）媒体进入上海的目标选择地。在以携程、拼多多、美团点评等为代表的龙头企业引领带动下，新兴业态层出不穷，“互联网+餐饮”、“+旅游”、“+物流”、“+文化”等各行业类型不断细分完善，相关产业集群呈现规模化、多层次蓬勃发展的景象。

近年来，长宁区人民检察院（以下简称“我院”）主动融入长宁发展大局，着力优化法治化营商环境，强化互联网企业权益保护，帮助企业堵漏建制，为“互联网+生活性服务业”健康发展提供优质检察保障，于 2018 年先后发布《关于充分发挥检察职能服务保障“互联网+生活性服务业”发展的实施意见》和《涉互联网企业刑事检察白皮书》，为“互联网+生活性服务业”发展建言献策，受到社会各界好评。在这一基础之上，今年，我院进一步总结提示各类互联网企业可能遭遇的刑事法律风险，在以案释法的同时为企业提供针对性防控建议，为企业规避风险及产业

健康发展保驾护航。

2016年1月至2019年9月，我院共办理涉互联网企业刑事案件212件321人，**呈现以下特点：**

**1. 受案数逐年上升。**自2016年以来，涉互联网企业刑事案件数量大幅增长，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，涉案人数明显上升，共同犯罪情形突出。

**2. 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%。作案手段往往构成破坏计算机信息系统类罪名或侵犯公民个人信息罪等罪名，但考虑到罪名竞合问题，最终依然认定为盗窃、诈骗等罪名。

**3. 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，多达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。

**4. 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。

# 案例一：何某等人伪造国家机关证件案

## 一、基本案情

2017年6月至2018年4月间，被告人何某在上海A公司业务拓展部工作期间，伙同他人先后伪造、变造42份工商营业执照后上传到公司平台，使10余家没有合法证照的商户违法在某外卖平台上线。

2017年2月至2018年6月间，被告人高某某在北京A公司业务拓展部工作期间，利用修图软件先后伪造变造8份工商营业执照上传到公司平台，使5家没有营业执照的商户在某外卖平台上线。

2017年10月至2018年4月间，被告人潘某某在B公司业务拓展部工作期间，利用Photoshop等修图软件先后伪造、变造41份工商营业执照上传到公司平台，使20余家没有资质的商户违法在某外卖平台上线。

## 二、司法处理

何某犯伪造、变造国家机关证件罪，被上海市长宁区人民法院判处有期徒刑三年，缓刑四年，罚金人民币五千元；高某某犯伪造、变造国家机关证件罪，被上海市长宁区人民法院判处有期徒刑一年，缓刑一年，罚金人民币一千元；潘某某犯伪造、变造国家机关证件罪，被上海市长宁区人民法院判处有期徒刑三年，缓刑四年，罚金人民币五千元。

### 三、风险提示

1. **网络食品交易第三方平台可能面临的行政风险。**根据《中华人民共和国食品安全法》第三十五条的规定，我国对食品生产经营实行许可制度。该法第六十二条规定了网络订餐平台必须履行对入网经营者实名登记和许可证审查义务，对入网经营者的违法行为负有阻止、报告和停止提供服务的义务，并对受损的消费者负有提供入网经营者真实姓名、地址和联系方式的义务。该法第一百三十一条规定，网络食品交易第三方平台提供者未对入网食品经营者履行审查许可证等义务的，由县级以上人民政府食品安全监督管理部门责令改正，没收违法所得，并处五万元以上二十万元以下罚款；造成严重后果的，责令停业，直至由原发证部门吊销许可证；……《网络食品安全违法行为查处办法》第三十五条规定，网络食品交易第三方平台提供者未设置专门的网络食品安全管理机构或者指定专职食品安全管理人员对平台上的食品安全经营行为及信息进行检查的，由县级以上地方食品药品监督管理部门责令改正，给予警告；拒不改正的，处5000元以上3万元以下罚款。该办法第四十三条规定，网络食品交易第三方平台提供者、入网食品生产经营者提供虚假信息的，由县级以上地方食品药品监督管理部门责令改正，处1万元以上3万元以下罚款。

根据以上法律规定，网络食品交易第三方平台未审查入网者许可证、未设置专人进行信息检查、提供虚假信息的，均可能受到行政处罚。

**2. 网络食品交易第三方平台可能面临的民事风险。**根据《中华人民共和国食品安全法》第一百三十一条第一款，网络食品交易第三方平台未履行相应审查义务，使消费者的合法权益受到损害的，应当与食品经营者承担连带责任。因此，消费者如果因为不合格商家的食品受到损害的，网络食品交易第三方平台要承担民事上的连带责任。

**3. 网络食品交易第三方平台可能面临的刑事风险。**《网络食品安全违法行为查处办法》第四十四条规定，网络食品交易第三方平台提供者、入网食品生产经营者违反食品安全法规定，构成犯罪的，依法追究刑事责任。具体到本案中，网络食品交易第三方平台的工作人员为了冲业绩，通过伪造、变造工商营业执照使没有资质的商户入网经营食品，其行为已经涉嫌刑事犯罪，而如果平台方在明知的情況下予以放任，则可能构成共犯。

**4. 网络食品交易第三方平台可能面临的商誉风险。**在前述三起案件中，三名员工为了完成公司业绩考核以及获取额外的收入，故意使用软件修改等方式伪造、变造工商营业执照，将一些不合格的餐饮服务提供者的材料提交公司。而公司未尽到审核义务，对三名职员提交的材料真实性、有效性未及时严格核查，导致数十家不合格的餐饮服务提供者进入某网络订餐平台，给食品安全以及消费者的身体健康造成极大的隐患，同时也将对公司的商业信誉和公众形象造成严重损害。

#### **四、防控建议**

**1. 严格入网审查。**根据《上海市食品安全条例》第五十三条规定，网络食品交易平台应当通过与监管部门的许可信息进行比对、现场核查等方式，对入网经营者的许可证件进行审查。网络订餐平台应当履行调查入网经营者的地址及证件真实性等义务，即要确认入网餐厅经营者姓名和许可证的信息真实有效。

**2. 规范日常检查。**《网络食品安全违法行为查处办法》第十四条规定，网络食品交易第三方平台提供者应当设置专门的网络食品安全管理机构或者指定专职食品安全管理人员，对平台上的食品经营行为及信息进行检查。专职人员不仅要负责食品经营行为是否符合法律规定，还要定期对已经登记的许可证等信息的有效期进行审查，对相关店铺的真实性予以核查，保证经营信息和经营行为均符合法律规定，保卫公众舌尖上的安全。

**3. 加强人员培训。**任何制度的落实离不开人，网络订餐平台竞争激烈，但任何市场行为均不能以损害消费者的利益为代价。为了使网络订餐行业科学有序健康发展，必须紧抓在岗人员的培训，让所有从业人员意识到规范操作的重要性，才能更好地将制度予以落实。

**4. 合理制定指标。**指标是考察员工业绩的重要依据，但唯指标论、忽视风险则会产生诸多问题。比如本案中，三名被告人为了完成指标不惜弄虚作假，触犯法律，最终受到了法律的制裁。网络食品交易第三方平台在制定业务扩张的指标时，应当明确必须遵守的行业准则，在弄虚作假等问题上必须一票否决，让员工

在开展业务的同时，守住底线，推动良性发展。

**附：相关法律法规：**

《中华人民共和国刑法》

第二百八十条第一款 伪造、变造、买卖或者盗窃、抢夺、毁灭国家机关的公文、证件、印章的，处三年以下有期徒刑、拘役、管制或者剥夺政治权利，并处罚金；情节严重的，处三年以上十年以下有期徒刑，并处罚金。

《关于本市办理部分刑事犯罪案件标准的意见》

一、关于伪造、变造、买卖国家机关公文、证件、印章罪，伪造公司、企业、事业单位、人民团体印章罪和伪造、变造居民身份证罪

伪造、变造、买卖国家机关公文、证件、印章三件以上的，处“三年以下有期徒刑、拘役、管制或者剥夺政治权利”。……

《中华人民共和国食品安全法》

第三十五条 国家对食品生产经营实行许可制度。从事食品生产、食品销售、餐饮服务，应当依法取得许可。……

第六十二条 网络食品交易第三方平台提供者应当对入网食品经营者进行实名登记，明确其食品安全管理责任；依法应当取得许可证的，还应当审查其许可证。



网络食品交易第三方平台提供者发现入网食品经营者有违反本法规定行为的，应当及时制止并立即报告所在地县级人民政府食品安全监督管理部门；发现严重违法行为的，应当立即停止提供网络交易平台服务。

第一百三十一条 违反本法规定，网络食品交易第三方平台提供者未对入网食品经营者进行实名登记、审查许可证，或者未履行报告、停止提供网络交易平台服务等义务的，由县级以上人民政府食品安全监督管理部门责令改正，没收违法所得，并处五万元以上二十万元以下罚款；造成严重后果的，责令停业，直至由原发证部门吊销许可证；使消费者的合法权益受到损害的，应当与食品经营者承担连带责任。

消费者通过网络食品交易第三方平台购买食品，其合法权益受到损害的，可以向入网食品经营者或者食品生产者要求赔偿。网络食品交易第三方平台提供者不能提供入网食品经营者的真实名称、地址和有效联系方式的，由网络食品交易第三方平台提供者赔偿。网络食品交易第三方平台提供者赔偿后，有权向入网食品经营者或者食品生产者追偿。网络食品交易第三方平台提供者作出更有利于消费者承诺的，应当履行其承诺。

#### 《网络食品安全违法行为查处办法》

第十四条 网络食品交易第三方平台提供者应当设置专门的网络食品安全管理机构或者指定专职食品安全管理人员，对平台上的食品经营行为及信息进行检查。

网络食品交易第三方平台提供者发现存在食品安全违法行为的，应当及时制止，并向所在地县级食品药品监督管理部门报告。

第三十五条 违反本办法第十四条规定，网络食品交易第三方平台提供者未设置专门的网络食品安全管理机构或者指定专职食品安全管理人员对平台上的食品安全经营行为及信息进行检查的，由县级以上地方食品药品监督管理部门责令改正，给予警告；拒不改正的，处5000元以上3万元以下罚款。

第四十三条 违反本办法规定，网络食品交易第三方平台提供者、入网食品生产经营者提供虚假信息的，由县级以上地方食品药品监督管理部门责令改正，处1万元以上3万元以下罚款。

第四十四条 网络食品交易第三方平台提供者、入网食品生产经营者违反食品安全法规定，构成犯罪的，依法追究刑事责任。

#### 《上海市食品安全条例》

第五十三条 网络食品交易第三方平台提供者应当建立食品安全管理制度，履行下列管理责任：

……

（三）通过与监管部门的许可信息进行比对、现场核查等方式，对入网食品经营者的许可证件进行审查；

……

## 案例二：仲某某等人伪造身份证件案

### 一、基本案情

被告人仲某某、赵某某、卜某某、彭某某使用本人身份证注册某网站外卖员，后因各种原因被网站封号。因无法继续使用本人身份证注册，为再次成为该网站外卖员，他们分别通过互联网向他人提供本人手持身份证的照片，伪造多张居民身份证件用于注册该网站账号，并在该平台接单进行跑腿业务。

### 二、司法处理

四名被告人均已被提起公诉。

### 三、风险提示

**1. 外卖员可能涉嫌犯罪的风险。**外卖员虚构代购物品的价格，自行打印购物小票，赚取差价，属于虚构事实隐瞒真相骗取他人财物，如诈骗数额较大，则构成诈骗罪。伪造身份证件电子图片用于外卖员账号注册的行为涉嫌伪造身份证件罪。外卖员通过自己的渠道采购烟酒、药品等需要行政许可才能经营的产品予以销售的，存在非法经营罪的风险。

**2. 食品、药品安全风险。**外卖员未遵循顾客指定地点购买，而是通过自己的渠道进行采购。例如，药品系从老家的药房购买，香烟系从小店批发，不排除买到假药、假烟的可能性，难以保障食品、药品安全，可能危及顾客健康。

**3. 外卖平台的商誉风险。**外卖员的代购行为均依托于外卖平

台，消费者受到损害首先想到的也是投诉网站，如果被害人通过网络自媒体等形式予以披露，势必对企业的商业信誉造成损害。

#### **四、防控建议**

**1. 加强外卖员注册及登录身份证验管理，提高注册成本和门槛。**严格审核用户注册、登录的身份验证程序，特别是对身份证信息的真实性进行审核，对于身份证照片重复性进行筛选，尽量从源头上杜绝虚假身份注册号的现象发生。

**2. 增强异常订单的识别能力。**涉案人员之所以伪造身份证电子照片进行注册，是因为使用外挂软件在外卖平台上频繁抢单，系统识别异常后对他们予以封号处理。企业应及时发现并修补系统漏洞，及时介入并限制抢单软件，必要时向公安机关报案。

**3. 加强与司法机关对接，建立违法犯罪行为的处置机制。**总结前期案件经验，查找漏洞并及时填补。加强与司法机关合作，配合公安、检察院调查取证，全面准确提供电子数据，详细解释交易流程和技术问题，协助打击违法犯罪，及时固定电子证据，屏蔽相关信息。

#### **附：相关法律法规：**

##### **《中华人民共和国刑法》**

**第二百八十条第三款** 伪造、变造、买卖居民身份证、护照、社会保障卡、驾驶证等依法可以用于证明身份的证件的，处三年以下有期徒刑、拘役、管制或者剥夺政治权利，并处罚金；情节严重的，处三年以上七年以下有期徒刑，并处罚金。

## 案例三：蔡某某等人盗窃罪

### 一、基本案情

2018年11月5日至11月8日，被告人蔡某某至本市长宁区长宁路某超市利用自助收银机，通过将未扫描结账的商品藏入已结账的商品里夹带离开超市的方式，三次窃取超市内的面包、排骨、牛奶等商品若干。

2018年12月25日至2019年1月15日，被告人俞某某在本市长宁区长宁路某超市通过自助收银机扫描商品后再取消支付价格较高商品的方式，将大量实际未结账的商品直接带离门店，前后共七次窃取门店内的牛、羊肉、银鳕鱼、男士精华液、牙膏、蜂蜜等商品，涉案价值共计8000余元。

2019年4月8日至5月12日，被告人张某某至本市长宁区长宁路某超市利用自助收银机，通过将未扫描结账的商品藏入已结账的商品里夹带离开超市的方式，五次窃取超市内的蜂蜜、牛排、对虾等商品若干，涉案价值共计7000余元。

### 二、司法处理

被告人蔡某某犯盗窃罪，被上海市长宁区人民法院判处拘役三个月，缓刑三个月，并处罚金人民币一千元；被告人张某某犯盗窃罪，被上海市长宁区人民法院判处有期徒刑七个月，并处罚金人民币一千元；被告人俞某某犯盗窃罪，被上海市长宁区人民法院判处有期徒刑八个月，并处罚金人民币二千元。

### 三、风险提示

随着科技的不断发展，商业模式也呈现多样化的趋势，其中“无人收款”或“自助缴费”模式因方便快捷、商业成本低等优势逐渐被商家和消费者所接受。风险与机遇并存，该模式在提供便利消费的同时，也不可避免存在监管的漏洞。“无人收款”或“自助缴费”主要存在以下风险：

**1. 消费者自身的信用风险。**诚信是一切交易的基本原则，自助缴费模式提升了用户购物体验、降低了企业经营成本，但同时也放大了信用风险敞口，一旦有不法分子起了歹念，很容易使企业的财产受到损失。

**2. 劣币驱逐良币的风险。**一旦不法分子“顺手牵羊”却得不到法律的制裁，那么对于诚实消费的顾客来说是不公平的。“顺手牵羊”大行其道，不仅有违社会主义核心价值观，也会使得新兴的经济模式遭受重创，不利于产业升级和发展。

### 四、防控建议

寻找“安防成本投入”与“消费者购物体验”之间的平衡点是提升商家监控能力可持续发展的关键。

**1. 发挥科技的作用，不断创新安防科技能力。**比如在商品结算区安装监控，方便办案取证；提升商品结算的智能化，对多次扫描结账又取消交易、单独购买塑料袋等行为进行预警提示等。

**2. 建议拓展预防思路，“堵疏结合”为监管增效。**比如可以引入“征信评级”的概念，尝试将上述盗窃违法犯罪行为和蚂蚁征

信、甚至中国人民银行的征信系统挂钩，从增加犯罪成本的角度预防犯罪。

**3. 建议加强安防培训，提升员工的责任意识。**通过调查发现，在新型零售超市中盗窃的行为人大多是看到有机可乘，临时起意，而往往一次得手后，监管的漏洞助推他们多次盗窃。如能赋予超市巡查员新的安防职责，提升在进出口、结账处的巡查力度，将对有贪念的行为人起到很好的震慑作用。

**附：相关法律法规：**

**《中华人民共和国刑法》**

**第二百六十四条** 盗窃公私财物，数额较大的，或者多次盗窃、入户盗窃、携带凶器盗窃、扒窃的，处三年以下有期徒刑、拘役或者管制，并处或者单处罚金；数额巨大或者有其他严重情节的，处三年以上十年以下有期徒刑，并处罚金；数额特别巨大或者有其他特别严重情节的，处十年以上有期徒刑或者无期徒刑，并处罚金或者没收财产。

## 案例四：余某某诈骗案

### 一、基本案情

2018年3月至7月期间，被告人余某某通过网络平台购买虚拟手机号码、非法获取银行卡号、姓名、身份证号码等大量公民个人信息，用于在某网约车平台注册账号和进行实名认证。后一次性使用上述账号，通过微信接单，为有需求的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。经司法审计，被害单位实际损失人民币6万余元，余某某非法获取公民个人信息500余条，代为他人打车非法获利共计人民币4万余元。

### 二、司法处理

被告人余某某犯诈骗罪，判处有期徒刑二年，并处罚金人民币六千元；犯侵犯公民个人信息罪，判处有期徒刑一年，并处罚金人民币五百元；决定执行有期徒刑二年七个月，并处罚金人民币六千五百元。

### 三、风险提示

1. 随着互联网产业的蓬勃发展，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，并且网络犯罪出现了职业化倾向，已然形成黑色产业链条。这些犯罪分子的行为严重损害了互联网企业权益，并破坏了公平、绿色、健康的司乘环境。



2. 犯罪分子还利用网络群组、平台非法买卖公民个人信息，传播利用互联网企业网站漏洞实施犯罪的方法，互联网的安全问题已不仅是企业个体问题，更开始成为社会问题，互联网企业应进一步提升反作弊能力。

3. 在打击网络黑产、维护网络安全方面，互联网企业在完善自身管理机制的同时，亟需与公安、司法机关以及相关部门密切配合、形成合力，共筑网络安全生态。

#### 四、防控建议

1. **优化平台系统，建立预警机制。**完善平台系统规则，严格审核用户注册、登录的身份验证程序，从源头上预防冒用他人身份使用平台打车的行为。对于历史订单多次严重迟延支付、预计乘车行程距离较远、车费金额较高的客户，可限制其先乘后付权利，要求其预付车费，并相应提升平台线路规划与车费预估的准确性。同时建立有效的预警机制，定期进行系统优化升级，及时修补系统漏洞。

2. **提升反作弊能力，建立高效处置机制。**充分运用大数据技术，完善异常订单发现机制，优化平台反作弊模型，增强异常订单抓取敏锐度，及时发现作弊行为。建立及时报告机制，疏通信息流转渠道，对命中模型的高危订单及时介入，对确认存在作弊行为的用户，采取有效的限制和追偿措施。

3. **加强与司法机关对接，建立违法犯罪行为的处置机制。**对于交易异常情形存在违法犯罪嫌疑的，应当建立专门处理机制，

及时固定电子证据、屏蔽相关信息、开展初步调查，立即向公安机关报案。对于进入司法程序的案件，应当积极配合司法机关办案，全面准确地提供电子数据，详细解释交易流程和技术问题，协助打击违法犯罪。

#### 附：相关法律法规：

##### 《中华人民共和国刑法》

第二百五十三条之一 违反国家有关规定，向他人出售或者提供公民个人信息，情节严重的，处三年以下有期徒刑或者拘役，并处或者单处罚金；情节特别严重的，处三年以上七年以下有期徒刑，并处罚金。

违反国家有关规定，将在履行职责或者提供服务过程中获得的公民个人信息，出售或者提供给他人的，依照前款的规定从重处罚。

窃取或者以其他方法非法获取公民个人信息的，依照第一款的规定处罚。

单位犯前三款罪的，对单位判处罚金，并对其直接负责的主管人员和其他直接责任人员，依照各该款的规定处罚。

第二百六十六条 诈骗公私财物，数额较大的，处三年以下有期徒刑、拘役或者管制，并处或者单处罚金；数额巨大或者有其他严重情节的，处三年以上十年以下有期徒刑，并处罚金；数额特别巨大或者有其他特别严重情节的，处十年以上有期徒刑或者无期徒刑，并处罚金或者没收财产。本法另有规定的，依照规定。

## 案例五：应某诈骗案

### 一、基本案情

2018年9月间，被告人应某向他人购买10余个具有“闪退”功能的某网站账户，尔后其通过该网络平台购买商品服饰、生活用品、数码产品等物，待收到商品后利用“闪退”功能申请退款，得款后未将商品退回商家，由此骗得各类物品共计价值人民币6000余元。

### 二、司法处理

被告人应某犯诈骗罪，被上海市长宁区人民法院判处有期徒刑七个月，并处罚金人民币一千元。

### 三、风险提示

近年来随着电子商务的快速发展，消费者通过电商平台购物已成为一种常见的生活方式，但有不法分子利用电商平台推出的诸如“闪电退”等便利消费者的相关服务实施诈骗等违法犯罪行为，扰乱了正常的市场经济秩序。目前此类案件呈高发态势，我院在办案件有21件24人，案值最高的达人民币30余万元。

1. 网络信息的高速扩散导致此种诈骗行为模式在不法分子当中广为传播，不仅给电商平台造成严重经济损失，也对区域法治化营商环境造成一定负面影响。

2. 电商平台针对用户所建立的信用体系以及预警机制尚不能及时反映因用户个人不良行为所导致的信用负面评价，需进一

步完善。

3. 电商平台在加强企业内部管理的同时，应将相关案件线索及时移送司法机关并加强沟通协调。

#### **四、防控建议**

**1. 完善用户信用体系，建立预警机制。**电商平台需加强用户信用体系建设，完善用户个人信息，并且对于历史订单退款退货多次出现异常的客户，可限制或关闭其信用额度，降低其信用评分。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，并加强与快递物流公司信息互联，及时发现虚假退货快递单号，从而减少损失。

**2. 优化平台系统，强化内部管控。**完善平台系统规则，严格审核用户登录的身份验证机制，从源头上预防冒用他人账号进行购物消费的行为，并且及时发现并修补系统漏洞。电商平台需要加强平台内部规章制度建设，严防平台账号泄露并流入市场，以免给不法分子以可乘之机。

**3. 主动对接办案机关，建立协同处理违法犯罪行为机制。**针对近期该类型诈骗案件频发的态势，电商购物平台需要建立或者完善对于违法犯罪行为的处理机制，发现相关案件线索第一时间向公安机关报案，并主动提供案件线索及掌握的案件证据材料，针对网络交易中专业问题向办案机关加以解释说明，共同维护良好营商环境。

## 附：相关法律法规

### 《中华人民共和国刑法》

第二百六十六条 诈骗公私财物，数额较大的，处三年以下有期徒刑、拘役或者管制，并处或者单处罚金；数额巨大或者有其他严重情节的，处三年以上十年以下有期徒刑，并处罚金；数额特别巨大或者有其他特别严重情节的，处十年以上有期徒刑或者无期徒刑，并处罚金或者没收财产。

## 案例六：刘某某非法获取公民个人信息、 敲诈勒索案

### 一、基本案情

2018年8月间，被告人刘某某采用黑客技术手段非法侵入某公司计算机信息系统，窃取大量注册身份信息、入住登记身份信息以及住宿信息，之后刘某某向该公司多名高管发送多封电子邮件以及含有部分上述信息的文件附件，以出售上述信息为要挟，索要价值人民币200余万元的数字货币，该公司随即报警，未予支付。

2018年9月7日，刘某某被公安机关抓获。公安机关从其处查获的硬盘中发现一含有大量公民个人信息的压缩文件，其中15万余条姓名、身份证号等公民个人信息以及10万余条公民住宿信息与该公司数据信息一致。

### 二、司法处理

目前，该案已由我院向上海市长宁区人民法院提起公诉。

### 三、风险提示

1. **公司员工网络安全意识欠缺。**相关证据显示，数据被窃取源于公司员工邮箱密码的泄露，之后，刘某某通过该员工邮箱，向公司内部员工发送多封钓鱼邮件获取相关VPN密码，继而入侵内网，获取更多服务器账号密码。公司员工应对公司网络系统安全具有较强的风险敏感度和风险防范意识，但该案件表明公司员

工保密意识和网络安全意识严重欠缺，为公司网络安全带来巨大隐患。

**2. 监测和预警不足。**相关证据显示，公司服务器被首次恶意登录之后，在一个月时间内，公司数据服务器被多次登录甚至攻击，至案发前，攻击者仍持续控制内外相关服务器。在此段时间内，公司始终未监测到异常，亦未能及时采取有效措施拦截攻击，可见网络系统监测和预警能力亟待提升。

**3. 加密措施不符合标准。**根据我国网络安全等级保护制度的要求及公司网络数据对公民个人信息权利和社会敏感度的重要影响，企业应采取严格的页面和数据加密措施，增加网络入侵成本。但该公司密码使用和加密技术明显不符合上述制度相关标准要求，导致大量用户信息被窃取后即可被轻易识别，甚至存在公司数据被利用实施犯罪等风险隐患。

#### **四、防控建议**

**1. 加强员工培训与教育。**应当以本案为教训，对全体员工开展警示教育，今后应定期开展对全体员工的网络安全风险意识培训，强化网络安全法律知识普及，强调公司网络系统出现安全问题带来的严重后果。同时，加强对内部技术人员的技术培训及其他专项培训。公司可明确不同岗位的隐私数据安全职责、与相关人员签署保密协议等，提高公司员工的网络安全意识，降低隐私和数据泄露风险。

**2. 建立有效的网络安全监测和通报预警系统。**根据《网络安

全法》第二十一条，网络运营者应按照网络安全等级保护制度的要求，有效地监测、记录网络运行状态。我国网络安全等级保护制度 2.0 标准（以下简称等保 2.0）已于 2019 年 5 月 13 日正式发布，将于 2019 年 12 月 1 日正式实施。在新标准中，《信息安全技术网络安全等级保护测评要求》提出了对“威胁情报检测系统”的要求。建议提前适应该标准要求，运用“威胁情报检测系统”检测网络威胁，强化公司网络全程监测预警功能，提高对网络攻击的溯源能力。同时，建议加强日常安全巡检制度和模拟渗透测试等，对公司网络系统进行定期检查和测试。

**3. 采取符合标准的数据加密措施。**根据《网络安全法》第二十一条，网络运营者应按照网络安全等级保护制度的要求，采取重要数据备份和加密等措施。同时，在密码技术应用等方面，即将实施的等保 2.0 比之前适用的等保 1.0 对网络经营者提出更为严格且明确的要求。建议详细了解等保 2.0 标准的新要求，尽快落实相关制度，采取诸如强密码使用、加密技术改进等有效的页面和数据加密措施，确保数据即使被窃攻击者也难以识别特定自然人。

#### **附：相关法律法规**

##### **《中华人民共和国刑法》**

**第二百五十三条之一** 违反国家有关规定，向他人出售或者提供公民个人信息，情节严重的，处三年以下有期徒刑或者拘役，并



处或者单处罚金；情节特别严重的，处三年以上七年以下有期徒刑，并处罚金。

违反国家有关规定，将在履行职责或者提供服务过程中获得的公民个人信息，出售或者提供给他人的，依照前款的规定从重处罚。

窃取或者以其他方法非法获取公民个人信息的，依照第一款的规定处罚。

单位犯前三款罪的，对单位判处罚金，并对其直接负责的主管人员和其他直接责任人员，依照各该款的规定处罚。

第二百七十四条 敲诈勒索公私财物，数额较大或者多次敲诈勒索的，处三年以下有期徒刑、拘役或者管制，并处或者单处罚金；数额巨大或者有其他严重情节的，处三年以上十年以下有期徒刑，并处罚金；数额特别巨大或者有其他特别严重情节的，处十年以上有期徒刑，并处罚金。

### 《中华人民共和国民法总则》

第一百一十一条 自然人的个人信息受法律保护，任何组织和个人获取他人信息的，应当依法取得并确保信息安全。

### 《中华人民共和国网络安全法》

第二十一条 国家实行网络安全等级保护制度，网络运营者应当按照等级保护制度要求履行网络安全保护义务，保障网络免受干扰，防止数据泄露或被窃取。

第五十九条 网络运营者不履行本法第二十一条规定的网络安全保护义务的，由有关主管部门责令改正，给予警告；拒不改正或者导致危害网络安全等后果的，处一万元以上十万元以下罚款，对直接负责的主管人员处五千元以上五万元以下罚款。

## 案例七：王某某敲诈勒索案

### 一、基本案情

2015年至2018年期间，被告人王某某为谋取不法利益，以本市多家超市卖场、亲子教育机构等为目标，通过向消防部门、市场监督管理部门等举报、投诉等方式，利用被害单位为维护经营、希望不被举报、投诉或撤回投诉等心理，胁迫被害单位向其支付“顾问费”等，共计敲诈所得人民币5.6万余元。

### 二、司法处理

该案为本市首例适用刑事法律办理的“职业举报人”敲诈勒索“顾问费”案。被告人王某某犯敲诈勒索罪，被上海市长宁区人民法院判处有期徒刑三年三个月，并处罚金人民币一万元。

### 三、风险提示

1. **企业经营行为合规审查不到位。**王某某在2年的时间内，为了实现敲诈勒索“顾问费”的目的，针对某一企业的消防安全、食品安全、商品宣传举报和投诉多达19起，经查证均属实。由此可见，相关企业存在质量管控意识不足、合规性审查不到位等问题，导致问题频发，主体责任和品牌维护的意识不够。

2. **投诉纠纷处理机制欠缺，“花钱买太平”方式盛行。**企业为了维护形象、降低投诉纠纷解决成本、尽快减少投诉或者促使举报人撤诉等动机而寻求私下解决，这种看似高效率、低成本的息事宁人处理方式，既给犯罪分子留下了反复敲诈勒索的空间，

也助长了经营者继续违法违规经营的侥幸心理，造成侵害消费者权益、损害企业市场竞争力的各种经营问题长期存在，对企业自身健康发展有弊无利。

### **3. 员工法治教育不足，缺乏应对侵害的法治意识和方法。**

涉案企业的相关负责人明知王某某有多次敲诈行为，却未及时将此事向上级反映，也未向公安机关报案，从而使犯罪分子敲诈屡屡得逞。直到王某某将敲诈的对象直接指向公司总部，才得以案发，否则敲诈行为还将持续。因此，企业在员工管理方面，缺乏日常性警示和基本法治教育，导致员工法律意识不足，运用法律武器保护自身权益的意识和能力不足，埋下了潜在的经营风险。

## **四、防控建议**

### **1. 加强消防安全意识，强化产品质量及广告宣传的监督管理。**

如存在消防法律法规不知晓、不熟知的情况，建议设立内部消防安全责任人，落实责任主体，加强消防知识的培训和演练，不定期开展消防大检查，强化经营场所、重点区域的“无死角”监控，始终把保护消费者人身安全放在第一位。建立对产品的条形码追根溯源机制，查明产品是否符合国家、行业标准，坚决杜绝伪劣、假冒产品；对商品的宣传语尽到及时、有效审核义务，一旦发现违反《中华人民共和国广告法》《中华人民共和国产品质量法》等法律法规的，立即做下架整改处理，保证商品品质与商品宣传的统一，避免在标识标签、广告宣传等领域出现易发多发的违法行为。

2. 进一步规范消费投诉的解决机制。企业应设立专门的部门处理消费者投诉，对于因产品缺陷或者瑕疵造成消费者损害的，应当依法予以赔偿，但坚决拒绝“职业举报人”“职业打假人”巧立名目所提出的各项非法要求。同时，对被举报的问题，经查证属实的，应当及时整改并进行通报，要求吸取教训，自查自纠，杜绝相同的问题被反复举报。

3. 加强对从业人员的法治教育。法治是最好的营商环境，以法治思维和法治手段解决经营中出现的问题，规避经营风险，才能达到消费者和商家的共赢。企业应当着重加强职业道德教育和法治教育，树立合法经营、诚信经营的理念，对相关投诉、举报，不能一味追求“摆平”，更不能以“花钱买太平”的方式纵容犯罪、掩盖经营问题。2018年本市工商行政管理局等部门联合出台了《关于有效应对职业索赔举报行为维护营商环境的指导意见》，明确要求在行政处罚过程中，经营者有主动消除或者减轻违法行为危害后果等情形的，可以依法从轻或者减轻处罚；违法行为轻微并及时纠正，没有造成危害后果的，不予行政处罚。这种初次轻微违法免罚制度给予了经营者及时自我纠正的机会，企业应当大力宣传相关法律法规和政策，加强从业人员的法治教育。

**附：相关法律法规：**

《中华人民共和国刑法》

第二百七十四条 敲诈勒索公私财物，数额较大或者多次敲诈

勒索的，处三年以下有期徒刑、拘役或者管制，并处或者单处罚金；  
数额巨大或者有其他严重情节的，处三年以上十年以下有期徒刑，  
并处罚金；数额特别巨大或者有其他特别严重情节的，处十年以上  
有期徒刑，并处罚金。

## 案例八：徐某提供侵入、非法控制计算机信息系统程序、工具案

### 一、基本案情

2016年12月，被告人徐某编写了一款名为“小白改机”的软件，并将该程序挂在自己及其招募的代理人员开设的QQ群组中，通过售卖卡密（即有一定使用期限的用户名及密码）进行谋利。该款软件具有修改安卓系统中的设备串号、AndroidID设备品牌、型号、设备名、系统版本等信息的功能，使得用户可以规避某外卖平台对于用户是否属于新注册用户的审查，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，给平台造成损失。

### 二、司法处理

被告人徐某被上海市长宁区人民法院以提供侵入、非法控制计算机信息系统程序、工具罪判处有期徒刑三年，罚金一万元。

### 三、风险提示

1. “补贴”“红包”等形式的优惠易成为诈骗的对象。在互联网企业成立初期或开展新业务期间，为了抢占市场或推广业务，常常会开展“补贴”“红包”等各类优惠活动，这些原本是面向消费者或商户的补贴极易成为诈骗的对象。

2. 网络犯罪出现职业化、精细化、产业化的风险。随着互联网技术的普及，黑客技术门槛变低，网络犯罪出现职业化倾向，

已然形成黑色产业链条。工具开发者、工具应用者和利用工具实施犯罪者都有明确的分工，网络犯罪呈现分工细化的态势。此特征在涉互联网企业犯罪中表现得非常明显。

#### **四、防控建议**

**1. 互联网企业应加大研发力度，堵住技术安全漏洞。**互联网企业应当提高风险意识，加大技术研发投入，做好技术防护工作，定期进行技术软件的检查维护与更新升级，完善抵御外部攻击的警报和应对机制。

**2. 互联网企业应建立异常行为的发现和处理机制。**提高异常数据、异常产品、异常交易的分析检测和预警提示能力，并完善预警后的应对预案，及时止损。对于同一个账号或同一手机号码多次异常交易的，或是存在异常商品信息、物流信息、消费者投诉集中的可疑商家，应当及时抓取并预警，采取账户封停等措施。

**3. 互联网企业应建立违法犯罪行为的处理机制。**对于交易异常情形存在违法犯罪嫌疑的，应当建立专门处理机制，立即向公安机关报案，并及时固定电子证据、屏蔽相关信息、开展初步调查。对于进入司法程序的案件，应当配合公安司法机关办案，全面准确地提供电子数据，详细解释交易流程和技术问题，如实报告损失，协助打击违法犯罪。

#### **附：相关法律法规**

《中华人民共和国刑法》



第二百八十五条 ……，情节严重的，处三年以下有期徒刑或者拘役，并处或者单处罚金；情节特别严重的，处三年以上七年以下有期徒刑，并处罚金。

提供专门用于侵入、非法控制计算机信息系统的程序、工具，或者明知他人实施侵入、非法控制计算机信息系统的违法犯罪行为而为其提供程序、工具，情节严重的，依照前款的规定处罚。

## 案例九：潘某合同诈骗案

### 一、基本案情

2016年1月至5月间，被告人潘某使用境外银行信用卡以自己的名义分别在A和B两个互联网平台向国内多家航空公司预定机票，在机票订单预订成功后即联系航空公司改签，然后向航空公司申请办理退票和退款，由于出票号的变更，航空公司将退票款退还至潘某指定的国内银行卡账户内。

与此同时，潘某利用国外银行卡的交易规则，就上述退款额向发卡银行以未收到服务为由提出拒付申请，A、B平台在收到同潘某使用的境外银行卡关联的并负责其资金结算的中银信用卡（国际）有限公司及美国运通国际股份有限公司信息反馈后，即支付120余万元。潘某以及其控制的境外银行卡收到中银、运通公司钱款75万余元。

### 二、司法处理

潘某因合同诈骗罪被上海市长宁区人民法院判处有期徒刑六年，并处罚金人民币十万元。

### 三、风险提示

1. 针对境外银行信用卡风控能力弱的风险。客户在互联网平台使用境外银行信用卡存在一定的风险，特别是遭遇客户恶意拒付时。本案中，潘某使用外卡预订机票，然后通过改签的方式换票、退票，从而将机票变现，随后向外卡银行提出交易异议，拒

付机票费用，从而实现对相应机票款的非法占有。A、B 平台面对该客户多次恶意使用外卡拒付时，并未与境外银行卡关联的资金结算方形成良好的沟通渠道，短时间内被拒付上百万元未提出有效异议，使公司财产遭受巨大损失。

**2. 异常数据检测水平弱、问题发现滞后的风险。**互联网行业的大部分诈骗案件，例如利用“外挂”骗取首单减免或补贴红包等，均存在企业对异常数据发现和処理能力不足的情况，无法第一时间对异常数据作出回应。针对潘某频繁的异常订单，平台并未及时采取有效措施，导致公司的损失持续扩大。

#### **四、防控建议**

**1. 完善数据信息建设，提高异常数据的检测能力和分析能力。**对于交易中发现的异常数据，比如同一个账号多次异常交易的，同一个卡号多次无法扣款的，应当及时抓取并预警，第一时间发现问题并采取账户封停等措施，降低网站的损失。建立信用模型，通过信用模型对客户进行预测，用信用体系结合反欺诈体系，进一步降低恶意拒付的风险。

**2. 引进高效的信用卡安全服务商。**在信用卡交易发生争议时，从信用卡安全服务商处获得及时反馈，缩短对欺诈交易的调查及防范时间。

**3. 完善航空公司业务流程。**及时反馈并推进航空公司在机票换开退票流程上的问题，实行支付原渠道退款，避免现金及银行卡退款，防止类案发生。

## 附：相关法律法规

### 《中华人民共和国刑法》

第二百二十四条 有下列情形之一，以非法占有为目的，在签订、履行合同过程中，骗取对方当事人财物，数额较大的，处三年以下有期徒刑或者拘役，并处或者单处罚金；数额巨大或者有其他严重情节的，处三年以上十年以下有期徒刑，并处罚金；数额特别巨大或者有其他特别严重情节的，处十年以上有期徒刑或者无期徒刑，并处罚金或者没收财产：

（一）以虚构的单位或者冒用他人名义签订合同的；

（二）以伪造、变造、作废的票据或者其他虚假的产权证明作担保的；

（三）没有实际履行能力，以先履行小额合同或者部分履行合同的方法，诱骗对方当事人继续签订和履行合同的；

（四）收受对方当事人给付的货物、货款、预付款或者担保财产后逃匿的；

（五）以其他方法骗取对方当事人财物的。

# 案例十：黄某某、邹某非国家工作人员 受贿案

## 一、基本案情

2015年11月至2016年7月，被告人黄某某利用担任某网购平台运营招商部美妆个护组负责人，负责商户的招商、运营推荐等职务便利，非法收受商户通过支付宝、微信及银行转账等方式给予的贿赂共计人民币20余万元，为商户谋取占据优质广告位的机会。

2016年6月至2017年11月间，被告人邹某利用担任某网购平台纸品类招商经理，负责商家综合性服务及平台营销活动资源对接的职务便利，非法收受他人给予的好处费49万余元，违反公司规定为他人获得“团免”“推文”的优先活动机会。

## 二、司法处理

上海市长宁区人民法院以非国家工作人员受贿罪判处黄某某有期徒刑十个月，判处邹某有期徒刑一年四个月。

## 三、风险提示

**1. 商业贿赂风险。**对于各类电商平台中的商户而言，客户浏览量即所谓“流量”大小直接影响其利润高低，由此催生出以金钱换流量的做法。常见方式是商户通过向平台营销人员行贿，从而换取参与平台促销活动机会，这种商业贿赂已经成为电商行业的潜规则。还有一种更为隐蔽的方式，即电商平台员工违反公司

管理制度，帮助亲友的企业入驻平台，并通过资源倾斜，直接获取利润或提成，破坏了公平的市场竞争环境。

**2. 利用信息优势涉及的其他犯罪风险。**有的企业员工可以轻而易举地获取商户信息，利用其掌握的平台拟处罚商户的名单，私下联系商户，谎称收取一定费用后可以帮助商户逃避处罚，从而骗得大量钱款，或者直接要求违规商户花钱买平安。有的企业工作人员利用职务便利，将企业提供服务过程中收集的公民个人信息对外出售并从中牟利，不仅侵犯公民个人信息，还可能引发电信诈骗案件。

#### **四、防控建议**

**1. 在员工入职培训和在岗培训中强化法治教育。**部分企业员工法治观念淡薄，对于套取补贴、商业贿赂、泄露公民个人信息等行为的法律性质和可能导致的法律后果缺乏明确的认知。企业在进行员工培训时，应当引入司法专业力量的支持，结合真实案例，开展有针对性的法治教育，提升员工遵守企业规章制度和法律规定的意识。

**2. 加强内部安全稽查、风险控制等监督制约机制建设。**企业应当根据本单位业务管理流程，并借鉴司法机关提供的典型案例，梳理监控风险点。对于重点岗位的员工，加大监督力度，可以制定定期轮岗制度或飞行检查机制，防止员工长时间在同一岗位上可能产生的贪腐现象。对岗位赋权时要注意处理好集权高效和分权制约的关系，加强投诉处理、合规审查和技术控制机制。

3. 建立互联网企业与司法机关的“亲”“清”关系，实现良性互动。依托司法机关优化营商环境的各项举措和平台，加强办案单位与互联网企业的联系，畅通信息沟通途径，及时反馈企业的司法服务需求，邀请办案单位进入互联网企业进行廉政讲评等，互联网企业也可以向办案单位传授最前沿的行业知识助力办案，实现共赢。

#### 附：相关法律法规

##### 《中华人民共和国刑法》

第一百六十三条 公司、企业或者其他单位的工作人员利用职务上的便利，索取他人财物或者非法收受他人财物，为他人谋取利益，数额较大的，处五年以下有期徒刑或者拘役；数额巨大的，处五年以上有期徒刑，可以并处没收财产。

公司、企业或者其他单位的工作人员在经济往来中，利用职务上的便利，违反国家规定，收受各种名义的回扣、手续费，归个人所有的，依照前款的规定处罚。

国有公司、企业或者其他国有单位中从事公务的人员和国有公司、企业或者其他国有单位委派到非国有公司、企业以及其他单位从事公务的人员有前两款行为的，依照本法第三百八十五条、第三百八十六条的规定定罪处罚。