目录

关于电诈等案件适用法律若干问题的意见

GOIP 小知识

“GOIP”是什么?

GOIP 是一种用于网络通信的硬件设备，通过嵌入式通信软件，能够接入 GSM、CDMA、WCDMA、LTE 等频段的手机卡。

GOIP 设备是指虚拟拨号集成通讯设备，具备多条线路并可配备多个手机 SIM 卡卡槽，支持手机电话卡接入，并将传统电话信号转化为网络信号，实现数百个电话号码同时通话，还可以通过服务器远程控制“GOIP 设备”，将电话拨出。

GOIP 设备利用 GOIP 来搭建虚拟拨号，将传统电话信号转化为网络信号，在全球范围内虚拟拨号，可以容纳数百个 SIM 卡，进行远程拨打电话、收发短信。

“GOIP”与“VOIP”

“GOIP”“VOIP”均属虚拟拨号集成通讯设备。“GOIP”是利用国内手机卡接入电话网络，使被骗事主来电显示的就是国内的手机号码。“VOIP”是利用国内固定电话线路接入电话网络，使被骗事主来电显示的就是国内固话号码，二者大同小异。

简单地说，在国外的诈骗分子拨打电话给事主会显示为国外电话，为了提高可信度，诈骗分子通过国内同伙用“GOIP”和“VOIP”设备把号码转换成国内号码，并同时拨打给多个事主，具有人机分离、远程操控、异地拨号等特点，是近年不法分子实施电信网络诈骗的重要方式。

功能/特征	VOIP	GOIP
网络电话	✓	✓
人卡分离	✓	✓
话费成本	国际漫游 > VOIP > GOIP	
数据中转	✓	✓
支持改号	✓	✗
需要特殊线路	✓	✗
支持通话中回拨	✓	✓
支持挂断后回拨	✗	✓

GOIP 诈骗的危害

（一）成本低，蔓延快，范围广

相比传统的电信诈骗，利用 GOIP 设备进行诈骗，只需一台设备和大量的 SIM 卡就可以实现批量的拨打诈骗电话，双向通话，规避一般改号软件不能回拨的问题，使电信诈骗的成本变得更加低廉。且 GOIP 设备的工作原理实现了“人卡分离”，诈骗分子和诈骗使用的设备往往不在同一处地方，使得诈骗分子可以在不同的地方设置更多的诈骗窝点，GOIP 诈骗案件呈现范围广、数量多的高发态势。

（二）伪装拨号，迷惑性强，流动性大

GOIP 诈骗一般采取远程操控、非接触式模式，诈骗分子某地设置部署的 GOIP 设备的机房，就可不同的地方通过网络拨出诈骗电话，通过虚拟拨号，让“00+”等开头的境外诈骗电话切换为国内手机号码，能任意切换手机号码拨打受害人电话，让受害人防不胜防，其实诈骗分子往往躲在其他省市甚至是国外某个角落。

（三）诈骗团伙组织严密、追踪困难，损失难挽回

利用 GOIP 设备进行电信网络诈骗的犯罪分子多为团伙作案，团伙组织严密，采取企业化的运作，分工很细，下一道工序的不知道上一道工序的情况，且随着近年来国内打击电信网络诈骗的高压态势，诈骗团伙开始不断向境外转移，GOIP 设备成为了他们在境外开展对境内实施电信诈骗的重要工具。

由于 GOIP 设备的反制拦截和信号溯源、调查取证非常困难，公安机关通常只能查获诈骗使用的 GOIP 设备，无法抓获诈骗团伙成员，所以受害人的财产损失也能以追回。此外，诈骗分子通过的远程拨号，“人机分离”，异地（境外）使用，逃避公安机关打击。

“简易 GOIP 组网”诈骗模式

GOIP：相当于一个大手机，一般可以插几张到几十张不等数量的手机卡，每一张卡就是一条线路，对应境外诈骗窝点的一个电话坐席。

GOIP 组网：一般由“GOIP+卡池设备”组成，配套的卡池设备可以插几十张到上百张不等的手机卡，而且卡池设备还可以与“GOIP”分离使用。

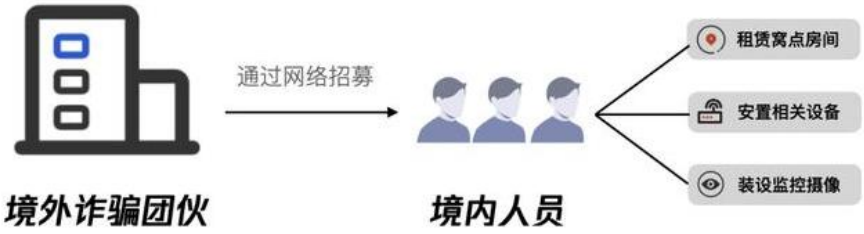
简易 GOIP 组网：犯罪嫌疑人仅仅利用多台手机搭配远程控制软件和音频对录线架设通讯网络后，境外犯罪分子就可以通过一些远程超控软件来控制其中的一部手机，通过微信、QQ 等网络软件与其中的另外一部手机进行联系，并将音频信号传至第一部手机，从而实现诈骗通话。

诈骗分子到底是怎么通过 GOIP 来实现远程操作的呢?

在境外的不法分子会招募境内工作人员来设置窝点，而窝点的设备一旦安装到位后，GOIP 设备就会扮演机身的角色，跟所在地通信基站取得连接，而 SIM 卡则会插在境外的卡池里。诈骗团伙把 SIM 卡拨号数据传输到 GOIP 设备上，将电话信号转换成网络信号，再让该设备与所在地通信基站连接，拨出电话。

比如，你要显示归属地在深圳的电话，你只需在深圳部署一个 GOIP 的机房，人可以在国外操作，实现人机分离，一机多号，逃避打击。

这时候，受害者接到的电话信号虽然来自本地，但实际上跟他们对话的诈骗人员往往躲在国外某个隐蔽的角落里。即使警方追查到了 GOIP 的窝点，也只能找到被安置好的设备，很难抓到不法分子。



利用 GOIP 设备进行电信网络诈骗的三种类型

第一种是传统GOIP。GOIP 设备相当于一个大手机，一般可以插 32 张手机卡，每一张卡就是一条线路，对应境外诈骗窝点的一个电话座席。它的升级版是“组网式 GOIP”，一般由“GOIP＋卡池设备”组成，从外观看是一大一小两个铁盒，配套的卡池设备可以插 128 张手机卡，卡池设备还可以与 GOIP 分离使用，进一步加大了案件侦破难度。

第二种是简易组网 GOIP。嫌疑人使用一根数据线将两部安装有远程操控软件的手机连接起来，境外犯罪分子通过远程操控，用钉钉等网络软件与其中一部手机进行语音联系，远程用另一部手机给受害人拨打电话，受害人接听后，实际上就是将第一部手机的网络通话语音通过音频数据连接线传至第二部手机，境外诈骗分子就实现了与受害人的直接通话，进一步增加了电信网络诈骗的迷惑性和风险性。

第三种是固网 GOIP。顾名思义，就是利用固定电话和宽带架设 GOIP 设备。嫌疑人租房，办理固定电话、开通宽带，架设语音网关，连接设备后，通过网络

联接、信令交换，将网络语音信号转化成信令语音信号，境外的诈骗分子就能利用该设备伪装成本地固定电话号码拨打电话，实施诈骗。

GOIP 设备可以随便使用吗?

GOIP 设备不能随便使用。根据《中华人民共和国电信条例》有关规定，使用 GOIP 设备必须通过相关部门的审批，否则均不得使用。

哪些情形疑似使用 GOIP?

1、如有发现有人存在携带大量手机卡、GOIP 等网络设备租房或“设备在人不在”的情况；

2、快递行业工作中如发现在同一地址或同一收货人，密集采购、安装、调试、维修 GOIP 等大批量网络设备的订单等；

3、遇到在网点开办多张银行卡、电话卡，大量购买、架设 GOIP 设备的情形。

帮助诈骗分子架设“GOIP”“VOIP”设备构成什么犯罪?

【帮助信息网络犯罪活动罪】

根据《刑法修正案》，明知他人利用信息网络实施犯罪，为其犯罪提供互联网接入、服务器托管、网络存储、通讯传输等技术支持，或者提供广告推广、支付结算等帮助，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。

《中华人民共和国反电信网络诈骗法》第三十八条

组织、策划、实施、参与电信网络诈骗活动或者为电信网络诈骗活动提供帮助，构成犯罪的，依法追究刑事责任。

前款行为尚不构成犯罪的，由公安机关处十日以上十五日以下拘留；没收违法所得，处违法所得一倍以上十倍以下罚款，没有违法所得或者违法所得不足一万元的，处十万元以下罚款。

除此之外，公民将自己名下的电话卡、银行卡以出租、出借或者出卖等形式

交给他人使用，被犯罪分子非法使用，支付结算达到一定数额的，这种行为就有可能构成“帮信”罪。

通过“GOIP”诈骗被认定犯诈骗罪的处罚

如果当事人的行为被认定构成诈骗罪，处刑需要根据诈骗的金额进行确定。具体是：

（1）诈骗数额较大的，处三年以下有期徒刑、拘役或者管制，并处或者单处罚金；

（2）数额巨大的，处三年以上十年以下有期徒刑，并处罚金；

（3）数额特别巨大的，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。

法律依据：《中华人民共和国刑法》第二百六十六条之规定，【诈骗罪】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。

如何防范“GOIP”诈骗?

1、如果有人向你推荐、架设 GOIP 设备，并给予小额的补偿，千万不要相信，这是违法犯罪的行为。

2、不轻信、不回拨陌生来电及信息，遇到“客服、工作人员”“等来路不明的陌生的电话，千万千万不要随便拨回去，应当拨打客服电话向官方渠道进行核实。

3、不要向陌生人透露自己的身份证号码、银行卡账号、手机验证码等个人信息，更不能向陌生人汇款、转账，转帐前一定要再三核实对方账户和身份信息。

4、谨防木马病毒和钓鱼链接，不点击可疑的网站链接，慎扫不明来历的二维码，慎连接免费的 WIFI。

5、如遇电信诈骗立刻报警。

6、GOIP 设备经常出现在出租房、居民楼屋顶、宾馆等场所，只要有电源，它就能运作成为电诈犯罪的帮凶。如看到 GOIP 设备请立即拨打 110 报警。

特别提醒：使用 GOIP 设备从事电信网络诈骗活动是犯罪行为。公安机关始终坚持严厉打击非法买卖、出租、出借、出售银行卡、电话卡和非法安装使用

GOIP 设备等违法犯罪行为，切勿贪图蝇头小利出租、出借、出售自己的银行卡、电话卡，更勿贪图“高薪”架设 GOIP 设备为诈骗分子提供帮助。**若发现非法安装、使用 GOIP 设备线索，请尽快向公安机关举报!!!**

防范电信诈骗“三不一多一要”

未知链接不点击，慎防木马病毒和钓鱼链接，不点击可疑的网站链接。

陌生来电不轻信，不论是否是境外来电，所有陌生电话都要谨慎对待，遇到“客服”、“工作人员”等来路不明的身份，应当拨打电话向官方渠道进行核实。

个人信息不透露，不要向陌生人透露自己自己及家人的身份证号码、银行卡账号、手机验证码等信息。如有疑问，可拨打 110 求助咨询，或向亲戚、朋友、同事核实。

转账汇款多核实，不能向陌生人汇款、转账，转账前一定再三核实对方账户和身份信息。

报案要及时，万一上当受骗或听到亲戚朋友被骗，请立即向公安机关报案，可直接拨打 110，并提供骗子的账号和联系电话等详细情况，以使公安机关开展侦查破案。

综合自检察日报、河南法制报、山西法制报、陕西法制网、澎湃网、黄河新闻网，海南、滨州、恩施等地公安、网警、反诈中心的相关报道

严防 GOIP 诈骗，这几种电话不要接!

以 00 或+开头的手机号，一般会显示归属地为境外，如果没有境外往来关系的话，基本上此类电话为诈骗电话。

以 400 开头的企业电话，如果自己和企业没有交集，那么此类电话很有可能是通过改号软件来拨打的诈骗电话。

以 95 开头且超过六位数字的电话，一般情况下 95 开头为大型企业的客服电话，只有五位数字，超过六位属于诈骗电话。（摘自：深圳移动严查 GOIP 诈骗，掀起反诈新攻势）

来源：深圳特区报　2023-04-05

犯罪预防视域下应对涉“GOIP”电信网络诈骗犯罪的对策

针对当前“GOIP”电信网络诈骗面临的人民群众警惕性低、难以控制 GOIP 设备流入市场、犯罪分子反侦查意识强等困难，要做到：

1 增强反诈意识，加强警企协作

单打独斗显然已经不是治理犯罪行为的最好解决方式，公民应当承担起维护社会治安秩序的义务。

2 控制 SIM 卡获取渠道和 GOIP 设备流入市场

首先，从犯罪预防的角度来讲，涉“GOIP”电信网络诈骗犯罪活动一定是围绕着运用 GOIP 设备来展开的，所以我们理应从 GOIP 的生产环节和流通环节开始治理。首先是生产环节，设备生产厂家应生产专属设备码不可更改的的产品，并且植入 GPS 定位系统，与公安机关密切协作，从源头上切断 GOIP 流通之乱。

其次，还在 GOIP 设备的流通环节上进行预防。对此类二手交易平台进行管控，减少 GOIP 设备流入市场。

除此之外，持续开展“断卡”行动，严格管控 SIM 卡，即使犯罪分子突破层层阻碍搭建了 GOIP 设备，也无法实施诈骗活动。

最后，相关政府部门应该找出管控漏洞，对涉及此类设备的黑灰色产业链条从环节和源头上进行打击和控制，大力组建机防人防系统，健全警务支撑机制，要强化资源配置和警种协作，打破警种间资源的应用限制和壁垒，推动不同警种间数据深度融合和情报信息互通，强化多警种联动作战模式，从源头上遏制此类犯罪的产生。

3 提高公安机关技术反制水平

提高公安机关的科学技术水平是打击犯罪的第一要务，涉 GOIP 电信网络诈骗犯罪依托电信，互联网实施，公安机关要加强软硬件设备建设，尝试将先进的科学技术引入到案件侦查过程中来，如利用大数据平台对海量数据进行预测分析研判预警，以及开发人工智能预警，将人工智能技术应用到预防犯罪中。

犯罪分子的犯罪手段更新迅速，为更好地从源头治理犯罪，公安机关应不断组织学习，提升自身科技水平并积极研究探索打击犯罪新方式，例如广东公安机关开展的“打猫行动”。

社会各层面如何增强反诈意识

除了公安等司法机关大力进行反诈宣传并严厉打击相关犯罪行为外，需要社会各方面、各阶层的参与，才能更好保护人民群众的“钱袋子”。

房东、房产租赁中介、宾馆行业工作人员，对租房或住房客户信息应仔细核对并登记，主动询问客户住房用途，提示其切勿从事违法犯罪活动，向其转达警

方打击各类违法犯罪的坚定决心，尽到告知提醒义务；如发现客户存在携带大量手机卡、 GOIP 等网络设备租房或“设备在人不在”等可疑情况，应该立即向公安机关报案。

网络设备销售及售后工作人员、快递公司，工作中如发现在同一地址或同一收货人，密集采购、安装、调试、维修 GOIP 等大批量网络设备的订单等可疑情况应该立即向公安机关举报。

金融系统、 通讯系统营业工作人员：遇到在网点开办多张银行卡、电话卡，大量购买、架设 GOIP 设备的客户等情况要按照相关审批程序规定，从严把关，遇到可疑情况应该立即向公安机关举报。

待业人员、寻求兼职人员：要对网络上发布的招工信息或兼职信息仔细甄别，切勿为了一己之私或蝇头小利，参与出租或出售手机卡、银行卡、对公账户、营业执照、收款二维码；为 GOIP 等网络设备订单提供场所、技术、售后等服务时要多加甄别，防止被不法分子利用，成为帮助其实施诈骗等违法犯罪活动的“帮凶”，情况严重的还有可能涉嫌犯罪，被追究法律责任

设备生产厂家应生产不可更改的设备码的设备，并植入 GPS 定位系统，厂家需要负起责任并且和公安机关密切协作，从源头上切断 GOIP 流通之乱。

GOIP 设备的流通环节上，对通过搜索轻易找到相关设备的二手交易平台进行管控，减少 GOIP 设备流入市场。（摘自：犯罪预防视域下涉 GOIP 电信网络诈骗犯罪的预防与打击）

来源：网络安全技术与应用　2023 年第 7 期

延伸阅读·“帮信罪”的罪与罚

帮助信息网络犯罪活动罪简称“帮信罪”，是指明知他人利用信息网络实施犯罪，为其犯罪提供互联网接入、服务器托管、网络存储、通讯传输等技术支持，或者提供广告推广、支付结算等帮助，情节严重的行为。

“帮信罪”有很多行为类型，比如收购、出售、出租银行卡、手机卡；提供或操作“GOIP”“猫池”“多卡宝”等设备，为电诈团伙搭建远程“机房”；利用社交媒体账号等方式为电诈团伙推广引流；为网络犯罪分子制作、封装、维护非法软件；职业“码农”团伙依附非法平台疯狂“跑分”等。

根据刑法规定，“帮信罪”的法定刑为三年以下有期徒刑或者拘役，并处或者单处罚金。根据《最高人民法院、最高人民检察院关于办理非法利用信息网络、

帮助信息网络犯罪活动等刑事案件适用法律若干问题的解释》第 17 条的规定，对于“帮信罪”被判处刑罚的，司法机关可以依法宣告职业禁止；对于被判处管制、宣告缓刑的，可以根据犯罪情况，依法宣告禁止令。此外，还会有相关行政处罚。

同时，惩戒措施也不可避免。针对银行卡，会有信用惩戒、限制业务、严管账户等措施，不仅在一定时间内影响相关人员的贷款和信用卡申请，5 年内还会被暂停相关单位和个人银行账户非柜面业务，支付账户所有业务等；针对手机卡，则会在惩戒期内停止行为人的新入网业务，各基础运营商只保留 1 个手机号码。（摘自：18 人被法院判刑 3 人因情节轻微被不起诉 剑指电信网络诈骗|参与“跑分”赚返利帮助洗钱危害大）

来源：检察日报　2022-08-15

综合报道

公安部公布十大高发电信网络诈骗类型

1、刷单返利类诈骗。

2、虚假网络投资理财类诈骗。

3、虚假网络贷款类诈骗。

4、冒充电商物流客服类诈骗。

5、冒充公检法类诈骗。

6、虚假征信类诈骗。

7、虚假购物、服务类诈骗。

8、冒充领导、熟人类诈骗。

9、网络游戏产品虚假交易类诈骗。

10、婚恋、交友类诈骗。

来源：公安部网站　2023-06-19

为犯罪分子提供银行卡、银行账户等的处罚

银行卡、手机卡，是犯罪分子争抢的“资源”。银行卡用来承接被害人款项，走账；手机卡乃至固定电话用来拨打诈骗电话，“引流”。

一个“卡农”，可能只拿几千元“好处费”或提成，但从他账户上“走”过的受害者钱款可能高达数百万。出借银行卡行为，看起来“危害不大”，在电诈犯罪链条中却必不可少。

根据最高人民法院、最高人民检察院、公安部 2021 年联合发布的《关于办理电信网络诈骗等刑事案件适用法律若干问题的意见（二）》，行为人明知他人利用信息网络实施犯罪，为其犯罪而收购、出售、出租信用卡、银行账户、非银行支付账户等支付结算帮助，数量达到 5 张（个）以上，或者收购、出售、出租他人手机卡、流量卡等通讯工具帮助，数量达到 20 张以上，以帮助信息网络犯罪活动罪追究刑事责任。最高刑期为有期徒刑 7 年。

上海市浦东新区人民检察院检察官朱波说，对于为他人提供推广、引流等帮助的犯罪分子，特别是与诈骗集团存在事前通谋、事中勾连，形成较为稳定协作关系的人员和组织者，一般以诈骗罪的共犯论处；对于明知他人实施信息网络犯罪活动，为他人提供软件开发、技术支持、账号维护等帮助行为的犯罪分子，一般以帮助信息网络犯罪活动罪论处。

电信诈骗受害者“劝阻难”

劝阻受害者是一大难点。很多时候即便对受害者进行劝阻，都难以阻止损失。“很多受害者完全被诈骗分子‘洗脑’，听不进。”上海市反电信网络诈骗中心负责电话劝阻的工勤主管吴明凯表示。

为何“难”？上海市公安局浦东分局反诈中心副大队长龚海青认为，是电诈犯罪分子通过话术给受害者构建了认知陷阱。如在以财色为饵的“投资”“刷单”“裸聊”类案件中，“再充值、转账一些，就把之前的还来（或把视频销毁）”，“利用受害者想要挽回的心理，持续要求转账汇款，实际上犯罪分子贪得无厌，转账越多损失越大。”（摘自：拆解电信诈骗：从洗脑开始，如何一步步掏空你的钱袋）

来源：环球时报　2023-06-13

提醒！这几种工作千万别碰，全部涉嫌违法犯罪！

一、帮助诈骗分子取现

不少不法分子为了快速转移赃款，会雇佣人员帮其在线下取现并转移资金，有些兼职工作是帮其买贵金属等，并许诺高额报酬，其实这些工作就是充当电信网络诈骗犯罪行为洗钱的“工具人”。

二、买卖电话卡和银行账户

出租、出借、出售自己的电话卡和银行账户，或是充当线下“卡头”“卡贩”，为了一时的利益变成了诈骗分子的帮凶，殊不知就是因为这些被卖出的大量“实名不实人”的电话卡和银行账户，被诈骗分子用于实施电信网络诈骗，使不少人因骗致贫，同时自己也会因此承担严重的法律责任。

三、搭建 GOIP、VOIP

诈骗分子大多藏身境外，他们会以“高薪招聘”为诱饵，诱使求职者在国内租房搭建虚拟拨号设备实现远程操控手机卡，给国内受害人拨打诈骗电话、群发诈骗短信来实施诈骗。通过这些虚拟拨号设备将境外电话转化为境内本地电话，增大了迷惑性，导致受害人更容易被骗。

四、冒充客服电话引流

有些诈骗团伙会招募“话务员”，要求入职者按照设定好的话术，按照非法获取到的公民信息名单拨打电话或发送短信，自称是各类平台的“客服”，引导受害人添加上游诈骗分子的联系方式。这种工作就是诈骗引流行为。

五、线下推广引流

线下推广引流多以赠送小礼品为诱饵，要求事主扫描二维码或是用拉人建群、发送虚假广告来免费领取小礼品。而这些所谓的兼职工作其实是帮诈骗分子进行地推式引流，为诈骗分子下一步实施诈骗作准备。

来源：商城县人民法院　2023-07-03

电信诈骗的 7 大类型

1、仿冒身份类

陌生人以权威名义恐吓？不存在所谓的“安全账户”

【套路】冒充秘书；冒充亲友；冒充公司老总；补助救助、助学金；冒充公检法电话；伪造特定身份(高富帅、白富美)；医保、社保；“猜猜我是谁”。

【防范建议】公检法执法部门有严格的办案程序，一定会有民警当面与事主做笔录，不会通过电话调查所谓的涉嫌犯罪等问题，也不会相互接转电话，不存在所谓的“安全账户”。同时，陌生人的电话，一定要小心。

2、约会交友类

巨额财富“莫名”就会砸向你？切勿轻信未曾谋面的他

【套路】编造自己家庭情况或频繁联系以取得对方的基本信任；一般只通过网络或电话交流，要求汇款而不见面；男性冒充海归，声称患病或受到政治迫害，要女方借大量金钱支援。女性声称父母家人患病或突遇事故，急需医治，寻求帮助。在约会过程中，来电谎称途中发生车祸，要对方把钱打到自己卡上。以不便充值为理由，要求汇款、充值话费或 Q 币等。

【防范建议】遇到非常热情，联系时间很短就主动要求确立情侣关系的人需要提高警惕。请勿相信任何未曾见面即要求汇款或充值的理由，即便见面后，对于涉及到金钱往来的事情，也需格外小心。

3、购物退款类

购物后，有人“好心”退款？小心别人要窥探你的账户密码！

【套路】假冒代购；退款；网络购物；低价购物；解除分期付款；收藏；快递签收。

【防范建议】不要轻信未知来源的“客服”“售后”，切勿乱扫不明二维码。

4、利益诱惑类

理财师竟会邀请陌生人投资发财？“内部消息”是诈骗者的谎言

【套路】诈骗方多称自己是证券、投资公司等内部人员，行骗目标为有一定经济能力的网友;联系不久即开始炫耀自身的投资获利丰厚,希望一起进行投资;承诺潜在受害者事先支付一笔费用后可获得数量可观的佣金;如网友起疑，提供虚假身份证、海外电话号码、伪造相关证件等方式博取信任，要求汇款。

【防范建议】不要相信任何所谓“内部消息”去委托他人进行投资理财。对于炫耀自身投资获利丰厚的人需要提高警惕。

5、虚构险情类

“外甥”来电要舅舅付嫖娼罚款？冷静应对突发紧急情况

【套路】通过虚构车祸、绑架、手术、危难困局求助、包裹藏毒品等意外不测，及合成照片勒索等，让用户惊吓不安的消息实施诈骗。

【防范建议】遇到此类情况，应向相关当事方进行核实，切勿随便转账。

6、生活消费类

遇特殊情况需身份证号、银行卡号？请拒绝陌生人的转账要求

【套路】针对日常生活中的各种缴费、消费等实施诈骗，如:冒充房东短信、欠费、购物退税、机票改签、订票、ATM 机告示、刷卡消费、引诱汇款。

【防范建议】验证信息真伪。拨打官方电话或通讯录中存有的号码，不要拨打短信中的电话号码。如果电话中提出要你转账，一律拒绝。

7、木马信息类。

老友的请柬还需打开信息链接？请通过正规途径核实真实性

【套路】校讯通短信链接、结婚电子请柬、相册木马、账户有资金异常变动等。

【防范建议】若收到此类来源不明的信息，应做到不相信，不点击，立即拨打正规客服电话，确认信息真实性。特别是兑积分、抢红包的网页打开后，往往要你输入银行账号与密码，此时千万要冷静，不要一时贪婪冒险尝试。

电信诈骗的 10 类高发多发电信诈骗

01 网络贷款诈骗手法揭秘“低门槛”广告+网贷 APP

国家反诈中心提醒：**警惕“无抵押、低利率”网贷平台**

当有人向你推销贷款时，一定要小心。诈骗分子先让你在虚假贷款网站或 APP 上填写个人信息，再以信息填报错误、贷款额度被锁定等理由，诱骗你缴纳保证金或者解冻金。任何声称“无抵押、低利率”的网贷平台都有极大风险。一

旦发现被骗，请及时报警。

02 网络刷单诈骗手法揭秘兼职刷单+网络博彩

国家反诈中心提醒：**所有刷单都是诈骗**

所谓刷单，就是通过网上购物方式为网店刷信誉或者充值刷流水，网店向刷单者返还货款并支付佣金的违法行为。诈骗分子往往以兼职刷单名义，先以小额返利为诱饵，诱骗你投入大量资金后，再把你拉黑。千万不要轻信兼职刷单广告，所有刷单都是诈骗，不要缴纳任何保证金、押金。一旦发现被骗，请及时报警。

03 “杀猪盘”诈骗手法揭秘网上“美女、帅哥”+投资“赢利”

国家反诈中心提醒：**网恋还能赚大钱一定是诈骗**

当有陌生人加你为好友时，一定要小心。诈骗分子往往先以甜言蜜语或者献殷勤等方式博取好感和信任，再向你推荐所谓“稳赚不赔、低成本高回报”的网络投资平台。当你越投越多时，就会把你拉黑。从网恋“一见钟情”开始，到参与网络赌博或投资诈骗结束，直到受害者倾家荡产甚至背负巨债，这就是“杀猪盘”诈骗。一旦发现被骗，请及时报警。

04 冒充客服退款诈骗手法揭秘“客服主动退款”+申请平台贷款

国家反诈中心提醒：**警惕“好心卖家”或“客服”**

接到自称“卖家”或“客服”的电话说需要退款或重新支付时，当事人一定要登录官方购物网站查询相关信息，不要点击对方提供的网址链接，更不能在这些网址上填写任何个人信息。一旦发现被骗，请及时报警。

05 假冒熟人诈骗手法揭秘用朋友头像加好友+“暂时借钱”

国家反诈中心提醒：**熟人借钱要先核实**

无论是谁，通过微信、QQ、短信让你转账汇款时，一定要用电话、视频等方式核实，切勿盲目转账。一旦发现被骗，请及时报警。

06 冒充“公检法”诈骗手法揭秘“公安调查”+“冻结账户”

国家反诈中心提醒：**转账汇款自证清白是诈骗**

凡是自称“公检法”要求你转账汇款自证清白的，都是诈骗。一旦发现被骗，请及时报警。

07 “荐股”诈骗手法揭秘“理财导师”+虚假平台

国家反诈中心提醒：**群里只有一根“真韭菜”**

一进股票群，套路深似海。“老师”“学员”都是托儿，炒股软件都是假，只有你是“真韭菜”。一旦发现被骗，请及时报警。

08 虚假购物诈骗手法揭秘网络广告+“购物送抽奖”

国家反诈中心提醒：**不轻信、不尝试**

在网络购物中发现商品价格远低于市场价格时，一定要提高警惕，谨慎购买，不要将钱款直接转给对方。一旦发现被骗，请及时报警。

09 注销“校园贷”诈骗手法揭秘“注销不良记录”+指导贷款

国家反诈中心提醒：**注销“校园贷”都是诈骗**

凡是声称你有“校园贷”记录需要注销、否则会影响征信的，都是诈骗，切勿转账汇款。一旦发现被骗，请及时报警。

10 买卖游戏币诈骗手法揭秘“低价充值”+“充值解冻”

国家反诈中心提醒：**私下交易存在被骗风险**

买卖“游戏币”、游戏账号时，不要轻信“低价充值”和“高价收购”，不要轻易点击对方提供的网址链接，一定要在官网上进行操作。一旦发现被骗，请及时报警。

认清诈骗常用的五步“剧本”

第一步：骗取信任。骗子通过网络购买等多种渠道收集受害者个人信息，例如身份证号、住址、消费记录等隐私来取得受害者初步信任，同时会通过改号软件将来电显示为警方办公电话，让受害人拨打 114 查询验证，进一步增强信任。

第二步：震慑。骗子会通过声色俱厉的语气，在彰显权威的同时强势震慑并控制受害人。

第三步：恐吓。骗子让受害者彻底相信自己卷入了一个重大案件或事件，随时可能被逮捕。为了增强恐吓，让骗局更加逼真，骗子会通过虚假政法机关官网或网络传真让受害人收到一份通缉令。

第四步：转账。利用受害人的恐慌心理，缓和语气，耐心诱骗受害人入局。

第五步：电话遥控转账。骗子声称资金调查，实则是要求受害人将银行卡插入 ATM 机，然后把卡内的资金转到指定的账户。

至此，整个诈骗过程完成，受害人卡上的存款将全部落入骗子手中。但这还不是骗局终结，很快，受害人还会继续接到威逼转账的电话，诈骗剧本要求，一旦上钩就要吃干榨净，直到卖车卖房。（摘自：全民反诈大行动：7 大类型、10 种骗术、5 个诈骗心法，请全员提前做好防范）

来源：日喀则市反诈骗中心　2023-05-05

全链条打击，遏制电诈上升态势

电诈境外窝点迅速扩张，诈骗手法不断翻新

目前，刷单返利、虚假网络投资理财、虚假网款、冒充公检法、婚恋交友等10种诈骗类型已经成为最常见的高发案件，占发案的80%左右；其中刷单返利类诈骗发案率最高，占发案的1/3左右；虚假网络投资理财类诈骗造成损失的金额最大，占损失金额的1/3左右。

诈骗分子大量使用境外通联工具，开发涉诈APP、云语音、虚拟币转账洗钱等新技术手段实施诈骗，逃避中国警方打击。一些犯罪分子使用成本更低、隐蔽性更强、操作更简单的新型“简易组网 GOIP”设备，在境外操控境内手机拨打诈骗电话，具有很强的伪装性，老百姓很难分辨。

随着国内打击的力度不断加大，电诈境外窝点迅速扩张，在一些国家和地区，形成赌诈园区，其中很多被包装成“工业园区”“科技园区”，然后打着“高薪招聘”的幌子，从事电诈、网络赌博等违法犯罪活动。一些学生、务工人员等群体被“机票报销”“稳赚不赔”“月入十万”等“优厚条件”诱惑，身陷诈骗窝点。

“在选择出国务工时，一定要慎重选择正规劳务公司，签订规范合同，不要被‘高薪招聘’蒙蔽双眼。”公安部刑侦局打击新型网络犯罪指导处处长张硕提醒。

强化源头管控，斩断违法犯罪资金链，挤压涉诈犯罪生存空间

近年来，多地公安机关与当地银行建立警银联动机制。银行网点筑牢资金“第一道防线”，加强客户身份识别，对银行账户风险和可疑信息早识别、早发现，积极与警方合作，力争从源头斩断违法犯罪资金链。

公安机关坚持问题导向，持续深入推进“断卡”行动，将打击重点瞄准卡贩、卡商，力争打掉源头、切断渠道、铲除土壤。同时，公安部结合反电信网络诈骗法，联合最高法、最高检进一步完善“两卡”犯罪法律适用标准，用足用好法律武器，全面提升打击质效。

依法严打严惩战果丰硕，法律政策不断完善，全国逐渐构建全链条重拳打击涉诈犯罪生态系统。各地区各行业全面梳理本地区、本领域存在的涉诈风险和管理漏洞，做到风险隐患清零。工信部开通“一证通查”服务和启动“断卡行动2.0”以来，组织集中排查处置涉诈高危电话卡近亿张，清理关联互联网账号近亿个，有力挤压了涉诈犯罪生存空间。

公安机关创新事前预防方式手段，最大限度减少电诈案件发生

电诈是可防性犯罪，事后打击不如事先防范。为了进一步树牢全民反诈意识、防骗自觉，各地公安机关创新电诈事前预防方式手段。

上海市公安局刑事侦查总队九支队支队长徐瑜介绍，通过搭建预警数据模型等工作措施，分析发现潜在的受害群众，进行分级分类处理，实现精准预警、有效防范。”。

浙江省诸暨市公安局陶朱派出所创建了企业微信号，对于放贷前要求缴纳解冻金、认证金、手续费等诈骗行为，及时发出微信提醒。微信号现已添加辖区群众 7 万多名，阻止了 200 余起电诈案件的发生。（原标题：不法分子不断翻新诈骗形式与作案手段，各地公安机关——全链条打击，遏制电诈上升态势）

来源：人民日报　2023-06-28

各地采取多种反诈措施，减少群众财产损失预警劝阻别忽视财产安全要重视

采取发短信、打电话、见面劝阻等方式分类开展劝阻

近年来，针对电诈高发态势和新特点新手段，各地警方聚焦事前预警劝阻，创新技战法，把潜在受骗人按照风险等级分级，相应采取发短信、打电话、见面劝阻等方式分类开展劝阻，对正在遭受电诈或有潜在被骗风险的人群开展劝阻工作。

从当前预警劝阻工作实际来看，诈骗分子引导受害人拒绝或不听从民警劝阻，导致诈骗行为不能及时制止的情况仍时有发生。

“骗子们的‘剧本’量身定制、随机应变，极易洞穿一些人薄弱的心理防线。”公安部刑侦局打击新型网络犯罪指导处处长张硕提醒：“我们每个人都可能成为骗子的目标，特别是在防范刷单、投资理财类诈骗方面，千万不要存在贪小便宜、一夜暴富和投机心理。如果警察上门劝阻，请务必听劝。”

预警劝阻工作涉及面广，需社会各界共同发力

面对紧急高危预警，既需要公安民警及时上门劝阻，还需要社区网格员发挥“人熟、地熟、情况熟”优势，破解“找不到、不听劝、来不及”的难题。

针对潜在受害人，多方叠加的见面劝阻提升防范诈骗的工作成效。近年来，各地公安机关积极调动社区工作者、网格员参与反诈工作，并在社区、乡村、企业、高校等建立反诈宣防志愿者队伍，构筑起依靠基层群团组织、覆盖一线基本

单元的防控体系，不断营造全警反诈、全民反诈的社会氛围。

强化大数据技术应用，提高预警精准性和劝阻效果

各地公安研发上线“预警画像”应用，运用大数据分类归集辖区电诈警情案件时空数据以及受骗对象基础数据，生成电诈案件热力图，展示近期不同区域内高发案件类型、作案方式、易受骗人群常见职业和年龄分布等，为一线民警开展预警劝阻提供精准信息。

来源：人民网-人民日报　2023-07-11

2022 年全国公安机关破获电信网络诈骗犯罪案件 46.4 万起

2022 年，全国公安机关破获电信网络诈骗犯罪案件 46.4 万起，缉捕电信网络诈骗犯罪集团头目和骨干 351 名。

公安部建立分级分类预警劝阻机制，累计向各地推送预警指令 2.4 亿条；工信部持续提升行业监测、预警、处置能力，累计拦截诈骗电话 21 亿次、短信 24.2 亿条，处置涉案域名网址 266 万个；中央网信办封堵境外涉诈网址 79.9 万个、IP 地址 3.8 万个；人民银行持续优化涉诈资金查控，协助公安机关紧急拦截涉案资金 3180 余亿元；中宣部、公安部、教育部、财政部等坚持广泛宣传和精准宣传相结合，组织开展“五进”宣传活动，不断提升群众识骗防骗能力。

各地区各部门将始终保持对电信网络诈骗的高压严打态势，坚持专项治理与系统治理、综合治理、依法治理、源头治理相结合，从严从实从细抓好重点任务推进落实，坚决遏制电信网络诈骗违法犯罪多发高发态势，坚决维护人民群众财产安全和合法权益。

来源：新华社　2023-05-30

警惕!“AI 换脸”新骗局

面对利用 AI 技术的新型骗局，广大公众需提高警惕，加强防范。

一、做好个人信息安全第一责任人

1、加强个人信息保护意识，防止信息泄露：不轻易提供人脸、指纹等个人生物信息给他人；不要轻易透露自己的身份证、银行卡、验证码等信息；不要贪图方便把身份证、银行卡照片等直接共同存放于手机内。

提示：发现 APP 过度、强制收集个人信息，请至 12321.cn 投诉。

2、陌生链接不要点、陌生软件不要下载、陌生好友不要随便加、不明二维码不要随便扫。管理好自己的朋友圈，不要向陌生人开启手机屏幕共享。

3、做好个人防护，安装安全软件，防止手机和电脑中病毒；对个人账户的安全　状况保持警惕，尤其是陌生设备的登陆情况，防止微信、QQ 等被盗号给亲朋好友带来麻烦。

4、对于不常用的 APP，建议卸载前注销个人帐号。

提示：APP 不提供个人帐号注销方式，或为注销帐号设置各类障碍的，请至 12321.cn 投诉。

二、远程转账务必多重验证，把好“钱袋子”

如果有人自称“家人”“朋友”“老师”“领导”通过社交软件、短信、电子邮件等以“手机掉水里了，学校需要紧急交辅导班学费”“人在境外旅游需要帮忙买机票”“给领导办私事需紧急转账”“遭遇车祸需要马上手术”“情况特殊，需要过桥资金拆借”等各种方式和理由诱导你转账汇款，务必第一时间提高警惕。在 AI 时代，文字、声音、图像和视频都有可能是深度合成的，在转账汇款、资金往来这样的典型场景，要通过回拨对方手机号等额外通信方式核实确认，不要仅凭单一沟通渠道未经核实就直接转账汇款！无论对方是谁！

提示：遭遇诈骗信息，请至 12321.cn 反诈专栏举报，如发生资金损失请及时报警。(原标题：中国互联网协会：警惕!“AI 换脸”新骗局)

来源：中国互联网协会　2023-05-25

关于电诈等案件适用法律若干问题的意见

对诈骗数额的界定

（一）根据《最高人民法院、最高人民检察院关于办理诈骗刑事案件具体应用法律若干问题的解释》第一条的规定，利用电信网络技术手段实施诈骗，诈骗公私财物价值三千元以上、三万元以上、五十万元以上的，应当分别认定为刑法第二百六十六条规定的“数额较大”“数额巨大”“数额特别巨大”。

二年内多次实施电信网络诈骗未经处理，诈骗数额累计计算构成犯罪的，应当依法定罪处罚。

实施电信网络诈骗犯罪达到相应数额标准从重处罚情形

1．造成被害人或其近亲属自杀、死亡或者精神失常等严重后果的；

2．冒充司法机关等国家机关工作人员实施诈骗的；

3．组织、指挥电信网络诈骗犯罪团伙的；

4．在境外实施电信网络诈骗的；

5．曾因电信网络诈骗犯罪受过刑事处罚或者二年内曾因电信网络诈骗受过行政处罚的；

6．诈骗残疾人、老年人、未成年人、在校学生、丧失劳动能力人的财物，或者诈骗重病患者及其亲属财物的；

7．诈骗救灾、抢险、防汛、优抚、扶贫、移民、救济、医疗等款物的；

8．以赈灾、募捐等社会公益、慈善名义实施诈骗的；

9．利用电话追呼系统等技术手段严重干扰公安机关等部门工作的；

10．利用“钓鱼网站”链接、“木马”程序链接、网络渗透等隐蔽技术手段实施诈骗的。

实施电信网络诈骗犯罪，诈骗数额接近“数额巨大”“数额特别巨大”的标准，具有上述规定的情形之一的，应当分别认定为刑法第二百六十六条规定的“其他严重情节”“其他特别严重情节”。

诈骗罪（未遂）定罪处罚规定

实施电信网络诈骗犯罪，犯罪嫌疑人、被告人实际骗得财物的，以诈骗罪（既遂）定罪处罚。诈骗数额难以查证，但具有下列情形之一的，应当认定为刑法第二百六十六条规定的“其他严重情节”，以诈骗罪（未遂）定罪处罚：

1．发送诈骗信息五千条以上的，或者拨打诈骗电话五百人次以上的；

2．在互联网上发布诈骗信息，页面浏览量累计五千次以上的。

具有上述情形，数量达到相应标准十倍以上的，应当认定为刑法第二百六十六条规定的“其他特别严重情节”，以诈骗罪（未遂）定罪处罚。

对掩饰、隐瞒犯罪所得、犯罪所得收益罪的规定

明知是电信网络诈骗犯罪所得及其产生的收益，以下列方式之一予以转账、套现、取现的，依照刑法第三百一十二条第一款的规定，以掩饰、隐瞒犯罪所得、犯罪所得收益罪追究刑事责任。但有证据证明确实不知道的除外：

1．通过使用销售点终端机具（POS 机）刷卡套现等非法途径，协助转换或者转移财物的；

2．帮助他人将巨额现金散存于多个银行账户，或在不同银行账户之间频繁划转的；

3．多次使用或者使用多个非本人身份证明开设的信用卡、资金支付结算账户或者多次采用遮蔽摄像头、伪装等异常手段，帮助他人转账、套现、取现的；

4．为他人提供非本人身份证明开设的信用卡、资金支付结算账户后，又帮助他人转账、套现、取现的；

5．以明显异于市场的价格，通过手机充值、交易游戏点卡等方式套现的。

实施上述行为，事前通谋的，以共同犯罪论处。

实施上述行为，电信网络诈骗犯罪嫌疑人尚未到案或案件尚未依法裁判，但现有证据足以证明该犯罪行为确实存在的，不影响掩饰、隐瞒犯罪所得、犯罪所得收益罪的认定。

以共同犯罪论处的情形

明知他人实施电信网络诈骗犯罪，具有下列情形之一的，以共同犯罪论处，但法律和司法解释另有规定的除外：

1．提供信用卡、资金支付结算账户、手机卡、通讯工具的；

2．非法获取、出售、提供公民个人信息的；

3．制作、销售、提供“木马”程序和“钓鱼软件”等恶意程序的；

4．提供“伪基站”设备或相关服务的；

5．提供互联网接入、服务器托管、网络存储、通讯传输等技术支持，或者提供支付结算等帮助的；

6．在提供改号软件、通话线路等技术服务时，发现主叫号码被修改为国内党政机关、司法机关、公共服务部门号码，或者境外用户改为境内号码，仍提供服务的；

7．提供资金、场所、交通、生活保障等帮助的；

8．帮助转移诈骗犯罪所得及其产生的收益，套现、取现的。

此外，负责招募他人实施电信网络诈骗犯罪活动，或者制作、提供诈骗方案、术语清单、语音包、信息等的，以诈骗共同犯罪论处。

涉案财物的处理

（一）公安机关侦办电信网络诈骗案件，应当随案移送涉案赃款赃物，并附清单。人民检察院提起公诉时，应一并移交受理案件的人民法院，同时就涉案赃款赃物的处理提出意见。

（二）涉案银行账户或者涉案第三方支付账户内的款项，对权属明确的被害人的合法财产，应当及时返还。确因客观原因无法查实全部被害人，但有证据证明该账户系用于电信网络诈骗犯罪，且被告人无法说明款项合法来源的，根据刑法第六十四条的规定，应认定为违法所得，予以追缴。

被告人已将诈骗财物用于清偿债务或者转让给他人，具有下列情形之一的，应当依法追缴：

1．对方明知是诈骗财物而收取的；

2．对方无偿取得诈骗财物的；

3．对方以明显低于市场的价格取得诈骗财物的；

4．对方取得诈骗财物系源于非法债务或者违法犯罪活动的。

他人善意取得诈骗财物的，不予追缴。（摘自：关于办理电信网络诈骗等刑事案件适用法律若干问题的意见（全文））

来源：检察日报　2016-12-21

对电信网络诈骗犯罪地的规定

电信网络诈骗犯罪地，除《最高人民法院、最高人民检察院、公安部关于办理电信网络诈骗等刑事案件适用法律若干问题的意见》规定的犯罪行为发生地和结果发生地外，还包括：

（一）用于犯罪活动的手机卡、流量卡、物联网卡的开立地、销售地、转移地、藏匿地；

（二）用于犯罪活动的信用卡的开立地、销售地、转移地、藏匿地、使用地以及资金交易对手资金交付和汇出地；

（三）用于犯罪活动的银行账户、非银行支付账户的开立地、销售地、使用地以及资金交易对手资金交付和汇出地；

（四）用于犯罪活动的即时通讯信息、广告推广信息的发送地、接受地、到达地；

（五）用于犯罪活动的“猫池”（Modem Pool）、GOIP 设备、多卡宝等硬件设备的销售地、入网地、藏匿地；

（六）用于犯罪活动的互联网账号的销售地、登录地。

伪造、变造证件等及利用其办理双卡、账户等的处罚

在网上注册办理手机卡、信用卡、银行账户、非银行支付账户时，为通过网上认证，使用他人身份证件信息并替换他人身份证件相片，属于伪造身份证件行为，符合刑法第二百八十条第三款规定的，以伪造身份证件罪追究刑事责任。

使用伪造、变造的身份证件或者盗用他人身份证件办理手机卡、信用卡、银行账户、非银行支付账户，符合刑法第二百八十条之一第一款规定的，以使用虚假身份证件、盗用身份证件罪追究刑事责任。

实施上述两款行为，同时构成其他犯罪的，依照处罚较重的规定定罪处罚。法律和司法解释另有规定的除外。

为他人用信息网络实施犯罪被认定为“帮助”的行为

为他人利用信息网络实施犯罪而实施下列行为，可以认定为刑法第二百八十七条之二规定的“帮助”行为：

（一）收购、出售、出租信用卡、银行账户、非银行支付账户、具有支付结算功能的互联网账号密码、网络支付接口、网上银行数字证书的；

（二）收购、出售、出租他人手机卡、流量卡、物联网卡的。

为网络犯罪提供帮助被认定为“其他情节严重的情形”的行为

明知他人利用信息网络实施犯罪，为其犯罪提供下列帮助之一的，可以认定为《最高人民法院、最高人民检察院关于办理非法利用信息网络、帮助信息网络犯罪活动等刑事案件适用法律若干问题的解释》第十二条第一款第（七）项规定的“其他情节严重的情形”：

（一）收购、出售、出租信用卡、银行账户、非银行支付账户、具有支付结算功能的互联网账号密码、网络支付接口、网上银行数字证书 5 张（个）以上的;

（二）收购、出售、出租他人手机卡、流量卡、物联网卡 20 张以上的。

电诈中被认定为犯掩饰、隐瞒犯罪所得、犯罪所得收益罪的行为

明知是电信网络诈骗犯罪所得及其产生的收益，以下列方式之一予以转账、套现、取现，符合刑法第三百一十二条第一款规定的，以掩饰、隐瞒犯罪所得、犯罪所得收益罪追究刑事责任。但有证据证明确实不知道的除外。

（一）多次使用或者使用多个非本人身份证明开设的收款码、网络支付接口等，帮助他人转账、套现、取现的;

（二）以明显异于市场的价格，通过电商平台预付卡、虚拟货币、手机充值卡、游戏点卡、游戏装备等转换财物、套现的;

（三）协助转换或者转移财物，收取明显高于市场的“手续费”的。

实施上述行为，事前通谋的，以共同犯罪论处；同时构成其他犯罪的，依照处罚较重的规定定罪处罚。法律和司法解释另有规定的除外。（摘自：关于办理电信网络诈骗等刑事案件适用法律若干问题的意见（二））

来源：最高人民检察院　2021-06-22