摘要：网络犯罪案件，已成为当今社会各类犯罪中占比较高的案件，由于网络犯罪案件涵盖领域极为广泛，刑事辩护领域中针对网络犯罪案件的思维、方法也数不胜数。为此，本文将对电信网络诈骗案件中末端人员关联犯罪的实体辩护进行重点分析，力求做到具体案件中辩护工作的精准化、精细化。

关键词：电信网络诈骗 末端人员 关联犯罪 实体辩护 罪名 建议

随着科技的迅猛发展与人类文明的不断进步，互联网已经成为人们生活中不可或缺的一部分。然而，在人们享受科技红利的同也产生了很多财产、个人信息等领域的安全问题。传统盗窃案件数量明显下降，电信诈骗案件随处可闻，关于互联网犯罪在很多领域出现了新问题，各种相关的计算机犯罪屡禁不止。目前，电信网络诈骗案件组织网络庞大、涉及领域极为广泛，由于网络环境的特殊性，很难抓捕到真正实施诈骗的团伙，大多是帮助取款、帮助网络建设、帮助转移涉案款物的帮助人员甚至是边缘人员，笔者将边缘人员看作关联犯罪人员。

本文旨在论述电信网络诈骗案件中关联犯罪人员的罪名认定及实体辩护问题。现实中，某些地区的司法机关机械性的适用法律（法规、解释等），认为只要帮助电信网络诈骗犯罪活动，即为诈骗罪的帮助犯，或者认为应当以掩饰隐瞒犯罪所得（收益）罪定罪，认为帮助信息网络犯罪活动罪较轻，不利于打击电信网络诈骗犯罪活动。因此，笔者通过自身办案经验及总结，对电信网络诈骗关联犯罪人员的罪名认定以及实体辩护问题进行深入阐述。

一、电信网络诈骗末端关联犯罪人员的基本概述

（一）电信网络诈骗的概念

电信网络诈骗，是指通过电话、网络和短信方式，编造虚假信息，设置骗局，对不特定受害人实施远程、非接触式诈骗，诱使受害人打款或转账的犯罪行为的诈骗型犯罪，而对特定人员石勇QQ、微信等网络工作实施诈骗则不应评价为电信网络诈骗。通常以冒充他人及仿冒、伪造各种合法外衣和形式的方式达到欺骗目的，如冒充公检法、商家（公司、厂家）、国家机关工作人员、银行工作人员等各类机构工作人员，以伪造和冒充招工、刷单、贷款、手机定位和招嫖等形式进行诈骗。

本文旨在论述电信网络诈骗案件末端关联犯罪人员的实体辩护研究，重点论述的末端关联犯罪人员是指使用银行卡、支付宝等账户帮助进行资金结算或者转移资金的人员，一般处在电信网络诈骗完成后的事后、最末端的资金处理阶段，可能构成如掩饰隐瞒犯罪所得及其收益罪、帮助信息网络犯罪活动罪等罪名。在实践中，我们常会遇到帮助利用涉案资金购买虚拟货币，之后再将虚拟货币的支付链接转给上线人员，或者专门帮助上线人员收购银行卡，帮助上线人员取款等案件情况。

（二）电信网络诈骗案件的特点、发展趋势及类型

既然要研究个罪构成及实体辩护问题，就要分析电信网络诈骗案件的基本特点、发展趋势及类型等。

1、电信网络诈骗案件的形势

据公安部2021年1月2日发布的数据显示，2020年以来，全国公安机关持续深入打击电信网络诈骗犯罪活动，集中开展“云剑-2020”“断卡”“长城2号”等专项行动，共破获电信网络诈骗案件25.6万起，抓获犯罪嫌疑人26.3万名，拦截诈骗电话1.4亿个、诈骗短信8.7亿条……

据360联合中国信息通信研究院发布的《2020年中国手机安全状况报告》（以下简称《360报告》）显示，2020年，360手机先赔共接到手机诈骗举报2656起。其中诈骗申请（被认定为具备诈骗情形的举报）1340起，涉案总金额高达1520.2万元，人均损失11345元，金融理财类诈骗是举报人数最多的诈骗类型。在所有诈骗申请中，金融理财占比最高达23.4%；其次是虚假兼职诈骗（占比18.4%）和交友诈骗（占比15.8%）等。从涉案总金额来看，金融理财类诈骗总金额最高，达482.9万元，占比31.8%；其次是身份冒充诈骗，涉案总金额393.2万元，占比25.9%；虚假兼职排第三，涉案总金额235.5万元，占比15.5%。黑产供应商也日趋“职业化”，出现了可以为博彩提供一条龙服务的“包网”平台，可以提供建站、维护、活动策划、支付接口、域名、服务器、漏洞防御、反套利、后台系统等一系列与博彩运作相关的服务。

2、电信网络诈骗案件的特点

（1）犯罪手段科技化。电信网络诈骗犯罪分子掌握了短信群发、电话号码改号、网络盗号、网上银行操作等技术，而这些操作与被害人之间都是非接触式的，这与过去诈骗的接触式操作特点有明显区别。诈骗犯罪者利用新型先进作案设备(智能手机、短信群发器、电脑、网络服务器等)以及网络手段和社交软件(微信、QQ等)，通过盗号来获取被害人的个人信息从而实施诈骗，有的电话诈骗犯罪分子已熟练掌握伪基站技术和VOIP技术，用技术手段通过改变号码来进行语音诈骗，更有甚者是

冒充被害人身份通过发信息手段让被害人的好友向其提供的账号里汇款来实施诈骗。随着电信网络技术的快速发展，电信网络诈骗技术亦已更新，犯罪分子从被害人信息窃取(通过语音电话或简讯，亦或钓鱼网站信息发送途径)到银行网银分批转账，再到ATM机取现的一整套诈骗流程操作非常熟练。

（2）诈骗方式多样化。传统的电信诈骗无非是利用电话、短讯采用冒充熟人或一些机构进行诈骗，而随着互联网技术的迅猛发展，现代电信网络诈骗方式已经变得五花八门，网络电话由于监管漏洞已成为犯罪分子作案的重要平台。此外，钓鱼网站的建立、越来越多的网络社交平台的出现都容易被电信网络诈骗犯罪者恶意利用，成为其犯罪的工具。犯罪形式上也呈现出多样化的特点，如冒充公检法诈骗、发送虚假中奖信息诈骗所谓的“手续费”、网购诈骗等具体诈骗方式已经去单一化，电信网络诈骗呈现出多样化的作案方式，给公安机关侦查工作制造了多重障碍。

（3）作案手段隐蔽化。电信网络诈骗犯罪相较于传统犯罪不同，它是通过虚拟网络来实施的，犯罪分子不与被害人直接接触实施的犯罪，没有传统刑事犯罪的作案现场，因其利用网络、邮件、短信、即时通讯等科技手段实施犯罪，所以被害人不知犯罪分子的外貌特点，而且被害人所掌握的犯罪分子的电话号或IP都是经过技术处理的虚假信息，这些隐蔽的作案手段都增加了警方破案的难度。

（4）犯罪现场流动化。电信网络诈骗犯罪分子利用互联网的灵活性和便捷性可以随时变换作案地点。即使被公安部门循着IP发现蛛丝马迹，此时犯罪分子早已逃之天天。电信网络诈骗犯往往分工明确，分别承担打电话、发短信、网络技术操作等工作。而这些分工也完全可以分散实施，所以公安部门实施抓捕时很难将电信诈骗集团一网打尽。

（5）犯罪群体职业化。电信网络诈骗犯罪由最开始的零散作案，到目前已经演变成组织化、团伙化、集团化的特点。电信诈骗犯罪大多是团伙作案，一般分为技术、信息、通话、转账、取款等几个不同部门。这些部门分工明确，技术部门负责租赁网络服务器，利用网络平台漏洞，借助VOIP网络技术为其他部门提供被害人个人信息、电话号码改号等诈骗“硬”技术支持；信息部门和通话部门主要是利用盗取的被害人信息进行拨打电话具体实施诈骗；转账和取款则是在诈骗得手后实施的程序，也是电信网络诈骗的最后阶段。当前，电信诈骗犯罪产业化趋势明显，从国内近期摧毁的几个电信诈骗团伙看，团伙职业化特征十分明显，出现了“公司型、集团型”结构。

（三）公安部部署“断卡行动”以来的案件形势

2020年10月10日，国务院打击治理电信网络新型违法犯罪工作部际联席会议召开全国“断卡”行动部署会，公安部副部长、部际联席会议召集人杜航伟强调，非法

开办贩卖电话卡、银行卡是电信网络诈骗案件持续高发的重要根源，危害十分严重。

杜航伟要求，要打击整治惩戒多管齐下，坚决打赢“断卡”行动攻坚战。各地各部门要坚持以打开路，以打促治，以打促防，综合采取多种措施，集中抓获一大批非法开办贩卖“两卡”违法犯罪团伙，整治一大批“两卡”违法犯罪猖獗的重点地区，惩戒一大批“两卡”违法失信人员，全力斩断非法开办贩卖“两卡”产业链，坚决铲除电信网络诈骗犯罪滋生土壤。

2020年至会议期间，按照全国打击治理电信网络新型违法犯罪工作电视电话会议部署要求，各地各部门深入开展打击治理工作，全国共破获电信网络诈骗案件15.5万起，抓获嫌疑人14.5万名，同比分别上升65.6%和74.1%；累计封堵涉诈域名网址21万个，拦截处置诈骗电话5100万余次、诈骗短信6.3亿余条，成功止付冻结涉案资金1000余亿元。

自全国“断卡”行动部署开展以来，截至2021年1月15日，共打掉涉“两卡”违法犯罪团伙7816个，抓获涉“两卡”犯罪嫌疑人14.8万名，公开惩戒涉“两卡”违法犯罪嫌疑人5.7万余名，累计治理行业网点、机构8869个，打击治理工作取得阶段性明显成效。

以上，为电信网络诈骗犯罪案件关联犯罪人员的基本概述。

二、针对关联犯罪案件的实体辩护的空间研究

本文中所提到的电信网络诈骗关联犯罪人员通常情况下主要涉及的罪名掩饰隐瞒犯罪所得（收益）、帮助信息网络犯罪活动、诈骗（共犯）等，大多是利用银行卡接受诈骗资金帮助取现，或者利用银行卡接收资金后购买虚拟货币再转给上线人员，再或者是出租、出售银行卡、手机卡等。然而在实践中，很多地区司法机关工作人员都是重刑主义者，呈现只要与重刑罪名沾边即向重罪靠拢的一种局面。但在上述地区很可能被直接评价为诈骗罪的共犯，结合笔者目前办理过的电信网络诈骗关联的五件帮助信息网络犯罪活动案件以及三件掩饰隐瞒犯罪所得案件和一件诈骗案的经验和心得，谈一下在电信网络诈骗案件关联犯罪的实体辩护研究，将主要从罪名认定及法律适用、犯罪数额的认定、数罪及犯罪种类、量刑情节、手段与行为是否正当化等方面进行阐述：

1、末端关联犯罪人员的罪名认定及法律适用

末端关联犯罪最为常见的是掩饰隐瞒犯罪所得（收益）罪和帮助信息网络犯罪活动罪，按照法律人的常规思维而言，主要看是否具有明知系诈骗所得而提供帮助的主

观明知条件来判断具体罪名的认定，再结合现有法律、司法解释、司法文件等规定进行分析即可。但笔者有不同的观点，所亲办的案件也均争取到较轻的罪名——帮助信息网络犯罪活动罪；笔者认为如果争取到定性的改变，我们就成功了一半，因此将重点论述定性即法律适用问题。

首先，我们来看两个罪名的相关规定。掩饰隐瞒犯罪所得（收益）罪——根据《刑法》第三百一十二条，明知是犯罪所得及其产生的收益而予以窝藏、转移、收购、代为销售或者以其他方法掩饰、隐瞒的，处三年以下有期徒刑、拘役或者管制，并处或者单处罚金;情节严重的，处三年以上七年以下有期徒刑，并处罚金。单位犯前款罪的，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，依照前款的规定处罚。《最高人民法院关于审理掩饰、隐瞒犯罪所得、犯罪所得收益刑事案件适用法律若干问题的解释理解与适用》（以下简称《掩隐解释》）中，关于掩饰隐瞒犯罪所得（收益）罪的立法本意以及入罪问题进行了详细阐述。刑法修正案(六)对原刑法第三百一十二条窝藏、转移、收购、销售赃物罪做了三方面修改:第一，行为方式增加了窝藏、转移、收购、代为销售以外的“其他方法”：第二，犯罪对象从“犯罪所得的赃物”扩大为“犯罪所得及其产生的收益”，罪名也相应修改为掩饰、隐瞒犯罪所得、犯罪所得收益罪；第三，提高了法定刑幅度，“情节严重的，处三年以上七年以下有期徒刑，并处罚金”。此后，刑法修正案(七)增加了单位作为本罪的犯罪主体，2014年4月24日，第十二届全国人民代表大会常务委员会第八次会议公布了《关于<中华人民共和国刑法>第三百四十条、第三百一十二条的解释》(以下简称《人大解释》),规定“知道或者应当知道是刑法第三百四十一条第二款规定的非法狩猎的野生动物而购买的,属于刑法第三百一十二条第一款规定的明知是犯罪所得而收购的行为”，明确了对收购珍贵、濒危野生动物之外的普通野生动物行为如何处罚的问题，指引适用刑法第三百一十二条。由此可见，刑法修正案（六）对《刑法》第三百一十二条修改的内容有三个方面：一是将犯罪对象由“犯罪所得的赃物”扩大为“犯罪所得及其收益”；二是对犯罪行为增加兜底性规定；三是提高了法定刑。修正案加重了对本罪的处罚宽度和力度，刑法对于赃物犯罪的立法呈一种严厉化的趋势。

在司法实践中，对于掩饰、隐瞒犯罪所得、犯罪所得收益罪的罪名到底如何适用尚不统一，有的认为应当定掩饰、隐瞒犯罪所得、犯罪所得收益罪，有的认为应当根据案情定掩饰、隐瞒犯罪所得罪或者掩饰、隐瞒犯罪所得收益罪。笔者认为，如何正确适用本罪的罪名，应当结合刑法的立法技巧来进行分析。在我国刑法中，对于罪名的适用有两种方式，一种是具体罪名，如故意杀人罪、抢劫罪。另一种是选择性罪名，选择性罪名又分为三种形式，一是手段选择性罪名，如走私、贩卖、运输、制造毒品罪，在这类罪名中，犯罪的对象是固定的，即毒品，但手段却可以选择。在适用罪名时，应根据犯罪嫌疑人所实施具体犯罪行为来定；二是对象选择性罪名。如打击报复会计、统计人员罪，盗掘古人类化石、古脊椎动物化石罪。这类犯罪中，犯罪对象是会计或统计人员、古人类化石或古脊椎动物化石，但手段是固定

的，适用罪名要根据犯罪嫌疑人所侵害的具体犯罪对象来选择。三是手段和对象选择罪名。最典型的是伪造、变造、买卖国家机关公文、证件、印章罪。这一类选择性罪名手段和对象均有多种，要根据犯罪嫌疑人所实施的手段和侵害的对象不同来选择罪名。根据以上的分析可以看出，掩饰、隐瞒犯罪所得、犯罪所得收益罪这一罪名的犯罪手段有掩饰和隐瞒两种，而犯罪对象则有犯罪所得和犯罪所得收益两种，符合选择性罪名的手段对象选择性罪名这一特征。因此在适用这一罪名时，应当根据案情分别适用不同的罪名，具体适用应为“掩饰犯罪所得罪”、“隐瞒犯罪所得罪”、“掩饰犯罪所得收益罪”和“隐瞒犯罪所得收益罪”这四种。

帮助信息网络犯罪活动罪是我国刑法第二百八十七条之二所规定的罪名，即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。单位犯前款罪的，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，依照第一款的规定处罚。有前两款行为，同时构成其他犯罪的，依照处罚较重的规定定罪处罚。

而《最高人民法院<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>的理解与适用》中关于帮助信息网络犯罪活动罪的阐述，近年来，网络犯罪呈上升趋势，各种传统犯罪日益向互联网迁移，网络犯罪呈高发多发态势，严重危害国家安全、社会秩序和人民群众合法权益。为进一步严惩网络犯罪，维护正常网络秩序，2015年11月1日起施行的刑法修正案（九）增设了刑法第二百八十六条之一和第二百八十七条之一、之二，规定了拒不履行信息网络安全管理义务罪，非法利用信息网络罪和帮助信息网络犯罪活动罪。刑法修正案（九）施行以来，各级公检法机关依据修改后的刑法规定，严肃惩处相关网络犯罪。依法严惩网络犯罪，切实维护网络安全，对于维护国家安全、社会秩序和人民群众合法权益，发挥了重要作用。但是，在查办案件过程中，有意见反映，刑法修正案（九）新增相关网络犯罪的定罪量刑标准较为原则，不易把握；另有一些法律适用问题存在认识上的分歧，影响了案件办理。鉴于此，为保障法律正确、统一适用，依法严厉惩治、有效防范网络犯罪，最高人民法院会同最高人民检察院，在公安部等部门的大力支持下，经深入调查研究、广泛征求意见、反复论证完善，起草了司法解释。2019年6月3日，最高人民法院审判委员会第1771次会议、2019年9月4日最高人民检察院第十三届检察委员会第二十三次会议审议通过了《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》（以下简称《帮信解释》）。

上述关于两个罪名的规定有一个重要的区别，后者是在网络犯罪的基础之上，前者是不限定环境的，而对于后者首要考虑的就是以信息网络犯罪为前提的帮助行为，所以笔者认为后者属于特殊法条，在与掩饰隐瞒犯罪所得（收益）情形较差时，应当优先适用后者；也不能用想象竞合犯的处断机制加以认定，在特定环境中适用特

定手段帮助特定的犯罪行为，应当选择特别法条。

再看《帮信解释》中针对帮助信息网络犯罪活动罪做出的第十二条规指出，明知他人利用信息网络实施犯罪，为其犯罪提供帮助，具有下列情形之一的，应当认定为刑法第二百八十七条之二第一款规定的“情节严重”：(一)为三个以上对象提供帮助的；(二)支付结算金额二十万元以上的；(三)以投放广告等方式提供资金五万元以上的；(四)违法所得一万元以上的；(五)二年内曾因非法利用信息网络、帮助信息网络犯罪活动、危害计算机信息系统安全受过行政处罚，又帮助信息网络犯罪活动的；(六)被帮助对象实施的犯罪造成严重后果的；(七)其他情节严重的情形。实施前款规定的行为，确因客观条件限制无法查证被帮助对象是否达到犯罪的程度，但相关数额总计达到前款第二项至第四项规定标准五倍以上，或者造成特别严重后果的，应当以帮助信息网络犯罪活动罪追究行为人的刑事责任。在开展辩护工作中，律师应当明确分析和掌握，当事人是否符合上述六种具体情形，如果符合其中一种或者两种以上情形的，且尚无证据证实与上游犯罪人员存在通谋或者意思联络的，就应当按照帮助信息网络犯罪活动罪来认定其罪名。

但在具体的司法实践中，很多办案人员认为帮信罪是一条兜底性罪名，不易轻易适用，因为实践中针对电信网络诈骗案件的侦诉审基本都是按照“两高一部”《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》（以下简称《电诈意见》）来处理，而该意见的第三条第五款规定，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……在很多办案人员眼中，只要犯罪构成与上述情形相似即应当以掩饰隐瞒犯罪所得（收益）罪定罪处罚，而帮助信息网络犯罪活动罪刑责较轻，不利于打击犯罪，应当择一重罪论处。

实则不然，依据《刑法》第三条规定，任何罪名的认定均应坚持罪刑法定原则，而不应当是罪刑由解释或者司法文件来规定的，建议律师在辩护工作中一定要坚持该原则。在电信网络诈骗末端的关联犯罪人员的罪名认定中，首先应当适用刑法直接规定的罪名，无论是掩饰隐瞒犯罪所得（收益）还是帮助信息网络犯罪活动，其次方可按照最高检、最高法单独或者联合依法出台的司法解释的指引进行定罪，而“两高一部”或者两高联合其他部委出台的司法文件则次之，笔者认为该类文件只能

作为办案指导性司法文件，虽然很多时候被应用到具体办案实践中，但该类型的文件并不属于正式的法律渊源，也不符合立法法的规定。因此，律师在辩护工作中要尤为重视法律渊源的引用。

刑法第二百八十七条之二已将帮助信息网络犯罪活动罪予以明确，属信息网络犯罪中的特别法条，应当优先适用，如果当事人明知上游人员利用信息网络实施犯罪，为其犯罪提供支付结算等帮助，其行为应当认定为帮助信息网络犯罪活动罪。《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》（以下简称《帮信解释》）第十二条第三款，明确规定了构成帮助信息网络犯罪活动罪的具体情形。而《电信诈骗意见》中，虽然规定了相关罪名的情形，但该司法文件的效力等级低于两高司法解释，更远低于刑法。换言之，刑法、司法解释等制定、修改，均符合立法法或者《中华人民共和国人民法院组织法》《中华人民共和国人民检察院组织法》等规定，实践中可以引用并写入判决书。另外，刑法第二百八十七条之二（刑法修正案九）于2015年11月1日实施，《电诈意见》于2016年12月19日实施，《帮信解释》于2019年11月1日实施，根据罪刑法定、从旧兼从轻等原则，《帮信解释》已明确规定了帮助信息网络犯罪活动罪的具体情形。

如上所述，在当事人的行为既符合帮信罪的构成又符合《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》规定的掩饰隐瞒犯罪所得罪的情形，律师应当全力主张适用帮助信息网络犯罪活动罪。如果能实现定性的改变，律师的辩护工作就成功了一半。

笔者目前亲办的五件帮助信息网络犯罪活动案件，均是起初以诈骗罪（XX被骗案）立案，后经与办案机关的多次沟通，在阅卷后与承办检察官多次沟通后，将罪名变更为帮助信息网络犯罪活动，至此辩护工作就已成功一半。

2、犯罪数额的认定

首先，应当明确帮助信息网络犯罪活动罪的数额与上游诈骗罪的犯罪数额不能相提并论。电信网络诈骗案件普遍都是通过银行卡交易流水、开户信息、转账信息等确定嫌疑人和受害人，再根据银行转账凭证等相关交易流水确定涉案的金额、利润分成等情况。关于诈骗数额的认定，在辩护思路中需要考虑的因素有：第一个是电信网络诈骗案件中犯罪集团的整体诈骗数额认定；第二个是案件中某个犯罪嫌疑人个体的犯罪数额认定。

而帮信罪的数额认定则不能机械性的将被骗金额或者说上述的金额直接认定。其一，帮信罪或者掩饰隐瞒犯罪所得（收益）罪只是电信网络诈骗中末端的、具有收尾性质的处理资金的一个环节，该罪的核心目的在于帮助上线人员去处理资金安全及

资金性质问题，自然所参与的金额与诈骗金额不能相提并论，在整个犯罪网络中出于末端位置，因此仅能以实际参与处理的资金数额来加以认定。其二，帮助信息网络犯罪活动，按照文义解释，自然是帮助行为，在整个犯罪体系中只是帮助作用，因此，在没有事前同谋的基础上就要以所起的作用来评价罪责，自然应当以所涉及的金额来认定。

其次，我们要针对具体数额进行分析。

①非参与期间数额的扣除。通过上述分析，作为电信诈骗末端人员，其参与的犯罪数额应当以实际参与的数额为准。根据《电诈意见》第四条第三款的规定，对犯罪集团首要分子以外的主犯，应当按照其所参与的或者组织、指挥的全部犯罪处罚。末端人员的关联犯罪自然更应当如此来认定——举重以明轻。对于未参与期间数额的扣除，是减少涉案当事人犯罪金额以及决定量刑结果的重要因素之一。因此需要明确当事人具体参与的时间点，对参与期间的认定和计算应当从两个方面考虑：第一，从加入到离开（或被查获）整体的参与期间内，对没有参与诈骗行为，由诈骗集团他人犯罪所得的数额予以扣除。第二，在被抓之后或者具有主观明知之前的部分应当扣除。

②不属于违法所得数额的扣除。根据最高检关于印发《检察机关办理电信网络诈骗案件指引》的通知，其中犯罪数额认定第三款规定，认定犯罪数额需要根据在案其他证据，认定犯罪集团是否有其他收入来源，“违法所得”有无其他可能性，或者应当排除其他合理性怀疑之后的来源应当明确。此外，《最高人民检察院关于人民检察院办理网络犯罪案件规定》第二十条规定，认定犯罪行为的情节和后果，应当结合网络空间、网络行为的特性，从违法所得、经济损失、信息系统的破坏、网络秩序的危害程度以及对被害人的侵害程度等综合判断，注重审查以下内容：（一）聊天记录、交易记录、音视频文件、数据库信息等能够反映犯罪嫌疑人违法所得、获取和传播数据及文件的性质、数量的内容；（二）账号数量、信息被点击次数、浏览次数、被转发次数等能够反映犯罪行为对网络空间秩序产生影响的内容；（三）受影响的计算机信息系统数量、服务器日志信息等能够反映犯罪行为对信息网络运行造成影响程度的内容；（四）被害人数量、财产损失数额、名誉侵害的影响范围等能够反映犯罪行为对被害人的人身、财产等造成侵害的内容；（五）其他能够反映犯罪行为情节、后果的内容。第二十一条规定，人民检察院办理网络犯罪案件，确因客观条件限制无法逐一收集相关言词证据的，可以根据记录被害人人数、被侵害的计算机信息系统数量、涉案资金数额等犯罪事实的电子数据、书证等证据材料，在审查被告人及其辩护人所提辩解、辩护意见的基础上，综合全案证据材料，对相关犯罪事实作出认定。

故排除不属于违法所得数额亦是辩护律师在电信网络诈骗案件末端人员关联犯罪中数额辩护的一个重要路径。

③其他证据不足数额的扣除。电信网络诈骗案件套路多样，细节复杂繁琐，对于涉案数额扣除的辩护思路笔者不能在一文中罗列详尽，此点做个兜底性的囊括。比如，被告人账户中发生的交易金额可能很大甚至数字惊人，但是目前报案的或者有证据证实为诈骗资金的，方可进入认定犯罪数额的领域，但没有证据证实系诈骗资金的则要主张事实不清或者不构成犯罪。根据《电诈意见》第六条证据的收集和审查判断第一款固定，办理电信网络诈骗案件，确因被害人人数众多等客观条件的限制，无法逐一收集被害人陈述的，可以结合已收集的被害人陈述，以及经查证属实的银行账户交易记录、第三方支付结算账户交易记录、通话记录、电子数据等证据，综合认定被害人人数及诈骗资金数额等犯罪事实。另外，根据《帮信解释》十二条第二款之规定，实施前款规定的行为，确因客观条件限制无法查证被帮助对象是否达到犯罪的程度，但相关数额总计达到前款第二项至第四项规定标准五倍以上，或者造成特别严重后果的，应当以帮助信息网络犯罪活动罪追究行为人的刑事责任。在其他金额没有达到前述的五倍的情况下，律师可以主张其余数额不构成犯罪，或者有证据证实帮助支付结算等涉嫌帮信罪的数额尚未达到立案标准，其他未查明是否系诈骗资金或者其他犯罪所得的数额的也尚未达到五倍的，律师自然可以争取无罪辩护。

以上，电信网络诈骗案件关联犯罪的金额辩护分析，在司法实践中能够起到较好的罪轻辩护目的。

3、被帮助行为是否构成犯罪也是实体辩护的一个重点问题

被帮助对象所实施的行为是否构成犯罪，也是实体辩护的一个重要模块。根据刑法第二百八十七条之二的规定，被帮助对象实施犯罪活动是本罪入罪的前提。但《帮信解释》第十二条第二款也确立了例外规则，确因客观条件限制无法查证被帮助对象是否达到犯罪的程度，但相关数额总计达到前款第二项至第四项规定标准五倍以上，或者造成特别严重后果的，应当以帮助信息网络犯罪活动罪追究行为人的刑事责任。因此律师需要考虑，上游犯罪是否成立，且数额尚未达到“五倍”的程度。最高人民法院法官周加海、喻海松在《<解释>的理解与适用》一文中谈到，两种情况不得适用上述例外规则：（1）对于帮助少数或单个对象的，仍要以被帮助对象构成犯罪为前提，如果查证被帮助对象不构成犯罪的，行为人也不构成本罪；（2）被帮助对象实施的必须是刑法分则规定的犯罪行为，如果仅是一般的违法行为也不可适用该规则。

帮助信息网络犯罪活动罪是指明知他人利用信息网络实施犯罪而提供支持或帮助，情节严重的行为，需以上游犯罪成立为前提。例如，上游人员意图利用电信网络实施诈骗，而雇佣他人发布相关的诈骗广告，而费用高达一万元，但该广告由于时间较短或者程序问题，再或者刚刚发布广告就被公安机关发觉等情形，仅导致一名被害人被骗2900元，诈骗罪尚未达到诈骗罪追诉标准，因此不足以证实行为人帮助信

息网络犯罪活动情节严重，不符合入罪条件。

再或者，张三等人帮助李四开发了一款具备充值结算功能的软件，但被李四用于赌博（开设赌场），而开设赌场的金额只有1800元，尚不构成开设赌场罪，而张三等人开发软件的费用为一万元，李四的行为自然尚不构成开设赌场罪，张三的行为也不能被评价为帮助信息网络犯罪活动罪。

以上，辩护实践中应充分考虑上游人员是否构成犯罪。

4、犯罪从属性等量刑情节以及与上游人员的量刑衔接问题

帮助信息网络犯罪活动罪或者是掩饰隐瞒犯罪所得（收益）罪，其本质在电信网络诈骗领域中均属于末端人员的关联犯罪，但是在关联犯罪中对当事人的地位应当充分考虑，并且在该层面中是帮助犯还是犯意发起方，将直接决定当事人在案件中的作用，进而直接影响着量刑结果。大多数的当事人均是末端人员，通过案卷显示，大多均是在他人雇佣之下参与到案件当中，换言之就是一个末端马仔，很可能只是末端马仔中的一个或者一组而已，真正组织实施处理资金阶段的人，即帮助信息网络犯罪活动或者掩饰隐瞒犯罪所得（收益）罪的犯意发起者极有可能另有他人。

因此，在梳理人物关系、作用的过程中，不难发现当事人在案件中的实际作用，如果现有证据可证实系雇佣之下参与案件，则一定需要争取从犯或者帮助犯，由于共同犯罪中的主犯尚未到案，法院在判决中往往不表述为从犯，一般表述为某某帮助某某某实施……行为，因此量刑的起步都会在法定刑以下。

另外，如果不争取从犯（或者帮助犯）的情节，极有可能导致量刑结果超过雇佣者。例如，A在B的雇佣下参与实施了掩饰隐瞒犯罪所得行为，犯罪数额20万元，而雇佣其参与本案的B如果是电信诈骗的帮助犯，现有证据仅能证实其参与帮助了20万元数额的诈骗行为，B的法定刑很可能在三年以下。但是A的刑期如果没有争取从属性的问题，很有可能在三年以上，这样将导致量刑极度失衡，直接帮助电信网络诈骗的人员获刑三年以下，帮助其掩饰隐瞒犯罪所得的人员的量刑却在三年以上。虽然，上线人员的抓捕难度非常大，我们不能苛求公安机关将全部人员一网打尽，但我们要通过在案证据（包括但不限于当事人及同案供述、被害人陈述、相关交易明细、聊天记录等）综合分析上线人员是否真实存在，凡能够证实上线人员真实存在，我们一定要争取当事人的从属性问题。首先，这是为当事人的利益在争取，其次是为避免上线人员到案后出现量刑失衡的情形。

以上，在电信网络诈骗案件末端人员的关联犯罪中，犯罪从属性问题以及与上游人员的量刑衔接同样是实体辩护中的一大重要路径。

5、目的、手段是否正当化的问题

正当化事由是指行为在形式上与犯罪具有相似性，但实质上不具有法益侵害性，因而在定罪过程中予以排除的情形。具有以下特征：（一）形式特征。正当化事由是一种非罪行为，既然不是犯罪，本不应在刑法中加以规定。但正当化事由不同于一般的非罪行为，它在形式上与犯罪具有相似性。（二）实质特征。正当化事由虽然与犯罪具有形式上的相似性，但它与犯罪之间存在本质区别，这就是正当化事由不具有法益侵害性。（三）法律特征。正当化事由在法律上规定不认为是犯罪，或者虽然在法律上无明文规定，但在司法中不认定为犯罪，因而在定罪过程中应予排除。律师在开展辩护工作中还要考虑当事人的手段、目的是否具备正当化的条件。

自公安部开展“断卡”行动以来，主要的末端人员体现在“两卡”，即向犯罪分子租售信用卡、手机卡，以及帮助上游人员处理资金，即接收资金后购买虚拟货币之后再转给上游人员的情形。那么，在笔者办理的案件中出现过两起案件，最终成功办理取保候审，在侦查终结时对当事人撤销了案件。主要列举两种情形：

一种情形是，很多人出于同事、朋友等面子的缘故，出借、出租了银行卡，之后该人将银行卡提供给电信网络诈骗团伙使用，短时间内发生巨大金额的交易。该案是海南地区某所小学的后勤临时帮厨人员艾某，在同事的多次请求下，声称借用银行卡导自己的信用卡用于存放资金，艾某出于情面不好拒绝，直至公安机关传唤艾某才得知，三个月时间卡内金额高达数千万元的交易流水，系诈骗资金，而后艾某被侦查机关刑拘，在报捕阶段，检察机关在笔者的沟通之下，未批准逮捕，进而取保候审，在案件侦查终结时公安机关对艾某的案件予以撤销。

另一种情形是，从事虚拟货币代购的人员，在不知情的情况下帮助了电信网络诈骗团伙购买虚拟货币的情况。该案中河南某自由职业青年李某，由于自己经常购买虚拟货币，虽在网络发布广告可以帮助购买虚拟货币，手续费为单笔金额的1%，在其不知情的情况下，接收网络诈骗资金35万元（一个账户累计转入）购买虚拟货币，获利3500元，在正常思维下其接收一个固定账户的资金，且获利比例未发现异常，直到案发其才知晓该35万元系诈骗所得。经笔者介入后，向公安机关提出不构成犯罪的意见：购买虚拟货币本身不是违法行为，接受一个账户的资金很难发觉异常，尚无证据证实李某明知违法犯罪所得而提供帮助，虚拟货币不属于法定货币，个人代理购买虚拟货币不属于非法从事支付结算，也不构成非法经营罪，并且在审查批捕阶段将前述意见与承办检察官进行了意见交换，最终结果与第一种情况相同。

结合上述两种情形，需要探析的问题是目的和手段是否正当化。无论出借银行卡、或者代购虚拟货币等行为是否最终侵害到刑法法益，都要从主客观一致的原则去分析犯罪的构成。单纯以行为来分析，两种情况都与构成犯罪的情形相符，单从行为本身看是不构成犯罪的，但结果却侵害刑法的法益，此时应当考虑到主客观一致的

原则，其主观目的也是具有正当性的，同样是不具有刑法违法行为的主观目的，因此就其主观与行为是否具有正当性来进行分析。

三、网络犯罪案件中辩护律师需要探索的相关领域

在如今已经突破50万人的律师队伍中，如何生存、发展，脱颖而出直到功成名就，或者说如何实现自身价值的有效实现，有或者说如何能真正为建设社会主义法治国家做出应有贡献，是一个永恒的话题，也是每一位律师要面对的问题。如今，律师专业化、行业化已经是一种趋势，在十年前刑辩律师是一种标签，但如今刑辩律师中又细分为很多专业领域，各个领域中都已涌现出很多著名律师，比如钱列阳、曹春风、王亚林等专业领域内卓著的专业化律师代表，是我们敬仰、钦佩的学习目标。笔者不是希望所有律师必须要走专业化之路，但至少通过自身亲办案件的经历来看，对待案件必须要有专业的心态和专业的知识搜集、积累。

首先，笔者在此建议在对网络犯罪辩护的案件中，要弄清楚一些问题和学习专业名词。检察机关在网络领域内进行了重点知识的普及，如最高检公诉一厅《网络犯罪案件技术法律术语解释汇编（一）》中就列举的十余种网络技术名词：

（1）IP地址（Internet Protocol Address）:是指互联网协议地址，是为了保证互联网上计算机设备之间的正常通信而为互联网上的每台设备分配的唯一的数字串编号。

在网络犯罪案件的办理过程中，通过对IP地址的追踪可以确定用于作案的设备的地理位置（经纬度等），为判断人机同一问题提供有利参考。

（2）域名:是由一串用点分隔的英文字母等符号组合的互联网上某一台计算机或计算机组的名称，用于在数据传输时标识计算机的电子方位。例如“www.baidu.com”是一个域名，和IP地址“220.181.38.148”对应。域名的产生，使计算机设备使用人在访问互联网上计算机设备时，不需要输入较难记忆的IP地址数字串，只需要输入方便好记的域名即可。

（3）域名解析:域名与IP地址之间是一一对应的，它们之间的转换工作称为域名解析。域名解析需要由专门的域名服务器（DNS）来完成，整个过程是自动进行的。

（4）域名服务器（Domain Name Server，DNS）:是进行域名和与之对应的IP地址转换的服务器。当一个计算机设备使用人在浏览器地址框打入某一个域名，或者从其他网站点击链接来到这个域名，浏览器向该用户的上网接入商发出域名请求，接入商的DNS服务器要查询域名数据库，看这个域名的DNS服务器是什么，然后到该服务器中抓取DNS记录，也就是获取这个域名指向哪一个IP地址。在获得这个IP

信息后，接入商的服务器就去这个IP地址所对应的服务器上抓取网页内容，然后传输给发出请求的浏览器。

（5）流量劫持:是指攻击者通过技术手段，非法拦截、修改或控制用户上网的行为，以此达到网络流量的引流甚至诱导用户安装木马程序、获取用户数据的非法行为。

流量劫持黑产链条主要包含两类作案团伙：一是有推广APP、网站、广告等流量需求的团伙，希望通过不法手段实现广告弹窗、网页跳转、主页锁定、安装推广、暗扣刷量等进行引流，从而变现牟利；二是流量劫持团伙，通过弹窗木马软件、捆绑流氓软件、DNS劫持、运营商基础设施劫持等，对用户进行流量劫持，对访问者的客户端进行主页锁定、网页跳转，向访问者推出弹窗广告、安装推广APP、暗扣流量等，从而与业务推广需求商进行分成牟利。

在司法判决中，对流量劫持类案件的处理，主要分为两类：一类是以网页中带有误导性广告、下拉框、菜单等手段，诱导用户进入特定网站，从而实现流量劫持的目的，并未采取技术手段控制、破坏他人计算机系统，一般以不正当竞争论处，归类为“非强制性”流量劫持；另一类是以非法控制、破坏他人计算机信息系统等方法，强制改变他人网站访问路径，归类为“强制性”流量劫持，应予刑事打击。司法实践中，流量劫持行为的刑事判例主要涉及到非法控制计算机信息系统罪、非法获取计算机信息系统数据罪、非法侵入计算机信息系统罪等罪名，具体详细内容不再一一列举。

然而，在末端人员的关联犯罪中，可能会涉及虚拟货币，律师就应当知道虚拟货币的来历、名称，如何购买，种类包含哪些。比如，知名的虚拟货币如百度公司的百度币、腾讯公司的Q币、Q点，盛大公司的点券，新浪推出的微币（用于微游戏、新浪读书等），侠义元宝（用于侠义道游戏），纹银（用于碧雪情天游戏），2013年流行的数字货币有，比特币、莱特币、无限币、夸克币、泽塔币、烧烤币、便士币（外网）、隐形金条、红币、质数币。目前，全世界发行的数字货币已达上百种，圈内流行“比特金、莱特银、无限铜、便士铝”的说法，尤其在很多案件中比特币较为常见。另外，如何购买虚拟货币，如何将虚拟货币变现或者是转出，同样时律师应当探寻的领域。

其次，行为的推演（类似于侦查实验的方式）。很多案件中律师都是在听当事人阐述如何操作具体的犯罪步骤（APP等），律师只是听其声而不见得懂其意。根据笔者专注从事刑事辩护以来，曾办理过网络犯罪案件主要包括：销售伪劣产品（假烟）、网络销售电子烟（烟弹型）、网络开设赌场、帮助信息网络犯罪活动（购买虚拟货币、出售出租银行卡等）、网络贩卖毒品、网络销售假冒注册商标的商品、电信诈骗（QQ等色情引诱式诈骗以及身份类诈骗）等利用电信网络实施的不特定客

体的案件。每当办理具体案件时，只要在法律允许的基础上，购买一些相关产品进行研究，或者注册相关的APP进行实景推演，发现在当事人实施犯罪行为的过程中可能存在的问题，以及寻找可能对当事人有利的情形与情节。

综上，笔者从电信网络诈骗犯罪末端人员关联犯罪的概述谈起，深入阐述末端人员涉及的重点罪名，再从实体辩护的关键领域进行逐一分析，又在从事网络犯罪辩护时的自身专业积累与探索和行为推演等方面提出少许建议，实则为笔者办理电信网络犯罪及关联犯罪案件的心得总结。

作者简介

刘钟歆，专注刑事辩护，重点研究毒品犯罪、死刑复核案件、涉枪案件、网络犯罪案件等疑难、重罪刑事辩护领域。

毕业于吉林大学。内蒙古蒙南律师事务所-毒品犯罪辩护研究中心主任，草原狼毒品犯罪辩护团队核心成员，中国药物滥用防治协会合成毒品研究分会委员。

连续三年被评为优秀律师、专业律师等奖项；

曾入围2020法治新时代十佳刑辩律师奖项。