游戏公司刑事司法实务系列一
游戏公司员工高发职务类犯罪透视与应对

作者：王旭东 | 龙家乐

2025 年 7 月 31 日，中国国际数字娱乐产业大会(CDEC)上发布的《2025 年 1-6 月中国游戏产业报告》显示，2025 年上半年国内游戏市场实际销售收入达到 1680 亿元，同比增长 14.08%，再度刷新历史纪录。但与此同时，7 月 30 日，中手游发布了一份内部反腐通告。通告显示，中手游旗下满天星工作室原总经理姜某因涉嫌严重职务犯罪，已被公安机关采取刑事拘留措施，案件正在进一步侦办中。无独有偶，7 月 2 日，B 站在内部邮件中通报，原游戏合作部总经理张某敏在 B 站工作期间存在严重的职务犯罪行为，已经被公安机关依法逮捕；7 月 1 日，完美世界发布针对反腐调查的内部公告，公告显示，多人在职期间严重违反公司制度及劳动合同约定，个别员工及供应商负责人涉嫌违法犯罪，多名涉事人员被公安机关刑事拘留。

由此可见，在行业光鲜的背后，游戏公司员工职务犯罪问题日益凸显。游戏产业乃至整个互联网行业的发展历程和技术特性造成了游戏公司员工职务类犯罪在法律适用、取证固证、内部防范等方面存在诸多争议和问题。基于此，本文尝试通过对游戏公司员工高发的职务类犯罪“职务侵占罪”和“非国家工作人员受贿罪”进行解读和分析，对相关罪名的法律适用和证据收集两个主要难点进行探究，并提出预防和办理相关案件的解决方案和实践建议。

如您需要了解我们的出版物，
请联系：

Publication@llinkslaw.com

一. 相关罪名在游戏公司的常见形态

(一) 职务侵占罪

职务侵占罪是游戏公司员工职务类犯罪中较为常见的类型之一，员工利用职务上的便利，将本单位财物非法占为己有，数额较大的即构成此罪。[1] 根据 2022 年 5 月 15 日施行的《最高人民检察院、公安部关于公安机关管辖的刑事案件立案追诉标准的规定(二)》的相关规定，职务侵占罪"数额较大"的起点为三万元。[2]

在游戏公司员工职务侵占的众多案件中，虚拟财产往往是职务侵占的主要客体。游戏公司的员工利用职务便利，绕过公司监管和审核，向游戏玩家非法发放游戏虚拟货币、装备，并以此获利的行为较为常见。笔者曾办理过多起游戏公司员工本人或与下游联运厂商员工内外勾结，利用自身职务之便，将分配给游戏运营人员、第三方合作伙伴的内部测试游戏币、游戏装备非法转卖给游戏玩家并获利的案件。

除此之外，游戏买量公司广告投放过程中的职务侵占行为也较为常见。如公司员工伙同广告代理商、广告经营者虚报广告价格，利用职务之便将公司广告费非法占为己有。同时，随着直播带货的兴起，游戏直播成为游戏买量行业的又一主要形态。主播与游戏公司双方之间的合作方式、主播在游戏玩家和游戏公司之间扮演的特殊角色、主播与游戏公司直播运营人员的特殊的对接方式，都为游戏公司相关员工职务侵占行为埋下了巨大的隐患。在笔者近期处理的某游戏公司直播部门员工职务犯罪一案中，相关员工便利用了自身巨大的职务权限、公司与主播间特殊的结算方式及主播与玩家之间的亲密关系，长期、巨额地侵吞了公司财产。

(二) 非国家工作人员受贿罪

公司员工利用职务上的便利，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，构成该罪。[3] 根据 2022 年 5 月 15 日施行的《最高人民检察院、公安部关于公安机关管辖的刑事案件立案追诉标准的规定(二)》的规定，非国家工作人员受贿罪"数额较大"的起点为三万元。[4]

游戏公司对外合作的业务类型较多，研发外包、游戏代理、推广渠道合作、广告投放等环节，都有可能发生收受贿赂的行为。需要注意的是，非公受贿行为在很多情况下与职务侵占行为伴随发生，在办理相关案件时需要进行区分和梳理。

上文提到的游戏公司员工与下游联运厂商员工内外勾结的职务侵占行为，相关员工同时也存在按照公司规定向下游联运厂商发放测试用的游戏装备和游戏币并收受下游联运厂商贿赂的行为;

1 《中华人民共和国刑法》第 271 条第 1 款。
2 《最高人民检察院、公安部关于公安机关管辖的刑事案件立案追诉标准的规定(二)》第 76 条。
3 《中华人民共和国刑法》第 163 条第 1 款。
4 《最高人民检察院、公安部关于公安机关管辖的刑事案件立案追诉标准的规定(二)》第 10 条。

同样，在上文提及的游戏直播负责员工职务侵占案件中，公司直播运营人员也存在收受主播贿赂的情形。

需要注意的是，非国家工作人员受贿罪的核心在于通过权钱交易破坏微观层面的企业管理结构和宏观层面的市场竞争机制，其本质是对法律所保护的经济秩序、公平原则及职务廉洁性的多重侵害，该罪名被归类为“妨害对公司、企业管理秩序罪”；而职务侵占罪的核心在于对单位财产权的直接侵害，同时伴随对企业管理秩序和市场经济运行机制的潜在威胁，一般情况下被归类为“侵犯财产罪”，非国家工作人员受贿罪的被害人并非行为人所属单位本身。上述两个罪名的不同直接影响着单位损害赔偿的主张及单位参与案件侦查、审查起诉和审判阶段的权利。

二. 法律适用难题

相较于传统行业较为固定的行为模式，游戏公司的核心资产在于虚拟数据，其商业模式建立在复杂的线上交易和技术操作之上，这使得游戏公司在处理员工职务类犯罪(指“职务侵占罪”和“非国家工作人员受贿罪”，下同)时存在法律适用上的显著难点。笔者将从以下三点就游戏公司员工职务类犯罪的法律适用难点进行分析。

(一) 虚拟财产的财产属性认可

游戏中的虚拟财产种类丰富，其价值受到各种因素的影响，具有较大的不确定性。不同类型的虚拟财产，根据表现形态、价值来源、评价标准的不同，价值认定存在较大的差别。如游戏币，其价值评估相对稳定，来源方式较为直观，通常情况下与游戏内充值比例相关联；而道具类或者装备类的虚拟财产，价值评估则相对较为复杂，获取方式分为官方购买、官方赠送、通过任务、副本、打怪等。从官方渠道购买的物品，虽然有稳定、公开的标价，但根据不同的活动和稀缺程度，玩家间的交易价格与官网价格会有很大的差异，而游戏版本的调整也会很大程度上影响不同道具的市场交易价格。

《中华人民共和国民法典》第 127 条确定了虚拟财产的可保护性，但在虚拟财产的价值认定方面尚无明确具体的法律规定。由于虚拟财产和实体财产在载体上的区别，造成了传统的物价鉴定机构，如物价局，无法对虚拟财产进行准确的鉴定。一般而言，游戏中的虚拟财产可能存在官方价、一口价和竞拍价等多种价格形式。而在司法审判实践中，有的法院是以嫌疑人实际收受的金额作为犯罪数额的计算依据，有的法院是以虚拟财产的市场价格作为犯罪数额的计算依据，造成了犯罪所得的计算方式并不统一。例如，在上海某网络科技公司员工沈某某职务侵占案中，上海市第一中级人民法院在二审阶段支持了以被告非法获利的数额而非虚拟财产的市场标价认定犯罪数额的意见。[5]

因此在司法审判实践中，游戏公司需要通过多种辅助证据向司法机关证明市场价格的合理性，以解决在审判过程可能出现的对公司财产保护“定性不公”或“定量不公”的问题。辅助证据的类

[5] (2020)沪 01 刑终 519 号。

型包括：虚拟财产市场价格的说明、玩家获得相关虚拟财产的成本分析、第三方交易平台的价格参考、游戏经济系统的影响报告以及相关司法专家的法律意见等。

(二) 技术犯罪手段的隐蔽性及其与传统罪名构成的适配难题

游戏公司员工职务类犯罪经常会借助先进的技术手段，这些手段有很强的隐蔽性和复杂性。例如，技术人员通过编写程序代码的形式，在游戏内或系统后台上植入相关指令，实现对虚拟财产的非法生成或者转移，这些操作具有很强的隐蔽性，很难在日常的检测中被发现。同时，嫌疑人还可以通过修改服务器日志、伪装 IP 等技术手段，掩盖犯罪行为轨迹，增加案件侦查和证据收集的难度；也可能通过编写脚本，实现批量生成道具，将其发送到特定的游戏账号，并删除操作记录，使公司在很长时间内难以察觉异常行为。

在面对这些高技术化、虚拟化的犯罪手段时，传统的职务侵占罪、非国家工作人员受贿罪等罪名的构成要件，暴露出难以完全适配的问题。传统的职务类犯罪，如职务侵占罪和非国家工作人员受贿罪，其构成要件主要围绕现实世界的有形财物和传统的管理秩序构建。例如，职务侵占罪的核心在于行为人利用职务便利，非法占有“本单位财物”；非国家工作人员受贿罪则强调利用职务便利，索取或收受财物并为他人谋取利益。游戏公司员工利用的“职务便利”往往是其对计算机系统、网络、代码、数据、漏洞的了解和访问权限。如何界定这种技术性便利是否构成刑法意义上的“职务便利”?例如，“一个普通员工偶然发现游戏漏洞并利用”与“一个专门负责漏洞测试的员工利用漏洞”，二者“职务便利”的程度和性质可能有所不同。在虚拟财产和数据犯罪中，行为人可能并非意图“永久占有”某个实体财物，而是通过修改数据、复制虚拟物品来获取经济利益。例如，复制大量游戏道具并出售，其目的在于变现，而非占有道具本身。这种对虚拟财产的“占有”内涵需要结合数字形态重新界定。传统的职务类犯罪罪名在设计之初，并未充分考虑到虚拟财产、数据、源代码等新型犯罪客体，以及通过网络技术手段实施的犯罪行为模式，这也为办理游戏公司员工职务类犯罪案件带来了巨大的挑战。

(三) 涉及跨境因素的法律难题

随着游戏出海浪潮的日渐兴起，游戏公司员工职务类犯罪涉及跨境因素的情形愈发常见。涉及的案件包括海外运营的游戏、海外涉案人员，以及非法收入在海外的流转等问题。海外因素的加入为办理游戏公司员工职务类犯罪案件进一步增加了难度。

例如，国内某经营海外游戏的公司工作人员利用职务便利，通过其控制的海外公司非法销售游戏装备和权限，办案过程中存在无法核实海外公司与国内员工的关联关系、无法通过司法手段确认非法销售所得、无法明确涉案员工的实际收益等问题，使得案件推进极其困难。又例如，在笔者办理的某起过往案件中，某公司高管被证实收受了海外区块链货币作为贿赂款，但在办案过程中始终无法掌握其收受的区块链货币的具体价值和流转链路。因此，在办理具备涉外因素的游戏公司员工职务类犯罪案件时，更考验办案人员的抽丝剥茧、把握关键证据因素的能力，同时也要加强与司法机关的交流与配合，借助公权力因素处理相关案件。

三. 证据收集与固定要点解析

游戏公司员工职务类犯罪的发生，往往与权限管理漏洞、技术监控不足、合规意识薄弱等因素密切相关。结合行业特性和犯罪行为特点，可从以下维度构建全链条预防体系。

(一) 电子数据的收集与保全

游戏后台数据是办理职务类犯罪案件的关键证据之一。在收集游戏后台数据时，需要遵循严格的法定程序，确保证据的合法性和完整性。首先，要及时对游戏公司的服务器进行封存和数据备份，防止数据被篡改或丢失。然后，通过专业的技术手段，提取与案件相关的操作日志、玩家账号信息、虚拟财产交易记录等数据。在实际操作中，可聘请专业的电子数据鉴定机构，运用数据分析软件对大量的后台数据进行筛选、比对和可视化处理，以发现潜在的犯罪线索和证据链条。员工在实施职务类犯罪过程中，往往会通过电子邮件、即时通讯工具等进行沟通和交易协商。因此，获取和审查这些电子通信记录对于查明案件事实同样至关重要。可以通过司法机关向相关通信服务提供商发出协助调查通知，依法获取员工的电子邮件内容、聊天记录等信息。在获取电子通信记录时，要注意确保证据的真实性和完整性，防止证据被篡改或删减。对于聊天记录，要重点审查聊天双方的身份信息、聊天时间、交流内容，尤其是涉及犯罪行为策划、交易细节、利益分配等关键信息。在审查电子通信记录时，还可以结合其他证据，如合同文件、资金流水等，进行综合分析，以形成完整的证据链。同时，日常取证中也要善于使用区块链取证工具，其中公证云、时间戳、IP360 等都是互联网案件取证较为常见的工具。

(二) 证人证言的获取与保全

游戏公司内部人员，如与犯罪嫌疑人同部门的同事、上级领导、相关业务环节的协作人员等，他们对公司的业务流程、犯罪嫌疑人的工作职责和日常行为较为了解，其证言对于证明犯罪事实具有重要作用。在获取公司内部人员的证言时，要注意选择合适的询问地点和方式，营造宽松、信任的氛围，鼓励证人如实陈述所知情况。对于与犯罪嫌疑人关系密切的证人，可能存在顾虑或干扰因素，需要通过耐心的思想工作和法律宣传消除其顾虑，确保证言的真实性。上级领导则可能对犯罪嫌疑人的工作表现、权限使用情况有更全面的了解，其证言可以帮助判断犯罪嫌疑人是否存在利用职务便利实施犯罪的可能性。

除了公司内部人员，外部相关人员，如游戏玩家、供应商、合作伙伴等的证言也不容忽视。游戏玩家作为虚拟财产的接收方或交易对象，他们能够提供与犯罪嫌疑人交易的具体细节，包括交易时间、交易方式、交易价格、所获得的虚拟财产种类和数量等信息。可以通过游戏公司的客服渠道、在线调查问卷、玩家社区公告等方式，征集相关玩家的证言。对于供应商和合作伙伴，他们可能在与犯罪嫌疑人的业务往来中发现异常情况，如在项目招投标过程中是否存在违规操作、在合作协议执行过程中是否有不合理的利益输送等，可以通过发函询问、实地走访等方式收集他们的证言。实践过程中，很多商业贿赂的发生及后期查证困难均是因为公司涉案业务的商事沟通均由涉案员工一人掌握，案发后公司内没有其他人员能够详细掌握相关的交易背景，公司和供应商没有良好的信任基础，因而造成案件溯源和查证的困难。

(三) 实物类证据与犯罪痕迹的挖掘

在一些游戏公司员工职务类犯罪案件中，犯罪嫌疑人可能会使用特定的硬件设备来实施犯罪行为，如电脑、服务器、存储设备等。对这些硬件设备进行检查，可以获取到重要的实物类证据和犯罪痕迹。在扣押相关硬件设备时，要做好详细的记录，包括设备的品牌、型号、外观特征、扣押时间和地点等信息。然后，由专业的技术人员对硬件设备进行拆解和数据分析。在对服务器设备进行检查时，可以查找是否有异常的登录日志、数据传输记录等。在实际操作中，要注意遵循电子证据取证规范，确保在检查过程中不破坏设备中的原始数据，确保证据的真实性和完整性。

犯罪嫌疑人的办公场所和活动轨迹也可能留下与犯罪相关的痕迹。在对其办公场所进行勘查时，要仔细检查办公桌上的文件资料、笔记本、便笺纸等，看是否有记录犯罪计划、交易细节、联系方式等信息的内容。同时，注意观察办公环境中是否有异常的设备连接、文件摆放等情况。此外，通过调取公司内部的监控视频、门禁系统记录等，了解犯罪嫌疑人在案发前后的活动轨迹，是否有异常的行为举止，如在非工作时间频繁出入办公区域、携带不明物品离开公司等。

四. 预防员工职务类犯罪的建议

游戏公司员工职务类犯罪的发生，往往与权限管理漏洞、技术监控不足、合规意识薄弱等因素密切相关。结合行业特性和犯罪行为特点，可从以下维度构建全链条预防体系。

(一) 构建精细化的权限管理与流程控制制度

1. 权限分级与动态调整

在权限分级方面，针对技术、运营、商务、采购等关键岗位，实行“最小权限原则”。

关于技术岗位，可以将虚拟财产生成、数据修改等核心权限拆解为“申请-审批-执行-审计”四个环节，以防出现单个员工掌握所有操作权限的情况，同时针对异常的服务器日志修改、IP 登录等行为设置预警机制。

关于运营、商务与采购岗位，可以在广告投放、联运合作等环节明确“询价-比价-合同签订-款项支付”的分离流程，同样做到预防单人主导全流程的情况出现；对主播合作、渠道推广的结算标准实行“双人复核制”，定期核查投入费用与实际投放效果之间的匹配度。

在动态调整方面，根据员工的岗位变动、项目周期实时回收或调整权限，离职员工权限需在离职前彻底注销，并留存权限变更日志备查。

2. 虚拟财产全生命周期管控

建立虚拟财产(包括游戏币、装备、账号等)的“生成-分配-流转-销毁”台账。

(1) 生成环节，将员工工号与虚拟财产生成记录进行关联，并严格限定内部体验币的使用范围，例如限定为仅可用于测试账号，以禁止将体验币向玩家账号转移。
(2) 分配环节，对分配记录额外标记“测试用途”(如“测试商城购买功能”)，并定期对体验币的分配情况进行审计，核查是否存在测试账号向玩家账号转移体验币、未标注分配用途等异常情况。
(3) 流转环节，对玩家间交易、官方回收等行为设置异常监测阈值，如单日单笔交易超过一定数量时即触发人工审核，并追踪虚拟财产流向是否与员工操作相关联。
(4) 销毁环节，所有销毁记录永久留存，不可删除或篡改，如需修改需经相关部门审批，并记录修改原因；若后续涉及玩家投诉或司法调查，可通过“虚拟财产 ID”逆向追溯其“生成-分配-流转-销毁”全链路，以提供完整的电子证据。

(二) 强化技术防控与数据安全体系

1. 全链路技术监控与审计

部署实时监测系统：对后台操作进行“行为画像”，自动识别批量生成虚拟道具、高频修改玩家数据、异常 IP 登录核心服务器等风险行为，触发预警后立即推送至合规管理部门。

设置日志为不可篡改：采用区块链技术存证关键操作日志，如虚拟财产生成记录、权限变更记录等，确保日志无法被修改或删除，为事后溯源提供不可篡改的证据链。

数据加密与访问留痕：对游戏源代码、玩家数据、买量数据等内容采用“传输加密+存储加密”的双重保护，员工访问时需通过“物理识别+动态口令”的双重验证，并留存访问时间、操作内容等详细记录。

2. 应用反舞弊技术工具

使用审计工具类软件，对广告投放数据、联运分成数据进行交叉校验。对比广告代理商的实际投放量与公司支付的广告费用，识别“虚报点击量”“刷量套利”等异常情况；分析员工与外部合作方(供应商、主播、联运厂商)的资金往来、通讯记录，标记高频联系、异常转账等潜在的利益输送线索。

(三) 完善常态化合规教育与风险警示

1. 分层分类进行法律培训

开展新员工入职培训：重点讲解职务侵占罪、非国家工作人员受贿罪的立案标准与典型案例，如虚拟财产侵占、广告费用虚报的法律后果，并组织新员工签订《廉洁从业承诺书》。

开展关键岗位专项培训：不定期组织技术、商务、采购、运营等岗位的员工学习相关法律法规，帮助员工建立清晰的法律红线认知。

2. 加强案例警示与文化建设

定期通报行业反腐案例：组织员工讨论案件中权限滥用的风险隐患与制度漏洞的具体表现，强化“伸手必被抓”的警示效果。

建立“廉洁激励机制”：对主动举报舞弊行为的员工给予专项奖励，并严格保护举报人信息，消除“不敢举报”的顾虑。

(四) 建立监督与应急响应机制

1. 内部审计与第三方核查结合

内部审计：合规部门定期对虚拟财产流转、广告费用支出等环节开展专项审计，重点核查权限与职责是否匹配、操作流程是否合规、异常数据是否有合理解释。

第三方核查：不定期聘请外部律所或审计机构开展独立的反舞弊审计，聚焦跨境业务(如海外子公司权限管理、跨境资金流转)、技术隐蔽性行为(如代码植入、日志篡改)等内部审计易遗漏的风险点。

2. 建立快速响应与止损流程

建立舞弊线索“接收-核查-处置”全流程响应机制。

(1) 接收方面：开通匿名举报邮箱、热线，设置密封式举报信箱。
(2) 核查方面：由合规部门牵头，联合涉及业务部门成员组成核查小组，明确核查范围与重点，开展核查并形成核查报告。
(3) 处置方面：发现疑似职务类犯罪行为时，立即冻结相关员工权限、封存服务器数据，由法务部门联合技术团队固定电子证据，必要时同步公安机关介入，避免证据灭失或损失扩大。
(4) 跨境业务的针对性防控措施

针对游戏出海中的跨境犯罪风险，需强化“属地合规+跨境协同”。

明确跨境权限边界：针对海外子公司与国内团队的权限配置，全面推行“清单式管理”模式。通过明确权限范围、操作流程及责任主体，划定权责边界，避免因权限模糊引发的管理漏洞，确保跨境业务操作全程可控、可追溯。

跨境资金与虚拟货币监控：对员工涉及海外区块链货币、跨境转账等行为进行重点监测，要求合作方不得使用虚拟货币结算，并签订《反洗钱合规承诺》。

加强司法协作：与海外当地律所、调查机构建立合作关系，提前储备跨境证据调取、司法协助的流程指引，确保在涉案人员、资金、数据位于海外时能快速启动协作机制。

五. 结语

预防员工职务类犯罪是一项系统性工程，需要从制度建设、技术防控、人员管理、教育培训、监督应急等多个维度统筹考虑，构建全方位、多层次的预防体系。只有建立完善的预防机制，才能有效降低职务类犯罪风险，保护企业合法权益，促进游戏行业的健康发展。游戏公司应当根据自身的业务特点和风险状况，结合本文提出的建议，制定符合实际情况的职务犯罪预防方案，并在实践中不断完善和优化，确保预防工作的有效性和可持续性。

如您希望就相关问题进一步交流，请联系：

王旭东
+86 755 3391 7631
edward.wang@llinkslaw.com

如您希望就其他问题进一步交流或有其他业务咨询需求，请随时与我们联系：**master@llinkslaw.com**

上海	北京	深圳
上海市银城中路 68 号 时代金融中心 19 楼 T: +86 21 3135 8666 F: +86 21 3135 8600	北京市朝阳区光华东里 8 号 中海广场中楼 30 层 T: +86 10 5081 3888 F: +86 10 5081 3866	深圳市南山区科苑南路 2666 号 中国华润大厦 18 楼 T: +86 755 3391 7666 F: +86 755 3391 7668
香港	**伦敦**	
香港中环遮打道 18 号 历山大厦 32 楼 3201 室 T: +852 2592 1978 F: +852 2868 0883	1/F, 3 More London Riverside London SE1 2RE T: +44 (0)20 3283 4337 D: +44 (0)20 3283 4323	

www.llinkslaw.com

Wechat: LlinksLaw

本土化资源 国际化视野