联合国打击跨国有组织犯罪公约缔约方会议

Distr.: General
25 March 2024
Chinese
Original: English

技术援助问题政府专家工作组
2024 年 6 月 3 日和 4 日，维也纳
临时议程*项目 3
有组织欺诈

有组织欺诈

秘书处编写的背景文件

一. 导言

1. 本背景文件由秘书处编写，旨在为技术援助问题政府专家工作组第十五次会议临时议程的议程项目 3 下的讨论提供便利。本文件简要而不全面地概述了为获得金钱或其他物质利益而针对个人或机构的各种不同类别的有组织欺诈，目的是促进在《联合国打击跨国有组织犯罪公约》框架内更有效地应对有组织欺诈。

2. 多年来，随着技术进步和社会变化，欺诈行为也发生了重大变化。欺诈行为变得越来越复杂，涉及运用心理操控和技术，利用机器学习、人工智能和其他技术来使犯罪自动化。欺诈行为的数量之多、程度之严重，对全世界人民、经济和繁荣构成了重大风险，公众对法治的信心也因此受到负面影响。然而，准确了解欺诈行为面临若干挑战。由于感到羞耻、自责或尴尬以及没有意识到犯罪发生，受害者往往不报告欺诈行为。此外，很大一部分欺诈目标是企业，其中许多企业为了避免损害其声誉而选择不报告这些犯罪行为。欺诈以匿名方式远程实施进一步使受害者和主管部门难以辨认犯罪人的身份，妨碍评估底层模式和相关风险的工作。此外，欺诈具有动态性质，它们不断适应法律、社会、商业和技术体系的变化，这意味着新的和创新的犯罪方法可能在静态的官方数据中不被注意到。

3. 国际社会已认识到，欺诈的规模令人担忧，需要共同努力防止和打击欺诈行为。[1]大会第 78/229 号决议重申了联合国毒品和犯罪问题办公室（毒罪办）的一项任务授权，即应请求向会员国提供技术合作和援助，以应对包括欺诈在内的一切形式有组织犯罪。这与《打击有组织犯罪公约》的宗旨是一致的；正如其第 1 条

* CTOC/COP/WG.2/2024/1。

[1] 见经济及社会理事会关于开展国际合作，预防、侦查、起诉和惩治经济欺诈及身份相关犯罪的第 2004/26、2007/20、2009/22、2011/35 和 2013/39 号决议。

所述，该公约旨在促进合作，以更有效地预防和打击跨国有组织犯罪。大会认识到欺诈性质不断变化，并且越来越多地利用技术来扩大其影响范围，因此在第74/177 号决议中吁请会员国探讨各种措施，并形成可能的结论和建议，以创造一个安全、有抵御能力的网络环境，特别是关注与身份资料欺诈有关的犯罪。

4. 人们普遍承认，欺诈可能是一种有组织的严重犯罪。[2]随着技术发展以及有组织犯罪的范围和规模迅速扩大，犯罪分子创造了各种新方法，在全球范围内大规模欺诈个人、企业甚至政府。这使有组织犯罪集团能够更有效地瞄准全球各地的受害者。[3]

5. 有组织犯罪领域内的欺诈行为具有鲜明的特点。首先，它主要涉及窃取钱财，而不是生产或分销非法物品，这一点将其与其他犯罪活动区分开来。第二，许多欺诈活动是远程进行的，技术为匿名通信和转移赃款提供了便利，犯罪人和受害者之间无需进行面对面的互动。第三，欺诈往往依赖于受害者自愿提供获取其钱财的渠道，成功与否取决于使合法和非法实体之间界限变得模糊的欺骗手段。这些因素影响欺诈者采用的方法，决定了他们必须具备的能力，并影响到有组织犯罪集团的结构。

6. 其中一些欺诈者隐藏在看似合法的企业或职业中。某些有组织犯罪集团利用在传统企业或商业规范之外模糊或不受管控的领域开展活动所获得的见解或技能，采用看似合法工作场所的结构。这可能涉及建立一支受薪员工队伍，实行明确的劳动分工，并实际上模仿合法企业的组织框架。不存在典型的从事欺诈活动的有组织犯罪集团。实施欺诈的可能是各种团体，包括匿名交易技术、数据和其他犯罪服务的网上犯罪网络；围绕某个地区或社交网络联合起来的有组织犯罪集团；为模仿合法员工队伍结构（如呼叫中心）组建的有组织犯罪集团；以及通过原本合法的组织或职业实施欺诈的白领罪犯。有组织犯罪集团往往没有等级制度，其成员之间的合作是流动的。

7. 然而，欺诈活动的策划方式比犯罪人的组织方式更有助于了解有组织欺诈。历史上，欺诈并没有像其他类型有组织犯罪那样受到同等程度的重视，有组织欺诈往往被视为参与其他更严重犯罪（如贩毒）的有组织犯罪集团的一种补充性的犯罪活动。[4]在《打击有组织犯罪公约》中，严重犯罪被定义为应处以至少四年监禁的犯罪。但在实践中，许多国家并没有将欺诈定为严重犯罪。因此，它不属于《打击有组织犯罪公约》的范围。此外，即使在欺诈行为被当作严重罪行进行惩处的情况下，量刑也不一定会反映出这种严重性。

[2] 欧洲联盟执法合作署（欧警署），《2023 年互联网有组织犯罪威胁评估》（卢森堡，欧洲联盟出版物办公室，2023年）；和国际刑事警察组织（国际刑警组织），《2022年国际刑警组织全球犯罪趋势简要报告》（2022 年 10 月）。

[3] 国际刑警组织，“国际刑警组织金融欺诈评估：技术推动的全球威胁”，2024 年 3 月 11 日。

[4] Michael Levi，《牛津有组织犯罪手册》中的“有组织欺诈”，Letizia Paoli 编辑（牛津，牛津大学出版社，2014 年）。

二. 有组织欺诈的类别

8. 欺诈是一种犯罪，包括在各种环境下针对不同受害者实施的各种各样的行动和行为。在学术研究中，欺诈被广泛定义为“以欺骗手段获取有价值的东西或逃避义务”。[5]因此，欺诈不同于其他形式的严重谋财犯罪，它是通过欺骗而不是武力或胁迫实施的。此外，受害者和犯罪人很少需要同时出现在同一地点，许多欺诈跨越国内和国际边界。许多国家的刑法中都有关于欺诈的内容，但其描述方式和具体程度各不相同。[6]有些法律对构成欺诈的行为只作了笼统的描述，而另一些法律则提及欺诈计划中突出的某些活动、产品或服务，例如冒充主管机关或操纵数据或未经授权使用数据。一些国家针对计算机欺诈、信贷欺诈、拍卖欺诈或针对企业的欺诈等各种不同类型的欺诈单独立法。然而，大多数法律定义中都包含欺诈的一些核心要素：利用欺骗手段获得不正当好处或利益，对他人或其他组织造成损害。欺骗通常被理解为不诚实、虚假陈述、诡计、花招、欺诈手段、滥用信任或隐瞒或遗漏信息。在许多情况下，犯罪人获益意味着对他人造成损害，但有些则使用影响或损害他人经济利益、不当损失或被欺诈等词语来强调对他人造成损害。损害的对象可能是个人、公司或国家。

9. 从采用的方法、针对的实体以及对受害者和更广泛系统的影响方面来看，欺诈犯罪大相迥异。因此，为了解欺诈的性质，将欺诈划分为多种类型。虽然在国家和国际各级还有其他类型的欺诈，但本背景文件侧重于为金钱或其他物质利益为目的针对个人和公共或私营机构实施的欺诈。为说明这一点，确定了以下主要类别，本背景文件以下各节将对此作进一步详细解释：(a)消费产品和服务欺诈；(b)消费者投资欺诈；(c)就业欺诈；(d)关系和信任欺诈；(e)冒充官员欺诈；(f)身份欺诈；和(g)针对企业或组织的欺诈。

10. 在各主要类别中，重点介绍与受害者预期欺诈性交易带来的利益或结果有关的主要欺骗形式。虽然这些类别并非有组织犯罪集团所特有，但犯罪和造成伤害的能力因其参与而大大增强。每个类别都代表了操纵受害者的一种不同的手段，但所有类别都可能是跨国的，并涉及参与有组织犯罪集团的共同犯罪人。有些类别案发率高，造成的总体影响巨大，而在另一些类别中，则对少数受害者造成严重伤害。

A. 消费产品和服务欺诈

11. 消费产品和服务欺诈是最常见的欺诈类型之一，大量公众报告称曾被欺诈，成为欺诈目标或曾接到销售欺诈性产品或服务的通信。这类欺诈涉及销售不存在或实际与宣传严重不符的产品或服务。欺诈者通常推销紧俏产品或以低于合法市场的价格提供产品和服务。一些欺诈者将其广告瞄准被认为最容易对特定骗局上钩的群体。欺诈可能涉及完全虚构的卖家和物品，也可能涉及虚假描述其所供应商品或服务的公司。当产品或服务已被收到但被认为构成虚假描述时，在确认是否构成欺诈上可能存在挑战。欺诈者有时利用受害者缺乏金融知识的弱点来销售

[5] Grace M. Duffield 和 Peter Grabosky，“欺诈心理学”，《犯罪和刑事司法趋势和问题》丛刊，第199期（堪培拉，澳大利亚犯罪学研究所，2001年）。

[6] 审查了 7 个不同区域中 26 个国家的法律定义：欧洲和北美洲；拉丁美洲和加勒比；北非和西亚；撒哈拉以南非洲；中南亚；东亚和东南亚；以及澳大利亚和新西兰。

贷款、保险计划或养老金产品等金融服务。这通常与未来才能体现价值的产品有关，欺诈者要么向受害者灌输未来业绩过于乐观的预测，要么没有适当解释相关风险。欺诈者还可能不向受害者披露费用、佣金或法律要求，这可能导致遭受进一步的损失和罚金。[7]

12. 消费产品和服务欺诈中常见的产品和服务包括宝石、宠物、活动门票、医疗产品、彩票或承诺高额奖励的抽奖，或保险等金融产品和服务。然而，由于欺诈者谋求不断适应和利用新市场和消费者需求，可用于欺诈计划的产品和服务几乎无穷无尽。

13. 各种媒体包括网络被用来推销产品和服务。它们包括虚假网站、合法的购物和拍卖网站、垃圾邮件、帖子或拨打大量推销和销售电话的所谓“锅炉房”。一些犯罪人利用活跃的市场获取通过合法或非法手段（如数据泄露或网上钓鱼活动）编制的线索名单或甚至历史受害者个人名录（所谓的“傻瓜”名单）。信息和通信技术大大提高了在全球范围内以较低成本推销和销售产品和服务的能力。在某些情况下，个人消费者可能会蒙受金钱损失，但销售平台或金融服务提供商可能也会造成经济损失，这取决于具体情况和犯罪人所采用的方法。主要方法包括：

(a) 为推销和（或）销售产品和服务而建立的虚假网站。犯罪人可能会利用社交媒体或垃圾邮件等数字渠道推销网站，或者可能操纵互联网搜索引擎，以增加搜索相关产品或服务者登陆其网站的可能性；

(b) 合法销售、拍卖或社交媒体平台上的冒牌卖家，他们利用以伪造或被盗身份开设的账户。这些卖家利用合法平台，从而接触到大量搜索产品和服务的用户。例如，一个有组织犯罪集团在多个拍卖网站上发布了成百上千个诸如汽车等高价值物品的拍卖信息。[8]

14. 网上消费者欺诈不一定很高深或很复杂。滥用合法销售或拍卖网站的行为可能只需要一个人在拍卖网站上开设一个账户并发布广告销售不存在的产品。然而，一部分消费者欺诈犯罪是跨国进行的，涉及有组织犯罪集团。这种组织很少在与受害者的交流中显露出来，而是在了解其背后的计划和准备工作的过程中才能发现。关键阶段包括建立和推销网站或平台，让受害者参与以维系欺骗行为（或诱使进一步付款）和资金转移。犯罪人采用各种方法收取款项，同时留下的财务线索很有限。采用的方法包括让支付服务提供商相信其公司是合法的，将客户转往虚假的支付网站，要求受害者使用预付借记卡付款，或利用钱骡的第三方账户或以被盗或虚假身份开设的账户。在其他法域活动的有组织犯罪集团通常在目标国招募共犯，以方便洗钱。[9]

[7] 见 Michael Skidmore，《保护人们的养老金：了解和预防骗局》（伦敦，警察基金会，2020 年）。

[8] 更多信息见联合国毒品和犯罪问题办公室（毒罪办），打击犯罪信息与法律网络共享平台（夏洛克数据库）知识管理门户，判例法数据库，美利坚合众国诉 Bogdan Nicolescu、Tiberiu Danet 和 Radu Miclaus 案。可查阅 https://sherloc.unodc.org/。

[9] Christine Conradt，“网上拍卖欺诈和犯罪学理论：以 Adrian Ghighina 案为例”，第 6 卷，第 1 期，《国际网络犯罪学杂志》（2012 年 1 月/6 月）；以及 Jack M. Whittaker 和 Mark Button，“了解宠物骗局：利用受害者账户进行预付费和不交付的欺诈案例研究”，《犯罪学杂志》，第 53 卷，第 4 期（2020 年 9 月）。

B. 投资欺诈

15. 投资欺诈通常涉及出售公司股票、债券或货币，有些欺诈计划则推销投资有形资产，从财产或商业开发到葡萄酒和烈酒等，不一而足。

16. 要实施这些欺诈，可能需要对有关市场的法规和相关管控制度的情况有敏锐的认识，合法和非法做法之间的界限可能很容易渗透，并且难以察觉。在某些情况下，犯罪人利用信任机制，注册为受监管实体或利用具有受监管地位的其他合法行为体。在占据合法和非法做法之间的这一灰色地带后，它们给执法机构或其他监管机构设置了障碍，这些机构需要掌握并提供充分和有力的证据证明存在欺骗行为，并证明犯罪已经发生。事实上，虽然不道德，但有些欺诈者采用的计划可能会对投资者造成严重伤害但不构成犯罪。金字塔和庞氏骗局是犯罪人常用的运作模式，投资计划依靠不断吸引新的投资者来自我维持，而不是从真正的产品或投资中产生回报，这些产品或投资也许根本不存在。

17. 投资欺诈似乎越来越多，部分原因是涉及加密货币投资的欺诈增多。这种新的投资欺诈手段利用数字空间提供的速度和灵活性，使犯罪人能够以相对较低的成本快速大规模营销。[10]在加密货币市场等新型金融市场中，监管方面的挑战导致存在更大的漏洞，可供欺诈者加以利用。加密货币投资欺诈采用的方法在技术复杂性和新颖性方面各有不同，其中一些技术是从市场操纵和金融诱骗等其他方法中移植过来的，其中包括开发和推销欺诈性加密货币投资平台以及所谓的“退出骗局”或“拉地毯”，这涉及人为夸大骗局代币的价值，而一旦犯罪人撤出所有投资资金，代币将变得一文不值。

18. 投资欺诈的成功取决于有效沟通，即使用各种伎俩说服潜在投资者，这些伎俩包括针对性或大众营销活动；进攻性销售技巧；和提供资源，以建立和维持可信性和信任，包括品牌信息、网站和其他营销材料。犯罪人可利用犯罪不同阶段使用的特定通信渠道或组合渠道。例如，与受害者的最初联系可通过钓鱼网站进行，随后是通过电话推销，然后通过欺诈网站继续进行欺诈。欺诈者可能会使用以下方法与受害者接触：

(a) 电话推销：使用呼叫中心或“锅炉房”进行攻击性推销和销售，通常采取有针对性地主动打电话的形式，使用从其他合法或非法行为体那里收集或购买的线索名单，这些行为体收集并出售消费者个人信息。在某些情况下，这些名单包括已知曾沦为受害者的个人，他们因此容易被类似的投资方法所骗，这个问题对弱势老年受害者而言尤为严重。呼叫中心可以由实施欺诈计划的犯罪人直接管理，也可以外包给能够提供这些“锅炉房”服务的专家。这些中心可能位于海外，有时位于对这些活动控制不那么严格的法域；[11]

(b) 网上：一些国家的网上投资欺诈大幅增多，通过社交媒体、欺诈网站和应用程序等网上通信手段进行初步接触，这些手段在欺骗中发挥了关键作用。由于可以获得数字技术和关于消费者的大型数据集，欺诈者从事大规模和有针对性推销的能力大增。例如，网络钓鱼活动可用于引诱和精确定位对所提供产品或服

[10] Arianna Trozze、Toby Davies 和 Bennett Kleinberg，“degens 和欺诈者：利用开源调查工具调查去中心化金融欺诈和洗钱”，《国际法庭科学杂志：数字调查》，第 46 卷（2023 年）。

[11] Neal Shover、Glenn. S. Coffe 和 Clintin R. Sanders：“拨号获取美元：机会、理由和电话推销欺诈”，《质性社会学》，第 27 卷，第 1 期（2004 年 3 月）。

务感兴趣的个人，从而为有针对性的后续通信提供基础。犯罪人通常利用社交媒体和数字通信应用程序来推销其产品，有时利用名人或流行文化形象说服受害者投资。当这些欺诈性加密货币计划渗透到主流金融市场时，可能会导致惊人的经济损失；

(c) 当面：投资往往涉及对受害者来说非常重要的大笔资金，有时面对面接触对于取得足够的信任以确保投资仍然很重要。一些欺诈者以现有社会或商业关系中的受害者为目标，利用已经存在的信任行骗。

19. 投资欺诈犯罪分子不遗余力地营造一种合法的假象，通常采用正式合法组织的结构、流程和措辞，包括明确的分工，按等级制度指定人员角色。行动的复杂程度各不相同，取决于其避免被怀疑或发现并继续犯罪的动机。[12]所谓的“骗了就跑”行动可以只运作很短一段时间，然后卷跑投资者的资金，其他一些计划则可以运作多年而不被发现。

20. 与针对公众个人的其他欺诈相比，投资欺诈受害者遭受的损失最大。[13]受害者被灌输了完全虚假或严重夸大的经济回报预期。许多投资者损失了其全部或大部分资金。无论采用哪种具体方法，欺诈者通常都会向受害者兜售一种投资将在未来产生价值的预期，这意味着受害者可能在最初投资数年后才意识到上当受骗。不同骗局和底层欺骗手段的特点可能差异很大，但这类骗局的结果一般都是投资者损失全部或大部分资金。一些例子包括：

(a) 完全欺骗，其中投资服务或产品从未存在过；

(b) 不正当销售无价值或定价过高的股票，获取不可能产生承诺回报或注定失败的高风险投资；

(c) 利用市场操纵技术，人为地向毫无戒心的投资者夸大投资价值。

21. 受害者经济损失的严重程度将取决于其经济或个人情况。这也可能取决于犯罪人使用的方法，例如针对人们的养老金储蓄，这可能会对个人受害者造成很大影响，[14]而一些加密货币投资可能侧重于从较多的受害者那里获得相对较小的金额。在金字塔和庞氏骗局受害者的情况中，在早期阶段投资和撤资者可能不会有任何资金损失。一旦钱财被窃，受害者可能会再次受到同一犯罪人或其他犯罪人的侵害，在某些情况下，这些犯罪人会标榜自己隶属于某一合法机构。他们声称有能力追踪和追回损失的资金，但要求受害者预付费用，这一伎俩被称为追偿欺诈。

C. 就业欺诈

22. 就业欺诈涉及在招聘网站上大规模推销虚假或误导性就业机会。合法部门利用网上招聘广告的情况显著增加，特别是自全球大流行病暴发以来，招聘者提供更灵活的工作安排和居家办公的机会。欺诈者利用人们对理想职位的需求，特别

[12] Michael Levi，“有组织欺诈与组织欺诈：网络与组织的剖析研究”，《犯罪学与刑事司法》，第 8 卷，第 4 期（2008 年 12 月）。

[13] 另见美国司法部，“司法部没收了超过 1.12 亿美元与加密货币投资计划有关的资金”，新闻稿，2023 年 4 月 3 日。

[14] 见 Skidmore，《保护人们的养老金》。

是在因资格或培训不足或当地经济中缺乏就业机会而导致这类合法机会有限的人群中。[15]研究表明，被这些欺诈者盯上的通常是经济上最无保障或处于绝望境地的求职者。

23. 这些欺诈行为通常涉及在网上发布完全虚构的或收益远低于广告数额的就业机会，比如商业机会、居家办公或模特机会的广告。在某些情况下，欺诈者要求受害者在就职之前预付款项；所标榜的理由五花八门，包括入门工具包、旅行、培训或信用评分检查。其结果往往是受害者损失钱财，却没有得到承诺的就业机会。在其他骗局中，欺诈者向受害者发送伪造的支票，以支付受害者的启用费用，然后声称他们付款超额，并要求受害者将资金转回给犯罪人。一旦支票被识别为伪造，受害者就会损失转出的资金，还要承担支票的费用。

24. 就业欺诈者还可能有动机窃取受害者在申请过程中提供的个人身份信息，使他们很容易遭到进一步欺诈。在某些情况下，这份工作还具有犯罪性质。例如，受害者可能被引诱协助洗钱（如充当钱骡）或充当快递员运送以欺诈方式购买的物品（即身份欺诈）。在一些最严重的情况中，受害者沦为被贩运人口，被强迫进行劳动或实施犯罪。[16]

D. 关系和信任欺诈

25. 在任何类型的欺诈中，建立信任的过程均起到至关重要的作用。然而，在关系和信任欺诈的情况中，犯罪人培养和利用个人关系的力量来建立必要的信任，以操纵和欺骗受害者，有时在多种场合这样做。在这些欺诈中，受害者并不期望得到产品或服务，而是期望与犯罪人建立真正的关系。这些欺诈的复杂性不在于对技术系统的利用，而在于受害者与犯罪人之间关系的动态变化。

26. 许多欺诈者在网上建立关系，并在几个月甚至几年的时间里利用社会工程技术来获取受害者的信任。受害者通常期待浪漫的关系，但也有其他形式，如获得信任的友谊，甚至希望与受害者的家庭成员建立关系。一些研究已发现老龄化和老年人口中因孤独、社会孤立和渴望建立新关系等因素存在脆弱性。犯罪分子通过交友或浪漫交往过程瞄准并利用这一弱点。此外，犯罪人可能会冒充处境困窘和需要资金救济的家属或朋友。这种欺诈可能具有针对性，并可能利用从朋友或亲戚的社交媒体帖子中获取的个人详细信息，从而使与受害者的沟通更加可信。沟通通常以发送文本消息的方式进行。有些例子显示人工智能被用来在电话中克隆家属或朋友的声音。

27. 这类欺诈的一个核心要素是婚恋诈骗，犯罪人在网上建立浪漫关系，以便欺骗和勒索受害者钱财。这可能会给个人造成巨额经济损失。这个问题影响到世界许多不同地方的受害者，它利用了在线社交网络的增长，更具体而言是利用了在网上寻找浪漫关系的更广泛的社会趋势。犯罪人往往会先在社交媒体或约会网站

[15] Alexandrea J. Ravenelle、Erica Janko 和 Ken Cai Kowalski，“好工作，骗人的工作：在 COVID-19 大流行期间侦测、规范和内部化网上招聘骗局”，《新媒体与社会》，第 24 卷，第 7 期（2022 年 7 月），第 1591 至 1610 页；和 Delali Kwasi Dake，“网上招聘欺诈侦测：针对加纳就业网站的基于机器学习的模型”，《国际计算机应用杂志》，第 184 卷，第 51 期（2023 年 3 月）。

[16] 关于这两种剥削形式的更多信息，另见《2002 年全球人口贩运问题报告》（联合国出版物，2022 年），以及毒罪办，《东南亚赌场、网络欺诈和为强迫实施犯罪活动的人口贩运：政策报告》（曼谷，2023 年）。

和应用程序上使用虚假身份接触受害者，并附上相应的个人资料说明。一名犯罪人可能会在不同身份之间转换，以瞄准和引诱潜在的受害者。一旦关系确立，犯罪人可能会先向受害者索要一小笔钱，然后再向其索要更大数额的资金，从而获取经济利益，他们通常会传递一种危机情景，用来向受害者传递压力和紧迫性（例如健康紧急状况或紧急旅行要求）。如果交换过性图像，受害者可能还会被勒索钱财。

28. 最近，浪漫欺诈还出现了与加密货币投资欺诈相结合的新版本。在浪漫诱饵欺诈或所谓的“杀猪盘”欺诈（出于对此类犯罪受害者的尊重，不建议使用该词）中，犯罪人会与网上受害者建立个人关系。他们不编造危机情景，而是利用亲密关系和信任诱使受害者参与欺诈性投资计划。对犯罪人来说，这可能包括额外的规划和筹备阶段，其中包括开发受害者可以访问的欺诈性网站或应用程序，甚至为投资者提供“客户服务”。[17]将加密货币投资融入骗局会产生许多后果：它扩大了潜在的受害者群体，包括来自年轻群体的受害者；将受害者引入到不熟悉的、动荡的高风险市场，这意味着他们可能没那么容易认识到自己是受害者；并给刑事调查人员将资金源头追溯到犯罪人带来更多困难。

29. 许多关于浪漫欺诈的研究都侧重于受害者及其经历，而不是没那么显眼的犯罪人。这些罪行通常被认为是有组织犯罪集团实施的跨国犯罪，其中一些集中在某些区域。在“杀猪盘”欺诈方面，一些有组织犯罪集团采用了更为复杂的类似企业的结构，其中有明确的分工（例如受害者联系、信息技术和洗钱），并招募一批缺钱和面临剥削风险的人，包括贩运人口。[18]

30. 不管受害者的特征如何，关系和信任欺诈都可能造成相当大的影响。受害者不仅蒙受经济损失，也会因信任破裂和重要个人关系丧失而遭受痛苦。此外，他们还受到严重的心理和情感伤害。有些人甚至可能拒绝接受自己是或曾经是欺诈受害者。

E. 冒充官员欺诈

31. 冒充官员欺诈（或冒充欺诈）是指操纵通信，假装自己来自公共或其他官方部门，如警察、税务机关、银行或政府部门。这些欺诈采用一系列借口和场景，包括冒充税务机关或其他政府部门并声称存在未偿还债务；冒充银行官员并声称银行账户中的资金面临犯罪分子的威胁；或冒充警方并声称发现受害者有刑事犯罪行为。

32. 冒充欺诈的一个主要显著特点是使用诱导话术，不去迎合受害者的需求和需要（如在消费者欺诈中），而是引起恐惧、害怕、焦虑和担忧。诱导受害者产生激动情绪，会阻碍其决策，使其更易于被操控。犯罪人会恐吓称，如果受害者不付款或转账，就会有负面后果，包括某种形式的法律回应。

33. 这些欺诈通常涉及大众传播，如垃圾电子邮件；使用社交媒体进行沟通；文本信息；或自动拨打电话，或所谓的“机器人拨号”，即使用录音信息自动拨打

[17] Cassandra Cross，“浪漫诱饵、cryptorom 和‘杀猪盘’：浪漫欺诈的演进步伐”，《当前刑事司法问题》（2023 年）；以及 Fangzhou Wang 和 Xiaoli Zhou，“网上浪漫骗局中的经济剥削劝导计划：中国杀猪盘剖析”，《受害者与罪犯》，第 18 卷，第 5 期（2023 年）。

[18] 毒罪办，“赌场、网络欺诈和贩运人口”。

电话。这些技术为同时与成千上万的受害者进行近乎同步的联系提供了便利，使他们具有极大的影响范围。

F. 身份欺诈

34. 身份欺诈[19]是指使用窃取的或伪造的身份信息直接获取受害者的货物、服务或资金，例如使用被盗信息进行购物或访问金融账户。身份欺诈可以在身份被滥用的个人没有进行任何直接通信或采取任何行动的情况下实施，因为目标往往是货物、服务或资金的提供者。通过这种方式，伤害波及受害的不同行为体，包括身份被滥用的受害者和资金被转走的金融服务提供商或其他公司，在某些情况下还波及使用被盗资金购买的货物或服务的提供者。

35. 犯罪分子可以获取不同形式的身份信息，每种信息都可以以不同的方式加以利用。其中有个人信息，包括个人在不同网络环境中的数字身份，如姓名或出生日期；金融账户数据，如信用卡卡号；在线账户信息，包括用户名和密码；以及生物特征数据，例如从电子设备窃取的数字指纹。

36. 犯罪人可以通过以下手段获取这些信息：入侵系统；社会工程手段，如网络钓鱼或短信诈骗活动；或进入出售数据的在线犯罪市场。这些数据可用于购买商品和服务，提交贷款和其他融资申请，或从受害者账户获取和转移资金。有关这些手段的其他信息包括：

(a) 系统入侵：一些诈骗者通过非法黑客技术、部署恶意软件或网络钓鱼等手段积极获取个人信息；

(b) 在线犯罪市场：涉及身份信息买卖的地下经济十分活跃，可被身份欺诈者加以利用。以这种方式获取信息的机会为欺诈者消除了一些技术障碍，否则他们可能就没有能力窃取个人信息；

(c) 社会工程学：这通常通过电子邮件或其他在线通信、文本信息或未经请求的电话发送的广告或其他未经请求的通信来实现，从而诱骗受害者提供个人信息。复杂程度各不相同，但假冒合法网站等更复杂的方法可能会导致更大的损害，使犯罪人能够直接访问在线账户。

37. 犯罪人实施身份欺诈所采用的手段多种多样。一些主要的方法包括账户接管、无卡支付和应用程序欺诈，这些方法的定义如下：

(a) 账户接管：在这些欺诈中，犯罪人获得访问用户账户的合法凭证。其中可能包括银行账户，也包括其他类型的金融账户（例如虚拟货币提供者）、零售网站或任何商品和服务提供者。该账户可用于多种目的，包括直接将资金转移到犯罪人控制的账户或使用该账户以欺诈方式购买商品或服务。在某些情况下，获取进入受害者账户的信息是通过随后的系统入侵获取资金、货物或服务所需的一系列步骤中的第一步。这可能涉及攻克安全措施，如双因素身份验证。因此，犯罪人寻求采取其他手段，如 SIM 卡交换和替代支付方法；

(b) 无卡支付：在网上或通过电话远程向供应商进行未经授权的购买。获得受害者的资金凭证足以欺骗金融服务提供商以及商业供应商，而无需与受害者直

[19] 另见毒罪办《身份相关犯罪问题手册》（维也纳，2011 年）。

接互动或接触实物支付卡。身份欺诈者利用受害者的资金凭证通常需要采取一些关键步骤：

㈠ 从网上犯罪市场获取知识、资源和资金凭证；

㈡ 伪装订单，以避免触发商业网站上的欺诈侦测算法；

㈢ 在无法追查到犯罪人的地址接收订单；

㈣ 以个人卖家身份转售物品或冒充主流在线市场的合法商家批量出售这些物品；

(c) 应用程序欺诈：这些欺诈利用个人信息的广泛可用性，并用它来以受害者的名义申请信贷。这通常是为了从金融服务提供商获得贷款。犯罪人必须获取一系列的个人综合信息（如姓名、地址或出生日期），才能可信地冒充个人。一种新出现的模式是利用技术，通过结合真实和伪造的标识符来创建合成身份。一旦建立起来，这些身份就可以慢慢培养，变得更加可信，以便最终提交高价值金融产品的申请。

38. 重要的是，实施身份欺诈并不取决于有组织犯罪和有组织犯罪集团的参与。然而，有组织犯罪所掌握的技能和资源使大规模实施身份欺诈并获取高额利润的能力大增。随着数字经济的不断发展，可用的在线目标激增，这种威胁变得尤为严重。操纵和滥用身份可在实施有组织犯罪中起到各种作用，包括追查犯罪活动实施者的工作。[20]

G. 针对企业或组织的欺诈

39. 针对企业或组织的欺诈通常涉及滥用内部系统或商业关系来欺骗受害者。这些欺诈可能由组织内部或外部的人员实施。另外有些欺诈是由合法的企业和行为体实施或使用合法产品来实施，而不是从一开始就以实施欺诈为目的的计划，有时是为了应对内部压力或可疑的工作做法或文化。

40. 针对企业或组织的欺诈的一些例子包括：

(a) 商业电子邮件欺诈是一种网络欺诈，数量庞大。各种规模和来自各种部门的企业和组织都是这类欺诈的受害者，它们通常由外部犯罪分子实施。犯罪人渗透系统，利用社会工程技术说服员工未经授权将资金转移到犯罪人控制的账户中。受害者可能会承受高额损失。第一步是渗透一个组织的通信系统，以便说服收件人相信他们是合法的。主要方法包括侵入工作人员的电子邮件账户；发送网络钓鱼电子邮件以获取工作人员的账户详细信息；或者利用通信提供商来冒充目标组织熟悉的域名。[21]犯罪人会使用各种话术套路，其中包括：通过开具假发票来利用两家公司之间的现有关系；发送声称来自高级工作人员的电子邮件，提出紧

[20] Simon Baechler，“证件欺诈：二十一世纪你的身份安全吗？”，《欧洲刑事政策和研究杂志》，第 26 卷，第 3 期（2020 年 6 月）。

[21] Norah Saud Al-Musib 等，“商业电子邮件犯罪（BEC）攻击”，《今日材料：会议记录》第 81 卷，第 2 部分（2023 年）；以及 Geoffrey Simpson、Tyler Moore 和 Richard Clayton，《十年来利用域名视觉冒充攻击公司的事件》，于 2020 年 11 月 16 日至 19 日由反网络钓鱼工作组在美国波士顿主办的电子犯罪研究研讨会上介绍的研究论文。

急资金请求；或冒充律师要求电汇转账以解决敏感问题。[22]通信可能会持续一段时间，犯罪人可能会花一些时间了解该组织及其系统，并在多种场合对其实施侵害；

(b) 财务报表欺诈包括多种方法，金融市场上原本合法的专业人员利用这些方法误导和扭曲投资者、监管机构和其他市场行为体等对公司或资金的财务健康状况和未来前景的看法。类似的会计欺诈还可能掩盖挪用、滥用或贪污资金的行为。这些欺诈的实施可能是为了应对实现预期业绩的压力，例如公司高管、流氓金融交易员或对冲基金经理在报告财务业绩的时候。在某些情况下，这些欺诈行为的影响会波及企业之外，包括外部的企业、部门甚至更广泛的经济领域；[23]

(c) 长期或短期公司欺诈可能由现有贸易公司或为欺诈目的而收购或设立的公司实施。这些公司建立信用记录、信任或信誉，用于欺骗买方、卖方或债权人提供货物或资金。这些公司在这样做时要么明知自己无法付款，要么并不打算付款。

三. 供审议的议题

41. 工作组不妨重点审议下列议题：

(a) 各法域中有组织欺诈的性质；

(b) 利用《打击有组织犯罪公约》来预防和打击有组织欺诈，以及将欺诈定为《公约》第 2 条所界定的严重犯罪；

(c) 开展有效国际合作的机会，包括与私营部门的合作；

(d) 在预防有组织欺诈、保护欺诈受害者和证人以及举报人、追查参与有组织欺诈的有组织犯罪集团方面分享信息，并促进为此目的建立伙伴关系；

(e) 确定在实施《打击有组织犯罪公约》以预防和打击有组织欺诈方面的相关技术援助需要。

四. 后续行动和可能的建议

42. 工作组不妨提出以下建议：

(a) 鼓励尚未将欺诈定为《打击有组织犯罪公约》第 2 条(b)项所界定的严重犯罪的缔约国考虑这样做，以确保在相关犯罪具有跨国性质并涉及有组织犯罪集团的情况下可根据《公约》提供有效的国际合作；

(b) 促请缔约国利用《打击有组织犯罪公约》提供的工具，在必要和适当时制定或修订国家立法，以预防和打击欺诈，包括有组织犯罪集团实施的欺诈；

[22] Alessandro E. Agazzi，“商业电子邮件犯罪和网络心理学”。可查阅 https://arxiv.org/。以及 Al-Musib 等，“商业电子邮件犯罪攻击”。

[23] 大不列颠及北爱尔兰联合王国，严重欺诈办公室，“高级银行家因操纵欧洲银行间欧元同业拆借利率被判处 9 年徒刑”，2019 年 4 月 1 日。

(c) 鼓励缔约国酌情与其他相关利益攸关方协商，分析有组织犯罪集团在有组织欺诈方面的活动趋势，并与联合国毒品和犯罪问题办公室分享这一信息和数据；

(d) 请联合国毒品和犯罪问题办公室在有预算外资源的情况下收集、分析和传播关于有组织欺诈的信息；

(e) 促请各缔约国在与《打击有组织犯罪公约》及其各项议定书所涵盖的有组织欺诈和相关犯罪有关的侦查、起诉和司法程序方面相互提供最广泛的国际合作，包括司法协助；

(f) 鼓励缔约国加强与相关利益攸关方的合作，包括与私营部门、民间社会组织、媒体、学术界和科学界的合作，以预防和打击有组织欺诈，包括为此开展教育和提高认识运动；

(g) 请联合国毒品和犯罪问题办公室在有预算外资源的情况下，继续开发技术援助工具，并根据请求提供技术援助，包括提供能力建设，以支持缔约国努力有效实施《打击有组织犯罪公约》，预防和打击有组织欺诈；

(h) 请尚未在打击犯罪信息与法律网络共享平台（夏洛克数据库）知识管理门户上更新本国关于有组织欺诈定罪问题的立法记录的缔约国更新这些记录。