



# 第十一届 联合国预防犯罪和 刑事司法大会



2005年4月18日至25日，曼谷

Distr.: General  
16 March 2005

Chinese  
Original: English

临时议程\*项目 6

经济和金融犯罪：对可持续发展的挑战

## 讲习班 5：打击包括洗钱在内的经济犯罪的措施\*\*

背景文件\*\*\*

### 目录

	段次	页次
一、 导言.....	1-4	2
二、 盗用身份.....	6-16	3
三、 洗钱.....	17-36	6
A. 洗钱的刑事定罪：法律框架.....	32-33	9
B. 对洗钱罪行的调查.....	34	9
C. 国际合作.....	35	10
D. 对犯罪收益的控制.....	36	10
四、 技术援助.....	37-47	10
五、 结论和建议.....	48-49	12
附件：供讲习班 5 使用的假想案例.....		13

\* A/CONF.203/1。

\*\* 本背景文件的提交有所推迟，因为需要进行更多的研究和磋商。

\*\*\* 秘书长谨感谢亚洲和远东预防犯罪和罪犯待遇研究所及瑞典政府协助举办讲习班 5。



## 一、 导言

1. 近来通信技术和运输的快速发展不仅改变了社会经济结构，还促进了全球化，使经济活动交易增加，种类更加多样，而且越来越具有跨国性质。这些变化为增长和发展创造了新机会，但随之经济犯罪也成为令全球关注的问题，犯罪集团的作案手法更加先进，其活动规模也有了不小的扩大。计算机的迅速普及、因特网服务用户的大量增加和以信用卡为基础的经济的扩展更是加速了这一趋势。由于其性质所决定，使用因特网作为工具的犯罪很容易超越国界，扩大到全世界。犯罪分子充分利用因特网和电子商务来进行跨国经济犯罪。这些犯罪的跨国性质妨碍了对案件的侦查，并使调查和起诉更加困难。犯罪收益的跟踪和追回也变得更加复杂。因此，全球化社会中的经济犯罪向国际社会提出了一个严重问题，妨碍了世界经济的发展。

2. 第十一届预防犯罪和刑事司法大会是一个机会，可借以广泛讨论经济和金融犯罪这个涉及面很广的问题。为了进行这项讨论，秘书处编制了一份工作文件（A/CONF.203/7），提出了可供讨论的若干议题，详细介绍了这种形式的犯罪所带来的问题，其中包括经济和金融犯罪的概念化，以及需要国际社会特别关注这些问题的理由。

3. 讲习班 5 为政府代表、专家和执业人员提供了一个进行交互式对话的机会，以便将重点放在各种形式经济犯罪的范围和影响上。这项重点对于制定切实可行的政策建议和探索国家行动和包括技术援助在内的国际合作的条件来说也是必要的。

4. 具体而言，讲习班 5 可以作为审议打击经济犯罪和洗钱的各项措施的出发点，其中包括讨论以下问题：

(a) 包括洗钱在内的经济犯罪的当前趋势，其中要特别关注这种犯罪的类型；

(b) 可在多大程度上使用现有国际法律文书，包括《联合国打击跨国有组织犯罪公约》（大会第 55/25 号决议，附件一）及其议定书和《联合国反腐败公约》（第 58/4 号决议，附件）来打击经济犯罪；

(c) 制定有效的预防战略；

- (d) 新的调查技术；
- (e) 设立有效的金融情报单位，包括这些情报单位之间更好的合作；
- (f) 国际合作和技术援助。

为了尽可能扩大该讲习班的实际指导意义，鼓励进行交互式的对话，本背景文件载有一个可供分析和讨论的假想案例（见附件）。

## 二、盗用身份

5. 联合国犯罪预防和刑事司法方案工作的一个指导原则是，必须确保在犯罪者的能力有所增长的时候，执法和刑事司法部门的能力也有同样的增长。该方案的另一个目标是在国内和国际上控制犯罪。审议对付盗用身份行为的国内和国际措施符合这两个目标。

6. 可以说，“盗用身份”涉及两种不同的非此即彼的活动。第一种活动是获取、收集和转让个人信息的准备阶段，个人信息可以是无形信息（如计算机屏幕上的虚拟信息），也可以是有形信息（从计算机屏幕或实实在在的文件中抄写到纸上的个人信息）。在这个阶段，并没有实际利用这些信息来试图或实际犯下某一罪行，如诈骗、偷窃或假扮另一个人。**获取**个人信息是为了将其作为一种犯罪手段在将来使用。盗用身份的另一种，即第二种活动是实际**利用**个人信息来试图或实际犯下某一罪行。在这种情况下，个人信息被用来设想一个在各方面全新的身份（A 假扮成 B），或让受害人相信交易的某个方面确如罪犯所言（例如某个银行账户的账户余额是 X 美元，而不是 Y 美元，因为该账户属于 B 而不是罪犯 A）。

7. 因此，盗用身份涉及最终导致犯下某一罪行，通常是经济罪行的一个或多个活动。在大多数国家，如果犯罪者实施犯罪（例如偷窃）的目的不是为了获取个人信息，则个人信息的获取和拥有本身不构成犯罪。不过，有越来越多的证据表明，盗用身份有助于实施国内和国际经济犯罪。

8. 在许多国家（如果不是大多数国家的话），犯罪者通常只在实际**利用**个人信息时，而不是在**获取**个人信息并打算将其用于以后的犯罪时承担刑事责任。例如，罪犯可以暗中获取个人信息，以便利用受害者的身份来进行诈骗、逃避抓捕或侦查，或在有些情况下实施与有组织犯罪或恐怖主义有关的罪行。在许多国家，除

非可以确定某项阴谋或有组织犯罪活动，否则不能将收集、获取、储存、处理、购买、出售、进口和出口无形个人信息（如计算机上的个人信息或从身份证件中抄来的个人信息书面清单）的行为定为犯罪。

9. 犯罪者用以获取个人信息的手段从技术复杂程度看各不相同。有些活动在几乎所有国家都属于犯罪（如偷窃），有些则不是。获取个人信息供今后犯罪时使用的一些比较常见的方式有：

(a) 偷窃钱包；从邮件中盗取文件；将邮件的接收地址从受害者的家改为犯罪者的家；

(b) 从废弃物中捡回确定受害者个人信息的文件，如信用卡号或银行账号（“垃圾搜寻”）；

(c) 未经授权而复制数字化数据（如记录信用卡或借记卡号码的“浏览”工具；在浏览借记卡时使用隐藏相机来拍摄个人密码）；

(d) 获取已故人员的个人信息来假扮其身份（“盗用死者名分”）；

(e) 从公共来源获取个人信息（如“肩后偷窥”，指在别人输入借记卡密码时在其背后从肩膀上偷窥）；

(f) 从因特网上获取个人简介，以便使用这些信息来假扮该个人；

(g) 使用因特网指示受害者访问某个看起来似乎是合法经营的网站。在网站上要求受害者披露个人信息。罪犯收集个人信息是为了在今后用于实施诈骗或其他形式的经济犯罪（这种活动称作“网上钓鱼”）；

(h) 危害大型数据库（如进入公共或私人计算机的数据库来获取个人信息，以便制作假身份证件）；

(i) 使用腐败的政府或公司雇员提供的个人信息来制作假证件（如假驾照）或从这些雇员手中获取假的身份证件。

10. 许多国家在处理盗用身份案件时面临的一个挑战是个人信息一般不符合“财产”的定义。从传统上讲，盗窃罪要求所盗取的无形和（或）有形的“物品”必须具备“财产”的特征。此外，要构成盗窃罪的犯罪要件，必须是从所有者手中

实际剥夺了这件“物品”。在许多国家，仅仅侵犯个人信息的机密性并不是构成偷窃或诈骗的充分要件。因此，在许多国家，如果在获取个人信息时没有实施刑事犯罪，则仅仅抄写这些信息或骗取他人的这些信息可能也不构成犯罪。不符合“财产”定义的个人信息的传播在大多数国家也不是刑事犯罪。在这种情况下，个人信息是一项实施犯罪的工具，但其获取、拥有和转让给他人本身并不是犯罪。

11. 除了许多国家在“财产”的法律定义或剥夺非法使用的“物品”的要求方面存在的局限性外，技术进步也改变了通过非法使用个人信息实施的经济犯罪的方式。例如，在发明计算机和因特网以前，个人盗窃他人的身份并使用该身份来假装别人进行贷款担保或从银行借款可能就是一个典型的诈骗案例。被告既具备犯罪的客观要件，也具备犯罪的主观意图。在罪犯和受害人之间通常也存在实际接触。

12. 计算机和因特网的出现助长了由不同的人实施一系列犯罪活动的犯罪。由于计算机技术通常可以隐藏真实身份，从而妨碍了对这些罪行的侦查。这就促使利用多个行为人，他们或彼此协调行动，或相互独立，但是都知道是为了犯罪目的而收集和转让个人信息。执法部门面临的挑战是最终导致犯下传统的经济罪行的一系列行为并不是一个行为人实施的。每个人都负责活动的一个特定方面，各个方面加起来才构成犯罪，例如诈骗。有组织犯罪集团就使用了这种经济犯罪方法，从而使个人能够免于刑事起诉。

13. 利用多个行为人来实施犯罪的例子如下：A 可能从计算机上抄取有关许多人的个人信息，然后将这些信息卖给 B。可以使用先进的技术，例如因特网来实施这一行为，或者采用比较传统的方式，例如用金钱来换取信息。B 充当中间人，将信息转卖给 C，C 利用这些信息来制造假证件。C 将假证件卖给不同国家的客户，这些客户使用假证件来对其他国家的受害者行骗。还有一些客户将假证件卖给有组织犯罪集团或恐怖主义分子来实施其他犯罪，如贩卖毒品、洗钱或走私。在许多国家，根据有关犯罪同谋或犯罪参与方式的任何法律，A 或 B 都没有实施犯罪，尽管他们的活动在向 C 提供必要信息制造假证件方面是不可或缺的。

14. 大多数国家都没有“盗用身份”这一罪名。因此，从统计角度讲，很难确定是否应将涉及盗用身份的诈骗行为归入诈骗统计数字。这就使得追踪非法使用个人信息犯罪的国际增长趋势的工作更加复杂。希望经济及社会理事会在 2004 年 7 月 21 日第 2004/26 号决议中要求进行的研究能够有助于更深刻地了解国内和跨国诈骗与非法使用和伪造身份的趋势。

15. 加拿大和美利坚合众国的最新统计数据涉及非法使用个人信息实施的诈骗行为，它们表明此类犯罪的性质有了重大转变。加拿大 Phonebusters 全国举报热线中心在 2002 年报告了 8 187 例盗用身份投诉案件，到 2003 年，这一数字大幅度增加，达到 13 359 例。据 Phonebusters 报告，盗用身份投诉案件中涉及的损失在 2002 年为 1 180 万加元，2003 年达到 2 160 万加元（见 <http://www.phonebusters.com>）。在过去的四年中，美国联邦贸易委员会报告说，盗用身份投诉数量高居向该委员会提出的消费者投诉之首。2003 年 9 月，该委员会公布的一项调查表明，在过去的五年里，共有 2 730 万美国人被盗用了身份。据报告，2002 年给消费者和企业造成了 530 亿美元的损失。<sup>1</sup>2003 年为联邦贸易委员会进行的另一项调查显示，估计该年约有 1 000 万盗用身份受害者花费了 3 亿小时来试图挽回其经济损失、恢复其信誉等级和名声。<sup>2</sup>加拿大良好企业理事会估计，2002 年盗用身份造成的消费者和商业损失总额为 25 亿加元。<sup>3</sup>

16. 信息的自由流动是因特网的命脉，因此也是在因特网上进行的贸易的命脉，但这也为罪犯盗取个人信息并用于犯罪提供了大量机会。暗中搜集和转让个人信息供以后犯罪使用，可能会削弱成员国的经济和国家安全。

### 三、洗钱

17. 按照一般的理解，“洗钱”是指对犯罪收益进行处理，以掩盖或隐藏其非法来源的活动。罪犯试图通过洗钱来保护和进一步享有或使用其犯罪所得的经济收益。因此洗钱对于大多数罪犯来说都是一个非常重要的过程，特别是当金融犯罪的主要目的是获得经济利益时。罪犯还利用洗钱来从事进一步的犯罪活动或为其犯罪组织筹集资金。

18. 在大多数情况下，洗钱都是通过非法利用或滥用现有的金融系统来实施的，因此这对金融系统和金融机构的健全提出了严重的挑战。受洗钱腐蚀的金融机构更可能成为进一步金融犯罪的目标，从而陷入恶性循环。在发展中国家，洗钱妨碍了经济发展或降低了经济发展的速度。洗过的金钱中有许多逃脱了国家金融管理部门的监督和管理，妨碍制订准确的货币政策和建立适当的税收体制。

19. 联合国 1988 年《禁止非法贩运麻醉药品和精神药物公约》<sup>4</sup>是联合国不断努力打击洗钱的第一个里程碑。打击洗钱的斗争起初以与毒品有关的犯罪收益的清洗为目标，但有一点变得越来越清楚，即与其他严重犯罪有关的洗钱也对社会造

成了同样的威胁，应当予以同样的处理。因此，近来的国际文书呼吁各缔约国对所有或大多数严重犯罪的洗钱进行处罚。

20. 2001年9月11日发生在美国的恐怖主义袭击引起了全球对恐怖主义的关注，国际社会很快就加大力度预防和阻止恐怖主义筹资达成了一致。鉴于对潜在洗钱活动和对潜在恐怖主义筹资活动的侦查和分析具有共性，在打击洗钱方面发挥领头作用的重要组织如果也参与处理恐怖主义筹资的问题，将会取得更大的效果。安全理事会迅速对这一需要做出反应，在其2001年9月28日的第1373（2001）号决议中成立了反恐怖主义委员会，该委员会与毒品和犯罪问题办事处的预防恐怖主义处一道构成联合国打击恐怖主义的集体行动中的一个组成部分。不过，应当指出的是，2001年9月11日之前就有的紧迫感促使在1999年成功缔结了《制止向恐怖主义提供资助的国际公约》（大会第54/109号决议，附件），该公约于2002年生效。洗钱问题金融行动特别工作组也扩大了其任务范围，其中包括恐怖主义筹资。

21. 洗钱的种类或技术不断发展。人们普遍认为罪犯往往比他们的对手，即调查机构抢先一步（或几步）发现某个国家打击洗钱的立法中存在的漏洞，因此熟悉最新的洗钱类型是调查机构和其他相关机构有效打击/制裁洗钱的前提。

22. 使用现金的经济使罪犯能够转移金钱或改变资产形式而不留下任何金融交易记录，调查人员在追踪资金流动和提取有关证据方面存在着重大困难。即使在拥有最先进的金融系统的国家，仍有一定程度的使用现金的经济来满足特定的需要。在正式金融部门尚未充分发展起来的许多发展中国家，使用现金的经济是最常见、最可靠的金融系统，对其进行管理绝不是一件轻而易举的事。通常利用首饰或宝石作为一种持有资产的方式的做法在这些首饰或宝石被用作现金替代品时也产生了同样的问题。

23. 使用正式金融机构以外的渠道转移资金或其他资产的替代汇款系统同样也会妨碍对洗钱的打击。许多替代汇款系统的信用来源于文化、种族或宗教社区，它们不按照国际金融机构管理标准的规定办理，通常既不需要客户的证件，也不保留金融交易记录。在有些国家，只有领取许可证的或注册为银行的机构才能提供金钱或价值转移服务，替代汇款系统在这些国家自然是非法的，是秘密从事的银行业务。在其他许多国家，这些系统则是合法的，在提供现代银行业服务以前早就存在了。

24. 非金融企业和专业的参与以及可能非法利用这些企业和专业来进行洗钱近来引起了国际社会的关注，因为这种案件越来越多。参与洗钱的人员中有律师、公证人、其他独立的法律专业人员、会计师（统称为“看门人”，因为他们的专业作用是保护金融交易的合法性）、贵金属或宝石的经销商、以及信托和公司服务提供者。鉴于这些企业和专业在金融交易方面起到的重要作用，人们越来越认为对洗钱实施管制的条例在某些情况下应当将这些企业和专业纳入其中，但不应当影响到与专业秘密有关的特权。

25. 境外金融中心长期以来一直是人们关注的解决洗钱问题的焦点，因为它们可能被用作洗钱者的安全港。不过，由于国际上的一致努力，许多境外金融中心通过撤销皮包银行的执照，或者严格针对公司的客户身份证明要求，已经改善了其做法。国家、区域和国际各级的宣传运动大大提高了公众对使用结构和经营并不透明的境外金融中心所带来的风险的认识。但还需要持续审查和监督这些中心的问题，特别是当通过因特网和其他先进技术同世界各地的境外金融中心做生意变得越来越容易的时候。

26. 已经制定了打击洗钱的若干国际标准。如前所述，联合国一直是这个领域的带头人，编写了许多重要的法律文书。1988年，大会通过了打击洗钱的《政治宣言》（S-20/2号决议，附件）和《行动计划》（S-20/4 D号决议）。《打击有组织犯罪公约》和《联合国反腐败公约》呼吁各缔约国加强打击洗钱活动的制度以及加强这种制度的实施。联合国还通过毒品和犯罪问题办事处的打击洗钱全球方案为这个领域提供了大量的技术援助。

27. 该领域国际标准的另一个主要来源是金融行动工作组。最初于1990年公布并于2003年修订的该工作组的四十条建议提供了详细的技术标准。该工作组还发表年度类型报告。尽管该工作组的成员数量有限，但是世界各地的有关区域机构都在协助其他国家遵守这些建议。

28. 国际标准的其他来源有巴塞尔银行监督委员会、国际证券委员会组织、国际保险主管人员协会和沃尔夫斯贝格集团，该集团由12个与透明国际合作的大型国际私人银行组成。

29. 近年来，国际货币基金组织和世界银行加强了它们对打击洗钱和恐怖主义筹资活动的参与，并与金融行动工作组共同制定了一个全面的遵守情况评估方法。

30. 金融机构还从特定时刻进行的经常业务交易获得了许多有用的信息。在这方面，私人金融机构和有关国家部门之间经常而有效的合作对于有效处理可能会引发调查和起诉洗钱案件的信息至关重要。

31. 如果金融机构怀疑或有适当的理由怀疑某些资金是犯罪活动收益，应立即将这些怀疑报告给为收集和处理这些信息特别设立的机构，如金融情报单位。金融情报单位是接收（并在许可的情况下要求提供）、分析和传播可疑交易报告及关于可能进行洗钱的其他信息的国家中心。设立金融情报单位是创建有效的打击洗钱的制度中的一个重要步骤。这些单位一般设在中央银行、财政部或警察局，但重要的不是它们设在哪里，而是它们是否在充分发挥作用。可疑交易报告是确保客户保持应有的警惕、查明可能的洗钱活动的一种重要手段。有关国家机构应就什么是可疑交易提供实际指南，供金融机构使用。

#### A. 洗钱的刑事定罪：法律框架

32. 有效的法律框架对于打击洗钱非常重要。洗钱罪的实质要件已被列入有关的国际法律文书，特别是 1988 年的公约、《打击有组织犯罪公约》和《联合国反腐败公约》。这些公约的缔约国有义务在其国内立法中列入将这些文书定义的行为定为犯罪的适当条款。此外，还呼吁缔约国考虑公约中规定可从客观实际情况推断构成犯罪要件的知识、意图或目的的条款。

33. 不过，各国在对洗钱活动的定义和处罚方面有许多不同之处。例如，在洗钱的前提罪行定义方面，有些国家在法律文本后附列了这些罪行，有些国家则采取所谓的临界值方法，将前提罪行定义为可以某种方式处罚的罪行。无论如何，《打击有组织犯罪公约》和《联合国反腐败公约》呼吁缔约国将广泛的一系列重罪列为前提罪行。

#### B. 洗钱罪行的调查

34. 如上所述，洗钱技术不断发展，调查技术则往往滞后。因此调查人员应掌握有关洗钱调查的基础知识和必要技能，包括有关法医调查和会计的知识与技能，并不断了解最新的洗钱类型，这是非常重要的。更重要的是，应向调查人员提供适当的技术设施和支持，供他们在日常工作中使用，并向他们提供加强其专业调查能力的培训机会。在这方面，鼓励拥有洗钱调查先进知识和技能的国家向机构能力较弱的国家提供技术援助，以避免为罪犯提供洗钱场所。

### C. 国际合作

35. 随着跨国金融犯罪越来越多，洗钱也越来越具备跨国性质。追踪和证实复杂的跨国货币流动历来是调查机构面临的一项挑战，因此，同任何其他跨国金融犯罪的调查一样，这方面的国际合作是极其重要的。这方面合作的一个例子是金融情报单位埃格蒙特小组，这是一个为推动世界各地的金融情报单位开展国际合作而成立的国际组织。

### D. 对犯罪收益的控制

36. 由于包括洗钱在内的经济犯罪的目的是为了获利，因此追踪、冻结、查封和没收犯罪收益是打击这些犯罪活动的最有效措施。国际社会同意采取的各种最新措施见《打击有组织犯罪公约》和最近通过的《联合国反腐败公约》，特别是其关于资产追回的章节。急需加强国内和国际努力，以进一步制定和充分利用这些措施。

## 四、技术援助

37. 联合国预防犯罪和刑事司法方案的首要目标是协助国际社会满足其在犯罪预防和刑事司法领域的迫切需要，及时为各国提供处理国内和跨国犯罪问题的实际援助。

38. 该方案的一个优先事项是考虑发展中国家和经济转型国家利用专业知识和其他必要的资源，在国家和地方两级建立和发展适当的技术合作倡议的需要。

39. 在第十一届大会框架内举办的讲习班是一个机会，可借以通过专家直接献计献策，以及通过分享信息和经验来提供实际援助。这些讲习班还将有助于审议与解决优先需要有关的概念和项目，加强技术援助和培训方面的双边和多边努力。

40. 要制订有效的技术合作方案，必须有适合请求国的既定需要但不重复其他实体的活动的灵活机制和项目。此外，打击经济犯罪和洗钱的有效方法还要求在若干部门之间提供连续的技术援助，其中包括提高认识和制订政策，建立和实施适当的法律基础设施，制定与管理金融部门有关的措施，以及提供有助于执法进程的援助。

41. 提供的援助可包括研究和信息交流，需要分析，顾问和咨询服务，考察访问，提高认识的研讨会，编写示范法和条例，法律法规起草援助，地方、国家或区域培训课程，以计算机为基础的训练单元，指导、借调和临时雇用，指导说明和最佳做法工具，以及通信和信息技术支持与培训。培训和援助可以通过国家或区域项目提供，也可能需要地方、双边和多边合作。

42. 制定适合每个国家的及时而实际的方案所面临的一个基本挑战是必须有能力准确确定有关的技术援助和培训需要。这种信息通常是各种来源和框架编写的，如双边和多边需要评估研究和评估活动、全球标准遵守情况评估、自我评估以及国家在区域和国际论坛上的发言等。

43. 充分规划的需要评估可以为有效安排提供援助的顺序及其协调打下一个坚实的基础。虽然有些国家表示对一般评估和与技术援助和培训有关的评估“感到疲惫”，但仍有一些国家呼吁进行此类评估，以协助确定和改进它们的需要。由于没有一个标准的框架，因此现在是一个机会，可加强国际合作，制定和实施提高一致性、减少重复的需要评估。

44. 在编制需要情况的材料时，应当确定援助的优先次序。只有在确定优先次序和适当的提供方式时首先考虑国家和地方的需要，而不是双边或多边捐助机构的政策或业务需要，技术合作才能是有效的。

45. 在审议考虑到了每个国家的需要而没有重复其他现有机制的活动的技术合作要求时，必然需要进行有效的协调。如何组织和实施这种协调一直是国际辩论的焦点，特别是在国际社会努力打击洗钱和恐怖主义筹资的背景下。在一再强调协调之必要性的同时，也强调协调机制绝不能控制或限制捐助者和提供者的任务和活动，不能充当援助请求国和提供者之间的“缓冲区”。因此，有一点是很明显的，即要实现技术合作的成功协调，协调过程必须是自愿的、灵活的，必须增加价值而不是成本，并且必须尊重捐助和提供组织的任务。

46. 除协调外，培养可持续的能力也是技术合作活动所面临的最重要的问题之一，若考虑到会员国在地理位置、国家大小、经济和社会发展、机构能力以及法律与行政制度方面的千差万别，则更是如此。接受国一贯要求捐助者和提供者从提供短期的、影响短暂的援助转向提供长期的国内培训、借调、考察访问、教员培训和临时导师。提供的援助应当能够支持若干年，如果提供了短期的国内或区域培训，则需要采取后续行动，以巩固知识和技能并将其制度化。不过，在经济

犯罪和洗钱领域，具备适当资格和经验的专家很少。因此，国际社会要求进行认真的规划和协调。双边和多边捐助者显然有机会通过增加长期培训课程、导师、借调人员和临时技术人员的供应来协助发展可持续发展的能力。

47. 在讨论打击包括洗钱在内的经济犯罪的措施时，承认私营部门的贡献是很重要的。虽然私营部门的组织经常在无意间成为实施此类犯罪的工具，但是这些组织也可成为遵守和预防的积极伙伴。鉴于私营部门的这些作用，它可在国家、区域和国际各级为技术合作做出重大贡献。这就提出了一项挑战，即找机会让私营部门参与公共和私营部门组织共同参与的合作性技术援助和培训活动。

## 五、结论和建议

48. 讲习班 5 将为国际社会根据第十一届大会区域筹备会议的建议，审议更有效地解决上述问题的实际方法提供一个机会。第十一届大会讨论指南（A/CONF.203/PM.1）中提出的问题也有助于确定讨论重点，如(a)打击经济犯罪和起诉洗钱案方面的成功案例和遇到的阻碍，包括根据打击洗钱的立法没收犯罪收益；(b)金融情报单位如何进行相互间的以及与其他机构之间的合作，确保在国内和国际合作中采取最有效的做法；以及(c)如何在非正式和使用现金的经济中最有效地执行打击洗钱的标准。此外，讲习班 5 还将努力促进《打击有组织犯罪公约》和《联合国反腐败公约》的批准和执行，特别是在与洗钱有关的条款方面。

49. 为了达到这些目标，还设计了一个假想案例（见附件），以便于与会者展开互动式的讨论。

### 注

- <sup>1</sup> Adam B. Schiff, 司法委员会犯罪、恐怖主义和国家安全小组委员会 2004 年 3 月 23 日会议录, 美国众议院, 第一〇八届国会会议, 第二期会议, 第 74 号, 第 15 页。
- <sup>2</sup> Synovate, 《盗用身份调查报告》, 为联邦贸易委员会编写 (2003 年 9 月) (<http://www.ftc.gov/os/2003/09/synovatereport.pdf>), 第 4 和第 6 页。
- <sup>3</sup> 加拿大银行家协会, “盗用身份: 需要采用新方法的老问题” (未出版), 2003 年 5 月, 第 5 页。
- <sup>4</sup> 联合国, 《条约汇编》, 第 1582 卷, 第 27627 号。

## 附件

### 供讲习班 5 使用的假想案例：打击包括洗钱在内的经济犯罪的措施

#### A. 导言

1. 设计下列假想案例是为了便于参加讲习班 5 的执业人员展开讨论，引发注重实际的讨论，以便将重点放在打击经济犯罪和洗钱的真正有效措施上。该假想案例提出了与经济犯罪和洗钱的预防、信息收集、调查和起诉有关的各种问题，例如：

- (a) 经济犯罪和洗钱的预防措施；
- (b) 通报情况者（告密者）；
- (c) 罪犯和调查人员对信息技术的使用；
- (d) 法人的责任；
- (e) 盗用身份；
- (f) 皮包公司；
- (g) 客户应有的警惕；
- (h) 同谋或参与；
- (i) 经济犯罪和洗钱的调查技术；
- (j) 罪犯和调查人员对信息技术的使用；
- (k) 机构间合作；
- (l) 国际合作，包括相互司法协助和引渡；
- (m) 洗钱的刑事定罪；

- (n) 金融情报单位的作用，包括这些单位之间的合作；
- (o) 可疑交易的报告；
- (p) 洗钱的作案类型；
- (q) 与非正式和使用现金的经济有关的问题，包括替代汇款系统；
- (r) 保险和可议付票据的使用；
- (s) 专业人员在打击洗钱活动中的作用；
- (t) 控制犯罪收益，包括冻结、没收、民事罚款或资产共享；
- (u) 受害人赔偿。

想参加讲习班 5 的人不妨提前研究一下下面的假想案例。

2. 该案例分为两个部分，第一部分介绍了背信违约和国际诈骗情况，其中包括经济犯罪中常见的、可视为洗钱之前提罪行的各种问题。第二部分描述了与隐藏和伪装有关的非法活动，以及第一部分所述的犯罪收益的进一步利用。

## B. 假想案例

3. 在下列叙述中，建议讨论的问题以**楷体**表示：

### 1. 银行经理的背信违约

- 1. 艾伦先生是 Xanadu 国的一位国民，是设在该国的 Finebills 银行经理。
- 2. 班纳先生也是 Xanadu 国的一位国民，经营着一家名为 Kondo 公司的不动产中介公司，该公司也设在 Xanadu 国。
- 3. Kondo 公司的财务状况恶化，班纳先生请艾伦先生向该公司发放 100 万美元贷款。
- 4. 由于艾伦先生是班纳先生的老朋友，他同意提供无担保贷款，尽管他知道这笔贷款可能无法收回（艾伦先生的决定违背了 Finebills 银行的内部条例）（**使公**

共和私营部门更加健全、公司管理及其他预防措施)。

5. 三个月后, Kondo 公司显然无力偿还债务(通报情况者或告密者, 假设某位银行职员举报了这一呆坏的贷款合同)。

## 2. 客户诈骗

1. 艾伦先生害怕对呆坏贷款承担责任, 让班纳先生想办法偿还贷款。

2. 班纳先生同其上司钟女士——Youngland 国常住国民——商量的此事, 钟女士提出以下建议:

(a) 由钟女士在 Youngland 国成立一家皮包公司, 即 Lownet 公司, 进行客户诈骗;

(b) 钟女士将通过因特网发布广告(使用信息技术), 声称 Lownet 公司可教会客户如何购买取消赎回权的被扣押不动产, 并承诺为此提供资金;

(c) Lownet 公司进一步承诺在客户每次与公司合作进行不动产交易时向他们每人支付 2 500 美元, 并且声称公司将在不动产售出以后进行利润分成。Lownet 公司将诱骗每个客户花 60 美元购买一盘介绍性的录像带, 并保证在满 30 天时全额退款。将用 100 万美元制作录像带;

(d) Lownet 公司还将出售其他录像带, 这些录像带比卖出的第一批录像带要贵得多;

(e) 做广告的目的是为了诱骗客户购买录像带, 钟女士并不打算真正帮助客户获得不动产;

(f) 要求客户将购买录像带的钱打入 Lownet 公司的银行账户;

(g) 在可能有客户询问此事时, 钟女士称自己是 Lownet 公司的主管皮塔尔女士, 说她的公司与 Finebills 银行有许多业务往来, 并提到艾伦先生的姓名;

(h) 当客户与之联系, 询问有关 Lownet 公司的事宜时, 艾伦先生向他们保证,

Lownet 公司是一家经营状况良好的公司（法人的责任）；<sup>a</sup>

(i) 如果计划成功，钟女士将向艾伦先生和班纳先生支付 200 万美元。

3. 艾伦先生和班纳先生同意钟女士的建议。

4. 钟女士向她在银行工作的一位朋友询问银行记录的处理情况，这位银行职员说银行的所有垃圾都放在银行外面的一个大垃圾箱里（系统的健全）。<sup>b</sup> 钟女士从银行垃圾里废弃的银行记录中收集到个人信息，以便在另一个国家开设银行账户（盗用身份）。<sup>c</sup>

5. 钟女士在 Youngland 国成立了一家国际社会称之为“境外中心”的皮包公司——Lownet 公司（皮包公司，专业人员的作用）<sup>d</sup>，并在该国的 Goldfingers 银行开立了一个账户（同谋或参与，客户应有的警惕）。<sup>e, f</sup>

6. 在因特网广告的诱惑下，有的则是因为艾伦先生的保证，世界各地的许多客户购买了录像带，使这一诈骗阴谋的收益达到 500 万美元，并汇入 Lownet 公司在 Goldfingers 银行开立的账户（调查技术、豁免、机构间合作）。<sup>g</sup>

### 3. 洗钱和对犯罪收益的控制

1. 钟女士将存在 Goldfingers 银行的 500 万美元收益转入 Zeitstaat 国的 15 个银

---

<sup>a</sup> 也就是说，Finebills 银行应不应该为艾伦先生的行为负法律责任。

<sup>b</sup> 这个事实提出了机构数据的机密性和保护该数据免受第三方干涉的问题。

<sup>c</sup> “盗用身份”涉及到收集个人信息数据供将来犯罪之用。这种“盗用身份”的方式称作“垃圾搜寻”。

<sup>d</sup> 也可讨论盗用身份的问题。如果钟女士在一位律师的帮助下成立了一家皮包公司，与会者不妨在开始讨论洗钱的时候讨论一下专业人员在预防此类犯罪中的作用问题。

<sup>e</sup> 通过提出“如果执法人员在任何客户实际成为受害人之前知道了这个计划，应该怎么做？”这个问题，与会者可以讨论《联合国打击跨国有组织犯罪公约》中规定的同谋或参与是否适用。

<sup>f</sup> 在开始讨论洗钱的时候，与会者不妨讨论一下 Goldfingers 银行本应采取哪些措施来防止皮包公司开立账户。

<sup>g</sup> 可使用调查技术，由执法人员假扮成潜在客户与钟女士联系，以获取信息。此外，这里可以通过提问“公诉人应该怎样获取足够的证据来起诉钟女士？”来讨论给予豁免权的问题。也可以讨论相互法律援助问题。另外，也可以通过设定向客户保护机构提出的要求使执法机构参与进来这一情景，来讨论机构间合作方面的问题。

行账户（可疑交易的报告）。<sup>h</sup>

2. 钟女士将从银行垃圾中收集的个人信息提供给迪伊女士，请她利用这些信息来制造假身份证件（盗用身份）。<sup>i</sup>迪伊女士用这些假证件在 Zeitstaat 国开了 15 个银行账户。迪伊女士是 Zeitstaat 国的国民，职业是会计（专业人员作为看门人的作用）。<sup>j</sup>

3. 在一段时间内，迪伊女士在 Zeitstaat 国的许多自动取款机上提取了这 15 个人账户中的资金（500 万美元），并且是以小面值取出的（可疑交易的报告，包括为分析使用信息技术）。

4. 应钟女士的要求，迪伊女士将 200 万美元现金带到 Xanadu 国，交给班纳先生。迪伊女士没有向 Xanadu 国或 Zeitstaat 国当局申明她携带着 200 万美元（现金携带者，并且可能是受管制的现金交付），并交给了班纳先生。班纳先生用许多自动取款机将小面值的 120 万美元存入了 Kondo 公司在 Finebills 银行开立的账户（可疑交易的报告，金融情报单位的信息共享，金融机构的作用），用于偿还 100 万美元贷款及其利息。<sup>k</sup>班纳先生为自己留下 40 万美元，送给艾伦先生 40 万美元。他们都为个人私用留下了这笔钱。

5. 应钟女士的请求，迪伊女士为她在 Zeitstaat 国买了一幢价值 200 万美元的别墅。迪伊女士通过 Zeitstaat 国的地下银行家埃祖拉（他在 Youngland 国有一位搭档贾巴尔女士）将剩下的钱（100 万美元）寄给了 Youngland 国的钟女士（替代汇款系统）。<sup>l</sup>钟女士向迪伊女士支付了 1 万美元的服务费，将 9 万美元用于个人享乐（赌博、博彩和吃饭等），从 Midmint 证券公司购买了 50 万美元的无记名

<sup>h</sup> 这里应当指出的是，不同国家确定可疑交易报告的标准各不相同，有些国家规定某一数额的金钱为报告的临界值，另外一些国家则采取比较一般的方法，要求银行报告它们认为“可疑”的交易，而无论金额多少。如果资金是以 SWIFT 等电子方法划转的，也可讨论与洗钱者使用的信息技术有关的问题。

<sup>i</sup> 这些事实说明了另一种形式的“盗用身份”，即实际使用个人信息数据来制造假证件，并将这些证件用于实施其他犯罪（本案中的犯罪为洗钱）。

<sup>j</sup> 这里也可以讨论洗钱的刑事定罪，包括从钟女士方面来说自有收益的清洗。

<sup>k</sup> 这里应该指出的是，在有些国家，艾伦先生将不会因为背信违约而承担刑事责任，因为贷款已经偿还。

<sup>l</sup> 这里也可以讨论其他形式的替代汇款系统，如 *hundi* 或 *hawala*。此外，也可讨论洗钱的其他作案手法（类型）。

证券，并在住所存放了 40 万美元现金。无记名证券存放在 Youngland 国 Handyfunds 银行的保险箱里。

6. 除了所有这些人员的刑事责任外，将要讨论的问题还有如何从这两个国家(即 Xanadu 国和 Zeitstaat 国)及 Youngland 国追回诈骗收益(控制犯罪收益的国内措施和国际合作，包括冻结、没收、民事罚款或资产共享)，以赔偿受害者。

---