西游记
SheppardMullin
美国盛智律师事务所

二零一五年九月十日

并不存在所谓的免费试用装

作者：Ted Max 和 Nicole Bagood

发表时间： 2015年5月18日

社交媒体使用户通过敲打几下键盘就毫不费力地与世界各地进行沟通，广告商利用社交媒体博主的力量，使其成为广告战的主力军，这种“消费者对消费者”的营销或是“消费者自主媒体”营销被人们所熟知。虽然消费者对消费者营销很普遍，特别是在时尚界，但利用博主向消费者推销时尚产品仍需遵守《联邦贸易委员会法案》。

近年来，社交媒体在大大小小时尚公司的营销策略中扮演着越来越重要的角色。特别是公司设法找到拥有大量社交媒体粉丝的个人，帮助推销他们的产品和服务。当博主提供时尚化妆品和美容产品的教程时尤其如此。在消费者对消费者的营销模式中，公司通常向知名博主提供时尚产品和/或服务的试用装以在其社交账户中进行宣传，得意地展示给成千上万的粉丝。

时尚博主与J. Crew, Jo Malone 和 Tiffany & Company这样的公司合作，收取产品作为礼品，公司期待这些个人把这些产品在其博客和/或其他社交媒体账户（例如，Facebook、Instagram等）上进行宣传。这种做法很受时尚公司的欢迎，因为这使他们能够以一种不易察觉但极具诱惑性的方式影响到大量的消费者。不过，这种做法的危险在于，可能因缺乏透明度欺骗消费者而承担违反《联邦贸易委员会法案》带来的责任。

《联邦贸易委员会法案》的核心是规制影响商业的不公平或欺骗行为。近年来，联邦贸易委员会（“FTC”）修改了其准则——《关于广告的认可和证明的使用指南》，目的是应对和打击潜在的社交媒体营销欺诈问题，进行消费者对消费者营销的公司必须遵守以下关键准则：（1）执行一项符合法律规定的披露政策；（2）确保员工和博主知晓相关规则；且（3）监督这些人代表公司的行为。根据这些准则，在博客和其他社交媒体账户中给产品/或服务写评论或做特写的博主，必须向其粉丝披露他们与时尚公司广告商或试用装提供者之间存在的任何关系。根据FTC广告行为司的副司长Richard Cleland所说，该披露要求的主要目的是促进社交媒体营销的真实性和透明度。FTC认为，知晓博主和公司之间的关系，哪怕这种关系小到一个免费试用装，都会影响到粉丝对博主认可或评论的产品的重视程度和信赖程度。

尽管这些准则已经存在一段时间，而且自1980年以来并没有更新过，但是一些时尚博主仍没有披露他们和不同品牌之间的关系。FTC的出版物“.com 披露：如何在电子营销中进行有效的披露”在确保符合披露要求方面是一个有用的工具。有史以来FTC还没有援引过《联邦贸易委员会法案》对时尚博主进行罚款，但是，如果仍然未能进行适当的披露，FTC可能会改变处理这个问题的方式。尽管每个博客的内容和为产品和/或服务进行的宣传不尽相同，但是最佳的做法是，所有的博主都应当披露任何这样的关系，并且参与消费者对消费者营销的公司应当建议他们的博客披露这种关系。◆

披露最终受益人的欧盟新规则

作者：Curtis Dombek和Neil Ray
发表时间：2015 年6月24日

6月5日，《欧盟公报》发表了新的欧盟反洗钱（“AML”）规则，即《第四版欧盟反洗钱指令》（“4AMLD”）和一部新的关于汇款相关信息的法规。总的来说，这项立法代表了修订后的打击洗钱和打击恐怖主义资金链的欧盟法律体系。欧盟成员国要在2017年6月26日之前，把《第四版欧盟反洗钱指令》的要求转化为国内法。

这部新“指令”的主要新颖之处，是引进了集中的UBO登记 —— 一种识别公司和信托的最终受益人（“UBOs”）的公开登记。这对欧盟实体的最终受益人（例如家族企业的所有人）的隐私可能影响深远。

《欧盟反洗钱指令》把“最终受益人”定义为最终拥有或控制客户（例如，一家公司实体或其他法律实体）的任何自然人，和/或进行一项交易或活动中被代表的自然人。在公司实体方面，“最终受益人”的定义进一步特指，最终持有一个公司实体超过25%的股份或投票权的股权、控制利益或所有者利益的自然人。如果无法识别最终受益人，原则上会把拥有高管职位的自然人登记为最终受益人。至少以下关于最终受益人的信息会包含在UBO登记中：

- 姓名；
- 出生年月；
- 国籍；
- 居住国；及
- 所持有受益利益的性质和范围。

UBO登记将开放给：

- 适格的官方机构和欧盟金融情报单位，无任何限制；
- 义务实体（例如履行“客户尽职调查”义务的银行、公证机构和律师）；及
- 能够证明存在“合法利益”（例如，涉及洗钱、恐怖主义资金链和相关上游犯罪行为 —— 例如，腐败、税务犯罪和诈骗）的公众。

在根据个案具体情况而定的例外情况下，例如，存在诈骗、绑架、敲诈等高风险时，欧盟成员国有权禁止义务实体或者公众获得UBO登记的部分或全部信息，而信托则适用不同的安排。在信托中，欧盟成员国必须为信托的最终受益人提供受欧盟成员国法律管辖的集中登记，原则上，信托UBO登记只对适格的官方机构、欧盟金融情报单位和执行客户尽职调查的义务实体开放，但不对公众开放。如果信托会产生税务后果，那么欧盟成员国必须在登记中包含有关信托和受该欧盟成员国法律管辖的同等法律安排的UBO信息。但是，“税务后果”的含义还未得到澄清。

该信托登记包含的信息应当包括以下主体的身份：

- 信托人；
- 受托人；

转至第3页

接第2页

- 信托监察人（如有）；
- 受益人或受益人群体；及
- 任何其他对信托实施有效控制的自然人。

在适当的时候，全国性的UBO登记和信托登记将有望在欧盟层面通过一个集中的欧盟平台实现互通。欧盟委员会则要在《欧盟反洗钱指令》生效后的四年之内，公开报告和在适当的时候公开在此领域的相关立法提议。

《第四版欧盟反洗钱指令》的其他要素包括，例如，重构与义务实体检查客户身份和汇报可疑交易的义务有关的、以风险为基础的客户尽职调查方法；对于严重、重复或系统地违反《第四版欧盟反洗钱指令》要求的行为，实施新的和更多的行政处罚；以及，对转账可追溯性的新要求，包括收款人信息（而不仅仅是付款人信息）。

经过利益相关人持久而集中的讨论之后，这些规则才得以生效。欧盟的意图旨在对洗钱行为制定更加严格的规则，以打击避税和恐怖主义资金链。欧盟议会的议员在立法程序的后期阶段才提出了建立集中登记，利益相关人应当关注《第四版欧盟反洗钱指令》的要求转化为国内法的进程，并且利用一切机会提出至今还没有得到解决的问题。◆

海外政府合约：提防合规风险

作者： Fatema Merchant
发表时间： 2015年6月24日

2015年6月16日，一家私人国防和政府合约公司 —— IAP全球服务公司，同意支付七百一十万美元，来和解因其向科威特政府官员行贿以获取一项科威特政府合约而违反“美国反海外腐败法”（“FCPA”）受到的刑事指控。就在同一天，IAP的前任“特殊工程和项目”副总裁 — James Michael Rama， 也向FCPA的指控认罪。对于美国的政府承包商来说，向外国政府提供服务和专业知识可以带来丰厚的利润，但是本次执法行动也凸显了与获取此种合约相关的风险。

背景

2004年，科威特的内政部（“MOI”）发起了一个叫做“科威特安全项目”的工程项目，目的是开发一个使用闭路电视的全国性监控项目。该项目分为两个阶段。阶段I是规划和可行性研究阶段，紧随其后的阶段II则是利润更加丰厚的安装阶段。MOI负责挑选帮助执行该项目的承包商。

IAP是一家总部位于佛罗里达的公司，它为美国军队和全球其他政府机构提供基础设施管理、技术服务和应急协助。IAP与美国政府之间存在几份合约，包括美国海军、美国海军陆战队和空军。

IAP与美国司法部达成了一份不起诉协议（“NAP”），同意因受到FCPA指控而支付刑事罚金、加强自身合规政策和程序，以及履行报告义务。根据认罪协议，Rama将于9月11日面临判刑。

交易内容

根据该份不起诉协议，2004年，Rama在为另一家国防承包商工作期间，被引荐给一位科威特顾问。Rama从这位科威特顾问处知晓了MOI将要实施的安全项目。2005年，Rama加入IAP并获得了“科威特安全项目”阶段I的合约。为了使自己在赢得利润更加丰厚的阶段II合约中处于最有

转至第4页

接第3页

利的地位，IAP决定如果其能够在阶段I中成为MOI的顾问，那么公司可以迎合IAP的自身能力，根据阶段II的要求提供定制的解决方案，如此一来IAP便可获得赢取阶段II合约的独一无二的优势。根据MOI和那位科威特顾问的指示，IAP成立了一家叫做“Ramaco”的壳公司来参与阶段I的竞标，以掩饰IAP对阶段I的参与和任何潜在的参与阶段II的利益冲突。Ramaco是IAP在“科威特安全项目”阶段I中的代理人。

IAP把从项目阶段I赚取的四百万美元中的一半，分给了那位科威特顾问，这部分钱款又作为回扣到了科威特政府官员的手中。根据不起诉协议，为了掩饰这部分钱款，IAP和Rama联合其他人设计出这样一套方案：在阶段I合约中代表IAP执行工作的一家科威特公司，会抬高提供合法服务的发票金额；在MOI支付Ramaco阶段I的合约价格之后，Ramaco会把钱款转移给IAP，IAP再把钱款支付给这家科威特公司；然后这家科威特公司再把那部分钱款中的一部分放给那位科威特顾问，用于向科威特官员行贿。

与合规有关的结论

IAP行动——2015年司法部的第一个公司FCPA执法行动——是针对发生在七至十年前的行为，主要围绕一个已经不在公司工作超过七年的个人。这项执法行动强调了这样一个事实：前员工数年前的行为仍然可能让一家公司支付上百万美元的罚金。重要的一点是，公司要培训和教育其管理层，知晓不合规对于他们的雇主的成本以及对于他们个人的成本。

尽管国内政府合约行业已经存在很多规制和监管，但是国外政府合约领域却更多地充满了腐败风险。作为美国的政府承包商来探索这个相对较新的从外国政府获取合约的领域，公司应当注意审核和加强其合规政策和程序，以预防FCPA风险。

不起诉协议要求IAP审核和修正其既有的合规政策和程序，至少要确保符合以下要素：

- 高层承诺：IAP将确保在其高级董事和管理层中营造出强烈的高层反腐败合规的氛围。
- 政策和程序：IAP将制定一项清晰的反腐败政策，包括FCPA和适用的外国法律，以及一部执行该项政策的书面合规准则。
- 以风险为基础的审核：IAP将定期进行审核以评估腐败风险，并根据那些风险调整其政策和程序。
- 监管和独立性：IAP将把合规指派给一位高级主管负责，该高级主管可自主决定向包括董事会在内的独立监督机构汇报工作。
- 培训：IAP将执行相关机制，以有效地对其董事、高管、员工和商务合作伙伴进行有关IAP合规政策和程序的培训。
- 汇报和调查：IAP将确保其拥有一个系统，可以秘密举报违反反腐败法律和IAP的政策和程序的行为，同时也要拥有一个调查潜在违法行为的可靠程序。
- 惩戒：IAP将执行恰当的程序，以解决和惩戒违反适用的反腐败法律和IAP的合规政策的行为，补偿不当行为造成的损害，并防止类似不当行为的发生。
- 与第三方关系：IAP将采取以风险为基础的、有关雇佣和监督代理商和商务合作伙伴的尽职调查程序。
- 并购：IAP将制定相关政策和程序，以在并购商务实体时进行以风险为基础的尽职调查。
- 监督：IAP将对其为评估预防和监测违反反腐败法律和公司合规准则的行为的有效性而设计的合规政策和程序进行定期的审核。

此次IAP行动应当使政府承包商们看到腐败的风险，以及违反FCPA行为的潜在严重后果。值得注意的是，不起诉协议中的很多要素，都阐明了司法部对以风险为基础的政策、程序和尽职调查的期望。那些要素为公司建立和强化其反腐败合规政策和程序提供了指引。常言道：预防总是胜于治疗。◆

美国商务部工业安全局（BIS）提议对入侵和监控软件进行出口许可

作者：Curtis Dombek 和Alexander Major
发表时间：2015年7月17日

美国商务部工业安全局（BIS）近期发布的一项关于对入侵和监控相关软件出口管制的规则的征求意见。该规则对美国出口管理条例（ERA）进行了修改，该规则旨在配合于2013年12月签订的关于常规武器和两用物品及技术出口管制的瓦森纳协议，上述协议是由41个参加国承诺在跨境武器和两用物品及技术交易中提升透明度和责任的多边出口管制制度。该规则涉及范围广泛，并建议在ERA商业管制清单（CCL）第4类中加入新条目，即增加对黑客和其他网络罪犯使用的“入侵软件”的管制。然而困难之处在于，现有规则的措辞（及解释）规定网络渗透测试产品也要受制于相同的出口许可要求，该产品可以通过使用“入侵软件”鉴定电脑缺陷。也就是说现有规则中对受管制的入侵软件的定义既包括好的软件也包括坏的软件，而这将对防御软件的有利研究和开发产生激冷效应。

BIS于2015年5月20日发布了通知，提议一项有关特定入侵和监控项目的出口、再出口、国内转让的许可要求的新规则。 提议特别提到“使用入侵软件鉴定电脑和网络设备缺陷的网络渗透测试产品”以及“对电脑和网络设备缺陷的专有研究和开发”。但是BIS在其保护美国免受恶意软件损害的努力中，也将受困于为上述相同目的的有利软件的开发，而BIS对此似乎很镇定。

规则将“入侵软件”定义为“应用于电脑或网络设备的，‘特别设计’或改进的通过‘监控工具’避免监测，或打击‘防护对策’的‘软件’”，且该软件有下列性能：

(a) 从电脑或网络设备中提取数据或信息，或修改系统或用户数据；或

(b) 修改程序或进程的标准执行路径，以允许其执行外部指令。

在BIS网站上的常见问题解答中，对于首要问题“BIS提议的规则是否管制‘入侵软件’，恶意软件，漏洞等等”，答案是规则不会对入侵软件本身设置许可条件。事实是规则将会对“产生、运营、交付‘入侵软件’和与‘入侵软件’进行交流的控制和交付平台”施加出口许可要求。规则同时包括好坏软件的原因是拥有我们赖以控制网络安全的软件的“好人”需要出口此类软件以测试并因此成功发展正确的防御软件，以防止新规则设法打击的网络攻击发生。这看起来十分可信。毕竟你需要知道防御的对象是什么才能设计正确的防御，要求一个国际软件团队设计对抗恶意软件和交付平台的防御软件，而不让他们为测试目的看见或运行相关恶意软件和交付平台，就好像要求他们蒙上眼睛进行设计。美国公司需要雇佣国际员工和分包商以更好的理解和战胜全球未决的网络威胁。该规则的不幸之处在于没有为好的软件提供救济，正因为如此，如果该规则最后被通过，美国的软件和网络安全公司可能会发现他们不能及时与全球分享其防御新的或未决的网络威胁的知识。或者说，新的许可管制要求会将威胁防御成果延迟一个月。对于今天的世界来说，上述延迟是十分关键的。每天都有新的网络威胁形成，并在全球同时发生。坏的软件不会等待出口许可的颁发。

此处忽视的重点是新规则不需要过度延伸和全面涵盖。例如，BIS曾对一项重要的牢固加密术的许可提供例外的先例，这可以在新规则中作为许可例外的模板进行考虑。在15 C.F.R. § 740.17 (a)(1)(ENC例外)案件中，公司与其国际开发团队为开发新产品的目的，分享牢固保密的加密术（所谓的(b)(2)加密术）不需要许可。类似的新规则例外可以解决产业对全球迅速响应新网络威胁的顾虑，可以使公司使用其全球网络以开发正确的防御。

虽然新规则的目的明确（并且是高尚的），但是实际上对大多数行业的打击过于直接，实在和危险。我们和行业都希望最终通过的规则不会损害我们安全运营网络依赖的防御工具。◆

Sheppard Mullin Beijing office (美国盛智律师事务所北京代表处):

中国北京市朝阳区
建外大街1号
中国国际国贸中心写字楼1座15层
邮政编码：100004
Telephone (电话): +86 10 5706 7500
Fax (传真) : +86 10 5706 7555

Sheppard Mullin Shanghai office (美国盛智律师事务所上海代表处):

中国上海市静安区
南京西路1717号
会德丰国际广场26楼
邮政编码：200040
Telephone (电话): +86 21 2321 6000
Fax (传真)：+86 21 2321 6001

Partners (合伙人):

Tony Mou (牟光栋) - tmou@sheppardmullin.com
Scott Palmer (彭明) - spalmer@sheppardmullin.com
Don Williams (魏廉) - dwilliams@sheppardmullin.com
James Zimmerman (吉莫曼) - jzimmerman@sheppardmullin.com

China Outbound Newsletter Coordinator (西游记协调者):

Cheng Xu (徐琤) - cxu@sheppardmullin.com
Sharon Xu (徐谦蓉) - sxu@sheppardmullin.com

西游记

SheppardMullin