制裁和 PEP 的演变

在历史上，制裁一直用于实现变革。制裁可能影响一个国家或个人的活动或政策——尤其是在发生了违反国际法或人权的行为，或者民主受到威胁之时。最近，制裁被用来打击恐怖主义活动以及涉及核扩散的国家。虽然具体形式各不相同，但金融制裁和贸易相关制裁一直都是使用最为广泛的制裁形式。

战争或禁运：制裁发展史

禁运可以追溯到美国开国元勋时代，当时，禁运被当作一种外交武器和战争的第一替代方案。在向英国运用经济杠杆的过程中，美国吸取了足够的教训，最终促使美国获得独立。从 1794 年到 1812 年，新共和国试图在海洋自由权与运用经济手段影响欧洲行为二者之间取得平衡。1812 年战争以来，美国财政部 (DoT) 就一直参与针对外国政府的经济制裁活动。

1917 年 10 月 6 日，《对敌贸易法案》获得通过，这是制裁发展史上的一个重要里程碑。《对敌贸易法案》效仿的是英国议会在 1914 年通过的同名法案，其目的是在二战期间禁止任何美国人与敌方及敌方的盟国进行贸易。法案将“敌方”定义为与美国交战的外国人和国家。《对敌贸易法案》的意义在于，通过它可以窥见国际制裁的未来走向，不合规导致的严重惩罚以及对资产没收行为的治理等。

组建外资控制办公室 (FFC)（为海外资产控制办公室 (OFAC) 的最前身）的授权就源于《对敌贸易法案》。二战期间，FFC 由财政部长执掌，其特定受限国民公告名单 (Proclaimed List of Certain Blocked Nationals)（也称为“黑名单”）中列出了被禁止在美国开展业务的德国、意大利和日本联系人的个人及公司。该名单是 OFAC 发布的特别指定国民名单 (SDN) 的前身。

OFAC 是在中国加入朝鲜战争之后，于 1950 年依据财政部的一道命令组建的。杜鲁门总统宣布全国进入紧急状态之后，处于美国管辖范围内的所有中国和朝鲜资产都遭到冻结。

在国际联盟和后来的联合国成立之前，人们并未从法律上正式讨论过制裁的合法性。1960 年到 1990 年间，制裁大多都是单边实施——多数均由美国发起。到 20 世纪 90 年代，很大部分是由政府间联盟实施的，这些联盟一般都包括西欧国家和美国。

现在，全球制裁行为的主体包括美国、欧盟和联合国（见图 1）。美国最近率领联盟与伊朗进行了谈判，内容包括在伊朗达到缩减核计划协议的要求时可能放宽对伊朗的制裁。同样地，在经历 50 年冷战之后，美国已开始与古巴开启关系正常化进程。

除伊朗和古巴以外，俄罗斯最近对金融机构产生了一些挑战。欧盟外交部长们最近批准把针对俄罗斯能源、防务和金融公司的“选择性制裁”再延长六个月。这些制裁原定于 2015 年 7 月 31 日到期。延长制裁很可能导致更多的俄罗斯和乌克兰个人及实体出现在 OFAC SDN 名单上。由于该地区大量爆发暴力事件，OFAC 已经 8 次向该名单新增个人姓名和公司名称。

伊朗、古巴和俄罗斯事件代表了不断变化的制裁目标。毫无疑问，这些变化会对现有资源形成限制。为了跟上步伐，金融机构需要部署更强大的反洗钱系统，以实现连续监控和负面新闻筛查，还需要改变思维模式，适应频率更高的监控需求。

将监管合规要求适用范围延伸到制裁以外

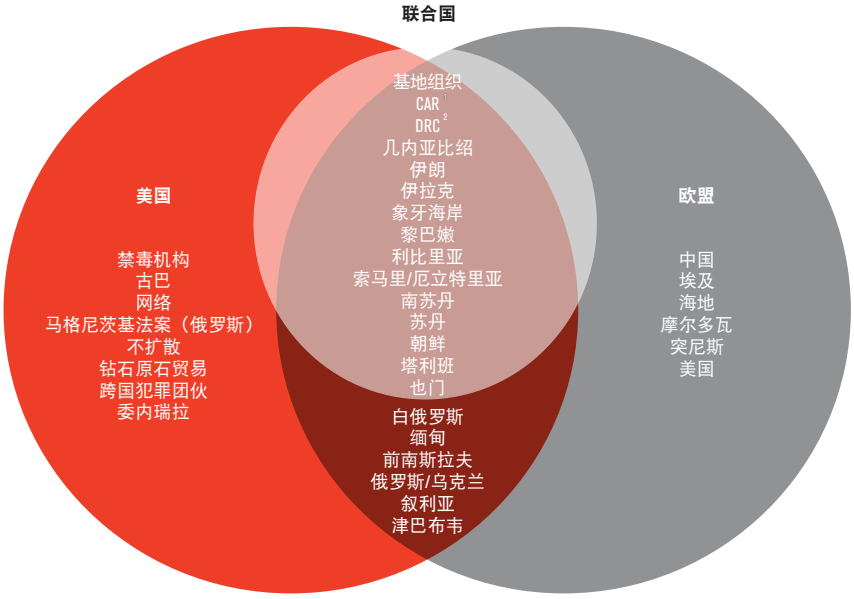
1970 年，美国国会通过《银行保密法》(BSA)，也称反洗钱 (AML) 法，其目的是防范金融系统的洗钱风险。BSA 由金融犯罪执法网络 (FinCEN) 负责实施，要求美国的金融机构登记和报告以现金购买金额超过 10,000 美元的可流通票据的行为，并报告可能指向洗钱、避税或其他犯罪活动的可疑活动。

在 1989 年巴黎 G7 峰会上成立了金融行动特别工作组 (FATF)——一个政府间组织——其目的是研究洗钱趋势，制定政策以打击洗钱活动。FATF 提出的 40 条建议为反洗钱措施树立了国际标准，允许各国在其宪法框架下实施这些原则。

1995 年，克林顿总统颁布总统令，禁止向威胁破坏中东和平进程的任何个人或组织转移资金、提供商品和服务，恐怖融资首次成为公众关注的焦点。特别指定恐怖分子 (SDT) 名单随之出炉，然后在 1996 年，又提出了外国恐怖组织 (FTO) 名单。国际方面，在 9/11 之后，FATF 的要求扩展到了恐怖融资。

20 世纪 90 年代后期还引入了“政治公众人物”(PEP) 名单，当时，在尼日利亚独裁者 Sani Abacha 的精心安排下，其家人和亲信系统性地从尼日利亚央行窃取资产。后来，PEP 出现在 FATF、《美国爱国者法案》第 312 条、《欧盟第四指令》和沃尔夫斯堡集团文件中。由于全球并无统一的 PEP 定

图 1 **全球制裁政权**



[1]中非共和国
[2]刚果民主共和国

资料来源：美国财政部
作者：jonathan masters，Julia ro

义，因此，多数国家均以 2003 年的 FATF 标准为基础进行定义。

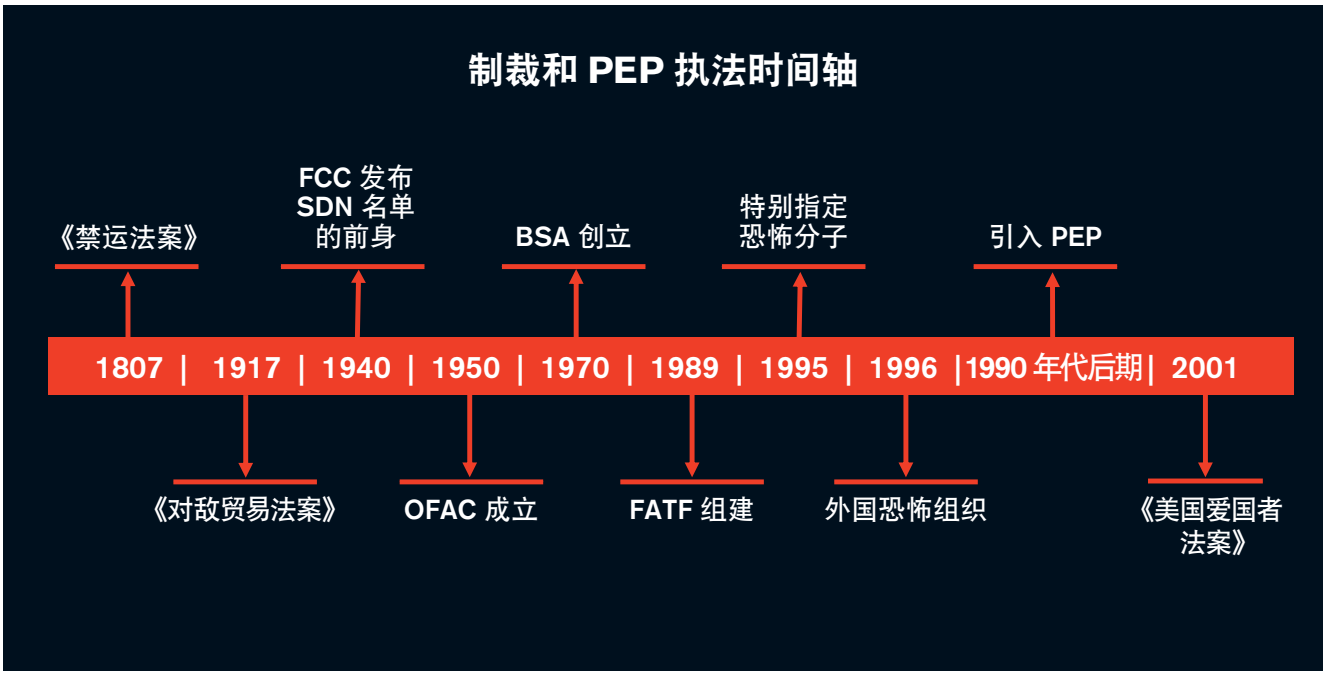
9/11：反洗钱和合规史上的转折点

9/11 恐怖袭击为美国和全球后十年的行动定下了方向。《美国爱国者法案》第三章对 BSA 的要求进行了大幅改动，以处理新出现的恐怖融资问题。法案同时为其他反洗钱相关要求（包括“了解你的客户”(KYC)）提供了一个平台。有序、详细的客户身份认定模式得到接受，全面的客户尽职调查 (CDD) 政策和程序，以及 CDD 向加强型尽职调查 (EDD) 的延伸，目前，这些都被认为是一个强有力的 BSA/AML 合规计划的基石。最有效的计划始于入职流程，包括强大的合规文化，把组织的各个层次全部纳入其中，从董事会成员和高级管理人员到调查人员。由于监管要求不断变化，因此，教育和培训对于机构反洗钱工作的成功起着重要的作用。

在 9/11 后的监管环境中，OFAC 针对恐怖主义和大规模杀伤性武器的制裁规定经过修订和更新。名单中的个人和实体增多了，名单更新更加频繁。同样地，联合国和欧盟的制裁方案也有所扩展。这些变化导致合规部门加强了对个人和实体进行筛查的力度和频率，尤其是针对恐怖融资的筛查。

虽然在 9/11 以前也需要审查，但 PEP 在过去 10 年中受到了更加广泛的关注，因为外国腐败问题的重要性日益凸显出来。臭名昭著的里格斯银行案仍然提醒着我们，在美国洗白外国腐败所得是多么的容易。最近，中东地区的政治动荡再次引发人们对外国腐败问题和被推翻政治领导人转移到海外的巨额财富的关注。FATF 指南暗示，如果一个人是外国 PEP，则此人在其所在国家同时也是一个国内 PEP。虽然最初的做法是仅筛查外国 PEP，但世界上发生的各种事件强调突出了同时筛查国内 PEP 的重要性。目前，FATF 多数成员国都加大了对外国和国内 PEP 的审查力度——开户时要筛查，其后适用加强监管措施，持续实施尽职调查程序。技术是实施全面筛查的主要促成因素。如果不使用技术手段，是不可能有效落实持续监控、跟上制裁变化步伐的。

《美国爱国者法案》将反洗钱计划要求的适用范围延伸到了金融机构以外，包括赌场、经纪商 / 经销商、货币兑换处、某些保险公司和共同基金。同时把存在洗钱或恐怖融资可能的部分客户类别划入高风险客户群体，这就要求更大的尽职调查力度。这些客户包括慈善机构、非政府组织 (NGO)、非居民外国人 (NRA)、外国领使馆和非银行金融机构。扩大反洗钱监管要求的适用范围意味着，美国政府机构（联邦和州政府机构以及欧盟的对等机构）肩负着更多的监管、监督和处罚责任。



日益重要的技术作用

早期的拦截软件乃应识别不轨者而生。此类软件对交易进行搜索，以发现与 OFAC SDN 名单相匹配的名字。随着名单上实体数量的增多，随着欧盟和联合国引入其他政府制裁名单，搜索过程变得越来越复杂。虽然拦截软件并非强制性要求，但在国际制裁监管要求不断提高的情况下，此类软件的确有助于合规工作的开展。

然而时代变了。金融信息、技术和通信领域的快速发展使得资金可以快速、轻松地流往世界上的任何地方，结果形成众多挑战。监管要求和合规要求继续提高，不轨者和流氓国家则想出各种新方法，试图避开能够发现其非法活动的系统和流程。制裁名单经常变化，数据格式混乱，拼写错误，别名，爆炸式增长的第三方参考名单，面对这些情况，如果不使用技术手段，机构根本不可能跟上步伐。

由此诞生了一个全新的行业，提供所谓的 BSA/AML 软件。自动化系统已经成为一种必不可少的工具，不但可以用来实时了解监管要求的变化并达到新的要求，还可用来有效地管理整个组织的风险，尤其是在处理大量客户信息和交易时。KPMG《2014 年全球反洗钱调查》为此提供了佐证。调查显示，交易监控系统支出在银行急剧攀升的反洗钱合规成本中占据最大份额。不断增长的合规成本催生了托管平台和软件服务 (SaaS) 模式。机构对这些选择推崇备至，对其安全控制措施也是满怀信心，相信它们可以有效地保护他们的客户数据。较低的总体拥有成本，快速部署和业务持续性，这些都是可以实现的部分主要优势。

依据各种政府制裁名单、第三方 PEP 参考数据库和负面媒体报道对客户和交易进行筛查，其中涉及的复杂性只不过扩大了名单管理服务的应用范围。这些服务有助于与过滤引擎实现无缝集成，并且还能消除费时费力的多名单管理流程。

在当今的环境中，数据质量和快速、准确处理大量数据的能力对于反洗钱计划的成功至关重要。技术可以提升效率，消除费力的人工操作流程，把资源解放出来集中处理其他问题。由于实时了解监管事件和全球事件至关重要，因此，合规专业人士应该选择采用持续 KYC 的系统，这取决于系统能否处理大量非结构化数据的规模、范围和不确定性，能否对冲风险。支持这种模式的系统模型运用机器学习和人工智能 (AI) 的方法来映射数百万个数据点以发现隐藏的风险，因此，可以为筛查流程注入创新。

数据可视化技术、高级分析技术以及可以把信息转化成有用情报的强大研究工具正在发展成为反洗钱计划“必不可少的工具”。其他重要特色技术包括：

- 模式识别——用于自动（无监督）发现可疑行为的近似类、族群或模式，或者用于匹配给定的输入。
- 神经网络——从样本学习可疑模式，用于以后发现可疑模式。
- 关联分析——评估组织、人和交易之间的关系和联系。

对于合规专业人士来说，更加复杂和强大的反洗钱解决方案的出现应当是个好消息，这类解决方案可以每天筛查机构的整个客户数据库，发现其中的制裁、PEP 和负面媒体报道，不会产生大量警告和误报。毕竟，对合规经理来说，过多的误报似乎是众所周知的棘手问题；难怪在《道琼斯 2015 年全球反洗钱调查》中，误报成为合规工作面临的最大问题之一。然而，合规专业人士在评估反洗钱供应商的解决方案时，不能仅仅考虑消除误报的必要性。同时还要了解银行的架构、对高层管理人员的报告要求以及哪些技术解决方案会通过银行的合规计划。反洗钱系统必须能跟上监管和银行政策的变化，发现并预防信誉风险，最重要的是，要向监管机构证明已经实施了充分的控制措施。

业务与技术的融合增进了与信息技术 (IT) 专业人士的协作，能快速响应监管机构针对模型验证、数据完整性和有效自动规划的审查要求。这一点至关重要，因为执法行动实施的惩罚现已从机构本身延伸到个人，银行的官员和董事都需要对反洗钱计划的缺陷承担责任。

结语

从过去的历史来看，各国政府（包括美国政府）很可能会继续把制裁作为处理地缘政治问题的第一选择。随着全球事件对世界舞台影响的增大，反洗钱将面临越来越复杂的挑战。为了正面应对这些挑战，技术必不可少。最好的合规计划首先要有强力的企业治理机制，还要包括面向整个企业层面的制裁和 PEP 风险应对之策，需要有训练有素的员工来管理合规，以及能跟上最新技术的系统和控制措施。

Carol Stabile，CAMS，Safe Banking Systems 资深业务经理，美国纽约米尼奥拉，carol.stabile@safe-banking.com