国际公认反洗钱师

CAMS 资格认证教程

ACAMS® Association of Certified Anti-Money Laundering Specialists®
公认反洗钱师协会®
出版

www.acams.org
www.acams.org.cn

国际公认反洗钱师

CAMS 资格认证教程

ACAMS® | Association of Certified Anti-Money Laundering Specialists®
公认反洗钱师协会®

www.acams.org
www.acams.org.cn

出版

国际公认反洗钱师
CAMS 资格认证教程

第六版

执行副总裁
John J. Byrne, CAMS

项目经理
Catalina Martinez

中文版审阅
许胧方 (Joyce Hsu), CAMS-FCI — *ACAMS 北亚区反洗钱合规策略总监*

在 CAMS 资格认证特别小组编写《国际公认反洗钱师 (CAMS) 资格认证教程》的过程中，
下列专业人士作出了重要贡献，为此我们致以诚挚谢意。

Bob Pasley, CAMS —*工作组主席*
Kevin Anderson, CAMS —*工作组主席*
Brian Stoeckert, CAMS —*工作组主席*
Paul Osborne, CAMS —*工作组主席*
Peter Wild, CAMS-Audit —*工作组副主席*
Barbara Keller, CAMS —*工作组副主席*
邓芳慧 (Hue Dang), CAMS-Audit — *ACAMS 亚太区执行长*
Samantha Sheen, CAMS — *ACAMS 欧洲区反洗钱合规策略总监*
Rick Small, CAMS — *ACAMS 咨询委员会*
Nancy Saur, CAMS — *ACAMS 咨询委员会*
David Clark, CAMS — *ACAMS 咨询委员会*
Vasilios Chrisos, CAMS — *ACAMS 咨询委员会*
Anna Rentschler, CAMS — *ACAMS 咨询委员会*
Dennis Lormel, CAMS — *ACAMS 咨询委员会*

Abbas Bou Diab, CAMS
Angel Nguyen, CAMS
Brian Vitale, CAMS-Audit
Brigette K. Miller, CAMS
Christopher Bagnall, CAMS
Christopher Randle, CAMS-Audit, CAMS-FCI
Dave Dekkers, CAMS-Audit
Deborah Hitzeroth, CAMS-FCI
Donna Davidek, CAMS-Audit
Ed Beemer, CAMS-FCI
Eric Wathen, CAMS
Gary Bagliebter, CAMS
Iris Smith, CAMS-Audit
Iwona Skornicka Castro, CAMS
Jack Sonnenschein, CAMS-Audit
Jeremy Brierley, CAMS
Jim Vilker, CAMS
Joel Conaty
Jurgen Egberink, CAMS
Kenneth Simmons, CAMS-Audit
Kok Cheong Leong, CAMS-Audit
Lauren Kohr, CAMS-Audit
Lindsay Dastrup, CAMS-Audit
Margaret Silvers, CAMS
Martin Dilly, CAMS-Audit
Nancy Lake, CAMS-Audit, CAMS-FCI
Peter Warrack, CAMS
Rachele Byrne, CAMS
Sean McCrossan, CAMS-FCI
Sharon McCullough, CAMS
Steve Gurdak, CAMS
Susan Cannon, CAMS-Audit
Susanne Wai Yin Ong, CAMS
Tatiana Turculet, CAMS
Venus Edano, CAMS
William Aubrey Chapman, CAMS-Audit
Yevgeniya Balyasna, CAMS
Zachary Miller, CAMS-FCI

在此，我们还要感谢各地 ACAMS 分会为资格认证的编写所付出的努力。

ISBN：978-0-9777495-2-2


CAMS
Certified
Anti-Money
Laundering
Specialist®

特别鸣谢中国工商银行对本教程的审定提供了宝贵支持，
本协会衷心感谢以下专家们的特殊贡献：

周玮	总经理
华耀纲	总经理
廉何	副总经理
吕筱文	高级专家
刘志鹏	处长
舒本胜	副处长
钱锋	副处长
陈醒蕾	副处长
金佳	经理
刘威	经理
苏飞	经理
楚玉环	经理
夏俊	经理
肖琴	经理
国锐	经理
谭钧元	经理
张陆驷	经理
王冰	经理
孟庆鑫	经理

目录

导论

第 1 章

第 4 章

开展调查和回应调查 202

关于 ACAMS

ACAMS 的使命是提高全球范围内专门从事洗钱侦测与防范工作的人员专业领域知识、技能和经验的交流，推动反洗钱政策和措施的妥善制定及实施。为实现这一目标，ACAMS 致力于：

- 推进洗钱与恐怖融资活动的国际侦测和防范标准；
- 让私营机构及政府机构的专业人员了解上述标准以及满足这些标准所需的策略和实务；
- 对会员的成果予以认证；以及
- 搭建网络平台，以便于反洗钱和反恐融资活动专业人员在全球范围内开展合作。

ACAMS 为全球范围内打击金融犯罪的从业人员制定职业标准，并向他们提供职业发展和交流的机会。尤其，ACAMS 重视以下目标：

- 通过前沿的教育、培训和认证，帮助反洗钱专业人员提高职业技能。为反洗钱专业人员提供一个交流各种策略和观点的论坛。
- 协助反洗钱从业人员妥善制定、实施并坚持行之有效的相关措施和程序。
- 在飞速扩张的反洗钱领域，为金融和非金融机构甄选及聘用国际公认反洗钱师提供帮助。

关于 CAMS 资格认证

由于洗钱和恐怖融资活动会威胁金融机构和非金融机构乃至整个社会的安全，因此培养能够监测金融犯罪、预防金融犯罪专业人员的需求日益迫切，挑战也日益艰巨。面对这一需求，ACAMS 在全球率先作出反应，建立起国际公认反洗钱师资格认证体系，统一并促进了反洗钱专业人员的职业标准。

CAMS 资格证书已获得全球公认，取得该证书即可证明阁下已具备足够的反洗钱专业知识。通过 CAMS 资格认证的反洗钱专业人员将成为行业的佼佼者，在其机构中发挥重要价值。

恭喜您选择了反洗钱领域最具声望且被国际普遍认可的资格认证。我们欢迎并邀请您开始一段崭新的旅程，该旅程将带领各位进入一个新的职业发展高度，并且让阁下可以获得国际认可以及同行和上级的尊重。

希望您坚持阅读，努力学习。预祝好运！

第 1 章

洗钱和恐怖融资活动的风险及方法

什么是洗钱?

洗钱是指对犯罪所得进行处理并掩饰其非法来源，以期将犯罪所得用于合法或非法活动。简而言之，洗钱就是将非法所得转为合法的过程。

犯罪活动产生巨额收益后，犯罪分子或集团必须通过某种途径使用这笔资金，但又不能引起外界对上述犯罪活动或犯罪人员的注意。犯罪分子通过掩饰资金来源，改变资金形态或将资金转移至不易引起外界注意的地点来实现这一意图。产生洗钱行为的犯罪（如上游犯罪）包括：非法销售武器、贩卖毒品、走私违禁品及其他有组织的犯罪活动、挪用公款、内幕交易、行贿受贿和网络欺诈。

金融行动特别工作组 (FATF) 是七国集团为促进反洗钱国际行动、树立标准，于 1989 年成立的跨政府间的一个国际组织。金融行动特别工作组首先纠正了洗钱仅限于现金交易这一错误观念。金融行动特别工作组针对洗钱“类型”的研究表明，洗钱活动几乎可以通过任何媒介、金融机构或企业完成。

《联合国打击跨国有组织犯罪公约》(2000)，又称《巴勒莫公约》，将洗钱定义为：

- 明知财产为犯罪所得，为隐瞒或掩饰该财产的非法来源，或为协助任何参与实施上游犯罪者逃避其行为的法律后果而转换或转移财产
- 明知财产为犯罪所得而隐瞒或掩饰该财产的真实性质、来源、所在地、处置、转移、所有权或有关的权利。
- 在得到财产时，明知其从犯罪行为或参与犯罪行为中所得而仍获取、占有或使用。

在洗钱定义中，“明知”是一项重要前提。在上述三点定义中均出现了“明知……为犯罪所得”这一表述，普遍应用了“明知”的广义含义。金融行动特别工作组反洗钱和反恐怖融资 40 项建议以及欧盟关于防止利用金融系统进行洗钱和恐怖融资活动的第四号指令（2015 年）均明确指出，构成洗钱犯罪要件的“故意”和“明知”包括从“客观实际情况”推定出的心理状态。

一些司法管辖区在洗钱案件中也运用“有意忽视”(willful blindness) 这一法律原则。这些法院认定有意忽视指“有意回避明知的事实”或者“故意放任”，即等同于切实明知资金的非法来源或客户在洗钱交易中的意图。

在美国 911 恐怖 事件发生后，2001 年 10 月，金融行动特别工作组将恐怖融资活动也纳入到洗钱的范畴。恐怖分子和洗钱者使用相同的方法来转移资金以避免被发觉，如拆分交易（为了避免被报告）、地下钱庄和哈瓦拉、亨递、飞钱等资金转移系统。但根据定义，洗钱的资金来源于犯罪活动（如贩毒和诈骗），而恐怖融资活动的资金还可能来源于合法途径。隐瞒用于恐怖主义活动资金的主要意图在于隐藏该资金的使用目的，而非来源。恐怖分子的资金可能用于运营费用，包括食品开销、租金以及恐怖行动开支等。和犯罪集团一样，恐怖分子也希望对交易地点和交易目的进行保密。

2012 年 2 月，金融行动特别工作组修改了其初始建议及解释，形成全新的 40 项建议，其中加入一条全新建议，强调采取措施以防范、抑制和阻止大规模杀伤性武器的扩散。

洗钱的三个阶段

洗钱往往涉及一系列难以分辨的复杂交易，但通常可分为三个阶段：

阶段一：处置——实际处理犯罪所得的现金或其他资产。

在这一阶段，洗钱者将非法所得投入金融系统中。洗钱者通常会通过向本地和国际上的金融机构、赌场、商店或合法企业循环投入资金来实现这一目的。

处置交易的示例：

- 混合资金：将非法资金与合法资金混和，将贩毒的现金投入到当地现金密集型企业，如：餐厅
- 外汇：用非法资金购买外汇
- 现金拆分：将现金分为多个小数额，存入多家银行账户，企图规避报告要求

- 货币走私：现金或金融工具（票据）的跨境实际转移
- 贷款：用待清洗现金偿还合法贷款

阶段二：离析——经过层层金融交易来隐匿资金来源，从而将非法所得与其真实来源分离开来。

第二阶段涉及将犯罪所得转变为其他形式并创建层次复杂的金融交易来掩饰资金的来源和所有权。

离析交易的示例：

- 通过电子资金转移，将资金从一国转移至另一国家，然后投入高级的金融期权和 / 或金融市场上
- 将资金从一家金融机构转移至另一家金融机构，或在同一家金融机构内开立的多个账户间进行互转
- 将现金换为金融工具（票据）
- 转售高价值商品和预付存取 / 储值产品
- 投资不动产和其他合法企业
- 投资股票、债券和人寿保险产品
- 利用空壳公司，掩盖最终受益所有权人和资产

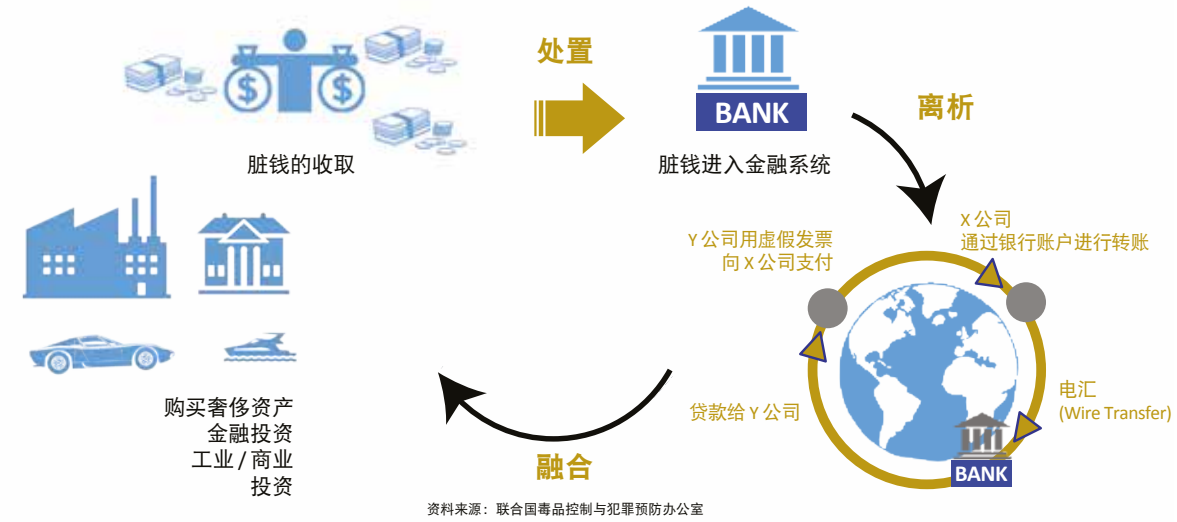
阶段三：融合——以看似正常业务或个人交易的形式将资金重新投入到经济活动中，使非法财富在表面上看似具有合法性。

这一阶段需要将洗白后的资金用于表面上看似正常的交易，从而给人具有合法性的感觉。例如，洗钱者可将资金投资于不动产、风险投资或奢侈资产。经过融合阶段后，再要区分合法和非法财富就难乎其难了。在这一阶段，洗钱者就有机会将犯罪所得转化为其自己的合法财富。融合通常很难发觉，除非个人或公司的合法用工规模、业务规模或投资企业规模与其个人财富、或一个公司的收入或资产之间存在着巨大差异。

融合交易的示例：

- 购买奢侈资产，如房产、艺术品、珠宝及高级汽车等
- 用于创立企业的财务投资计划或风险投资计划

洗钱的阶段



洗钱的经济和社会影响

洗钱是为犯罪分子创造收益的犯罪行为。这种行为不分国界，反洗钱和反恐融资立法及监管制度薄弱、不力或不足的司法管辖区最易受到这种行为的冲击。然而，大型发达的金融中心也极易受到洗钱活动的威胁，因为这种地方往往交易数额巨大，让洗钱犯罪分子有机可乘而混迹其中，繁多的服务种类也为他们进行交易提供了便利。由于大多数洗钱分子都希望能使用他们的犯罪所得，因此他们的最终目的是在稳定的金融系统中进行资金转移。

洗钱对经济和社会都有着巨大的影响，对发展中国家和新兴市场尤其如此。可以轻易转移资金的机构，或不经调查即可投入资金的系统都是滋生洗钱活动的温床。坚持合法、专业的道德标准对维护金融市场的诚信具有关键作用。

如果洗钱行为未被查出，可能会对宏观经济造成下列潜在影响：

- **滋生有组织犯罪和贪污现象：**洗钱成功有助于提高犯罪活动的收益。一个国家或地区成为洗钱天堂后就会吸引犯罪分子进行犯罪。通常来说，洗钱和恐怖融资活动的庇护所具备以下特点：
  - 洗钱上游犯罪（即可能令司法管辖机构判定为洗钱罪的形式犯罪）数量有限。
  - 反洗钱法律法规所管辖的机构和人员对象的类型有限。
  - 执法不严、惩罚不力、以及相关规定不利于没收或冻结与洗钱相关的资产。

— 监管能力有限，不能有效监控和监督洗钱和恐怖融资法规的合规问题。

洗钱犯罪猖獗，滋生更多腐败。通常有组织的犯罪集团会渗入司法管辖系统，直接导致公共机构和私营机构产生贪污现象。犯罪分子可能通过贿赂政府官员、律师和金融机构或非金融机构的员工，以便继续从事犯罪活动。

在法规和执法薄弱的国家，贪污也容易引发洗钱活动。导致金融机构的行贿受贿现象增加，律师、会计师、立法机构、执法机构、警察局、监管机构，甚至法院和检察官也会牵涉入行贿受贿活动中。

而制定全面的反洗钱和反恐融资框架则有助于遏制犯罪行为，使犯罪分子无法从此类活动中获益，进而降低他们在国家内进行犯罪活动的热情，尤其是在执法力度强且能没收犯罪所得的国家。

案例分析

2001 年，美国国家安全委员会在一份报告中指出，俄罗斯的多家机构正利用以色列庞大的俄罗斯移民社群，非法生产 CD 并清洗收益。在俄罗斯黑帮看来，以色列是一个“洗钱胜地”。以色列警方估计超过 40 亿美元的脏钱流入了以色列境内，而其他方面评估这一数字应为 200 亿美元左右。这些犯罪团伙在贫困城镇购买了大量土地，并接管了当地的一切事务，从慈善机构到市政厅无所不含，甚至还亲自挑选了几名人员，作为当地和国家机构官员的候选人。这又为犯罪团伙提供了更多防护，确保他们可以享受政策福利，获得有关部门的保护。

- **损害合法的私营机构：**在洗钱对微观经济的影响中，私营机构是重灾区之一。

  众所周知，洗钱者会利用表面上合法且从事合法业务的前台公司或企业，但实际上这些公司或企业受控于犯罪分子。他们将非法活动所得收益与合法资金混合，以此掩盖真实的收入来源。这些前台公司往往拥有大量非法资金，可用于为产品和服务提供补贴，从而以远低于市场价的价格进行销售，因此相对于合法企业，他们拥有更大的竞争优势。这使得合法企业很难与前台公司展开竞争。显然，这些犯罪企业的管理原则与传统自由市场原则相互矛盾，导致对宏观经济产生进一步的负面影响。

  最后，通过利用前台公司及对其他合法企业进行投资，洗钱所得可用于控制某些国家的整个产业或经济部门。由于资产和大宗商品价格的人为扭曲造成资源的不合理配置，增加了货币和经济动荡的可能性。这也为避税提供了工具，从而造成国家或地区财政收入的减少。

- **削弱金融机构：**洗钱和恐怖融资活动会危害一个国家或地区金融部门的健康发展。它们会对个别银行或其他金融机构（如证券公司和保险公司等）的稳定性造成负面影响。犯罪活动一直与全球范围内一些银行的破产相关，包括第一家互联网银行欧洲联盟银行 (European Union

Bank) 以及里格斯银行 (Riggs Bank) 的破产。通常，建立并维护有效的反洗钱 / 反恐融资制度是金融机构维持其营业执照的重要前提。任何不合规行为都可能使其遭受巨额民事罚金，甚至被撤销执照。

- **对外资的削弱效应：**虽然发展中经济体对投资来源没有太多选择，但一旦外界认为某国的商业和金融产业秩序已遭破坏且处在有组织犯罪行为的威胁下，则将对该国的外商直接投资产生削弱效应。要维持一个有利的商业环境，就必须扫除这些障碍。

- **失去对经济政策决策的控制或考量，并执行了错误的经济决策：**鉴于洗钱过程涉及巨额资金，在一些新兴市场国家或地区，这些非法所得可能会大大高于政府的预算资金，令政府无法控制经济政策，或因宏观经济统计错误而引发政策失误。

  由于洗钱者将资金再投资到不易被侦测到的领域，而非回报率更高的领域，因而可能对货币和利率造成负面影响。因无法预料的资金跨境转移而导致的汇率和利率波动也时有发生。由于洗钱犯罪的存在，货币需求会在某种程度上从一个国家或地区转移到另一个国家或地区，产生误导性的货币数据。这会对利率和汇率的波动产生负面影响，而对于以美元为基准的经济体来说，由于追踪货币流通总额的不确定性变得更大，这种影响将尤为严重。最后，鉴于人为扭曲资产和大宗商品价格会导致资源的错误配置，洗钱也会对货币的不稳定性造成更大的威胁。

- **经济扭曲和不稳定：**洗钱者的初衷不在于从投资中盈利，而是保护其非法所得并隐匿资金的非法来源。因此，他们所“投资”的活动并不一定会对资金所在国产生经济利益。此外，鉴于洗钱和金融犯罪从某种程度上将资金从合理的投资转向可以隐匿资金来源的低质量投资，经济增长可能因此受阻。

- **税收损失：**在非法活动的基本形式中，逃税对宏观经济的影响可能最为明显。洗钱使政府税收缩水，从而间接危害诚实的纳税人。它也使政府征税变得更加困难。这一收入损失通常导致政府税率高于正常水平。

  政府收入不足是许多国家或地区经济困难的核心，而改善这一状况正是大多数经济稳定计划的主要关注点。国际货币基金组织 (IMF) 一直致力于帮助其成员国提高征税能力，而国际合作与发展组织 (OECD) 则一直推动多个司法管辖区朝着税收透明迈进。

- **私有化的风险：**一些国家或地区试图通过对土地、资源等国有资产或国有企业私有化，对经济进行改革，但这些私有化措施往往会受到来自洗钱活动的威胁。一旦政府内存在贪污或内幕交易等问题，就可能将私有化任务交由犯罪组织负责，这将可能使民众遭受经济损失。此外，由于私有化举措往往具有经济收益，因此也会成为洗钱的工具。过去，犯罪分子曾通过购买码头、度假村、赌场和其他国有资产来隐匿非法收益，并进一步深入开展犯罪活动。

- **国家或地区的声誉风险：**洗钱或恐怖融资活动庇护所的名声可能会危害国家的发展和经济增长。这将减少合法的全球性机遇，因为外国金融机构在与位于洗钱天堂的金融机构进行交易时，需耗费巨资进行额外的审查。

  位于洗钱天堂的合法企业可能会因为所有权控制问题而遭受到额外审查，从而面临着进入国际市场机会减少（或将面临支付更多准入费用）的局面。一旦国家的金融声誉受损，要想恢复声誉的难度极大，而且需要大量额外资源来矫正原本只需要适当的反洗钱控制就可以防止的问题。其他影响还包括，对国际组织和其他国家或地区所采取的具体措施产生影响，以及会使政府获得援助的资格受损等。

- **国际制裁风险：**为防止金融系统中出现洗钱和恐怖融资活动，美国、联合国和欧盟等管理机构可能会对其他国家、机构或个人、恐怖分子及恐怖组织、毒贩等对安全构成威胁的个人和团体实施制裁。美国财政部下属的海外资产控制办公室 (OFAC) 管理并执行美国经济和贸易制裁。

  国家可能会面临全面制裁或特定制裁。如某国受到全面制裁，则与该国进行的所有交易都将遭到禁止。如为特定制裁，则与海外资产控制办公室特别指定国民名单和黑名单上列出的某些特定行业、机构或个人的交易将受到禁止。如不遵守，可能会面临刑事或民事处罚。针对反洗钱 / 反恐融资制度存在关键缺陷，且针对不符合国际标准的国家和地区，金融行动特别工作组还制定了一份高风险和非合作司法管辖区名单。金融行动特别工作组呼吁成员国对这些国家和地区采取相应的应对措施，例如，金融机构在与上述国家及地区的自然人和法人进行交易或商业往来时，应进行增强型尽职调查，以敦促其改善反洗钱 / 反恐融资制度。

- **社会成本：**洗钱会产生巨大的社会成本和风险。洗钱是保持犯罪盈利的重要因素。它也是毒品犯罪、走私犯罪和其他刑事犯罪滋生的幕后推手。为了打击洗钱所造成的严重影响，执法和其他费用（如因戒毒治疗造成的医疗成本上升）再不断提高，政府开支和预算的成本也需要相应增加。

  依赖犯罪所得的金融机构在多个问题上面临挑战，包括如何充分管理资产、负债和运营，如何吸引合法客户等。他们还面临被排除在国际金融系统外的风险。洗钱的负面影响通常涉及声誉风险、经营风险、法律风险、集中风险，具体表现包括：

— 盈利业务的流失

— 资金撤出导致的流动性问题

— 代理银行业务被终止

— 调查费用和罚款

— 资产扣押

— 贷款损失

— 金融机构股票价值下跌

- **声誉风险 (Reputational Risk)：**声誉风险是指关于一个机构业务和相关活动的潜在负面公共报道（无论准确与否）使公众对该机构的诚信丧失信心。以银行为例，如果一家银行因涉及洗钱丑闻而导致潜在借款人、存款人和投资者可能拒绝与其进行业务往来，则构成该银行的声誉风险。

  优质借款人流失会减少银行盈利性贷款的发放数额，增加银行整体贷款组合的风险。存款人可能会撤走资金。此外，一旦存款人得知银行可能不稳定，银行再也无法依赖这些人的银行存款作为资金来源，存款人可能宁愿选择支付高额罚金也不愿将资金存放在有问题的银行，从而导致意料之外的提款，产生流动性问题。

- **经营风险 (Operational Risk)：**经营风险是指因内部流程、人员或系统不足或者因外部事件而导致损失的可能性。这类损失常因机构减少或代理银行服务的减少、终止或业务经营成本增加所致。借款或融资成本的增加也是经营风险的一大因素。

- **法律风险 (Legal Risk)：**法律风险是指因诉讼、不利判决、不可强制执行的合同、罚金和处罚导致机构损失、支出增加甚至是机构被关闭的可能性。例如，合法客户可能成为金融犯罪的受害者，遭受金钱损失并起诉金融机构要求赔偿。监管机构或执法部门的调查可能导致成本的增加、罚金以及其他形式的处罚。此外，某些合同可能因部分犯罪客户的欺诈而无法强制执行。

- **集中风险 (Concentration Risk)：**集中风险是指因向一个借款人或借款人集团发放过多信用或贷款而造成损失的可能性。监管法规通常限制银行向单一借款人或由相关借款人组成的集团提供过多资金。缺乏对特定客户的了解，或谁是幕后的客户，或者缺乏对该特定客户与其

他借款人关系的了解，都会将银行置于这种风险之中。尤其当存在关联交易方、关联借款人以及用于偿还贷款的收入或资产来源相同时，也可能导致贷款损失。当然，无法强制执行的合同及用假名签订的合同也可能导致贷款损失。

基于上述原因，各国际机构发布了多份声明，如巴塞尔银行监管委员会 2014 年发布的*《洗钱和恐怖融资风险健全管理》*指南以及*金融行动特别工作组发布的《反洗钱、反恐融资与反核武器扩散融资的国际标准》*。

反洗钱 / 反恐融资合规制度与个人责任

近年来，各国针对受监管金融机构的高层管理人员发布了多项指南，并通过了多部法规，以明确此类人员的个人责任，并弥补反洗钱和制裁合规制度所存在的缺陷。

2014 年，美国财政部金融犯罪执法网络 (FinCEN) 和美国金融情报中心 (FIU) 对金融机构发布了一份通稿，提醒其建立强大的合规文化，并明确所有员工都有责任遵守反洗钱 / 反恐融资相关法律法规。2015 年，美国司法部发布由副总检察长 Sally Quillian Yates 编制的备忘录《公司违法行为个人责任指令》。

该备忘录亦称《Yates 备忘录》，旨在提醒检察官在对企业违规行为进行民事和刑事调查时，还应关注个人违反相关法律的行为。另外，备忘录还提出企业不得包庇负有刑事或民事责任的个人。尽管《Yates 备忘录》并非专为反洗钱 / 反恐融资问题而制定的，但近期美国监管机构针对金融机构采取了一系列执法行动，表明了美国对反洗钱 / 反恐融资合规缺陷的持续关注。

2015 年，英国金融市场行为监管局 (FCA) 颁布了针对高级管理人员制度的最终规定，以规范银行业的个人责任。为防止金融犯罪的发生，高级管理人员制度规定金融机构必须明确指定一名高管人员，如执行层级别的洗钱报告专员 (MLRO)，以确保该机构制定并实施了有效的措施，用以打击金融犯罪。如该机构的反洗钱 / 反恐融资制度出现任何违规行为，该高管人员需承担个人责任。

2016 年 6 月 30 日，纽约州金融服务局 (DFS) 颁布了一项最终规定，要求受监管机构建立适当的“交易监控和筛选制度”，以实现下述目的：

(i) 在达成交易后，监控其是否遵守银行保密法和可疑活动报告规定等反洗钱法规；以及

(ii) 防止与美国财政部海外资产控制办公室 (OFAC) 实施经济制裁的对象进行非法交易。

该最终规定于 2017 年 1 月 1 日开始生效，要求受监管机构的董事会或高级官员每年向纽约州金融服务局提交证明，表明其已采取所有一切必要措施，以满足交易监控和筛选制度的要求。

从表面来看，该法规仅针对纽约州境内机构，但在纽约州运营的诸多外国银行也须遵守该法规的规定。法规管辖范围涵盖根据纽约州《银行法》获银行执照的银行、信托公司、私人银行、储蓄银行、储蓄和信贷协会，以及根据纽约州《银行法》获得纽约州银行业务经营许可的国外银行分行或代理机构。此外还适用于根据《银行法》获得执照的非银行金融机构，如支票兑现公司和货币服务提供商。

案例分析

从 2003 年至 2008 年，Thomas Haider 在 MoneyGram 公司担任首席合规官，该公司是一家专门从事货币转账的货币服务企业。Haider 的职责包括确保 MoneyGram 公司执行有效的反洗钱 / 反恐融资制度，能及时汇报可疑交易。同时，他还主管 MoneyGram 的反欺诈部门。

在其任职期间，收到数千次客户投诉，这些客户称自己遭遇了“彩票”或预付费欺诈案件，在诈骗分子的指示下，他们将钱款通过 MoneyGram 设在美国和加拿大的各代理机构汇给诈骗分子。尽管 Haider 和 MoneyGram 的反欺诈部门收到了数量惊人的投诉，却并未针对任何投诉或投诉所涉代理机构展开调查。如若展开调查工作，Haider 先生就能暂停或终止那些参与违法活动代理处的业务活动。

2014 年 12 月，美国金融犯罪执法网络做出民事处罚决定，认为 Haider 既未能实施合理的反洗钱制度，进行有效审计，也未能及时关闭具有高风险的代理机构。受美国金融犯罪执法网络调查的影响，2008 年，Haider 被 MoneyGram 解雇，2014 年，他个人被处以 100 万美元民事罚款。金融犯罪执法网络还力图禁止 Haider 继续从事金融服务业相关工作。

洗钱的方法

洗钱手段不断推陈出新，必须持续监控各种形式的洗钱活动，以便采取及时有效的监管措施。非法资金可通过各种不同的商业渠道转移，如活期存款、储蓄和经纪账户、贷款、电汇和转账等产品和服务，或通过金融中介进行，如信托公司、公司服务提供商、证券交易商、银行及货币服务企业等。

洗钱犯罪分子会试图从金融系统找到洗钱的最佳手段。随着世界上不少国家和地区的政府都对银行部门规定了反洗钱义务，洗钱活动逐渐转向非银行金融部门以及非金融企业和行业。

金融行动特别工作组及其同类区域性组织定期发布类型报告，来协助认识“监管变化并更好地了解洗钱和恐怖融资活动的基本机制”。其目标是报告部分“这些领域的关键方法和趋势”，同时确保 FATF 40 项建议仍具有有效性和相关性。本章将经常提到这些类型，因为它们对洗钱的各种方法和情境提供了很好的示例。

银行和其他储蓄机构

银行历来都在洗钱三阶段中占据了重要地位，今后也将如此。以下是利用银行和其他储蓄机构洗钱需要关注的特殊领域。

电子资金转账

电子资金转账是指任何以电子手段（如自动结算中心 (ACH)、电脑、自动柜员机 (ATM)、电子终端、移动电话、电话或磁条）完成的资金转账。电子转帐既可在国内进行，也可跨境，其作为转移资金最迅速的方式之一，每天的交易量多达数百万笔，金额高达数万亿美元。

联邦电子资金转账系统 (Fedwire)、环球银行金融电讯系统 (SWIFT) 和纽约清算所银行间支付系统 (CHIPS) 等系统每天都需处理上百万笔电汇或转账信息。这样一来，非法资金转账可以轻易地隐藏在这每天数百万笔的合法转账交易中。举个例子，洗钱犯罪分子可能会进行未经授权的国内或国际电子资金转账，如自动清算中心借记或在盗取的信用卡上预支现金，并将资金放入用于接收转账的账户中。另外，洗钱犯罪分子也可能盗取信用卡，使用盗取的资金购买商品，然后通过出售商品为犯罪分子提供现金。

洗钱犯罪分子也会在洗钱的第二阶段，即离析阶段，利用电子资金转账。这样做的目的是，在每一层交易中，都将资金从一个账户转移到另一个账户，从一家银行转移到另一家银行，从一个国家或地区转移到另外一个国家或地区，从而使执法部门或调查机关难以追踪资金的来源。

为了躲避对各阶段的侦测，洗钱者可能采取基本的防范措施，如改变转账的金额，确保每笔转账金额相对较小，低于报告阈值以及尽可能利用声誉良好的机构。

然而，近年来电子资金转账的验证流程已经得到强化。很多交易监控软件供应商建立了复杂的运算法则来进行监测，或在发现利用电子转账系统进行洗钱或其他可疑交易时，触发警报。但是，任何系统都无法确保万无一失。

利用电子资金转账方式进行洗钱有以下特征：

- 资金进出于金融保密庇护所、没有明显的业务理由进出于高风险地区、或者资金转账与客户的业务或历史交易不符。
- 代表外国客户接收大笔转入资金，但理由不充分或者没有理由。
- 接收大量小额转入资金或通过支票和汇票进行大量小额存款。转账资金或存款的全额或大部分被转往其他地区的另一个账户，交易方式与客户业务或历史交易不符。
- 资金活动无法解释、交易重复进行或以反常方式进行。
- 收支与合法合同、商品或服务没有明显关联。
- 和同一个人不同的账户进行资金往来。

远程储蓄

远程储蓄 (RDC) 是银行提供的一种产品，客户可以扫描支票，通过向银行发送电子影像进行储蓄。这项服务为客户提供了更多的便利，客户无需再去银行或自动取款机存入支票。之前，这项服务仅供商业客户用专门的扫描仪使用，但现在许多银行允许个人客户使用手机拍摄支票的照片，即可进行储蓄。远程储蓄为银行降低了交易处理成本，有助于促进非纸质交易的发展。因此，远程储蓄在代理银行服务中的使用也日益增多，因为这一方式可以简化储蓄和结算流程。代理银行服务是指一家银行向另一家银行提供银行服务。

远程储蓄的便利可能会受到洗钱犯罪分子的青睐，因为他们无需去银行接受风险检测。一旦洗钱犯罪分子能够进行远程储蓄，他们就能轻易地通过账户转移支票。他们还可能会利用多个扫描仪、多个符合条件的手机等图像设备，让其他洗钱犯罪分子也能通过该系统进行交易。洗钱犯罪分子还可以令他人开立一个账户，供其储蓄。如果没有合理的管控措施，远程储蓄也可能被滥用，导致违反制裁规定（如在受制裁的国家进行交易）。

除了被用于洗钱外，远程储蓄还存在很大的欺诈风险。远程储蓄最大程度地简化了人工审查流程，导致篡改支票或同一支票多次存入等可疑欺诈信号变得难以识别。通常，欺诈行为无法预防，仅能在发生后才发现。

为了控制远程储蓄的风险，必须将其与其他管控措施结合，如监控和欺诈预防系统。事实上，银行每推出一种新产品都应结合使用相应的管控措施。管控措施包括审查远程储蓄中提交的文件，查看是否存在连号以及无收款人的支票或汇票；将单个远程储蓄账户活动的总金额也纳入整体交易监控范围；为远程储蓄设置适当的储蓄限额；为真正需要该产品的客户提供这一服务；如发现远程储蓄中存在欺诈行为，应迅速采取合理措施。

代理银行业务

代理银行服务是指一家银行（称为“代理银行”）向另一家银行（称为“委托银行”）提供银行服务。通过在全球建立众多的代理关系，银行可为自身及其客户（该银行未在客户所在地开展实体经营活动）从事国际金融交易。大型国际银行往往同时充当全球成千上万家其他银行的代理银行。

委托银行则通过代理关系获得广泛的服务，包括现金管理（如各种货币的利息存款账户）、国际资金电汇、支票清算、通汇账户和外汇兑换等服务。

在建立代理账户之前，银行应该能够回答关于委托银行的基本问题，包括银行的所有者以及其监管性质。如果委托银行的信用良好，则可能获得部分信贷产品（如信用证和为信用卡交易而开立的商业账户）代理服务。代理银行向规模较小、知名度不高的银行提供的服务可能局限于非信贷现金管理服务。

洗钱者能够通过代理银行服务洗钱基于以下两大原因：

1. 从本质上讲，代理银行服务关系使得金融机构可以代表其他机构的客户进行金融交易。这种间接关系意味着，代理银行在向既未经本行验证身份又未获得任何第一手信息的个人或实体提供服务。
2. 由于金融机构为其客户的客户处理大量交易，所以通过代理账户流通的资金数额可能会对金融机构产生巨大的威胁。鉴于金融机构通常无法获得实际交易方的信息来鉴别其是否正常，识别可疑交易的难度也大大增加。

代理银行造成的其他风险包括：

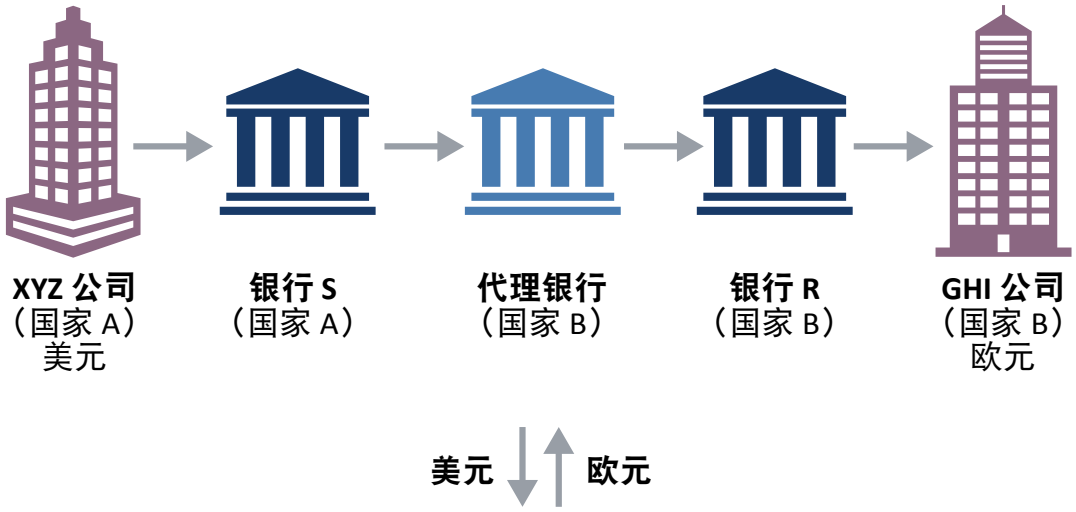
- 代理银行也许能了解委托银行所适用的监管法律，但要了解该银行受其监管机制监管的力度和有效性却更为困难。也不利于确定所建立关系的委托银行的风险等级。
- 确定委托银行反洗钱监控措施的有效性也是一大挑战。虽然要求客户填写合规问卷将提供一定的帮助，但代理银行仍依赖委托银行自身对可以使用代理账户的客户进行尽职调查。

- 部分提供代理服务的银行可能不会向其委托银行询问该委托银行向其他机构提供服务的情况，比如连环代理。这意味着代理银行更加难以了解更下一级委托银行的客户身份或业务活动，甚至是其所提供的金融服务类型。

  案例分析

  2015 年 3 月，佛罗里达州的 North Dade 社群发展联邦储蓄互助社 (North Dade Community Development Federal Credit Union) 因有意违反美国《爱国者法》、《银行保密法》和储蓄互助社法规规定，遭美国监管机构关闭。该储蓄互助社仅设有一处办公地点和五名员工。该互助社的经营目标为给本地社群的成员提供基础的金融服务。但金融犯罪执法网络发现它与拉丁美洲和中东等高风险司法管辖区的货币服务企业建立了代理银行服务关系。2013 年，该储蓄互助社为货币服务企业客户处理现金汇票约 5,500 万美元，汇出电汇 10 亿美元，退回支票 500 万美元，远程储蓄 9.85 亿美元。金融犯罪执法网络称这些资金可能用于洗钱或支持恐怖组织。此外，金融犯罪执法网络还发现该社存在一些小型储蓄互助社不会存在的商业行为，导致产生大量的反洗钱 / 反恐融资违规行为，如违反银行保密法制度、交易记录和报告等规定。North Dade 储蓄互助社被处以 30 万美元民事罚款。之后，其金融监管机构美国国家储蓄互助社协会确认该互助社违法了多项法规及联邦规定，并对其进行了取缔。

代理银行服务交易示例
（单一代理）



通汇账户

在有些代理关系中，委托银行的客户能够通过委托银行的代理账户进行交易（包括电汇、存取款以及开立支票账户），且无需事先通过委托银行进行清算。这类账户称为通汇账户 (PTA)。而在传统的代理关系中，委托银行会接受客户的指令并将指令传达给代理银行。在这些情形下，委托银行可以在完成交易前实施一些不同级别的监管。通汇账户与普通代理账户有所不同，因为外国银行客户可以直接控制代理银行中的资金。

通汇账户子账户持有人的个数近乎不限，包括个人、商业企业、金融公司、交易所（或货币兑换处）甚至是外国银行。提供给“子账户持有人”的服务以及通汇账户的条款在代理银行和委托银行签订的协议中皆有明确规定。

以委托银行的名义持有的通汇账户通常包括以银行账户号码编码的支票和用来确定子账户（委托银行客户的账户）的数字密码。但有时，子账户持有人未经过代理银行的身份确认。

在通汇账户关系中，可能威胁代理银行反洗钱防御系统的要素包括：

- 与设立在监管不足或尚不成熟且许可法律宽松的离岸金融服务中心的外国机构开展通汇账户业务。
- 在通汇账户关系中，代理银行将委托银行视为唯一的客户，未能对委托银行的客户按该行规定实施客户尽职调查政策和流程。
- 在通汇账户关系中，子账户持有人拥有资金存取权。
- 与委托银行的附属机构、代表机构或其他办事处相关联的通汇账户，此等通汇账户允许委托银行提供与分支机构相同的服务但却不受监管。

  案例分析

  隆巴德银行 (Lombard Bank) 是一家获南太平洋岛国瓦努阿图授权许可的银行，在迈阿密的美国运通银行国际部 (AEBI) 开立了一个通汇账户。该行获准对该账户拥有多个授权签名。

  隆巴德银行的客户与美国运通银行国际部没有关系。但该行通过其在 AEBI 的通汇账户，为其在中美洲的客户提供几乎所有的银行服务。隆巴德银行甚至还向客户提供支票本，允许他们在其通汇账户中存取资金。

  隆巴德银行的通汇账户子账户持有者可将现金存入隆巴德银行在四个中美洲国家的代表处。隆巴德银行随后将这些现金转至其在迈阿密的附属机构，即隆巴德信贷公司 (Lombard Credit Corporation)，然后再存入 AEBI 的通汇账户。隆巴德银行的客户还可以把现金存入位于迈阿

密的隆巴德办事处，该办事处与 AEBI 在同一大楼内。此等现金也被存入 AEBI 的通汇账户内。截至 1993 年 6 月底，在两年多的时间里，隆巴德银行迈阿密附属机构共收到 104 笔现金，金额高达 20 万美元。这导致 AEBI 无法查明隆巴德银行客户存入 AEBI 通汇账户的现金来源，因此在了解您的客户、尽职调查、交易记录和监管要求等方面存在重大反洗钱 / 反恐融资合规隐患。

集中账户

集中账户是指为了便于处理和银行内部多笔或单笔客户交易而设立的内部账户，这些交易通常发生在同一天。银行将多个地点的资金集中到一个账户中（如集中账户），该账户也被称为特殊用途账户、综合账户、清偿账户、暂记账户、当日账户、流动账户或托收账户。集中账户通常用来为私人银行、信托和保管账户、资金转账以及国际附属机构的交易提供便利。

如果客户身份识别信息（如姓名、交易金额和账号）与金融交易分离的话，集中账户就可能滋生洗钱的风险。如果彼此分离，审计线索因此丧失，该账户就可能被滥用或受到不当管理。

使用集中账户的银行应采取相适应的政策、程序和流程来监督交易并保留这些账户的记录，包括：

- 在总分类账票据上要求双重签名。
- 禁止客户直接接入集中账户。
- 在客户账户报告中记录客户的交易情况。
- 禁止客户了解集中账户的情况或有能力直接指示员工通过该账户进行交易。
- 保留妥当的交易和客户身份识别信息。
- 由独立第三方不时对该账户进行核对。
- 建立及时的差异解决流程。
- 识别并监控交易频繁的客户姓名。

私人银行业务

私人银行业务是一项全球性业务，利润丰厚，竞争激烈。自 2008 年金融危机后，美国和欧洲加大了对私人银行及其开展的业务的审查力度，尤其是税务筹划业务领域。

私人银行为富有客户提供高度个性化和保密的产品和服务，费用往往依据“所管理资产的数额”决定。私人银行业务通常半独立于银行的其他部门。

私人银行家在争夺高净值客户时面临的激烈竞争催生了全球范围内加强政府监管的要求。激烈的竞争使得客户关系经理和营销人员在争取新客户、增加其管理的资产净值并为其所在机构贡献更高比例的净收入方面面临巨大压力。此外，私人银行大部分“关系经理人”的薪酬主要基于其为所在机构拉来的资产数额而定。

以下因素可能导致私人银行容易被用于洗钱：

- 公认的高额利润。
- 激烈的竞争。
- 强大的客户。
- 与私人银行相关的高度保密性。
- 关系经理人与其客户之间紧密的信托关系。
- 以佣金为基础的客户关系经理人薪酬机制。
- 由客户关系经理人形成的保密和谨慎文化。
- 客户关系经理人作为客户代表保护客户权益。
- 客户利用私人投资公司降低受益所有人的透明度。
- 客户在多个司法管辖区存有私人和商业存款。
- 客户可能会通过利用并控制多家法律机构，为其个人或家庭进行财产规划。

案例分析

1994 年，美国运通银行国际部 (AEBI) 聘用的两家私人银行被判定为墨西哥 Juan Garcia Abrego 贩毒集团洗钱。对于其犯罪行为，他们以该行业竞争残酷、薪酬支付方法特别以及“国际银行家在发展新客户方面面临压力且多劳多得”等理由为自己进行辩护。

在美国，里格斯银行与智利前总统奥古斯特・皮诺切特保持着密切的关系。该行工作人员曾乘坐皮诺切特的私人飞机往返智利，并为之提供几十万美元的银行本票。这笔资金随后被证明是腐败所得。里格斯银行还通过不动产交易协助资金的转移，从而掩饰资金与皮诺切特的关系。里格斯银行成立于 19 世纪，具有良好的声誉，但在 2004 年 5 月，该银行因违反美国《银行保密法》而被处以 2,500 万美元的罚金。随后在 2005 年，该银行承认其多次违反《银行保密法》，且对于智利奥古斯特・皮诺切特和赤道几内亚政府所有及控制的银行账户间的

可疑交易，未能进行如实报告。里格斯银行被处以 1,600 万美元的罚金，是同等规模的银行中金额最大的一笔刑事处罚。该银行也主动提出关闭其使馆银行及国际私人银行业务部门。随后该银行被收购，里格斯退出历史舞台。

利用私人投资公司开展私人银行业务

在离岸或国际金融中心，私人银行客户通常是“非居民”，这意味着他们在居住国以外的国家开展银行业务。他们的资产可能需要转移到境外，并以设在金融保密天堂的私人投资公司 (PIC) 等公司组织形式的名义持有。私人投资公司是指由个别银行客户或其他人在离岸司法管辖区设立并用来持有其资产的公司。作为“空壳公司”，他们成立的目的在于满足客户的保密需求以及各种税务和信托意图。私人投资公司是近年来很多重要洗钱案件的一大要素，也是绝佳的洗钱工具。

离岸金融庇护所（即通常的私人投资公司设立地）的保密法可以隐匿受益所有人的真实身份。作为保密的另一个层面，部分私人投资公司会设立名义所有人，该人作为公司的受益人。其身份可能仍然保密，有时还享有律师 - 委托人特免权或其他类似的法律保护。很多私人银行往往通过某一家在离岸金融保密庇护所的附属信托公司为其客户建立私人投资公司。犯罪分子可能会建立复杂的空壳公司网络，令在某一离岸司法管辖区注册的公司与其他管辖区的公司或账户挂钩。

案例分析

2014 年，以色列国民银行 (Bank Leumi) 承认其借助在瑞士和卢森堡的离岸分支机构，帮助 1,500 余名美国纳税人掩藏资产。据报告，在之前的几年里，以色列国民银行曾派遣多名私人银行经理到美国，与美国客户会面，讨论其离岸资产组合及避税策略。该银行帮助客户在伯利兹等离岸司法管辖区注册的代名公司掩藏其私人离岸账户，并借助假名或不具名账户，为客户开立多个账户。该银行还提供“邮件暂存”服务，为美国客户提供贷款，并以其未向美国税务部门申报的离岸资产作为抵押。最后，以色列国民银行被处以 2.7 亿美元罚款，并被勒令停止为美国客户或以美国国民为受益所有人的账户办理私人银行及投资业务。为支付该笔罚款，以色列国民银行将其分支机构 Leumi Private Bank 和 Bank Leumi （卢森堡）出售。

政治公众人物

金融行动特别工作组在 2012 年发布的《反洗钱、反恐融资与反核武器扩散融资的国际标准》中，将政治公众人物 (PEP) 分为两类：

- **外籍政治公众人物：**指在其他国家被赋予重要公共职能的人物，如国家元首、资深政治家、高级政府官员、司法或军事官员、国有企业高管或重要政党官员。

- **国内政治公众人物：**指在本国被赋予重要公共职能的人物，如国家元首、资深政治家、高级政府官员、司法或军事官员、国有企业高管或重要政党官员。

正如以下这些案例所示，政治公众人物成为一些金融机构问题的来源：

- **马里奥·维拉努埃华 (Mario Villanueva)** 是腐败的墨西哥肯他纳罗州州长。根据美国禁毒局 (DEA) 的说法，他曾帮助将 200 吨可卡因走私至美国。截至 2001 年，他在纽约雷曼兄弟公司持有私人银行账户达 5 年之久，存款金额约 2,000 万美元。美国禁毒局认为这笔资金是其收受墨西哥毒贩的贿赂所得。

- **里格斯银行**案件揭开了涉案金额达上亿美元的交易网络。里格斯银行在过去多年间为南美洲和非洲两个大陆的独裁者们提供便利，其中就包括智利的**奥古斯特·皮诺切特**和赤道几内亚的**特奥多罗·奥比昂**。这些账户是使馆银行投资组合的一部分，几十年来，这一投资组合一直是该银行的特色产品。

- **弗拉迪米洛·蒙特西诺斯 (Vladimiro Montesinos)** 是秘鲁情报服务部前部长，也是秘鲁前总统阿尔布托·藤森的首席顾问。他在纽约州的纽约银行开立了用来存储贩毒分子行贿资金的账户。纽约的美国运通国际银行、美洲银行、巴克莱银行和瑞士银行等其他机构也为蒙特西诺斯设立了账户。另外，他还利用空壳公司，在全球范围内挪用公款、走私枪支、贩毒和洗钱，金额超过 4 亿美元。

- **阿诺多·阿莱曼 (Arnoldo Aleman) 和拜朗·杰里兹 (Byron Jerez)** 分别是尼加拉瓜的前总统和税务专员。二人在迈阿密的 Terrabank N.A. 开有账户，他们通过这些账户使用贪污所得在南佛罗里达州购买了数百万美元的定期存单和共管式分户产权物业 (condominium)。

- 乌克兰前总理**帕夫洛·拉扎连科 (Pavel Lazarenko)** 在旧金山的美洲银行、商业银行、太平洋银行、美国西部银行以及数家证券公司（包括波士顿飞驰、罗伯森·斯蒂芬斯、汉鼎风险投资有限公司和美林银行）都拥有自己的账户，其在这些账户中数百万美元的资金是他作为乌克兰政府首脑期间勒索所得。

- **克罗内·维克特·凡纳洛·嘉瑞多 (Colonel Victor Venero Garrido)** 上校是一名玻利维亚军官，美国联邦调查局描述他为弗拉迪米洛·蒙特西诺斯“最为信任的挡箭牌”。他在迈阿密花旗银行和加利福尼亚北部信托公司拥有自己的账户，并在这些账户中存有 1,500 余万美元的受贿与勒索所得资产。

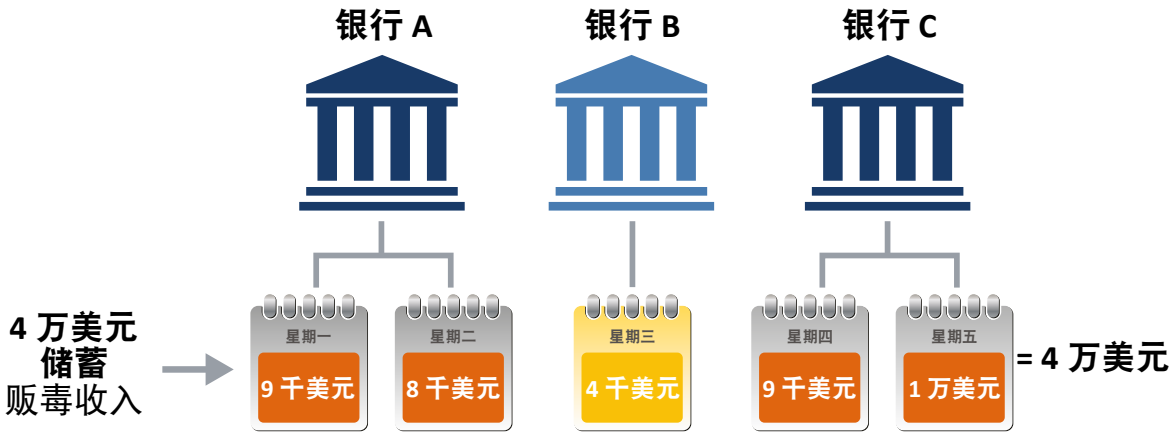
- **马里奥·鲁伊兹·马修 (Mario Ruiz Massieu)** 是墨西哥负责贩毒检控的前副总检察长。上世纪九十年代中期，他在休斯顿的得克萨斯商业银行开立了自己的私人银行账户，并存入毒贩向其行贿的 900 万美元现金，时间长达 13 个月以上。
- 直至 2009 年去世，**奥马尔·邦戈 (Omar Bongo)** 在中非地区的加蓬担任总统长达 41 年之久，他曾使用离岸空壳公司，通过私人银行账户，转移资金达 1 亿余美元，该资金来源可疑，其中还包括向家人提供的大笔现金。

拆分交易

拆分交易 (Structuring) 是为逃避可能引发的报告或记录而设计出来的一种洗钱交易方法。这可能是最常见的洗钱方法。很多国家将其定为犯罪，且必须通过提交可疑交易报告进行上报。从事拆分交易的个人可能是受雇于洗钱者的“拆分洗钱人员”(runner)。他们在多个银行存入现金并购买金融票据，但金额都低于要求报告的阈值。

拆分交易可在包括银行业、资金服务企业和赌场在内的很多场合或行业进行。“拆分洗钱法”是拆分交易中一种常见的洗钱法，该方法利用多人存储多笔现金存款或购买多项金融票据或银行汇票，但其额度均不超过报告阈值，以逃避侦测。

现金拆分交易案例



拆分交易是异常活动报告中最常见的交易形式。以下为一些常见案例：

- **客户将一笔大额交易分割成两笔或数笔金额较小的交易。**

亨利想要进行金额为 1.8 万美元的现金交易，但了解到一次性存入会超过 10,000 美元的现金报告限额，将被提交货币交易报告，于是他分别在三家银行各存入 6,000 美元。

- **一笔大额交易分割成两笔或数笔金额较小的交易并由两人或更多的人来完成。**

  Jennifer 想要转账 5,000 美元，但了解到在其所在国，转账金额超过 3,000 美元就需要上报，她便自己转账 2,500 美元并请朋友为她转账 2,500 美元。

- **一位中国富人将他的钱财转移至伦敦。**

  李先生将其获得的一百万英镑分为多笔每份为 4 万美元的资金，并通过他的朋友和业务伙伴将之转移至伦敦的一家英国银行里。他之所以不汇到他自己在伦敦开立的银行账户，是因为中国政府对超过 5 万美元的外汇交易采取了管控措施。

  案例分析

  自 1980 年代初期该案例被证实以来，拆分交易就一直层出不穷。尽管该案例已过去很长一段时间，但这种将交易额拆分至报告阈值以下的方法仍然有人使用。

  Isaac Kattan 是位旅行社老板。他被控参与清洗毒资，金额约为每年 5 亿美元现金。不同城市的快递人员会来到他的住处，留下成箱成包的现金。这些人是毒品分销者的信使。资金用来向哥伦比亚的供货商付款。达德郡的大美洲银行是 Kattan 最喜欢的存钱场所。在收受其贿赂后，该银行主管在接受大量现金存款时不会提交现金交易报告 (CTR)。

  Hernan Botero 也被控参与洗钱，但数额比 Kattan 小。他每年在自己位于棕榈海滩附近的住处清洗约 1 亿美元的非法资金。Botero 在美国受到指控，联邦法院的证据表明，他曾通过贿赂位于佛罗里达州种植园的地标银行 (Landmark Bank) 的主管和员工来存入资金。存款几乎每天都源源不断地从 Botero 的前台公司运来至银行。这些资金从地标银行汇入哥伦比亚银行在迈阿密的账户。然后这些资金可以轻易汇回哥伦比亚。Kattan 和 Botero 被判在联邦监狱服刑 30 年。

外国洗钱经纪人的交易拆分流程如下所示：

1. 替外国洗钱经纪人工作的拆分洗钱人员使用真名或假名在 A 国开立大量支票账户。有时这些拆分洗钱人员会利用洗钱经纪人提供死亡人员的身份证明文件去开户。
2. 拆分洗钱人员使用洗钱经纪人提供的资金去开户，账户金额通常是不太显眼的一两千块钱。
3. 为了减少银行的怀疑，洗钱经纪人有时会在该账户存入用于支付生活费用的额外资金，用以表明该账户的合法性。

4. 一旦开户成功，拆分洗钱人员就在刚领取的支票上签名，收款人、日期和金额处则保持空白。
5. 他通常以快递的方式将已签名的空白支票寄给 B 国的洗钱经纪人。
6. 拆分洗钱人员可用同样的方法开立二十几个支票账户。洗钱经纪人在 A 国同时拥有 20 多个支票账户的情形并不少见。
7. 每当支票账户的金额积累到几千美元时，洗钱经纪人就签发支票，用以支付从 A 国出口货物到 B 国的货币经纪人客户，从而清空账户。
8. B 国的洗钱经纪人可使用成百上千个这样的账户，这样每年就有数千万美元通过这些账户得到转移。

微型拆分交易

另一种将大额现金存入金融系统的形式为“微型拆分交易”。微型拆分交易与拆分交易本质相同，但其交易级别更小。在存入 1.8 万美元时，微型拆分交易不会只将资金分两笔存入，而可能会拆分成 20 笔交易，每笔金额在 900 美元左右，令可疑交易更难察觉。

在哥伦比亚贩毒集团一案中，美国毒品销售人员使用与账户相关联的提款卡将现金所得存入纽约的账户。这些提款卡由哥伦比亚的同伙持有。资金定期存入账户，由哥伦比亚同伙收取，再转给毒枭。在一个发生在纽约的案件中，有人因在曼哈顿各家银行逐个存款而被执法部门追踪。当执法部门拦截他时，他持有 16.5 万美元的现金。

侦测微型拆分交易的方法包括：

- 使用柜面存款单而非预制存款单。
- 在开立账户后立即频繁地进行活动，所留的文件非常初步且不完整。
- 频繁存入与典型企业或个人银行活动不一致的微小金额。
- 存入现金后在 ATM 提取，特别是在高风险国家或地区提取。
- 没有明显业务联系的第三方向企业账户存入现金。

信用合作社和住房互助会

信用合作社，亦称为住房互助会，非盈利性质，是由成员持有并运营的民主型金融合作性组织。

信用合作社没有客户；该组织的成员同时也是所有人。信用合作社为会员提供所需的金融服务，依照“一会员一表决权”的理念开展管理工作。会员必须购买合作社的初始资本份额，才能享受其提供的产品和服务。信用合作社的会籍以储蓄者和借贷者的共同点为基础，他们可能来自同一社群、机构、宗教或工作单位。

各信用合作社的规模和复杂程度可能会大相径庭。成员数量从几百名到数十万名不等，所管理的资产也可能达到数百亿美元。各信用合作社服务领域也有所不同，有些仅满足成员的一些特殊需求，而有些则提供大多数零售银行都提供的全套产品和服务。

多数信用合作社主要为社群成员提供个人银行业务。由于各信用合作社采取的成员吸纳模式不同，其中有些合作社还可能吸纳中小型企业或机构账户持有人为其成员，但这一做法在某些司法管辖区是遭到禁止的。通常，信用合作社不参与贸易融资，不建立代理银行服务关系，也不与大型企业，特别是有国际银行业务需求的企业建立联系。

在许多司法管辖区，信用合作社依靠中央信贷机构开展各项服务。中央信贷机构就如信用合作社的贸易协会。它由多个信用合作社共同所有，帮助这些合作社解决其金融需求。服务包括与资金流动性相关的业务；与监管义务有关的研究、培训和支持工作；共享包括支票清算和电子资金转账 (EFT) 处理在内的操作或后台流程。通常，他们会帮助各信用合作就共用服务进行协商以达成一致，签订共享合同，使得许多小型信用合作社可以利用规模经济的优势，而这一效果是其无法独立实现的。

在多数国家和地区，对信用合作社的监管要求和监督与银行十分相似。他们拥有和银行相似的资本、流动性和风险管理、账目记录及报告义务，但由于各机构各自受到来自地区或联邦监管机构及监管措施的监管，因此不同机构间受到的监管可能存在细微差异。FATF 将信用合作社列为“金融机构”，因此遵循 FATF 建议的国家级反洗钱 / 反恐融资制度对信用合作社采取了与银行类似的监管措施。

英国反洗钱联合指导小组 (JMLSG) 在 2006 年 11 月发布的指南中表示，尽管信用合作社因平均规模小，产品数量少，面临的洗钱风险较低，但它们也容易被洗钱和恐怖融资活动者所利用。JMLSG 发现信用合作社提供的金融服务越多，洗钱的潜在风险就越大，因为信用合作社（或住房互助会）倾向于覆盖更大的客户群，并可能为潜在犯罪分子提供更多用来隐匿其非法所得的途径。

JMLSG 在 2014 年 11 月发布的指南中，将高风险交易归纳为：向第三方转账，第三方以现金为他人付款以及开户时不愿意提供身份信息。鉴于信用合作社通常交易数额较小，其成员的活动符合常规，因此该指南指出，交易额高于正常数额以及成员表现异常也应被视作洗钱活动的危险信号。

JMLSG 甚至建议信用合作社监控儿童账户中的异常活动，因为家长可能本着此类交易更加掩人耳目的想法，将儿童账户中的资金用于非法目的。此前曾发生过破产的公司利用儿童银行账户继续运营的案例。

非银行金融机构

信用卡行业

信用卡行业包括：

- 信用卡协会，如美国运通、万事达、威士之类的机构，这些机构允许其会员银行发行信用卡，授权商家接受这种信用卡，或两个功能兼具。
- 发卡银行：吸收潜在客户并发行信用卡。
- 收单银行：处理接受信用卡商家的交易。
- 第三方支付处理商 (TPPP)：与发卡银行或者收单银行达成协议，为商家和其他商业实体提供支付处理服务，尤其是代表与第三方支付处理商的金融机构无直接关系的商户展开交易。

信用卡账户不太可能被用于洗钱的处置阶段，因为该行业通常限制现金支付。它们更可能被用于洗钱的离析和融合阶段。

案例

洗钱犯罪分子 Josh 用事先投入银行系统的非法所得预付信用卡，在其账户中创建贷方余额。此后，Josh 申请信用卡退款，以此进一步模糊资金来源，从而完成离析。然后，他使用已存入银行账户的非法资金和信用卡退款购买了一套厨房设备。通过上述步骤，他成功将非法资金融入金融系统。

洗钱犯罪分子可以将非法资金存入离岸银行的账户，然后使用与该离岸账户相关的信用卡和借记卡存取资金。同样，他也可将现金转入监管较松的离岸司法管辖区，存入离岸银行并通过信用卡或借记卡存取这些非法资金。

2002 年，在一份题为《通过信用卡洗钱的未知领域》的报告中，美国国会监督机构——美国政府问责办 (U.S. Government Accountability Office) 列举了如下多个利用信用卡洗钱的虚拟场景。“洗钱犯罪分子在美国设立合法公司企业作为非法活动的‘前台’。他们在总部位于美国的银行中开立银行账户并以‘前台公司’的名义获得信用卡和提款卡。将来自非法活动

的资金存入美国的银行账户。在美国银行设有分支机构的另一个国家，他们使用信用卡和提款卡从美国银行账户中提款。资金由位于美国的同伙存入并用于信用卡还款或预付信用卡。银行的在线服务使得支票账户和信用卡账户间的资金转账成为可能。”

第三方支付处理商

第三方支付处理商 (TPPP) 一般是银行客户，为商家和其他商业实体提供支付处理服务，它们使用自己的商业银行账户为商户处理支付事宜。它们通常不受反洗钱 / 反恐融资规定约束。

传统上，它们与在美国拥有实体营业场所的零售商（即商户）签订协议，帮助其收取客户应付资金。所涉交易主要包括信用卡支付，此外还包括自动清算中心 (ACH) 借记和远程支票 (RCCs) 或即期汇票存款。随着互联网的普及，TPPP 的服务对象现涉及本国和其他国家的商家，除传统零售商外，还有互联网企业和预付费旅游及网络游戏企业。TPPP 代表商户与金融机构进行交易，且当前服务范围逐渐扩大，令金融机构难以识别真正的交易主体。

TPPP 服务的各类商户令其极易受到洗钱、身份盗用和欺诈等非法活动的利用。例如，为电话推销、赌博（在线赌博、赌场等）或在线商户提供服务或远程支票的第三方支付处理商对金融机构造成的风险更大，因为这些机构极有可能涉及客户欺诈和洗钱活动。

TPPP 风险案例：

- **与多家金融机构建立关系：** TPPP 可能与多家金融机构保持业务关系，令金融机构难以查明其完整的客户关系。这是参与可疑活动的 TPPP 有意为之，目的是妨碍金融机构识别可疑活动和退出业务合作关系。
- **洗钱：** 犯罪分子可能会利用 TPPP 掩饰交易，并清洗犯罪所得。其中一种方式是通过国际自动清算中心从国外直接将资金汇至金融机构。TPPP 所进行的交易数量之多导致这种活动无法被识别出来。
- **未授权交易的高回报率：** 参与可疑活动或被犯罪分子利用的 TPPP 所获得的未授权交易回报率可能高于平均水平。在商业层面，违法商家的回报率与 TPPP 总交易额相比或许尚可接受，但与个人发起者相比，其回报率明显偏高。

应谨记，无论是 TPPP 还是其他金融机构开展的信用卡交易，巨大的交易额都并非“可疑”或“异常”活动的必备条件。例如，可能存在为数众多的小额交易、无法辨别其模式的回头客、捐赠者或接收国际捐款或其他支付的交易，这些交易的信息与客户提供的公司信息或其历史活动不符。因此，有必要实施严格的客户增强尽职调查和交易监控措施，以监测出可疑活动及不宜与之建立业务关系的客户。

货币服务企业

FATF 将货币服务企业 (MSB) 或资金转账或价值转移服务 (MVTS) 定义为转账或兑换货币的机构。这些机构通常提供货币兑换、转账、支票兑现和汇票服务。

各司法管辖区的货币服务企业法律有所差异。例如美国金融犯罪执法网络 (FinCEN) 规定，具有以下一项或多项能力的个人，无论是否长期经营，无论是否以有组织机构的形式存在，均视为货币服务企业：

- **外汇交易商：**此类货币服务企业提供货币兑换服务（如美元兑换为欧元）。通常位于各国边境处、机场和外籍人口多的社区附近。
- **支票兑现公司：**零售商或独立的公司均能提供支票兑现服务。根据其运营模式，货币服务企业为客户或商业机构兑换支票。除支票兑换外，此类货币服务企业还提供其他金融服务，如账单支付、购买汇票及国内或国际转账。
- **旅行支票或汇票发行机构：**旅行支票或汇票发行机构负责处理支付事宜，通常利用代理机构销售流通票据。
- **货币转移服务商：**货币转移服务商接收货币或资金后，通过金融代理商、机构或电子资金转账网络进行转账。著名的货币转移服务商有西联汇款、MoneyGram 和 PayPal。
- **预付存取服务供应商或销售商：**事先向预付存取服务供应商支付资金或资金价值，之后可通过电子设备或工具，如卡片、密码、电子序列号、手机验证码或个人身份证号等工具取回或进行转账。预付存取方式也可称为储值卡。预付存取有开放式和封闭式两种：
  - **开放式预付费卡**可在支持该卡支付网络的商家处购买商品，也可在与相关网络相连的自动柜员机上取得现金。开放式预付存取卡通常印有美国运通、Visa 或万事达卡等网络的标识。
  - **封闭式预付费卡**通常仅限在发卡商户处购买商品或服务。预付存取销售商指在某一天预付存取超过一定阈值的人。
- **美国邮政署：**美国邮政署销售汇票，因此也视为货币服务企业。

金融犯罪执法网络在 2012 年颁布的一份最终规定中对货币服务企业的定义进行了详细说明，规定应根据企业在美国境内的经营活动判定其是否是货币服务企业，而不是其是否在美国设有实际代理商、代理机构、分支机构或办事处。该最终规定也表明，随着互联网等技术的发展，位于其他国家的企业也可以为美国个人或机构提供货币服务。无一例外，所有货币服务企业均必须在美国金融犯罪执法网络登记。

而加拿大规定，货币服务企业指参与外汇交易，资金转账，或者向公众兑现或销售汇票、旅行支票等金融票据的企业。此类企业必须在加拿大金融交易和报告分析中心 (FINTRAC) 登记。

货币服务企业可以是小型、独立企业，也可能是一家大型跨国机构。其可能以货币服务为主营业务，也可将之作为主营零售店铺业务的附属服务。以货币服务为附属业务的企业通常包括杂货店、药店、餐厅和酒吧。它们的经营行为包括但不限于工资支票兑换和预付卡销售活动。大多数货币服务企业都拥有实体经营场所，但只在互联网上经营，不设实体办事处或代理商网络的货币服务企业数量正逐渐增加。

传统的货币服务企业通常为服务需求未被满足或未开立银行账户的个人提供服务。这促使此类企业在银行服务不足或不存在的地区经营业务。另外，与金融机构相比，他们的某些服务费用通常较低。例如，通过金融机构进行国内或国际电汇既耗时，又耗费成本。而通过货币服务企业进行相似的交易耗时短且成本低。除电汇服务外，他们还提供账单支付、发薪日贷款和商业支票兑现等服务。

货币服务企业分为委托企业和代理商。委托企业主要提供货币服务，发行汇票和旅行支票或提供资金转账服务。在美国，委托型货币服务企业必须制定书面的反洗钱政策、流程和内部控制措施，指定反洗钱官，提供反洗钱培训，开展独立审查 / 审计，并监控交易中是否存在可疑活动。

代理商除其自身的产品和服务外，另提供货币服务类服务。代理商可以是以支票兑现为主营业务的委托型货币服务企业，但其资金转账服务通过委托型资金转账服务商完成。使用此类资金转账服务的代理企业必须与委托型货币服务企业签订代理服务协议。建立委托 / 代理关系有助于委托型货币服务企业扩大服务范围和市场份额，但不会带来额外开销。委托型货币服务企业的代理商须与委托型货币服务企业遵守相同的联邦和州法规（如反洗钱程序和可疑活动监控）。

以下是货币服务企业被犯罪分子利用的案例：

- 近年来，医疗业的欺诈案件大幅增加。有欺诈行为的医疗公司（如家庭医疗公司）将欺诈获得的支票交给支票兑现公司，他们知道这些公司不会索要付款人的身份证明，不会报送或者报送错误的现金交易报告 (CTR)，也不会将他们的可疑活动报告给政府。此类支票兑现公司中可能存在犯罪分子的内线，或者认为相关法律法规会给客户造成负担，不惜违反相关规定为客户减轻此类负担，从而为经营业务提供便利。

- 犯罪分子通过缩减员工工资，以极低的成本获得工伤保险保单。获得保险证明后，组织者们再将这些证明“出租”给个人或企业，赚取费用。因为这些保单以欺诈方式获得，员工将不再受到保障，如果发生工伤，将面临高昂的医疗费用。犯罪分子通过在货币服务企业兑现支票来隐藏薪资，进而规避特定的记账措施。犯罪分子靠此获得巨额利润，却严重损害了员工的利益。
- 洗钱犯罪分子利用汇款经纪机构和货币兑换所，用当地货币向目标国的犯罪组织提供资金。洗钱犯罪分子/经纪人随后将犯罪所得的美元出售给那些希望合法购买货物用于出口的外国商人。

  案例分析

  本案例取自 FINTRAC 针对加拿大货币服务企业发布的《洗钱类型和趋势》报告。

  两名嫌疑人涉嫌大众营销欺诈案。这两名犯罪分子利用货币服务企业对美国居民实施欺诈行为。他们向美国居民寄送假支票，令其返还部分资金。

  其中一人拥有两个身份和多个地址，是大多数通过货币服务企业电子资金转账的受益人。他（或她）在短时间内有规律地收到美国欺诈受害者的电子资金转账。几乎所有的转账金额都低于规定的阈值，因此在对其金融活动产生怀疑之前，该犯罪嫌疑人已收到了许多电子资金转账。一年中，有超过三十六份针对该嫌疑人的可疑交易报告。

  另一个人与其居住地址相同，但显然该地址从未在收取电子资金转账时使用过。该嫌疑人被认为是此欺诈案的主谋，因为他（或她）曾数次被判犯有欺诈相关罪行。在政府收到过的一系列多重现金存款报告和货币服务企业支票存款报告中，他曾被标识风险较高。他还收到过来自欧洲的欧元电子资金转账。

  而电子资金转账主要收款人（拥有两个身份和八个地址的人）可能利用了多家货币服务企业代理商（分布于近二十个不同地点），试图掩饰其欺诈行为。他利用货币服务企业发行的支票进行支付。一家银行提交的可疑交易报告指出，他用现金和支票在两个不同的银行账号中进行了多笔存款。

关于货币服务行业最大的误解就是认为其缺乏监管。事实上，许多货币服务企业都接受着国家级和地方级监管者的多重监管，并且一般都制定了反洗钱合规制度。此外，他们还受与其保持业务关系的银行的监控。但是，不同的货币服务企业接受的审查在程度上各不相同，而出现这一情况的主要原因是一些货币服务企业设立的要求十分简单。此外，许多货币服务企业规模较小（即只经营一个商店），与大型全国企业相比，反洗钱制度相对薄弱。因此银行在与货币服务企业建立业务关系时，尽职调查最重要的一个方面就是要确认该企业执行了健全的反洗钱制度（如相关程序、培训和可疑活动监控），在其进行经营活动的司法管辖区有合法执照并登记。

保险公司

保险公司为世界各地的客户提供风险转移、储蓄和投资产品，服务对象覆盖各种类型，包括个人、大型机构和政府等。保险业运营方式中很重要的一点是保险公司经营的大多数业务通过代理商或独立经纪商等中间机构进行交易。除特殊情况外，保险公司须遵守反洗钱规定。

与其他金融机构相比，保险业的洗钱风险相对较低。例如，财产、意外事故、产权或健康保险单不具有投资性质，无法累积现金，无法选择在不同个人间转移资金，也不能以其他方式隐藏或转移资金。即便如此，保险业的一些部门，如人寿保险和年金，也是洗钱和恐怖融资犯罪分子的首要目标。保险行业对洗钱的敏感性在很多方面与证券行业相似，在某些司法管辖区，人寿保单被视为类似于证券的投资工具。

FATF 2004 - 2005 年度洗钱类型报告指出，整个保险业中，人寿保险最受洗钱犯罪分子的青睐。人寿保险产品覆盖范围广，灵活度高，同时回报率也不容忽视，因此具备进行大额投资的条件。许多人寿保单会在投保人死亡后，支付一笔固定金额的赔偿金，也有一些人寿保险产品，如终身人寿保险，还具有投资价值，这类保险在保单持有人取消后，还可产生额外的现金价值。这些特点在为保单持有人带来巨大价值的同时，还为洗钱犯罪分子提供了诸多机会，可将其非法所得合法化。最常见的类型通常涉及国际交易，表明保险业的洗钱行为已拓展至跨境交易。

没有退保金额的人寿保险产品对洗钱犯罪分子吸引力最小。有退保金额且可从保单首日起指定受益人的保险产品吸引力最大。

年金则是另一种具有现金价值的保单类型。年金是一种投资，在预付一笔资金后，它会在未来进行一系列定期支付。

年金合约可能使犯罪分子有机会利用非法资金来获得即期的或是延迟支付的收益流，这种收益通常从特定日期开始按月支付。在两种情形下，保单持有人可将大笔资金放入保单并期待基于这一投资获得固定或可变的资金增长。当潜在的保单持有人更加关注保单的取消条款而非收益时，就有存在洗钱的可能。

保险行业的脆弱性表现在:

- **缺乏对中介机构的监管和控制:** 保险经纪人对保单具有很大的控制权和自由度。
- **对销售人员的监督过于分散:** 保险公司可能拥有完全受控于保险公司的员工（即专属代理人）。非专属代理人提供保险公司的产品，但并非保险公司员工。他们与多家保险公司合作，为客户提供最佳产品组合，可能因游走在不同的保险公司间而被忽略。如果他们中有人与洗钱犯罪分子联手，就可能会努力去寻找反洗钱监控措施最薄弱的保险公司。

- **以销售业绩为目标：**经纪人所关注的是销售保险产品，因此他们通常会忽略各种洗钱信号的存在，如缺乏对财富的解释或用异常方法支付保费。

通过保险公司进行洗钱的示例包括：

- 有些保单以单位信托或共同基金的形式操作。客户可以溢资投保，并在支付提前退保罚金后将资金转入或转出保单。当保险公司（如以支票的形式）返还这笔资金时，洗钱者就成功地模糊了资金与犯罪活动之间的联系。
- 购买或赎回整付保费保险债券是主要的洗钱工具。该债券可以从保险公司购得并在债券到期前折价赎回。此时，保险公司会以“洗净的”支票形式支付债券余额。
- 保单撤销期允许投资者在签署保单并支付保费后的短时间内撤销保单且无需支付罚金。这一流程使得洗钱者有机会获得保险支票，以此证明资金的合法性。但是，随着越来越多的保险公司受反洗钱制度要求约束，此类洗钱的侦测和报告更为容易。
- 当潜在的保单持有人更加关注保单的取消条款而非收益时，就有存在洗钱的可能。洗钱者用非法资金购买保单，然后告诉保险公司他已改变主意，不再需要这份保险。在支付罚金后，洗钱者赎回保单并获得一张由声誉良好的保险公司开据的干净支票。

FATF 2004 - 2005 年度洗钱类型报告中指出了更多保险业存在的洗钱类型：

- 签订保险协议时，由未曾进行正常身份识别程序的第三方（即非保单持有人）支付保单。保险公司并不清楚资金来源及保单持有者和该第三方的关系。
- 客户实际上并非寻求保险的保障，而是将之作为投资机会。犯罪分子可以用大笔资金购买多份人寿整付保费保单，作为一整套投资保单，以进行洗钱。另一种方式是用大笔保费存款支付年度保费。此类保单与整付保费保单一样，客户可通过其利用保险公司进行巨额投资。由于年度保险费必须全额支付，因此反洗钱风险较低的人寿保险产品也具有高风险整付保费保单的一些特征。

保险业的大多数业务均通过中介机构展开。因此，出现洗钱活动的主要原因是中介机构在对反洗钱监管规定的遵循上表现不佳。

公司在评估洗钱和恐怖融资风险时，必须考虑其是否允许客户：

- 使用现金或现金等价物来购买保险产品。
- 以整付保费或一次性付款形式购买保险产品。
- 以保险产品的价值作抵押进行贷款。

证券经销商

证券行业因不同公司的反洗钱制度存在差异，且交易额巨大，为犯罪分子提供了秘密洗钱和恐怖融资的机会。储蓄银行业的规模与全球资本市场相比，实乃小巫见大巫。据世界银行统计，2015 年仅上市公司的市场资本总额就高达 61.7 万亿美元。

早在 1992 年，FATF 就和国际证券事务监察委员会组织 (IOSCO) 合作，敦促加强对证券业的反洗钱监控。IOSCO 的总部设在蒙特利尔，是一个致力于监管证券和期货市场的全球性政府间组织，商品期货交易委员会 (CFTC) 也是其会员之一。也是其会员之一。打击证券领域的洗钱活动面临一个难点，即证券行业几乎不涉及现金。电子转账和票据是该行业运作的方式。一般来说，洗钱者会在通过其他方法在金融系统中处置好现金后，再利用证券部门洗钱。

该行业存在洗钱风险的原因在于:

- 国际性。
- 交易速度。
- 在不对本金造成重大损失的前提下将持有证券转换成现金的便利性。
- 在多个司法管辖区之间发出、接收或中转电汇的常规用途。
- 竞争激烈、佣金驱动的行业环境（正如私人银行一样，这一点成为忽视客户资金来源的强大动因）。
- 经纪公司可作为代名人或受托人持有证券账户的做法，允许隐匿实际受益人的身份。
- 反洗钱制度薄弱，未建立有效的客户尽职调查、可疑活动监控等控制措施。

通过证券部门清洗的非法资金可能来自部门内外的非法活动。对于源自部门以外的资金而言，通过证券交易成立法律实体可以隐匿或模糊资金来源（即离析）。对于证券市场内部的非法活动（如挪用、内幕交易、证券欺诈、市场操纵），这些交易或操控获得的非法资金必须进行清洗。在这两种情况里，证券部门为洗钱犯罪分子带来了两大优势: 既可以清洗非法所得，又能获得额外利润。

在证券行业，洗钱可以通过仅用于存放资金而非用来交易的客户账户进行。这样，洗钱犯罪分子就可以规避他们认为具有更严厉反洗钱控制措施的银行渠道。“洗售”或对冲交易是洗钱的其他表现形式。这些交易涉及对特定证券的撮合交易，从而制造交易的假象。洗售通过多个账户来生成盈亏抵消，并在表面上不受共同管理的账户间转移仓位。

FATF 2009 年发布的《证券行业洗钱和恐怖融资活动类型报告》指出下列领域的洗钱风险最高：

- 批发市场
- 不受管制的基金
- 理财
- 投资基金
- 不记名证券
- 汇票

证券业面临的独特挑战包括：

- **证券的多样性和复杂性**

证券既有为针对某个客户需求而量身定制的产品，也有为一般大众提供的产品。既有简单易懂的大众型产品，也有相对复杂、专业性较高的产品。要解决证券业存在的风险，应对基本证券知识加以了解。

- **高风险证券**

尽管大多数证券由正规公司发行，但不受监管或因非法目的发行的证券仍存在风险。在美国，不在交易所进行交易的证券通常在场外进行交易，具有多个层级，如“粉单市场”，这些交易仅需进行极少的申报，因此使得隐藏受益所有人等信息变得十分容易。这种情况不利于确定是否与受制裁司法管辖区或公司存在联系。证券公司不仅需要识别有风险的证券，还需要制定流程，限制各个平台上进行的证券交易。

- **多层风险和第三方风险**

证券业涉及众多参与者，包括金融机构、证券经销商、财务顾问、汇款代理、证券贷方、保管人、中介经纪商和销售代理机构。多层的中介机构中还可能包括跨境组织，使得控制措施标准化难以实现，进而给整体合规带来了挑战。

FATF 指出了全球证券市场存在的可疑活动标志。与证券行业更相关的可疑信号包括：

- 证券公司的一位老客户突然变现所有资产，将其在某一司法管辖区的财富转移出来。
- 客户不顾损失、佣金或其他账户或产品相关费用，开立账户或购买产品，包括提前取消长期证券。
- 证券账户用于支付或向外电汇，但证券交易活动很少或没有（如用作存款账户或转账渠道的账户）。
- 客户的交易出现持续损失。这一情况可能是将价值转移至另一方的信号。
- 一方以高价购进但亏血本出售给另一方的交易。这一情况可能是将价值转移至另一方的信号。
- 客户不熟悉某金融产品的业绩和详情，却仍希望进行投资。
- 客户有亲友在证券发行商工作，或从客户的交易模式可以看出其掌握了非公开信息。
- 同家证券公司的两个或多个不相关账户突然同时就一项非流动或低价证券（低价股票）进行交易。
- 客户存入符合下列条件的证券：1) 数量多，2) 账户名称异常，3) 按经验应制定约束性说明，但实际没有制定，或 4) 获得证券的方式不合理。

  案例分析

  2016 年 6 月，一家注册证券经销商 Albert Fried & Co. (AFCO) 因未能按联邦证券法规规定监控客户交易以识别可疑活动，被美国证监会起诉，后达成和解。客户 A 在四个月内通过 AFCO 买进卖出四只低价股票，共计 1.19 亿股。其中有一天，其交易占单只股票日成交额的 85%，其他大多数时间的交易占 50% 以上。

  有许多危险信号本应引起 AFCO 注意，使其可以进一步开展调查或报告，例如：1) 客户进行交易时，股票发行商正在进行宣传，2) AFCO 知道客户 A 在 AFCO 账户买入该发行商的证券后不久，该发行商就开始执行 5:1 的反向股票分割计划，3) 因客户 A 在至少三个证券上的交易，AFCO 接受了数次监管和刑事调查，以及 4) 客户 A 售出该发行商的证券后仅 3 个月，证监会就中止了该发行商股票的交易。

各证券经销商有义务监测危险信号，并实施额外的尽职调查，在低价股票交易显示异常时更应如此。在证券业中，犯罪分子利用证券经销商清洗犯罪所得或实施欺诈的现象十分普遍。加拿大金融交易和报告分析中心 (FINTRAC) 提供了一个类似案例，值得大家研究：

案例分析

公司 X 的股票在美国进行场外交易，一个犯罪团伙涉嫌操纵公司 X 的股价，该行为一般称为“哄抬股价，逢高卖出”。嫌疑人 1 以低价买进该公司的股票。该团伙对公司发展前景进行虚假报道，令其股价迅速攀升，这是哄抬物价的一个常用手段。据执法机关称，犯罪分子在股票上涨后出售股票，然后通过一个有组织犯罪团伙清洗其出售股票所得的资金。

再由嫌疑人 2 将公司 X 的股份证书存至一个经纪账户中。该嫌疑人被怀疑是上述有组织犯罪集团的代名人。存入股份证书后不久，嫌疑人 2 就开始对股票进行结构性销售，这是该类欺诈中“逢高卖出”阶段的特征。抛售股份后，嫌疑人 2 申请以保付支票的形式提前交割。

保付支票存在嫌疑人 2 在与该经纪公司无关的一家金融机构开立的账户里。嫌疑人 2 又向位于美国中部的一家公司进行多项电子资金转账，该笔转账的受益所有人为嫌疑人 1。

零售证券经销商是该产业的前沿防线，也是最为脆弱的地带。管理层经常向其施压，要求其开发更多客户并争取更多资产。客户账户中的资产越多，他们获得的佣金就越多。洗钱者可能通过允诺高额或固定的佣金来利用这一点。因此，证券经销商有必要了解其交易对象，并监控可疑活动。

在美国，证券交易委员会 (SEC) 和金融业监管局 (FINRA) 在《银行保密法》的指引下，要求证券经销商，无论大小，均须执行反洗钱制度，包括设立反洗钱专职岗位、进行客户尽职调查、可疑活动监控、培训和独立审计。还规定证券经销商受证监会和 / 或金融业监管局监管，以监控其是否遵守了反洗钱监管规定。未执行反洗钱监管规定或执行存在缺陷的证券经销商，可能会面临巨额罚款及刑事处罚。

非金融行业

赌场

赌场是最能生成现金的行业之一。一掷千金的赌客、巨额利润、信贷融资以及其他各种因素相互结合，推动大量现金在赌场与赌客间来回流动。在法律允许经营赌场的地方，客户和赌场间的现金流高达数十亿美元。

赌场以及其他博彩相关业务，如赌马、抽奖和赛马等，仍与洗钱犯罪活动有着紧密联系，因为它们为新近获得且没有明显合法来源的财富提供了很好的借口。赌场提供的服务因其所在的管辖区和该管辖区采取的反洗钱的措施不同而有所不同。

通过赌场洗钱通常发生在处置和离析阶段，如将待清洗的资金从现金转换成支票或利用赌场信贷，增加一层交易，再将资金转出。洗钱者可用犯罪所得的现金购买筹码，而后又要求赌场通过支票形式向其兑付。赌客通常不会要求其用现金购买筹码的那家赌场使用支票进行兑付，他表示自己将去国外旅游，而该赌场恰好也在该国设有连锁赌场，赌徒希望这笔款项能在外国赌场使用，然后在该国使用支票提取资金。洗钱犯罪分子还可取得赌场信贷额度，再利用非法所得资金进行偿还。

FATF 在 1997 - 1998 年度洗钱类型报告中指出，博彩企业和彩票在洗钱活动中的使用日益频繁。在报告中，FATF 提供了毒贩利用赌场和其他博彩设施洗钱的案例。以下为一种与赛马和博彩相关的洗钱手法：当某人确定要通过赌博清洗脏钱时，他首先要明确其赌注中最终可通过赌博机构支票或转账赎回的数额，且这笔资金与博彩所得相同，并完全可以验证。这种方法更难侦测，因为此人确实接收了博彩收益。

赌博公费旅游是一种以赌场为基础的旅行方式，同样具有极大的洗钱风险，因为公款消费客户主要通过第三方，即赌场中介将资金转移至国外，并通过多家赌场进行多层交易，以掩饰资金来源、资金所有权和赌客的身份。在一些司法管辖区，赌场还可与赌场中介签订协议，出租私人赌博室。有时，赌场中介还会代替赌场来监控赌客的活动，发放和收取赌场信贷。另外，一些司法管辖区还允许赌场中介收集资金，以掩饰各客户的消费情况。一些地区的持证赌场中介可能是其他国家赌场中介的挂名机构。此类挂名中介通过赌场的持证赌场中介为赌场提供客源，而该持证赌场中介可能无法在赌场所在国取得执照。这些无证次级赌场中介可作为无证信贷收取机构，并可能会与有组织犯罪网络有联系。这将带来极大的风险，可导致赌场与赌场中介间达成非正式合作，违反反洗钱 / 反恐融资规定。

FATF 在其 2009 年的一份报告中指出一些司法管辖区未对赌场中介及其代理机构的营业资格进行规定，令上述风险进一步上升，报告强调需确保赌场中介运营商受刑事规定约束，进行透明的金融交易，采取相关的反洗钱 / 反恐融资举措。

金融犯罪执法网络 2008 年指导意见和 FATF 2009 年赌场和赌博业报告中指出了以下需特别注意的行为：

- 试图逃避反洗钱报告或账目记录规定的行为，如：
  - — 客户在短期内，通过一系列货币交易，偿清一大笔信贷，如欠债支票或空头支票，且各交易数额均未超过报告阈值。
  - — 超过两名客户各自均购买少量筹码，进行最低限度的赌博后，要求将所有筹码兑换为赌场支票。

— 客户的奖金超过 10,000 美金，但要求支取少于 10,000 美金的现金，剩余金额以筹码支付。之后该客户去柜台兑现剩余筹码，且金额小于报告阈值。

— 客户通常会通过介入另外一位客户来拆分交易，以避免提交现金交易报告或纳税申报表。

— 如被要求出示身份证明，客户会将需兑现的筹码数量减少到报告阈值以下。

- 在柜台仅要求银行类的金融服务，如：

— 客户向或通过非居住国或非商业运营所在国家的银行 / 非银行金融机构电汇非赌博收益。

— 客户将赌场当做暂时资金存储机构，在短时间内频繁地向赌场账户中存入资金，并要求将其转入国内或国外的银行账户中。

- 进行最低限度的赌博，但无法提供合理解释，如：

— 客户购入大量筹码，但只进行最低限度的赌博，之后再将筹码兑换为赌场支票。

— 客户使用赌场信贷购买筹码，进行最低限度的赌博后，用货币偿还信贷，并将筹码兑换为赌场支票。

— 客户存入大量小面额纸币，再在赌桌上换成筹码，进行最低限度的赌博后，在柜台换成大面额纸币。

— 客户向老虎机里塞入大量小面额纸币（“以钱换钱”），进行最低限度的赌博后或不参与赌博就在游戏层或柜台将领款券换为大面额纸币，或将从老虎机获取的、看似合法的奖金兑换为赌场支票。

— 客户频繁用货币购入筹码，且购买额均小于报告阈值，进行最低限度的赌博后，不兑现筹码。

— 客户转账至赌场，存入挂名账户中，再在赌桌上兑换为筹码，进行最低限度的赌博，之后再将筹码兑换为赌场支票。

- 异常赌博和交易模式，如：

— 两位客户频繁大额赌博，进行对赌，如：

> 在轮盘赌中“红黑”或“单双”均选；

> 在百家乐中，“跟庄”和“不跟庄”均选；

> 在花旗骰中，“过线”或“来线”与“不过线”或“不来线”均选。

— 在体育赛事下注中，客户定期下对注（即同时赌两支球队赢），确保总损失降至最低（称为“两面下注”）。

— 客户要求签发可在第三方支付的赌场支票，或收款人不明确的支票。

— 客户用多种票据（银行本票、汇票、旅行支票或外国汇票）存入巨额存款或偿还大笔欠债支票，但金额少于 3,000 美金，以避免进行身份验证。

— 客户从储蓄账户中取出巨额现金，要求签发多张赌场支票，每张支票金额低于 10,000 美元。

— 客户在账户中存入巨额资金，长时间不使用后，取出或转账。

不仅个别行为存在洗钱风险，赌场所选择的客户种类也容易引发风险。赌客进行高额赌博后，就被视为豪赌客户，之后可不对其进行尽职调查，这将使赌场无法明确其资金来源。在无法确定赌博资金来源的情况下即允许赌客赌博，这一做法可能导致赌场犯下弥天大错。美国财政部可能会在近期发布规定，要求美国的赌场查明豪赌客户的资金来源。尽管现有法规并未就查明资金来源做出明确规定，但建议赌场获取某些客户的更多信息，及时发现国际电汇和大笔现金储蓄等高风险交易，将此措施作为风险为本方法的一部分。

美国金融犯罪执法网络对行业中缺乏反洗钱制度的几家超大型赌场进行了处罚，展现了对该问题的重视：

- **天宁皇朝酒店和赌场 2015 年被处以 7,500 万美元罚款**——该赌场未能制定并实施反洗钱制度（没有专门的反洗钱专员，缺乏反洗钱政策和程序以及独立的反洗钱制度检验措施），导致赌场未提交数千份现金交易报告，赌场内的员工还帮助 VIP 客户进行可疑交易（特别是拆分交易）。

- **Trump Taj Mahal 赌场 2015 年被处以 1,000 万美元罚金**——该赌场没有设立有效的反洗钱制度，未提交可疑活动报告和现金交易报告，也未进行适当地记录。

- **凯撒宫 2015 年被处以 950 万美元罚款**——该赌场“对于某些获利最高、风险最大的金融交易，没有进行申报”，在全世界推行私人沙龙，但并未对电汇等交易进行合理的监控，以监测可疑活动，并公开允许客户匿名赌博。

- **Sparks Nugget 2016 年被处以一百万罚款**——该赌场的“合规制度出现系统性瘫痪”，合规部经理未发挥作用。Sparks Nugget 命令其合规部经理减少与监管审查部门的来往，令其无法查看完整的监管测试报告文件，也无法正确编制可疑活动报告。

除进行合适的记录和申报外，赌场在其反洗钱 / 反恐融资制度中还应制定相应流程，令赌场在接受客户资金准备赌博前，即能确定资金来源，进行客户尽职调查，而不单单依靠事后合规调查。

尽管对赌场来说，进行增强型客户尽职调查 (KYC) 和资金来源查询的要求刚刚兴起，但现已有一些工具专门针对该行业的调查。最佳流程应能结合各种国际来源的信息，包括刑事和法庭、证券交易机构、金融机构、政府和世界各地列出的各种名单、政治公众人物或事件、负面新闻和商业机构，还能进行身份验证，在运营第一线即开展尽职调查。

案例分析

2013 年，美国司法部对拉斯维加斯金沙集团的洗钱调查一案发布最终结果，该集团最终支付 4,700 万美元进行和解，以避免对其豪赌客户在拉斯维加斯的赌博进行刑事诉讼，特别是在墨西哥拥有一家制药工厂的墨西哥华人叶真理。

在 2006 和 2007 年间，叶真理在金沙集团主要以电汇和银行本票方式存入五千多万美元，据称该资金主要是非法生产合成药物的犯罪所得，所得收益达 1 亿美元。2007 年，叶真理在墨西哥住所的 2.07 亿美金遭扣押，这是迄今为止所涉扣押现金数额最高的一起案件。

司法部收集的证据表明，叶真理采取了多项措施，以避免洗钱行为被发现，并运用了多种经典的洗钱方法。叶及其助理通过两家银行和七家墨西哥货币兑换处将现金电汇至金沙集团及其子公司。电汇汇出方是一家公司和个人，金沙集团无法联系到叶真理本人。美国司法部称，叶真理还将资金从墨西哥的货币兑换处转至金沙集团的香港子公司，再从该子公司转至拉斯维加斯。叶真理的多数电汇均缺乏足够信息，无法证明他就是真正的受益人。此外，金沙集团还允许叶真理多次转账至与该集团无关的账户，即 Interface Employee Leasing 的航空服务账户中，该账户的用途为支付公司飞行员的薪水。

赌场无需受到场所限制。近年来，在线赌场和赌博运营的数量持续攀升。尽管在某些司法管辖区，在线赌博需要接受监管，但仍有大量在线赌博公司处于非法运营状态。例如，据英国赌博协会规定，在英国运营业务且设有赌博设备的公司，或设备在英国境外，但通过英国的企业运营业务的公司应获得远程赌博执照。安提瓜和巴布达颁布了互动式赌博规定以管理在线赌博，要求建立合规制度。

然而，在线赌博交易主要通过信用卡或借记卡进行，确实为网络犯罪分子提供了一个很好的洗钱途径。网站运营商主要是不受监管的离岸公司。这会对金融机构产生影响，因为在线赌博网站通常在离岸银行拥有账户，而这些银行又会使用声誉良好的国内代理银行。执法和监管机关很难追踪通过这些账户进行转移的非法资金来源及其所有权。

因为对网络犯罪分子的监管和敏感性不一致，一些信用卡发卡商已开始禁止在在线赌博中使用信用卡。金融机构可浏览商户代码，确认接受信用卡的公司类型以及无卡交易代码（即持卡人不在赌场也可通过读卡器进行交易），从而帮助银行杜绝在线赌博交易。但除信用卡外，还有多种方式可以为在线赌博提供资金，如预付费卡、电汇、点到点转账、虚拟货币和手机运营商账单支付。

MONEYVAL 是评估反洗钱措施特设专家委员会。该委员会是欧洲理事会的常设监督机构。其在 2013 年发布的名为《使用在线赌博进行洗钱和恐怖融资》的活动中指出了多种洗钱类型。包括：

- 洗钱犯罪分子勾结离岸在线赌博运营商，将非法所得资金存入赌博账户，再以奖金的名义取出。在线运营商抽取一定比例的收益作为佣金，洗钱者向税务部门申报奖金，用于合法用途。
- 洗钱犯罪分子勾结专业赌博人员，将非法所得资金投入在线赌博网站中。赌博人员从奖金中抽取佣金，再将剩余资金转给洗钱犯罪分子。
- 洗钱犯罪分子用盗用的身份向在线赌博账户中存入资金。他或她用这些资金进行赌博，以获得奖金或仅损失数额在可接受范围内的方式取回资金。

贵重物品（贵金属、珠宝、艺术品等）交易商

欧洲反洗钱指令制定的通用框架将黄金、钻石和其他高价值物品纳入反洗钱监控体系之中。2006 年 1 月生效的美国《爱国者法》要求特定制成品（包括贵金属、宝石和珠宝）交易商制定反洗钱计划。但在其他很多司法管辖区，这些行业还未被纳入反洗钱监控体系。

2015 年 7 月，金融行动特别工作组发布了一份名为《黄金业相关的洗钱 / 反恐融资风险和漏洞》，对洗钱类型做出进一步说明。黄金制品具有内在价值高、体积小及方便运输等特点。黄金买卖方便，可以与世界上绝大多数地区的货币进行匿名交易。由于黄金可以融化并铸成各种形状，所以相比宝石，人们更愿意接受黄金。无论形状如何（金块或首饰成品均可），黄金都可以保留其价值，因此它也成为推动财富转移的一大途径。在某些地区，黄金背后深刻的文化或宗教意义也增加了其需求。

报告提出了两项重要发现：

1) 黄金是一种极富吸引力的洗钱工具。犯罪分子可以通过黄金将非法所得转换为方便转移的匿名资产。
2) 黄金市场的丰厚利润令其成为犯罪分子的目标。了解黄金市场的各个阶段和上游犯罪的类型对识别洗钱行为有着至关重要的意义。

案例分析

美国国土安全调查局 (HSI) 的调查人员侦破了一起“旋转木马”案件。在该案件中，珠宝商将贩毒收益转换为等值的黄金。一个犯罪组织与纽约的一家黄金供应商合作，清洗贩毒收益高达数百万美元。HSI 经调查发现，该黄金以“金色颜料”的名义从哥伦比亚进口到美国，之后又对外称为“金条”。金条运至纽约后，珠宝商与贩毒团伙合作，将黄金伪装成扳手、螺帽、螺栓、皮带扣和拖车栓钩等寻常物品。这些物品将再出口至哥伦比亚，所申报价值远低于其真实价值。物品运至哥伦比亚后，又被重铸成金条，以“金色颜料”的名义出口至美国。最终，有 23 名珠宝商因涉嫌洗钱及其他违法行为遭到拘捕，查获 140 千克黄金、100 多颗散装钻石、280 万美元、118 千克可卡因、6 支枪支和两辆汽车。

在有些情况下，交易根本没有发生，却以虚假发票的形式表现出来。为了证明资金转移是为了支付装船货物的货款，洗钱者还会利用书面材料。虚假发票欺诈也是惯用的洗钱手段，发票金额是否高出或低于所谓的货物或服务价格在所不论。

下列交易同样容易被洗钱者利用，需特别引起注意：

- **向物主以外的个人付款或收款：**如果有人拿出贵金属要求精炼并声称其物主有权将其出售，但要求向另一人付款，则该交易就比较可疑。将资产从一种形式变为另一种形式（如将未精炼的黄金变为精炼黄金或国际金融系统中的资金）或将资产从一人手中转移到另一人手中都需要“贵金属交易商”的参与。
- **贵金属池账户：**这些账户的持有人是极少数规模巨大而且业务复杂的贵金属公司，它们在全世界范围内运作。它们替客户接收并持有贵金属，并允许该客户随时提取。客户还可要求返还贵金属、销售贵金属并返还货币所得或将贵金属转交给他人。因此，某国的精炼客户可提供黄金碎片用来精炼，从而在精炼商联合账户体系中设定黄金存入，并在其后要求该精炼商基于这一存入向他人转交。

案例分析

2003 年 6 月 5 日，美国移民海关执法局 (ICE) 特工从曼哈顿钻石区的 7 家珠宝行中逮捕了 11 人，指控其参与国际洗钱计划。特工收到情报，称哥伦比亚贩毒集团通过购买、走私和出售钻石与黄金进行洗钱。这些贩毒集团指示其美国员工用毒资在纽约购买宝石，将其走私到哥伦比亚并出售给当地精炼商以换取“干净”的比索，以便消除货币的使用风险。基于这些信息，ICE 特工于 1999 年对纽约涉嫌参与洗钱的多家珠宝行展开调查。根据控方陈述，装扮成毒贩的便衣特工与珠宝商取得了联系，告诉珠宝商他们想用非法资金购买黄金和钻石，以便

将这些贵金属走私到哥伦比亚并重新出售给精炼商以换取“干净”的现金。而这些珠宝商自愿接受了便衣特工约 100 万美元的毒资，并将黄金熔炼成小物件，如皮带扣、螺丝钉和扳手，以方便走私到哥伦比亚。

钻石的非法贸易已成为世界某些地区武装冲突的重要因素，恐怖组织也可能使用来自这些地区的钻石资助自己的活动。

钻石行业的个人与实体也参与了利用钻石洗钱的复杂案例。和黄金一样，涉及钻石的洗钱手段中，直接使用非法资金购买宝石是最为简单的一个类型。

金融行动特别工作组指出，涉及贵重物品经销商的常见洗钱活动包括零售外汇交易、伪造发票或发票欺诈、钻石交易公司将账户中的合法收入与非法所得混合，特别是这些账户间的国际资金转账。有些被侦测到的洗钱交易是清洗走私钻石非法所得的掩护。有时，钻石交易被用来清洗其他犯罪活动的非法所得。

规模达上亿美元的艺术品产业也可以成为便利的洗钱工具。艺术品拍卖行的匿名代理人会为那些珍贵的艺术品投入动辄百万美元的资金。其后，代理人从离岸金融庇护所的账户中通过电汇方式向拍卖行付款。对于洗钱者来说，这是个理想的洗钱机制。

案例分析

美国毒品执法局 (DEA) 和美国国税局 (IRS) 联手，于 1992 年发起了著名的“迪内罗行动”(Operation Dinero)，他们在安圭拉岛经营一家虚设银行，以便调查国际毒贩的金融网络。执法机构在不同的司法管辖区内成立公司并将其伪装成为毒贩提供洗钱服务的前台公司。哥伦比亚卡利市的贩毒集团成员与该“银行”联系出售毕加索、鲁本斯和雷诺兹的名画，总额达 1,500 万美元。这些名画后来被美国没收。

艺术品和古董经销商以及拍卖行应遵循以下原则，以降低被动参与洗钱的风险：

- 要求所有艺术品卖主提供其姓名和地址。要求他们填表声明作品并非赃物且他们有权出售，然后在表上签名并填写日期。
- 确认新卖主和客户的身份和地址。对任何叫价与市场价值不符的艺术品都应持怀疑态度。
- 如果有理由相信某一作品可能是盗窃所得，应立即与遗失艺术品登记处 (www.artloss.com) 联系。该机构是全球最大的私人遗失艺术品数据库，其中包括由执法机关、保险商和个人报告的 10 万多件遗失艺术品。
- 如果客户要求现金付款，就要格外小心。没有确凿可信的理由，不得接受现金支付。

- 了解反洗钱法规。
- 任命高级职员来接受员工的可疑交易报告。

旅行社

旅行社也可被用于洗钱，由于旅行社有理由购买高价机票，在酒店及其他与度假相关的事务上花费资金，洗钱犯罪分子可借机将非法资金混入合法资金，使非法资金看似合法。

案例分析

以厄瓜多尔一座著名山脉命名的“钦博拉索山行动”(Operation Chimborazo) 是 20 世纪 90 年代中期的一项大规模多国联合行动，行动的目标是涉嫌清洗毒资的可疑企业。行动主要针对雨果·奎瓦斯·甘博亚 (Hugo Cuevas Gamboa) 的洗钱组织，此人是卡利贩毒集团 (Cali Cartel) 洗钱犯罪的主犯。1994 年，执法机关打击了拉美国家的多家企业，其中就包括旅行社。在阿根廷的一次搜捕行动中，当局逮捕了一家旅行社的老板，该旅行社所属的洗钱组织每周清洗来自 22 个国家共计 5000 万美元的毒资。

涉及旅行社的洗钱方式包括：

- 以高昂价格为他人代购机票，随后由其本人去退票。
- 将电汇拆分成小额交易以规避交易记录要求，来自国外的电汇尤为如此。
- 利用虚假预订信息和身份证件建立旅游运营商网络，从而捏造出合法的国外旅游团支付款项。

交通工具经销商

此行业包括全新和二手交通工具的经销商和经纪商，交通工具涵盖诸如轿车、卡车和摩托车等陆路交通工具，固定翼飞机和直升机等飞行器，以及大小船只。

涉及交通工具经销商的洗钱风险和洗钱手段包括：

- 将现金存款拆分成金额低于报告限额的数笔款项，或使用连号支票或汇票购买交通工具。
- 从事交通工具交易并连续买进卖出全新或二手交通工具，以生成错综复杂的交易层次。
- 接受第三方支付，尤其是来自洗钱监控宽松的司法管辖区的第三方支付。

多数涉及交通工具经销商的洗钱案件都有一个共同特点，即购买交通工具的资金不上报。

在有些案例中，汽车经销商允许毒贩将他们的汽车换成价格更低的款式，并用支票而不是现金来支付差价，政府当局因此指控汽车经销商涉嫌参与洗钱活动。在一个“低价置换交易”洗钱计划中，毒贩将价值 3.7 万美元的保时捷置换成价值 1.7 万美元的福特野马。经销商明知他们是毒贩还与其进行此类交易，违反了反洗钱法规。

案例分析

2011 年，美国财政部认定黎巴嫩加拿大银行 SAL 及其分支机构 LCB 为首要洗钱关注金融机构，指控其帮助某国际贩毒及洗钱集团从事洗钱活动。美国官方机构坚称，该国际贩毒及洗钱集团的相关人员抓住 LCB 的管理复杂、内部控制不力、缺乏谨慎的银行标准等弱点，广泛利用 LCB 从事非法活动。

该犯罪集团指定美国人 Ayman Joumaa 接应从南美运来的大量可卡因，负责协调运输、分配和销售工作，并将在欧洲、中东地区销售可卡因所得的收入合法化，每月洗钱数额高达 2 亿美元。洗钱手段多种多样，其中就包括通过交通工具经销商洗钱。具体而言，Ayman Joumaa 将大量现金投入多个交易所，其中一家更是归其所有，然后将货币存入在 LCB 开设的账户。随后，Ayman Joumaa 或交易所要求 LCB 以电汇方式转移部分资金，通过可疑的拆分电汇转账，将该集团的美国代理行账户中的资金转移至多个位于美国的二手车经销商，且部分经销商已在其他毒品相关调查中分别被认定为犯罪分子。经销商利用收到的汇款在美国购买交通工具，送至西非或其他海外目的地，获得的收益最终转移至黎巴嫩。

守门人：公证人、会计师、审计师、律师

世界各国总是将一些责任赋予某些专业人员，如律师、会计师、公司创建代理人、审计师和其他金融中介人员。这些人有能力阻止或帮助非法资金进入金融系统。

守门人的责任包括识别客户身份，对客户开展尽职调查，保存客户的交易记录，并上报客户的可疑交易。其中有些规则还禁止守门人通知或告知涉嫌参与可疑交易的客户。违规的守门人可能受到检控，支付罚金甚至入狱服刑。

在欧盟和其他一些国家，守门人必须承担强制性的反洗钱义务。金融行动特别工作组 40 条建议还涵盖了包括律师、法律专业人员以及其他守门人在内的所有独立法律专业人员（*参阅第三章关于金融行动特别工作组 (FATF) 40 项建议的内容*）。

金融行动特别工作组在 2013 年度洗钱类型报告中指出，由律师、公证人、会计师和其他专业人员提供的下列服务对潜在的洗钱犯罪分子最为有用：

- 创建并管理公司或其他复杂的法律安排（如信托）。这类做法可以模糊犯罪所得和犯罪人员之间的联系。
- 购买或出售资产。资产转移既可以掩护非法资金的转移（离析阶段），也可将经过初步清洗流程的非法资金用于最终投资（融合阶段）。
- 从事金融交易活动。有时这些专业人员可能代表其客户从事各种金融活动（如开具和兑现支票、存款、从账户取款、参与外汇零售业务、购买和销售股票以及发出和接收国际资金转账）。
- 提供金融和税收建议。拥有大量投资资金的罪犯可能伪装成希望将税负最小化或为避免未来债务而寻找资产处置办法的个人。
- 为金融机构提供引介。
- 开展特定诉讼。
- 建立并管理慈善组织。

多数情况下，犯罪分子利用法律专业人员获得受人尊敬的形象，避免引起金融机构的问讯或怀疑，如果将来受到调查，也可在调查程序中增加一道环节。此外，法律专业人员可能故意滥用客户的合法账户，在客户不知情的情况下进行转账。

报告还叙述了恐怖融资中的洗钱危险信号：

1. 客户：
    a. 过于隐秘。
    b. 聘用代理人或中介，或以不正当理由避免正面接触。
    c. 不情愿或拒绝提供转账通常所需的信息或文件。
    d. 正担任或曾经肩负高级公共职务，或为此等人物的专业服务人员或亲属。
    e. 据知曾因侵犯财产罪接受调查（即犯罪分子从犯罪活动中谋取重大利益，例如盗窃、挪用公款等）。
    f. 据知与犯罪分子有联系。
    g. 对某些事务异常好奇，反复询问普通标准的实行程序。
2. 参与方：
    a. 是高风险国家的本土人士、居民，或在此等国家成立。

b. 无明显的商业关系而互相关联。

c. 相互关系令人怀疑交易的真实性质。

d. 在较短时间内出现在多起交易中。

e. 丧失行为能力或未到法定年龄，此类参与无合理解释。

f. 试图掩饰交易的真正主人或参与方。

g. 不负责管理交易。真正的负责人反而不是交易的正式参与方。

h. 不是恰当的代表。

3. 资金来源：

a. 通过异常支付方式提供。

b. 高危国家的担保金。

c. 某新成立公司收到的一笔无合理解释的巨款，包括海外资金。

d. 得到的资金比同类企业高得多。

e. 以过高或过低的价格作为抵押而取得。

f. 从与企业经营目的不符的大规模金融交易中取得。

4. 律师：

a. 与客户距离过远或汇款所得无合理理由。

b. 不具备提供特定服务所需的经验。

c. 无合理原因而收取远高于正常费用的报酬。

d. 人选经常更换，或客户无合理理由而聘请多个法律顾问。

e. 提供前任专业人员拒绝提供的服务。

5. 预付金：

a. 所涉交易的运作形式、典型规模、频率或执行情况异常。

b. 所涉交易与客户的正常业务活动不符，并反映出客户未适当了解其所需的专业活动的性质、对象和目标。

c. 无合法或经济原因，而建立复杂的所有者结构或跨国参与结构。

d. 客户交易历史无记录，无法证明其以往商业活动。

e. 前后不一致，最后时刻改变指令而无任何解释。

f. 没有合理的商业、金融或税务理由而进行交易或增加复杂性，导致税费或开支更高。

g. 独家保存文件或其他物品，持有大量储蓄金，或在不提供法律服务时使用客户账户。

h. 不考虑开支问题或在收到资金后放弃交易。

i. 在异常情况下，无合理依据而要求取得管理或处置资产的授权书。

j. 诉讼的解决过程过快或过于轻松，预聘的法律专业人员几乎未参与或毫无参与。

k. 无依据或相关交易而要求向第三方付款。

金融行动特别工作组在其洗钱类型报告中就律师如何帮助建立复杂的洗钱程序而援引了如下案例:

案例分析

一名东欧人利用某公司主管的虚假身份在一家比利时银行开设账户。该账户接收到一些海外汇款，其中包括来自“我们的客户之一”的汇款。这些资金随后用于购买房产，以支票形式付给公证员。公证员注意到，有时，该公司购买房产后会资源清偿，相关人员从该公司买回房产，而回购价格远高于初始出售价。至此，这名东欧人可得到初始售价和额外资金收入，并将这笔钱存入金融体系。他因而能够利用公司账户、前台公司客户、购买房产、跨境交易、电汇等手段来洗钱，据警方介绍，这笔非法资金来源于有组织犯罪活动。这家公司似乎仅仅是为了开展房产交易而设立的空壳公司。

案例分析

一名律师因共谋洗钱而获刑。该律师帮助其客户将毒品收益用于投资，他首先以客户妻子的名义设立一家公司，然后安排该公司向另一家（非犯罪化）客户提供贷款。随后，他起草了一份虚假的建筑工程合同，将还款伪装成犯罪公司向非犯罪公司提供建筑服务所得的报酬。他还捏造了一份本票，由其客户妻子签署，但并未向任何一方提供本票副本。该律师还指导其客户如何在不触发上报要求的情况下，将放贷所得现金存入银行。上诉法院维持了对该律师的判决，但将其发回重审，因为上诉法院发现，该律师在犯罪活动中利用“特殊技能”（法律技能），而区法院未据此加重量刑，滥用了自由裁量权。

鉴于律师和客户间存在保密关系，要求律师成为反洗钱 / 反恐融资领域的守门人这一问题充满争议。以下选择都曾被谈及：

- 推迟法规的颁布，直到开展过充分的教育。
- 针对无特权的交流，加强律师的内部控制和尽职调查义务。
- 利用政府和私营机构的联合机构来规范参与金融活动的律师，要求他们在此等机构注册并接受其监管。
- 设计新的混合方法，如通过来自 FATF 的指导性说明或最佳实践标准完成。

在美国，守门人问题的核心在于要求适用的范围，特别是适用报告要求的金融交易的定义。美国的很多监管部门希望该范围与欧盟指令所规定的范围一致。欧盟要求其成员国确保将该责任落实到广泛的专业人员中，包括审计师、律师、税务顾问、房地产经纪人和公证人。

即使美国不会采用欧盟和英国的守门人标准，部分现行动议的治外法权范围已将从事国际交易的律师纳入其所要求的范围。

投资和商品顾问

商品期货和期权账户也可充当清洗非法资金的工具。它们是什么?

- 商品：食品、谷物和金属等常常在商品交易所进行大量交易的商品，它们通常以期货合约交易的形式出现。
- 商品基金：多个投资者的共同资金，用于进行期货和期权合约交易。
- 期货 / 期货合约：在未来某一时间以设定价格购买或出售特定数量的商品的合约。
- 期权 / 期权合约：此合约创设以设定价格在特定期限后购买或出售特定数量的某种商品或股票的权利，但不是义务。
- 综合账户：由期货经纪商 (FCM) 为他人持有的账户。多个账户持有人的交易混合在一起，持有账户的期货经纪商也不知道他们的身份。

商品交易顾问 (CTA) 是指为获得报酬或利润而直接或间接地为他人提供咨询意见的人。咨询的内容包括交易期货合约、商品期权和 / 或掉期的价值或是该交易是否划算，或发布有关交易期货或商品期权的问题分析或报告。CTA 同时负责托管期货账户交易活动。CTA 负责管理此类账户，因而具备独特优势，可发现涉嫌洗钱的活动。因此，他们需要认清哪类活动可能涉嫌洗钱和恐怖融资，并执行合规程序，侦测并制止此类活动。

负有类似责任的其他人员包括：

- 商品基金经理人：汇集会员资金，进行期货或期权合约交易的经理人或律师。
- 期货经纪商 (FCM)：寻求或接受期货合约或商品期权订单并就订单的执行收取佣金的公司或个人。
- 商品中介经纪商 (IB-C)：寻求或接受客户的商品期货订单但不接受资金的公司或个人。商品中介经纪商分为有担保的经纪商和独立经纪商。
- 担保中介经纪商：与期货经纪商之间签有排他性书面协议的中介经纪商，期货经纪商应对中介经纪商的行为承担责任。
- 独立的中介经纪商：须遵循最低资本和财务报告要求的经纪商。这类经纪商可以向任何期货经纪商引介客户。
- 投资顾问：就证券和投资提供建议，并管理客户资产。

该行业会被用于洗钱的方式：

- 通过向无关联账户或高风险国家转账以撤回资产。
- 经常性地向账户注入资产或从账户中提取资产。
- 从与该客户不相关的第三方账户中用支票提款或电汇款项。
- 客户要求提供保管服务，从而保持匿名。
- 在离析计划中，资金先转移给资产管理顾问再转入其他机构的账户。
- 使用非法所得为客户投资。
- 转移资金以隐匿其来源。

信托与公司服务提供商

信托与公司服务提供商 (TCSP) 参与公司的建立、行政或管理。他们是指任何向第三方提供下列任意一种服务的个人或企业：

- 担任创建法人的代理机构。
- 担任（或者安排他人担任）公司的董事或秘书、合伙制企业的合伙人，或其他法人的类似职位。
- 为公司、合伙制企业或任何其他法人或组织提供注册办公地、营业场所或通讯地址。

- 担任（或安排他人担任）书面信托受托人。
- 担任（或安排他人担任）第三人的代名股东。

2010 年，金融行动特别工作组发布《滥用信托与公司服务提供商的洗钱活动》，报告指出，信托与公司服务提供商在许多司法管辖区尚未得到认可。但在这些司法管辖区，信托和公司服务可由律师和其他专业人员提供，而这些人员已受到监管。例如，在许多司法管辖区，律师可接受委托为客户组建公司，使客户在所处司法管辖区以外持有资产（如游艇、住宅或商业地产等）。金融行动特别工作组注意到，有些信托与公司服务提供商应要求对客户负有保密义务，而这与反洗钱报告制度的要求存在冲突。

尽管绝大多数公司和信托都拥有合法目的，但由这些专业人员组建的法律实体或其他类型的法律关系却经常被洗钱计划所利用。

金融行动特别工作组于 2010 年发布的《滥用信托与公司服务提供商的洗钱活动》列举了该行业的漏洞和危险信号，具体如下：

- 未针对认证和上报要求实行监管指南，或实行的指南前后不一。
- 为确保从业人员具备足够的技能、能力和诚信，对从业人员的市场限制有限。
- 行业内的记录前后不一。
- 信托与公司服务提供商可无证经营。
- 根据司法管辖区的要求，信托与公司服务提供商的客户尽职调查可由其他金融机构执行。

该行业的潜在洗钱标志包括：

- 涉及复杂、不透明的合法公司和安排的交易。
- 向空壳公司支付“咨询费”，该空壳公司成立于外国司法管辖区或因设有无数空壳公司而闻名的司法管辖区。
- 使用的信托与公司服务提供商，其所在的司法管辖区不要求信托与公司服务提供商攫取、保留或向有关部门提交其所成立公司结构的受益所有权情况。
- 使用的法人和法律安排，其所在的司法管辖区未制定反洗钱 / 反恐融资法律或此等法律薄弱，或者该司法管辖区对信托与公司服务提供商的监督和管控不力。
- 使用的法人和法律安排，其所在的的司法管辖区实行保密法律。
- 多笔跨公司贷款交易或跨司法管辖区电汇的目的不明或不合法。

根据透明国际 (Transparency International) 的观点，关注服务提供商而非公司或信托的理由在于，后者仅仅是洗钱犯罪分子所利用的工具而已。犯罪分子拥有的公司并不能保护它自己，但服务提供商却可以。服务提供商可以通过尽职调查，降低与其有关系的公司被滥用于洗钱的风险。正因如此，各国家和地区对服务提供商的监管才会至关重要。

法规应明确规定服务提供商如何开展业务，包括提供商选择的董事如何作为受托人履行其信托义务和职责。透明国际在 2004 年的报告中指出，第一个将此类活动纳入监管的司法管辖区是直布罗陀，该地区于 1989 年颁布了相关法规。其他离岸管辖区或已经引入了某种形式的监管措施，或计划在将来着手引入。

法规不统一；从简单的最低资本化要求到全面监管，存在各种不同程度的监管。通常，法律的管辖范围也会有所限制，某些类型的活动会被排除在外。有时法律不允许监管者在未经客户允许（或没有法院传票）的情况下获取客户文件，因此，监管者不太可能检查持有金融许可证的机构是否充分履行了客户尽职调查职责。此外，虽然有些司法管辖区将服务提供商纳入了反洗钱监管（如将合规要求作为获得许可证的条件），但很多司法管辖区并不如此。除了适用于公众的义务外，服务提供商不承担额外的反洗钱义务。透明国际指出，由于标准存在差异，那些希望利用公司或信托作为犯罪目的的人员便很容易找到缺乏反洗钱监管要求或反洗钱监管不够的司法管辖区。

房地产

房地产行业中的洗钱活动泛滥。将非法资金投入房地产是清洗钱的传统方法，在政治、经济和金融稳定的国家尤为如此。

托管账户通常由地产经纪商和经纪人以及其他受托人持有，用来储存被托付给某人保护和处置的资金。每天都有大量地产和商业交易通过托管基金实现。此类账户可用于开展大量不同类型的交易，因而对洗钱犯罪分子极具吸引力。托管账户可以通过银行本票、电汇或公司支票等形式，将资金转移给看似合法的个人或公司。鉴于托管账户可能存在大量交易活动，洗钱犯罪分子可轻易掩饰账户中的非法活动，同时使账户操作看似合法。

在许多房地产交易中，承押人通过按揭存入一张大额支票，交易完成时，买方提供支票和现金（然而，本节下文将介绍，使用现金购买房地产的情况越来越普遍）。为了洗钱，产权保险代理商可于某一日在多家银行存入多笔现金（每笔的金额都低于报告的限额）并记入不同的虚构交易。这些储蓄看上去是正常的商业活动，但它们仍可能表现为希望隐藏其资金来源的个人为了购买房地产而进行的持续资金积累。这些资金最终可能以银行本票、电汇、公司或代管支票的形式，直接从托管账户支付给虚构的个人或者空壳公司。每次交易还包括大量常规付款活动，包括使用所得资金

向出售方付款、支付按揭、地产佣金、税收、实现优先权以及其他款项。在银行和其他观察家看来，交易完成时的资金链支出看上去是一套合法交易。由于常规托管账户的活动规模和数量会掩盖“起伏”（即账户的突然变动）或与洗钱相关的多笔储蓄，洗钱可因此得以轻易隐藏。

在该行业中，我们还会碰到“反向倒手”。洗钱犯罪分子会找到愿意合作的房地产经销商，此人同意以大幅低于实际价值的价格向洗钱犯罪分子出售资产，然后再秘密接受差额款项。由此，洗钱犯罪分子可用 100 万美元购买实际价值 200 万美元的房产，然后私下将差额秘密转给卖方。洗钱犯罪分子持有该房产一段时间后，按 200 万美元的真实价格将其出售。

在“回贷”的洗钱手法中，罪犯为同伙提供一定数量的非法资金。然后同伙以“贷款或按揭”的形式将同样数额的资金返回给提供人，并附上所有必要的“贷款或按揭”文件。此举制造出毒贩资金“合法”的假象。毒贩再通过“合法”且有计划的还款巩固该计划的“合法性”。

2008 年 4 月，金融犯罪执法网络 (FinCEN) 通过分析可疑活动报告 (SAR)，发布了《房地产中的可疑洗钱活动》评估报告。这份报告对诈骗者和洗钱犯罪分子加以区分。如果贷方遭受威胁其机构收入的抵押欺诈骗局，无论诈骗分子是否得逞，贷方会提交可疑活动报告，但贷方很难发现洗钱犯罪分子发动的抵押贷款诈骗。这是因为洗钱犯罪分子使用非法资金，定期准时向贷方还款，竭力制造一切正常的假象。例如，据报道，有关房地产行业的可疑活动报告中，仅有 20% 涉及可疑拆分或洗钱。

澳大利亚交易报告和分析中心 (AUSTRAC) 于 2015 年发布的一份简报指出，房地产是澳大利亚的一大重要洗钱渠道。这份简报显示，2012 至 2013 年期间，因涉嫌洗钱而充公的房地产总价值超过 2,300 万澳元。简报指出，房地产之所以成为极具吸引力的非法资金清洗渠道，有以下几个原因:

- 可用现金购买。
- 最终受益所有人可得以掩饰。
- 这项投资相对稳定可靠。
- 可通过翻新和装修提升价值。

与其他洗钱手段相比，通过房地产买卖洗钱过程相对简单，无需进行规划或具备专门技能。洗钱犯罪分子可通过投资房地产，将大量犯罪所得融入合法经济（处置和离析阶段）。房产既可出售获利，也可用作住宅、投资或度假使用（融合阶段）。

在澳大利亚，利用房地产洗钱的常见方式包括:

- 利用第三方无价值买家，即所谓的“无前科人士”。

- 用贷款和按揭掩饰洗钱活动，洗钱犯罪分子可能通过用大量现金还贷，将非法资金融入经济。
- 操控房产价值，通过提高或降低价值，掩盖未被发现的现金支付，或“快速翻转”，通过接连买卖，提高价值。
- 拆分用于购买房产的现金存款。
- 出租购得的房产，收取房租，从而将非法资金合法化。
- 在购得的房产中实施犯罪活动，例如生产大麻或合成毒品。
- 利用非法现金装修房产，提高价值后出售，以此盈利。
- 利用前台公司、空壳公司、信托及其他公司结构，掩饰受益所有人以及与犯罪分子的明显关联。
- 利用房地产经纪商、转让人、律师等守门人，隐藏犯罪分子的参与事实，使洗钱过程复杂化，制造交易合法的假象。
- 海外犯罪分子投资本地房地产，隐藏自身资产，避免被其所在的司法管辖区的相关部门充公。

一些房地产交易涉及受监管的反洗钱 / 反恐融资产业，例如在交易期间向金融机构贷款、存款或取款，针对利用此类交易洗钱的活动，这份报告提出了识破洗钱活动的方法。报告还列举了一些危险信号，这些信号一旦出现，特别是几种信号同时出现，应采取进一步监控和调查。这些危险信号包括：

- 在购买房产、支付首付或还贷时，为筹集资金而多次使用现金。
- 短期内进行多次买卖，有时房产的价值过高或过低，或利用无价值买家。
- 向离岸贷方借款。
- 购房资金来源不明，例如使用一笔来自国外的汇款，而汇出方和受益人为同一人。
- 所有权是客户与欲购房地产所在国的唯一联系。

2015 年，《纽约时报》刊登题为《秘密高楼》的系列报道，第五篇报道揭露了 200 多家空壳公司的秘密，在位于曼哈顿中心的高端楼盘时代华纳中心，这些公司拥有共管式分户产权物业 (condominium)。该调查性系列报道指出，全美最昂贵的住宅房产中，近一半由空壳公司买走。时代华纳中心 37% 的共管式分户产权物业归外国人所有，其中至少有 16 处房产受到政府调查，涉嫌住宅和环境欺诈等。这些外国业主包括俄罗斯、哥伦比亚、马来西亚、中国、哈萨克斯坦和墨西哥的政府官员或其亲属，他们主要通过有限责任公司购得这些房产。房产证上的签署栏通常字迹潦草或为空白，或由注册过联系方式的律师签字。

《纽约时报》指出，目前没有法律规定要求美国的房地产行业识别受益所有人或调查其背景。2016 年（《纽约时报》的系列报道发表后），金融犯罪执法网络开始发布一系列“地区目标企业整顿令”(GTO)，帮助执法机关识别未使用银行融资，而是通过有限责任公司或其他不透明结构购买豪华住宅的个人。每份“地区目标企业整顿令”实施的 180 天内，对于在特定美国都市以现金全款购买高端住宅的空壳公司，如果房产金额超过该地区设定的上限，则美国产权保险公司必须识别空壳公司背后的自然人。非常值得注意的是，这里的“现金全款”是指不使用传统的融资方式，而非使用真正意义上的现金。

国际贸易活动

国际贸易活动对一体化经济至关重要，涉及多个领域，包括银行、货币兑换、自由贸易区（自贸区）、跨境支付、港口、发票、货物、货运、空壳公司、信用票据等，这些领域本身往往即为复杂交易，可能受到洗钱和恐怖融资犯罪分子恶意操控。贸易洗钱和黑市比索交易是两大重要的洗钱手段，在非法融资中非常奏效。两种手段通常会恶意利用自贸区。

自由贸易区（自贸区）

超过 135 个国家共设有 3,000 多个自贸区，自贸区在国际贸易中发挥着必不可少的作用。自贸区是针对特定的贸易相关商品和服务设立的指定区域，区内实行特殊的监管和税收政策。自贸区通常临近发展中国家的入关港口，但又与其相分离，通常实行不同的法规。大多数大型自贸区还位于区域金融中心，连通国际贸易枢纽与全球金融市场。全球典型的自贸区包括巴拿马科隆自贸区和中国上海自贸区（官方名称为中国自由贸易试验区）。

根据金融行动特别工作组于 2010 年 3 月发布的《自贸区易受洗钱危害的薄弱环节》报告，自贸区存在的系统性弱点包括：

1. 反洗钱 / 反恐融资保障措施不足。
2. 地方有权机关缺少监管。
3. 对商品、法律实体的检察程序薄弱，包括适当的记录和信息技术系统。
4. 自贸区和本地海关缺乏合作。

自贸区的监管宽松，使侦查非法活动变得更加困难，也为贸易洗钱机制提供了温床。此外，金融行动特别工作组在报告中还指出，一些自贸区达到了城市规模，致使进出货物、卸货、重新标签等活动很难得到有效监控。一些自贸区每年的出口规模高达数十亿美元，但缺乏监管、检查货物和贸易交易的权威机关。

基于贸易的洗钱手段

如果男式内裤和女式内衣以每打 739 美元的价格进口到某国，导弹和火箭发射器以每个 52 美元的价格出口，而全套马桶设备出口价不足 2 美元，则我们必须对这些危险信号加以重视。这些操纵贸易价格的做法表明存在洗钱、避税或恐怖融资活动。

在 2006 年 6 月的一份题为《贸易洗钱活动》的报告中，FATF 将贸易洗钱定义为掩饰犯罪所得，通过贸易转移价值，试图使非法来源收入合法化的过程。在实际操作中，这可以通过虚报价格、进出口数量和质量来实现。此外，基于贸易的洗钱手段在复杂程度上各不相同，它通常与其他洗钱手段混合使用，从而进一步模糊资金的真实来源。

洗钱犯罪分子向境外转移资金的手段是：使用非法资金购买贵重产品，然后以超低价格向外国同伙出口，并由其按照产品的真实价格在公开市场出售。为了使交易具有表面合法性，合作伙伴可能通过金融机构获得贸易融资，而这通常又会涉及信用证和其他贸易文件。

2006 年，金融行动特别工作组的研究表明，贸易洗钱是犯罪活动的重要渠道，鉴于国际贸易与日俱增，这种手段也越来越容易成为洗钱和恐怖融资活动的重要渠道。另外，随着应用于其他洗钱手段的标准日益有效，基于贸易的洗钱手段将更具吸引力。

2016 年 2 月 1 日，香港金融管理局协助香港银行公会制定《打击以贸易进行洗钱活动的指引文件》，文件指出，了解每笔贸易交易的商业目的是明确洗钱风险的关键要求。《指引文件》列举了六种利用贸易活动洗钱的手段，包括：

1. **高开发票或低开发票：**
    - 高开发票：卖方以高于市场公平价格的数额为商品或服务开具发票，借此从买方处谋取差价利润（即商品或服务的售价高于在公开市场的价格）。
    - 低开发票：卖方以低于市场公平价格的数额为商品或服务开具发票，借此向买方转移差价利润（即商品或服务的售价低于在公开市场的价格）。
2. **超量装载或装载不足：**发票中记录的商品数量和实际装载的数量有出入，使买方或卖方借机谋取差额利润。

3. **空箱运载：**买卖双方共谋虚假贸易，准备妥当所有文件，显示商品已售，已发货，款项已付妥，但实际并未发送任何商品。
4. **空壳公司：**利用空壳公司，降低交易所有权的透明度。
5. **多次开票：**对同一批装载商品开具数张发票，使洗钱犯罪分子以这些发票为由，借机支付数笔款项。
6. **黑市贸易：**通常指黑市比索交易，即外国进口商利用境内转账为商品付款。

信用证是另一洗钱手段。信用证是由银行签发的信用票据，保证在满足某些条件时，代客户向第三方付款。信用证通常用于为出口提供融资，由于出口商希望确定商品的最终买家会按时付款，买方购买银行信用证可为出口商提供付款保障。之后，买方的银行将信用证转给付款所在地的代理银行。商品装运、进口港收货、清关并发运后，出口商就通过信用证收取货款。洗钱者可以利用信用证将资金从外汇控制措施不严的国家转出，从而造成开展进口交易活动的假象。此外，在通过操纵进出口价格进行洗钱时，信用证也可以作为一个幌子。另一种非法利用信用证的方法为通过电汇，将根本不存在的贸易活动伪装成合法活动。

2012 年 7 月，亚太反洗钱工作组 (APG) 发布《APG 贸易洗钱类型报告》，再次肯定了 FATF 于 2006 年得出的研究结论。亚太反洗钱工作组的研究报告指出，缺乏贸易洗钱的数据资料是妨碍制定解决方案的一大重要因素。为便于识破各种形式的贸易洗钱，本报告列举了司法管辖区、商品、公司结构和上游犯罪等方面的具体特点和危险信号。

报告总结道，预防或打击贸易洗钱的策略必须旨在瓦解贸易洗钱结构，同时保证合法贸易不受阻碍。这要求采用一体化全局性方法，重视跨部门协作和国际间合作，使资料和数据标准化，组建国内特别工作组，开展针对贸易洗钱的培训，并进行进一步调查。

案例分析

2011 年 2 月，美国财政部认定黎巴嫩加拿大银行 LCB 为首要洗钱关注金融机构，指出黎巴嫩真主党从贩毒和洗钱活动中谋取资金支持，其中包括贸易洗钱活动。在这些非法活动中，贸易洗钱牵涉全球范围的消费品，包括在美国购入二手车，运到西非转卖，其中一部分非法所得被控流入真主党。

2014 年 5 月，金融犯罪执法网络 (FinCEN) 发布一份关于流入账户和贸易洗钱使用情况的咨询意见。这份咨询是 2010 年墨西哥法律限制墨西哥银行接纳美元现金存款可能造成影响的产物。随后，这一限制进一步扩大，限制墨西哥货币兑换所和经纪公司接收类似存款。此外，金融犯罪执法网络还围绕该限制引发的大额现金走私趋势，发布指导文件，指出利用流入账户转移墨西哥犯罪团伙非法所得呈上升趋势。

根据金融犯罪执法网络的定义，流入账户是指“在一个地区开设的个人或公司账户，该账户收到多笔通常低于现金报告限额的现金存款，然后在另一地区内取出，存取活动的时间间隔极短。”以下方法可识破可能涉及流入账户的活动：

- 在美国某个州开通的账户接到不明人士从另一地区的分行存入的多笔现金存款，每笔均小于 1 万美元（现金报告限额）。
- 公司账户接到的存款来自于非业务开展区。
- 开设流入账户或向该账户存款的人不了解该账户的活动、账户所有人或资金来源。
- 某公司账户接到来自本州以外的存款，该笔借记似乎与经营目的无关。
- 收款人和金额栏的字迹与该接收州外现金存款的账户发行的支票签署栏的字迹明显不同。
- 流入账户发出的电汇或支票被存入某墨西哥银行的美国代理账户，或在此结算。

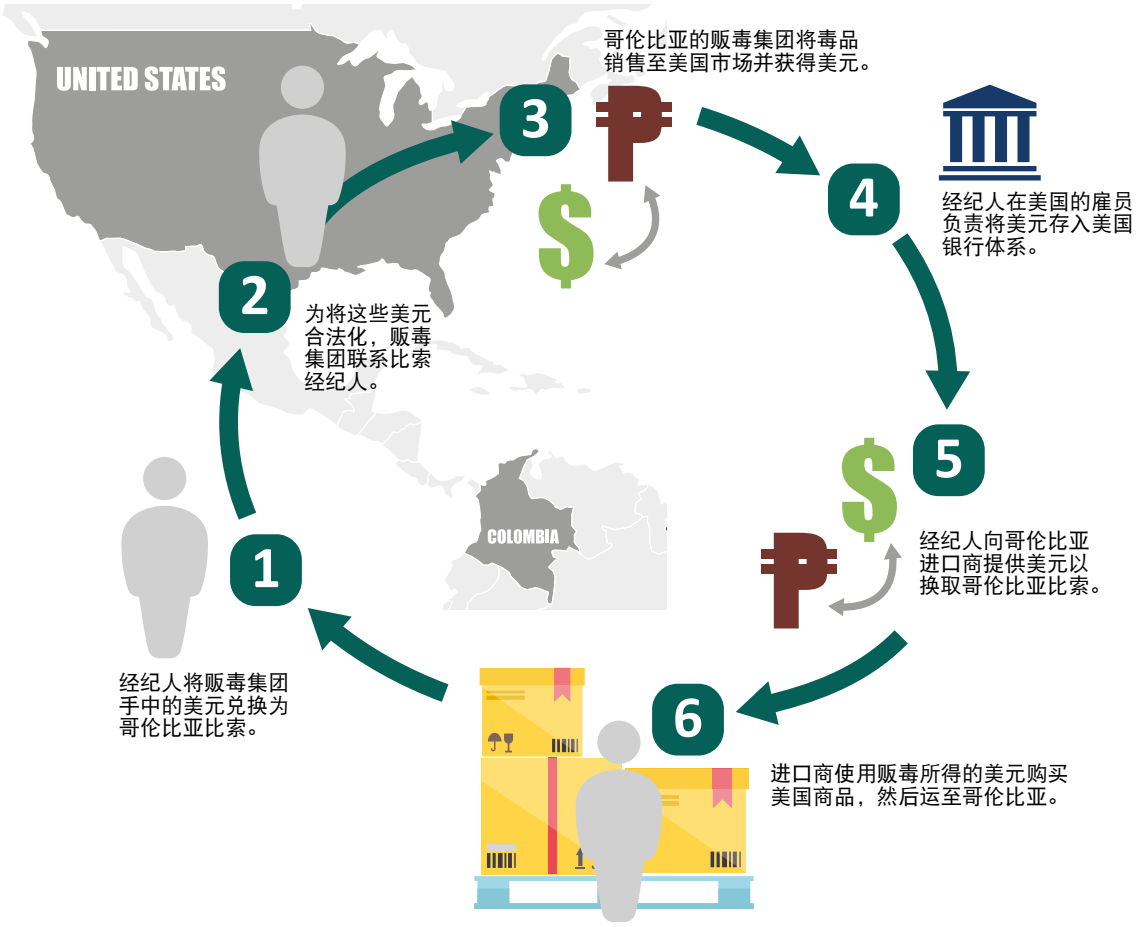
黑市比索交易

黑市比索交易 (BMPE) 是一种贸易洗钱形式，即哥伦比亚比索经纪人买入在美国的非法活动所得，并存入他们在美国银行开通的账户中。经纪人向合法企业出售这些账户的支票和电汇单，供他们在美国购买商品和服务。尽管黑市比索交易最常牵涉美国，但这种活动也见于全球其他地区。

上世纪 50 年代，哥伦比亚进口商创造了在黑市上购买美元的 BMPE 机制，从而规避从官方渠道购买美元以及用美元购买进口商品征收的国内税收和关税。上世纪 70 年代，哥伦比亚贩毒集团开始利用黑市比索交易机制，将在美国的贩毒所得转换成哥伦比亚比索。为什么？这种交易降低了资金被没收的风险并更快地获得资金，即使需要向比索经纪人支付一笔佣金仍非常划算。

2010 年 2 月 18 日，金融犯罪执法网络发布《就贸易洗钱问题对美国金融机构的咨询意见》，文件指出，由于美国银行加强尽职调查，黑市货币交易机制已经从哥伦比亚黑市比索交易发展出多个变种。为将非法资金融入金融系统，常见的第一步处置手段是将资金拆分成现金、汇票，或其他金融票据。然而，洗钱犯罪分子目前开始通过在多个银行握有大量银行账户的个人或公司，将大额现金从美国走私到国外。走私的美元被存入外国机构，通常为墨西哥机构，但也见于中美和南美国家，随后再以支付跨国贸易商品和服务的形式，转汇至美国及其他主要贸易国家。

黑市比索交易案例



2014 年 4 月 24 日，美国司法部公布对某进出口公司所有人的刑期判决，该公司曾将数百万美元的非法活动所得从美国转移至墨西哥。这份新闻稿描绘了牵涉美墨两国的典型黑市比索交易，详情如下：

> 某个非法活动参与者（例如毒贩）在美国持有美元，他需要将这笔钱转移至墨西哥，并兑换成比索，于是他找到一名比索经纪人。这名比索经纪人联系向美国商家（例如 XYZ 公司）购买商品、需用美元付款的墨西哥公司。比索经纪人将非法获得的美元作为墨西哥客户购买货物的货款支付给美国商家（例如 XYZ 公司）。一旦货物运至墨西哥后，由该墨西哥公司转售以换取比索，这些比索再经由比索经纪人，落入墨西哥毒贩手中。

案例分析

2014 年 9 月，大量执法行动揭露了加州洛杉矶时尚区存在的猖獗洗钱活动，这些活动涉及黑市比索交易。洛杉矶市中心的 100 多个街区分布着 2,000 多家企业。时尚区的这些服装企业被贩毒集团用于清洗非法资金。非法分子利用毒品交易所得的大额现金购买纺织品，并运送至墨西哥及其他国家。出口商品的销售所得再以贩毒集团所在国的货币形式，流回他们手中。2014 年 9 月 10 日，美国国土安全调查局特工在执法时缴获 9 千万美元，创下美国有史以来单日缴获数额之最。这些现金存储在多所住处和公司的各种储物设备中，包括文件盒、帆布包、背包，甚至是宾利轿车后备厢中。2014 年 9 月 26 日，金融犯罪执法网络 (FinCEN) 发布《地区目标企业整顿令》，降低了现金限额，并对洛杉矶时尚区的特定纺织品相关企业实行新增记录要求，以期打击贩毒集团的活动。

案例分析

2015 年 4 月，金融犯罪执法网络发布另一份《地区目标企业整顿令》，同样降低了现金报告限制，并对 700 多家迈阿密电子产品出口商的特定金融交易实行新增记录要求。据金融犯罪执法网络表示，这份整顿令旨在打击贩毒团伙使用的复杂黑市比索交易计划，包括墨西哥的锡那罗亚贩毒集团、Los Zetas 贩毒集团等。执法调查显示，成熟的贸易洗钱或黑市比索交易等计划曾利用这些公司，将在美国贩毒所得的资金换成商品运往南美，在当地贩卖以换取当地货币，最终转移给贩毒集团。这份《地区目标企业整顿令》有利于提高受监管企业的交易透明度。

新型支付产品及服务的风险

互联网、新型支付平台和电子货币改变了人们开展商业活动、与他人交易以及消费者购买商品或服务的方式。过去，街角的小商店只能为本地消费者服务，如今，它可以借助网络，服务于更广泛的全球消费者。数字支付平台已经改变了消费者以及监管环境对商家或资金转账的认识。鉴于技术成本越来越低，全球社会互联度更高，劳动力的技术能力快速提升，且企业发挥推动作用，新型支付产品及服务日益发展，不断打破金钱的使用方式和地点限制。一般而言，这些新型支付系统的服务功能和融资机制是风险产生的根源。

预付卡、移动支付以及互联网支付服务

2006 年 10 月，金融行动特别工作组发表的一份报告研究了利用新型支付技术（预付卡、互联网支付系统、移动支付和数字化贵金属）进行洗钱的手段。报告发现，尽管对这些支付方法都有合法的市场需求，但它们都存在被洗钱和恐怖融资活动利用的风险。此外，新型支付方法的跨国提供商可能比在某一特定国家或地区内运营的提供商具有更大的风险。该报告建议，应继续保持警觉以进一步评估新兴技术对跨国和国内监管框架的影响。

预付卡与现金的特点一致，可吸引犯罪分子，包括: 携带方便、额度巨大、兑换便利以及可匿名持有。通常，预付产品要求消费者在购买商品或服务前事先支付一定费用。每次支付时从预付卡或产品的余额中转走一笔资金，用完为止。预付卡分为开放型和闭合型。开放预付卡多由美国运通、维萨或万事达公司发行，可以由一人直接购买并“充值”，并像普通借记卡一样由此人或他人在世界各地购买商品时使用，或在 ATM 机上取现。闭合预付卡仅可用于特定用途或服务，例如用于在线或现场向某个商家或零售商付款。预付卡既有一次性产品，数额有限不可充值，也有可充值产品，可在消费后补充卡内资金。

尽管预付卡种类多样，使用方式各异，但它与借记卡的运作方法相同，都需要与某一账户关联。每张卡可能拥有一个对应账户，或者存在某一联合账户，为所有的预付费卡提供资金。储蓄机构或非银行机构可以发行卡片并持有账户；联合账户通常由银行发卡机构持有。

该报告指出预付卡的潜在风险因素包括:

- 匿名持卡人。
- 匿名资金。
- 匿名资金获取方式。
- 高价值限额以及个人获取卡片数量不限。
- 可通过 ATM 机在全球范围内取现。
- 离岸发卡机构可能无须遵从任何管辖区的法律。
- 替代大量现金走私。

电子钱包（也被称为 e 钱包、储值卡或智能卡）是指在集成电路芯片上进行电子储值的卡片。预付卡使用磁条来存储账户信息，而电子钱包实际上是将资金存在记忆芯片中。

可能防止这些支付方式受洗钱犯罪分子利用的措施包括：

- 限制卡片的功能和取款额度（包括最高限额和流转限制，以及每位客户的持卡数量）。
- 将新支付技术与金融机构和银行账户进行关联。
- 给该系统制定存档和记录的标准程序，以方便日后审查。
- 允许调查机关查阅和查封相关记录。
- 为这些措施制定国际标准。

根据反洗钱联合指导小组发布的《电子货币指南》（2012 年），电子货币是“一种预付方式，可用于同时向多方付款，收款方可为不同的法人或自然人”。电子货币产品可为卡片或网上账户。发行机构可为银行、住房互助会或专门的电子货币机构。典型的电子货币包括从零售商处购买商品时使用的预付卡，或用于在线购买商品或服务的虚拟钱包。英国的所有电子货币机构均受英国金融市场行为管理局监管，须遵循《电子货币条例》（2011 年），该法律要求这些机构满足所有的反洗钱 / 反恐融资和制裁要求。

《指南》列举了电子货币易受洗钱和恐怖融资活动利用的固有风险因素，包括：

- 无交易限额，或限额很高。
- 跨境交易频繁。
- 一些商业活动的业务风险较高，例如赌博。
- 资金来源于不明人士。
- 利用现金融资，资金来源不留任何电子痕迹。
- 利用其他电子货币融资，供资人或资金来源不明。
- 无面对面交易活动。
- 某些特点增加了卡片功能，可进行人对人、企业对人、企业对企业、人对企业的交易。
- 消费者可持有无数钱包。
- 商业价值链被割裂。

继 2006 年发布洗钱类型报告后，金融行动特别工作组 (FATF) 于 2010 年再次发布类似报告。随着市场不断发展，金融行动特别工作组又于 2013 年发布《预付卡、移动支付及互联网支付服务“风险为本”方法应用指引》。这份指引介绍了新型支付方式的大量固有风险，例如：

- **无面对面关系及匿名：**
  - — 新型支付方式可用于快速将资金转移至世界各地，用于消费或从 ATM 机取现。
  - — 预付卡的购买、注册、充值、续费及使用均可匿名进行。
  - — 预付卡可轻易转给第三方，而发卡机构无从得知。
  - — 消费者可通过中介、网络或移动支付系统进行消费。
  - — 在无面对面核验的情况下，增加身份欺诈风险，或消费者提供虚假信息以掩饰非法活动的可能性。
- **触抵更多地区：**
  - — 开放预付卡通常可凭借全球支付网络，支持本国或跨国付款。
  - — 预付卡发行机构可能设立于某一国，但通过中介或网络在全球范围内出售卡片。
  - — 在跨国运输活动中，预付卡因体积小而比现金更易受到滥用。
  - — 移动和网络支付服务可将资金转移至全球各地。
  - — 付款所在地和收款所在地的反洗钱 / 反恐融资监管体系可能存在差异。
- **融资方式：**
  - — 支持现金融资或对续费不设限会增加预付卡风险。
  - — 将预付卡作为实际现金跨境运输的替代方式。
  - — 移动和网络支付服务的融资方式繁多，例如通过银行账户供资，非银行方式包括汇款、电子货币、虚拟货币等。
- **获取现金：**
  - — 利用 ATM 机网络转移预付卡资金，可在某国充值，从另一国家取现。
  - — 移动和网络支付方式与预付卡的结合使用越来越常见，以便充值或取现。
- **服务拆分：**
  - — 使用预付卡开展的交易通常要求几方参与，包括项目经理、发卡机构、持卡人、支付网络、分销机构和中介。

— 移动和网络支付服务要求多个互相关联的服务供应商互相协作，他们必须与国外同等职能的人合作，才能完成跨境交易。

— 利用中介，依靠无关联第三方获取客户。

— 新型支付方式供应商持有银行账户，定期通过银行系统进行交易，与中介或合作伙伴清偿账户，银行可能无法得知交易的最终客户。

该指引还指出，如果考虑以下方面，新型支付方式的洗钱和恐怖融资风险可能得到缓解：

- **客户尽职调查 (CDD)：**

  — 是否执行客户尽职调查，应调查到何种程度，视产品造成的风险大小而定。

  — 新型支付方式的功能越强大，就越需要实行增强尽职调查。

  — 在非面对面核验中利用第三方数据库验证客户信息，并结合网络和社交媒体上已有的开源信息。

- **充值、储值和地域限制：**

  — 设定初始充值限额。

  — 设定地域或续费限制。

  — 限制某产品在特定地域的功能。

  — 限制某产品在购买特定商品和服务时的功能。

  — 考虑向客户提供个人层面的服务。

  — 针对预付卡：

    > 限制充值、时效以及取现条件。

    > 限制预付和可取金额。

  — 针对移动支付：

    > 设定单笔交易的最大限额。

    > 设定取现最大限额。

    > 交易频率及累计金额。

    > 限制每日、每周、每月、每年或以上所有时长的交易限额。

- **资金来源：**
  - — 考虑对特定产品的资金来源设限。
  - — 考虑根据充值或账户限制，识别现金融资。
- **记录、交易监控和报告：**
  - — 保留付款和资金转账的交易记录。
  - — 保留交易参与方的身份信息。
  - — 保留并识别相关账户。
  - — 保留交易日期及相关金额。
  - — 针对移动支付方式，获取付款人和收款人的手机号。
  - — 落实并利用交易监控相关类型。

虚拟货币

虚拟或数字货币是数字空间的交易媒介。既可兑换为法定货币（例如政府发行的货币），也可作为真实货币的替代品。虚拟货币分集中化和非集中化两种。集中化虚拟货币（例如以前的 Liberty Reserve）采用集中存储、单个机构管理的模式。非集中化虚拟货币（例如比特币）没有存储或管理机构，仅作为点到点交易媒介，不需要任何中介机构。2014 年，金融行动特别工作组发布《虚拟货币、核心定义及潜在反洗钱 / 反恐融资风险》，报告指出，虚拟货币还有可兑换和不可兑换之分，可兑换虚拟货币（即比特币和 WebMoney）具有相同价值，可兑换成真实货币，而不可兑换货币（即 Q 币和魔兽世界金币）仅可用于特定领域。

虚拟货币诞生后，人们无需借助集中式银行或权威机构，即可将价值转移到世界各地。2009 年，比特币生态系统诞生，这种加密协议可通过点对点网络实现价值转移，无需依靠集中式银行结构。作为一种虚拟货币，比特币是价值转移的单位。比特币与其他金融工具类似，另一方愿意付出的价值决定了比特币的价值。比特币具有与法定货币类似的价值，由经济和市场因素决定。比特币可换算成任何地方的具体货币。

随着虚拟货币市场逐渐风行，和参与该生态系统的个人与企业数量增加，2013 年 3 月 18 日，FinCEN 发布对虚拟货币的解释性指导文件，将该生态系统内的参与者分为三类：

- “用户”指获取虚拟货币以购买商品或服务的人

- “交易者”指将虚拟货币兑换为真实货币、资金或其他虚拟货币的企业
- “管理者”指发行虚拟货币、有权兑换此等虚拟货币的企业

指导文件指出，虚拟货币的管理者或交易者是参与货币转账的货币服务企业，必须遵守适用于资金转账者的注册、报告、记录保存等监管要求，例如实行反洗钱合规制度。

在一场典型的虚拟货币交易中，使用者在交易者处设有虚拟钱包或账户，可用于交易。使用者从交易者处获取虚拟货币，可通过其账户转移资金。使用比特币进行交易时，交易双方的个人身份信息不会透露给对方或者第三方。尽管区块链和公开的分布式账本记录了每笔交易，可提供传统现金交易无法提供的有用信息，但并不包含相关钱包背后的实际操作人身份信息。因此，“了解您的客户”(KYC) 是合法交易者的反洗钱制度中的重要组成部分。

调查者追查非法资金动向时，可能无法获取所有权信息，而只有上一个环节提供的钱包地址。然而，交易背后的技术和公开交易记录可提供钱包地址的关联信息，帮助调查者摸清所有权情况。帮助使用、购买和转移虚拟货币的虚拟货币企业是重要的信息来源，可提供有关钱包所有权和资金来源的详细信息。

全球各地对虚拟货币企业的监管力度各不相同，有些地区要求企业对交易承担反洗钱 / 反恐融资职责，有些则仅向金融行业提供咨询意见，说明这些企业作为客户所带来的风险。部分国家完全禁止金融行业与虚拟货币企业开展业务。

案例分析

Liberty Reserve 是提供电子货币（自定名为“LR”）支付和转账服务的网站，位于哥斯达尼加。2013 年 5 月，金融犯罪执法网络 (FinCEN) 发布《根据美国《爱国者法》第 311 条的调查通知》，将 Liberty Reserve S.A. 这一金融机构认定为首要洗钱关注对象。当月晚些时候，美国关闭了该网站。当时，Liberty Reserve 在全球共有 550 万个注册用户，进行过 7,800 多万笔金融交易，总价值超过 80 亿美元。

Liberty Reserve 在美国拥有 20 多万用户，但该机构从未在金融犯罪执法网络注册为货币服务企业。Liberty Reserve 未对使用其系统的用户进行账户注册核验，仅要求用户提供常用邮箱，并许可一名用户开设多个账户。用户可向网站支付额外的“隐私费”，以后通过 Liberty Reserve 系统发放资金时，可隐藏自己的内部特殊账户号码。用户注册账户后，可匿名向全球各地的 Liberty Reserve 用户转账，资金立即以 LR 虚拟货币的形式进入对方账户，实质上未核实的账户持有人可利用该网站将 LR 货币转移给其他同样未核实的账户持有人。

账户资金来源于持有大量 LR 货币的交易者和第三方实体，这些货币则是从传统的资金渠道购得。交易者成为未经许可的汇款经纪机构。技术上，这种设计旨在通过交易者从源头上（传统渠道，如现金或电汇）将资金转为数字货币，然后再用数字货币购买非法物品，或通过不同的交易者将其从 Liberty Reserve 取出。2016 年 5 月，Liberty Reserve 的创始人 Arthur Budovsky 因经营洗钱公司，被判 20 年监禁。四名共同被告均对其指控认罪，仍有两名共犯逍遥法外。

案例分析

2013 年 9 月，美国司法部开启一项公诉，指控网站 Silk Road 的持有人和经营者涉嫌参与贩毒、盗取计算机资料和密谋洗钱，该网站成立于 2011 年，是一家黑市网站，帮助用户匿名购买或贩卖非法毒品、武器、盗窃的身份信息等非法商品或服务，躲避执法机关的调查。Silk Road 作为一个全球黑市交易网络平台，为匿名犯罪交易提供经纪服务，数千名贩毒分子和其他非法商家利用这一网站，向数十万名买家贩卖非法商品或服务。2015 年 5 月，Ross Ulbricht 因运营和持有非法网站，被曼哈顿联邦法院判处终身监禁。Silk Road 运营期间认可的唯一货币为比特币。

用于非法融资的公司组织形式

公司组织形式有多种，一些被用于非法融资活动。例如，犯罪分子可利用公司组织形式洗钱、进行行贿及其他腐败活动、掩藏资产、逃税等。公司、合伙制企业、信托公司等受滥用的组织形式均是最大程度实现所有权和真实目的匿名的最佳方式。

上市公司及非上市有限公司

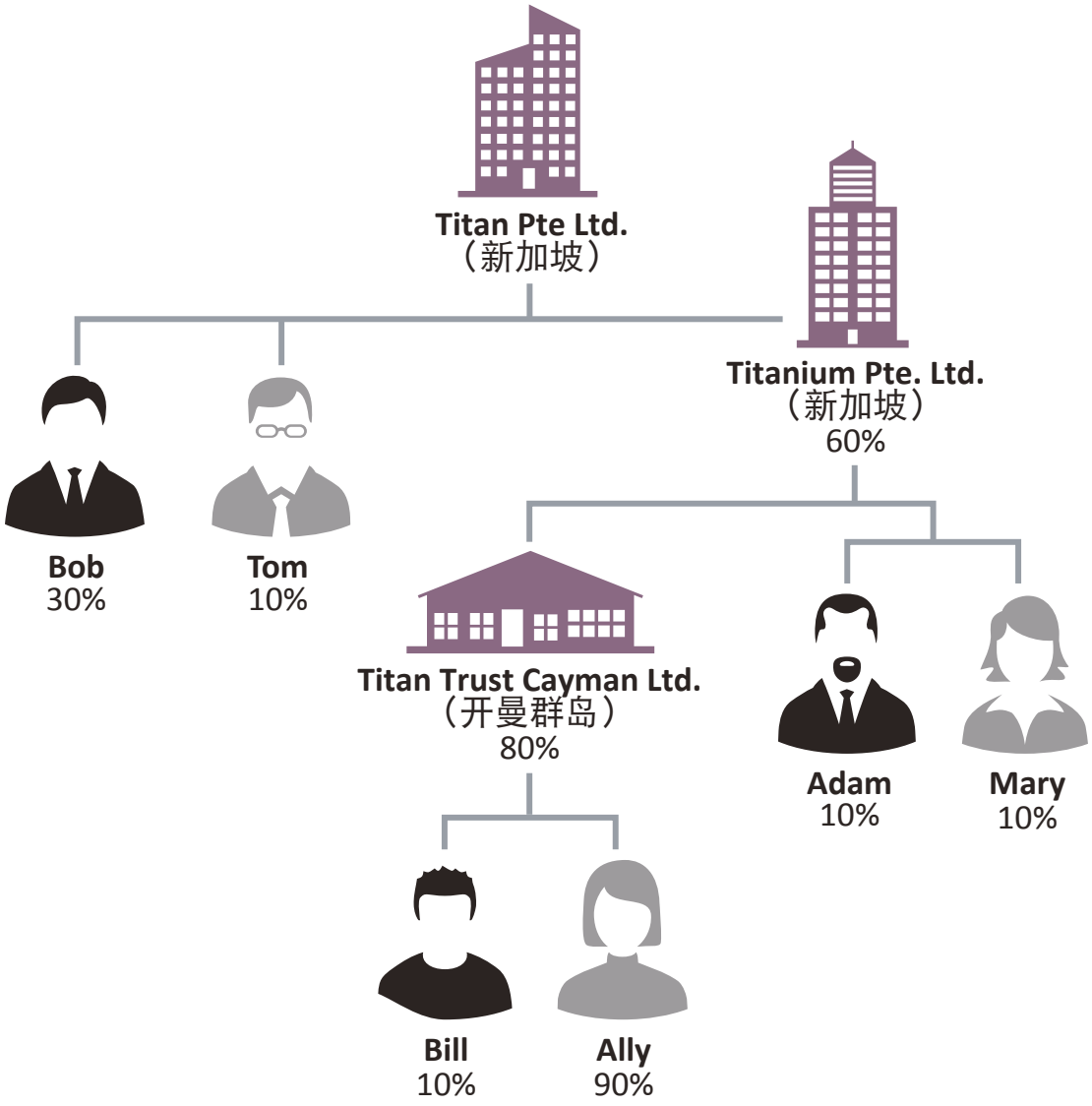
大多数司法管辖区的公司结构分为上市公司和非上市有限公司两种。上市公司的股份可自由获取和交易，对股东数量通常无限制，所有者和董事会成员的信息公开，公司受到较为严格的监管。非上市有限公司则与其相反，这种公司不可公开交易，股份数量也有限，所有者可为一人及以上，受到的监管相对宽松。

最常受到非法活动滥用的公司组织形式是有限责任公司 (LLC)。有限责任公司的所有者和管理人员可匿名，因而很受犯罪分子喜爱；几乎任何人都可以拥有或管理一家有限责任公司，包括外籍人士及其他商业机构。

有限责任公司的成员相当于公司的股东，管理者则相当于公司的高管或董事。有些有限责任公司可能没有专职管理者，而是由其成员负责管理工作。金融犯罪执法网络已采取一系列措施，以便更好地监控有限责任公司，因为并非每个州（特别是美国本土的有限责任公司）都对有限责任公司采取相同的措施和管控（特别是对管理者、最终受益人和代名人的监控、记录和报告）。

国际商业公司 (IBC) 是指在某人或公司常驻国境外建立的公司，通常出于保密或资产保护等原因在离岸司法管辖区设立。国际商业公司可降低所有者在其所在国的透明度，以及离岸公司在注册国的透明度。因此，这种公司具有以下优势：可保护资产，可进入多个投资市场，不动产规划优势，可获取合法的税务优势，可作为控股公司。国际商业公司的固有风险包括：通常设于避税天堂，通常需要当地代理参与，该代理可能会进一步降低国际商业公司的透明度（例如该代理作为代名所有者或董事），并帮助以国际商业公司的名义开立账户。私人投资公司 (PIC) 的建立和受利用方式与国际商业公司类似；然而，这种公司通常仅限于在税收中性的离岸金融司法管辖区持有投资资产。

公司组织形式案例



公司成立时的不记名股票

不记名债券和股票证书或者“不记名股票”表面上属于“持有人”，这使其成为主要的洗钱工具。不记名证券被转移后，由于没有所有者的登记，资金的转移发生在债券或股票证书实质交付之时。持有债券或股票的人基本可以主张所有权。

不记名股票为掩饰合法所有权提供了很多机会。为防止此问题的发生，金融行动特别工作组在 40 项建议中指出，金融机构的员工在签发、接受或设立不记名股票和信托前应询问受益所有人的身份。金融机构应保留这些信息的记录并与执法机关适当共享。

很多金融行动特别工作组成员国允许发行不记名股票并坚持认为，通过账面记录转移的方式，不记名股票在促进此类证券买卖时具有合法作用。有资料表明，不记名股票还可用来隐藏所有权，以实现税务优化的目的。

不记名支票其实就是无条件支付令（议付工具），见票后，金融机构必须向持票人而非向票据本身载明的特定收款人支付。不记名支票在很多国家都有应用。除非交易超过某一特定额度，否则金融机构通常不需要验证不记名支票出示人的身份。经原始被支付人背书后，记名支票也可能成为不记名支票，金融机构需向出示人支付。

空壳公司

尽管空壳公司可能出于合法目的而设立，但也可能被用于将犯罪所得转换成合法收入，或将犯罪所得混入合法收入中。金融行动特别工作组表示，使用空壳公司和空架公司来帮助洗钱是被记录较多的一种洗钱类型。金融行动特别工作组对此的定义如下：

- **空架公司：**不进行任何经营活动的公司。创建后便束之高阁。随后出售给需要已成立的而非新成立公司的个人。
- **空壳公司：**成立时没有实际重大资产或业务的公司。

2006 年 10 月，金融行动特别工作组发布了一份题为《包括信托和公司服务提供商在内的公司工具滥用》的报告。金融行动特别工作组在报告中指出，在有些司法管辖区，人们可以轻松地创建和解散各种公司组织形式，这种情况尤其值得关注，因为这使得公司既可用作合法目的（如企业财务、兼并和收购，或者地产和税务筹划），也可以被那些涉足金融犯罪的人员滥用，用于隐匿资金来源及所有权。

空壳公司可以在岸设立也可以离岸设立，其所有权结构也形式多样。股票可以面向自然人或法人，记名发行或不记名发行。有些公司创建目的单一或只持有单一资产。其他公司则可能是多功能实体。犯罪集团藉由通过合法途径注册空壳公司，来从事其非法的业务。它们经常从律师、会计师和秘书公司那里购买且是现货供应，是洗钱的便捷工具。有时，空壳公司发放不记名股票，任何持有该股票的人都是真实所有者。避税庇护所及其严格的保密法规可能进一步隐匿这些空壳公司的真正所有者。此外，这些信息可由要求保密的专业人员拥有。

金融行动特别工作组对影响洗钱防范和侦测系统有效性的规则和具体做法进行审查后发现，空壳公司及其代名人是清洗犯罪所得的常用机制。2001 年，一份题为《加拿大的洗钱活动：对 RCMP 案件的分析》的报告指出，出于洗钱目的而组建或控制空壳公司具备四个相互关联的原因：

1. 空壳公司企图将犯罪所得现金转变成替代性资产。

2. 通过使用空壳公司，洗钱者可制造非法资金来自合法渠道的认识。空壳一旦组建成功，就可在银行或其他金融机构开立商业账户。需要处理大量现金交易的传统行业对洗钱者格外具有吸引力，如零售店、饭店、酒吧、电子游戏室、加油站、食品超市等。非法所得可以由此作为合法收入存入银行账户，非法收入既可单独存入，也可与企业的合法收入混合存入。公司还为罪犯分子提供合法雇佣员工的来源，这反过来又有利于树立受人尊敬的企业形象。

3. 空壳公司一旦成立，就可运用大量合法或伪造的商业交易进行洗钱。此类交易包括由犯罪分子控制的公司间的借贷，虚假费用或薪水支出，将非法资金伪装成商品或服务交易的应付款进行转账，或者用犯罪所得购买不动产或将犯罪所得伪装成空壳公司发放的按揭来购买不动产。作为犯罪组织和其他洗钱工具之间的媒介，这些公司经营灵活，可以满足洗钱者的特殊需要。例如，犯罪组织通过房地产洗钱，就可将房地产公司、按揭经纪公司和建筑开发公司整合起来以方便获得房地产。

4. 利用空壳公司来隐藏其犯罪所得的所有权也很奏效。代名人可以充当所有者、董事、主管或股东。某国的公司还可作为别国公司的子公司（尤其是具有严格保密制度和信息披露法规的避税天堂），这对所有权调查造成了极大的障碍。通过将资产（如房地产）登记在公司名下，空壳公司还可隐藏罪犯资产的所有权。

犯罪企业还可利用真实企业来清洗非法所得。这些企业与空壳公司的不同之处在于，它们合法经营，以批发或零售的方式提供不同行业产品或服务。加拿大的报告指出如下与犯罪分子控制的公司有联系的洗钱手法：

- **使用被指定人作为所有者或董事：**为了划清与犯罪活动的联系，使用被指定人作为公司的所有者、高管和董事。被指定人一般没有犯罪记录。此外，由律师成立的公司一般注册在律师名下。
- **离析：**有些案件牵涉多家公司，其中许多公司的所有权层级非常复杂。这有助于隐匿犯罪所得的所有权，推动非法资金在公司的转移，模糊书面线索。
- **贷款：**犯罪所得可通过犯罪分子控制的公司间的借贷合法化。在一个案例中，毒贩将 50 万美元存入空壳公司名下的银行账户。这笔资金随后又“贷给”毒贩投资的餐厅。这种看似合法的资金使用制造了一种假象，即该资金合法地融入经济中。为避免外界怀疑，这 50 万美元的贷款也需支付利息。

- **虚构经营支出 / 虚假发票：**犯罪企业一旦在不同国家控制了公司实体，就可使用“双重发票”的洗钱手法进行洗钱。离岸公司从其位于其他国家的附属公司订购产品，并向其银行账户支付全款。两家公司都由犯罪集团拥有，商品的“货款”实际也是早前设法转移出境的非法资金回流。此外，如果附属公司报出高价，母公司记录就会显示较低水平的利润，这意味着母公司需要的税款也会减少。这种操作也可反向进行。离岸公司从母公司以很高的价格购买商品。商品真实价格和实际支付价格之间的差额被存入附属公司的账户。
- **出售企业：**犯罪分子出售企业时，他就获得了资本的合法来源。除非法资金可以流转外，出售企业还有其他益处，由于该企业表面上有用大量的现金流，所以更具投资吸引力，从而实现更高的售价。
- **购买已经归犯罪集团所有的企业：**“购买”已经归犯罪集团所有的公司是非常有效的洗钱方法。这是将此前秘密流往避税庇护所的非法资金回流最常用的方法。离岸犯罪所得被用来购买一家已经由犯罪企业拥有的公司。这样，洗钱者就成功地将秘密流往避税庇护所的大笔非法资金回流。
- **支付虚假薪水：**除了将犯罪所得申报为合法经营收入外，犯罪分子控制的公司还通过给某些犯罪活动的参与者发放“薪水”，将黑钱“漂白”。

信托

信托是私人授信安排，让与人或信托人将资产授信给他人，以便将来转给受益人。让与人 / 信托人通常安排第三方受托人根据信托合同的指示管理其资产。信托公司通常被视为和让与人相独立的法律实体；因此，信托往往有助于不动产规划和资产保护。让与人 / 信托人通常在指示中明确资产的分配方式，指示仅用于法律目的。

信托分为两种：一种是可撤销信托，让与人 / 信托人可终止信托；另一种是不可撤销信托，信托关系一旦建立，让与人不可终止。信托资产（本金）的资金可通过多种方式转给受益人，包括向受益人提供本金产生的收入，定期向受益人提供利息或本金，或对资金的发放设置条件（例如达到某种教育程度）。信托还可指定不动产继承人在信托协议到期后接收住宅（例如在让与人或受益人死后）。信托的灵活度和保护性相当高，已作为合法工具存在几个世纪。

无论离岸与否，信托账户在洗钱领域的重要性不可小视。它可用于将非法现金转换成不易招致怀疑的资产的第一步；它有助于掩饰犯罪资金或其他资产的所有权；也经常作为不同洗钱工具和手段间的基本联结点，如房地产、空壳企业和活动企业、代名人和犯罪所得的储蓄和转账。

在某些司法管辖区，建立信托可能是为了利用该国严格的保密规则，隐藏信托资产的真实所有人或受益人身份。信托关系也被用来隐藏合法债权人的资产，防止其因司法诉讼遭到查封，或隐藏资金流与洗钱和避税计划的各种联系。例如，资产保护信托 (APT) 是不可撤销信托的一种特殊形式，通常在海外创立（即设立），主要目的是保留和保护个人财产不受其债权人追索。资产所有权被转移给指定的受托人。资产保护信托通常用来保护资产，往往呈税收中性。其最终功能是为受益人服务。有些支持者宣称，资产保护信托允许外国受托人无视美国法庭命令并方便地将信托资产转移至另一司法管辖区，以应对威胁信托资产安全的法律诉讼。

对受益人的支付也可能被用于洗钱，因为无需证明这些款项是报酬或用于支付服务费用的资产转移。

律师经常作为受托人为其客户托管资金或资产。这样律师就能开展交易并管理客户的各种事务。有时，脏款以客户、代名人或客户控制的公司的名义存放在律师事务所的总信托账户。另外，管理信托账户也是律师常规职责的一部分，律师通过这些账户，代表客户接纳不动产并替其付款。

恐怖融资

2001 年 9 月 11 日恐怖袭击后，七国集团财政部长于 2001 年 10 月 7 日在华盛顿敦促所有国家冻结已知恐怖分子的资产。自此，不少国家都致力于协助查封恐怖主义资产。为此，各国就本国当局认为与恐怖主义有联系的个人和组织向金融机构发出警示。七国集团要求 FATF 于 2001 年 10 月 29 日在华盛顿主持召开恐怖融资主题“特别全体会议”。在此次会议上，FATF 发布了前八项特别建议，后来编入目前的 FATF 建议。*（详见第 2 章）*

第 5 项建议倡导各国将恐怖融资活动定为犯罪，包括资助恐怖组织和恐怖分子的行为，即使该笔资金并不直接用于实施恐怖活动，该建议还倡导各国将以上犯罪认定为洗钱活动的上游犯罪。如此一来，即可将反洗钱法规适用于恐怖融资活动，并加大检举和打击力度。切断对恐怖分子和恐怖组织的资金支持是扰乱其活动、防止恐怖袭击事件发生的必要手段。

恐怖融资与洗钱的异同

人们总是同时提起洗钱和恐怖融资活动，但往往忽视了两者间的重要差别。企业实施的很多监控措施都同时针对打击洗钱和反恐融资活动这两大目标。《2015 年美国恐怖融资风险评估》指出，为打击洗钱活动而实行的管控措施也加强了美国识别、遏制、扰乱恐怖融资活动的能力。因与恐怖组织有相关《银行保密法》记录而受到执法机关调查的人员中，58% 的人涉嫌参与洗钱活动，包括拆分交易。

然而两者毕竟是不同的犯罪，虽然至今没人能创建有效的恐怖主义金融档案，但一些关键差别的存在仍可帮助合规专员理解两者的差异并区分可疑恐怖融资活动和洗钱。

恐怖融资活动和洗钱的最根本差别体现在资金来源方面。恐怖融资活动将资金用于非法政治目的，但其资金本身并不一定是非法所得。为恐怖分子开展洗钱活动的目的是为恐怖活动提供资金。负责筹集资金的人并非洗钱资金的受益人。相反，洗钱所涉及的资金均为非法活动所得。洗钱的目的在于确保金钱可以合法使用。开展非法活动的个人通常为洗钱资金的最终受益人。

从技术角度看，恐怖分子与其他犯罪集团所用的洗钱方法是类似的。尽管拥有合法来源的资金不需清洗，但恐怖组织有必要隐藏恐怖活动与其合法资金来源之间的联系；原因之一是便于将来继续充分利用该来源。如此一来，恐怖分子采用与恐怖组织类似的手段，包括：走私现金、拆分交易、购买金融票据、电汇，以及使用借记卡、信用卡或预付卡。哈瓦拉体系这一非正规资金转移体系绕过合法的银行体系，采用个人信赖网络进行跨国资金转移，也在转移恐怖资金时发挥了一定的作用。此外，恐怖组织筹集的资金也会用于食品和房租等日常开销，并非只用于恐怖活动。

侦测恐怖融资活动

美国设立的对美恐怖袭击全国调查委员会 (National Commission on Terrorist Attacks Upon the United States) 在 2004 年发布关于恐怖融资活动的专题研究报告 (Monograph on Terrorist Financing)，文件指出，“9·11”劫机者和他们的金融支持者都不是国际金融体系的使用专家。恐怖分子的书面线索将他们和他们的资助人联系到一起。但他们仍足够老练地将自身融入宏大的国际金融体系，没有暴露自己作为犯罪分子的身份。当时的洗钱监控主要关注毒品走私和大规模金融欺诈，未对劫机者参与的交易投入足够的关注。自“9·11”事件以来，全球各地极大加强了对恐怖融资的侦测和打击。另一方面，恐怖分子和恐怖主义融资者为了应对这一变化，采取了更广泛、更多样的资金募集和转移手段，迫使执法机关和金融机构加快创新，提高警惕。

案例分析

“9·11”劫机者通过美国和外国的金融机构持有、转移并收回资金。他们主要通过电汇和现金存款或从海外带入旅行支票，将资金存入美国账户。部分成员将资金留在其外国账户中，通过 ATM 机和信用卡交易在美国提取。劫机者在进入美国前从巴基斯坦中转，并在此处获得来自德国和阿联酋资助人的资金。基地组织的整个计划耗资约 40 - 50 万美元，其中约 30 万美元通过劫机者在美国的账户获取。在美国，劫机者的主要支出是飞行培训、差旅以及和生活费用。

通过还原可用的财务信息，美国国税局和美国联邦调查局明确了“9・11”恐怖袭击劫机者获得资金的方式以及资金在其账户中流转的方式。19 名劫机者在 4 家银行开立了 24 个国内账户。以下是根据劫机者的美国账户整理的财务状况：

账户情况：

- 平均使用 3,000 - 5,000 美元现金或现金等价物开立账户。
- 开户身份为外国政府颁发的签证。
- 进入美国后 30 天之内开户。
- 部分账户为共用账户。
- 所用地址通常不是永久地址而是邮箱，并且经常更换。
- 劫机者在账户上通常使用同一个地址或电话号码。
- 12 名劫机者在同一家银行开户。

交易情况：

- 有些账户直接接收或发送来自或汇往阿联酋、沙特阿拉伯和德国等国的小额电汇。
- 劫机者多次试图提取超出借记卡限额的现金。
- 经常询问账户余额情况。
- 资金存入后迅速提取。
- 绝大多数交易低于报告要求的限度。
- 账户资金来自现金和海外电汇。
- ATM 交易发生时，有一名以上劫机者在场（数名劫机者在同一台 ATM 机上进行了一系列交易）。
- 使用借记卡的劫机者不是账户所有人。

国际活动：

- 两名劫机者由他人在美国匿名为其存款。

- 所有 4 架飞机上的劫机者都曾购买海外旅行支票并带入美国，这些旅行支票中的部分资金被存入美国的支票账户。
- 一名劫机者在 1998 年和 1999 年通过电汇获得来自同一个人的大笔资金，该笔资金存在德国银行账户。
- 1999 年这名劫机者在阿联酋开立了一个账户，并授权给那位过去一直给其德国账户汇款的人对阿联酋账户进行管理。
- 在 15 个月内，该劫机者在阿联酋的账户向其在德国的银行账户电汇 10 余万美元。

为了揭开恐怖融资活动不为人知的一面并给全球金融界提出建议，FATF 发布了用于识别恐怖融资活动方法与机制的指南。这份题为《金融机构侦测恐怖融资活动指南》的报告于 2002 年 4 月 24 日出版，介绍了恐怖融资活动的一般特征。其目的在于协助金融机构判断某一交易是否需要经过额外审查，从而更好地识别、（适时）报告并最终避免涉及恐怖活动的资金交易。FATF 在这份报告中建议，金融机构在评估潜在可疑活动时应做出“合理的判断”。为避免成为恐怖融资活动的通道，金融机构必须关注以下因素：

- 将账户作为某人的前台掩护，而此人可能与恐怖分子有联系。
- 账户持有人的姓名出现在可疑恐怖分子名单中。
- 经常向非营利组织账户存入大笔现金。
- 账户交易金额大。
- 账户持有人的业务性质与其银行活动之间缺乏明显的相关性。

FATF 建议，金融机构就应记住这些情形，注意查看典型的洗钱标志行为，包括低余额的不活动账户突然收到电汇存款，其后每天都有提现交易发生，直到该笔款项被全部提空，以及客户在被要求提供所需信息时不够合作。

恐怖分子如何筹集、转移和储存资金

全球各地的制裁行动已有效减少传统的恐怖主义资助国对恐怖组织的资金支持，导致这些组织开始寻求其他资金来源，以便其开展恐怖袭击。

2015 年 12 月，时任联合国秘书长潘基文在一次联合国安全理事会会议上指出，“恐怖分子利用各国金融和管理机制的薄弱环节进行筹资。他们利用新技术和工具转移资产并绕开正常渠道以躲避追踪。他们与毒品和犯罪集团等组织结成极具破坏性但获利丰厚的联盟。此外，他们还滥用慈善事业以欺骗民众向其提供捐助。恐怖分子不断采取各种技巧，开发多种资金来源。”潘基文表示，恐怖分子筹集资金的手段包括石油交易、勒索、隐蔽的现金快递、绑架、人口和武器贩运、敲诈等。

利用哈瓦拉和其他非正规价值转移体系

替代性汇款体系 (ARS) 或非正规资金转账体系 (IVTS) 通常与非洲、亚洲和中东地区的民族有关。替代性汇款体系通常绕过正规银行体系，以信托方式进行跨国价值转移。该体系在不同的国家或地区拥有不同的名称：哈瓦拉（Hawala，阿拉伯语，意为“变化”或“改变”）、亨递（Hundi，印地语，意为“收集”）、及第 (Chiti) 银行业务（意指该体系的运行方式）、地下钱庄（中国）和坡依款（Poey Kuan，泰国）。

早在数个世纪前，哈瓦拉就出现在印度和中国，旨在协助资金实现安全便捷的转移，此时西方金融体系尚未建立。希望将资金汇回国内的商人会将其资金存放在通常拥有贸易企业的哈瓦拉从业者处。在收取小额费用后，哈瓦拉从业者会通过安排确保该笔款项可在另一国的另一个哈瓦拉从业者处提取，而那位哈瓦拉从业者通常也拥有自己的贸易企业。两个哈瓦拉从业者则通过常规贸易流程进行账户清算。

如今，该流程基本保持原样，世界各地的商人通过自身的账户为第三方进行跨国资金转账。在这种资金转账方式下，存款和取款通过哈瓦拉“银行家”而非传统金融机构进行。第三方往往是需向母国进行小笔汇款但又不愿支付银行电汇费用的移民或海外劳工。人们合法利用哈瓦拉等非正规资金转账体系可能出于以下原因：资金转账更便宜快速，汇款接收国的银行服务有限，文化偏好，以及对正规银行体系缺乏信任。该体系通常不存在货币的实际转移且缺少关于身份验证和记录保存方面的正规手续。转移资金时，人们会通过便条、快递、信函、传真、电子邮件、短信或网上聊天等传递密码，再经过某种电信手段确认。几乎任何载有可识别数字的文件都可用作收款人在另一国家或地区收取该款项的证明。

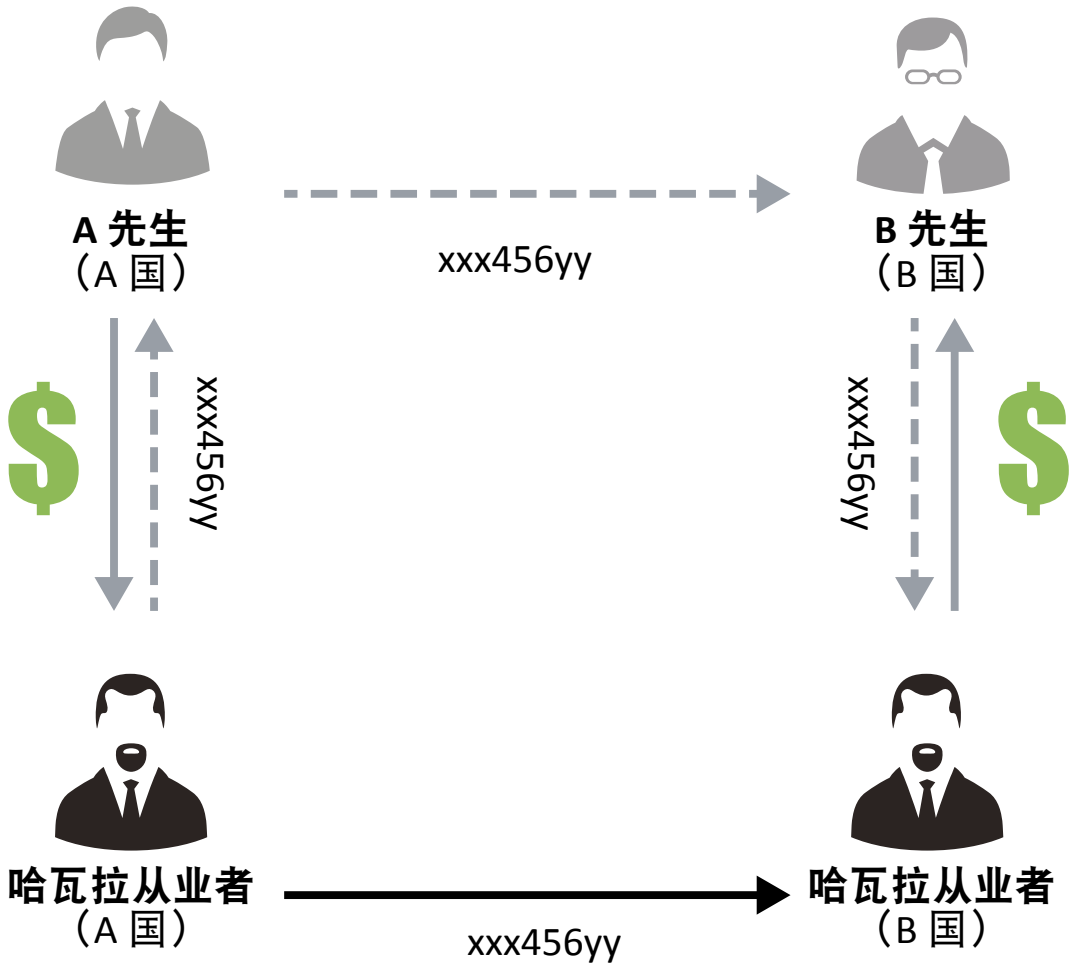
随着反洗钱措施在世界范围内的推广，不受政府监管的哈瓦拉对洗钱者和恐怖分子的吸引力与日俱增。2013 年，FATF 发布《哈瓦拉及类似服务供应商在洗钱 / 恐怖融资中的作用》，文件指出，对哈瓦拉及类似服务供应商的监管和监督仍是有关部门面临的一大重要挑战，并表示在其他领域，哈瓦拉及类似服务供应商受到的监管和监督越少，洗钱和恐怖融资风险越高。这些资金转移手段

对洗钱犯罪分子极具吸引力，因为经纪人将通过电话、传真和电子邮件等方式收到收款方的详细信息，几乎不会留下任何书面证据。近期，有关部门一直在关注哈瓦拉及类似代理对先进互联网技术的使用情况，并怀疑他们专门采用受保护的网络服务开展活动并维持账户，不留手动操作记录。

鉴于哈瓦拉是一个汇款体系，它可用于洗钱的任何一个阶段。它可以提供一种有效的处置手段：哈瓦拉从业者收到现金后，可将现金存入银行账户。并向银行工作人员解释其为合法业务所得。他还可能将部分现金用于支付业务费用，减少将现金存入银行账户的必要性。哈瓦拉从业者通常利用合法公司或幌子公司运作，掩护其活动，并将资金混入企业账户。

将资金从一账户转移到另一账户且尽量不留下书面线索是很多离析计划的一个部分。基本的哈瓦拉转账鲜少留下书面线索。经过离析后，在哈瓦拉转账中追踪资金更是难上加难。这可通过使用多个国家的哈瓦拉从业者以及分散转账时间来实现。

哈瓦拉交易案例



哈瓦拉技术几乎能将资金转变成任何形态，很容易在洗钱循环的融合阶段为资金提供表面合法性。该资金可重新投资于合法（或表面合法）业务。哈瓦拉从业者可以轻易地安排从美国向巴基斯坦的转账，然后再以商业投资形式转回美国。

哈瓦拉对恐怖融资活动也很有吸引力，因为它们不像正规金融机构那样始终受到政府的正式监管，也无需保留标准格式的详细记录。尽管部分哈瓦拉人员的确保存有部分分类账，但这些记录通常采用特殊的速记形式且保留时间很短。2001 年 9 月 11 日前，基地组织通过哈瓦拉转移了大量资金。基地组织动用了十几名可靠的哈瓦拉从业者，他们理所当然地知道资金的来源和用途。基地组织还动用了一些对资金来源和用途不知情的哈瓦拉从业者，这些人很可能怀疑其交易对象为基地组织，但却仍愿意参与交易。

案例分析

2011 年 8 月 18 日，Mohammad Younis 在曼哈顿联邦法院认罪，承认未经许可经营了美国与巴基斯坦之间的转账业务。其中一笔转账用于资助 Faisal Shahzad 于 2010 年 5 月 1 日在纽约市时代广场企图实施的汽车爆炸袭击，袭击者 Faisal Shahzad 被判处终身监禁，目前正在联邦监狱服刑。2010 年 1 月至 5 月期间，Younis 协助开展哈瓦拉业务，为纽约市的多名人员提供资金转账服务。2010 年 4 月 10 日，Younis 参与两笔独立的哈瓦拉交易，客户分别从美国康涅狄格州和新泽西州来到纽约市长岛与他约见。在上述两笔交易中，尽管 Younis 对这些资金的用途均不知情，但他在一名巴基斯坦共谋的指示下，给交易客户提供了数千美元现金。Younis 从未持有州政府或联邦政府颁发的资金转账业务许可证。他曾向多位客户提供资金，其中包括 Shahzad。Shahzad 因于 2010 年 5 月 1 日试图在时代广场引爆汽车炸弹而受到十项指控，当年 6 月 21 日，Shahzad 认罪。在认罪训示期间，Shahzad 承认于 2010 年 4 月在美国收到一笔现金，用于准备在 5 月 1 日实施爆炸。据 Shahzad 介绍，这笔现金由位于巴基斯坦的塔利班组织联系人安排，该组织是一个位于巴基斯坦的武装极端组织，其训练 Shahzad 如何制作和使用爆炸装置。2010 年 9 月 15 日，Younis 被美国联邦调查局和纽约联合反恐特别工作组的特工逮捕。他在法庭上供认无照经营资金转账业务。

滥用慈善组织或非营利组织 (NPO)

自 2001 年发生“9·11”恐怖袭击事件以来，美国政府发起恐怖融资追踪制度 (TFTP)，旨在识别、追踪和调查恐怖组织的资金来源。截至目前，美国政府已利用该制度侦破并关闭 40 多家慈善组织，它们被用作潜在募资前台机构。

慈善组织已经有意无意地成为恐怖分子筹集资金和洗钱的工具。因此，部分慈善组织收到的善款金额大幅下降，甚至成为其宣称的不公平调查或指控的对象，这种情况在与穆斯林有关的组织中尤为明显。金融行动特别工作组于 2014 年发布的《恐怖分子滥用非营利组织 (NPO) 风险》中指出：“非营利组织对国际社会的重要性显而易见。这些组织朝气蓬勃，为成百上千万的民众提供无可估量的服务。”然而，本“类型项目”发现，尽管恐怖分子和恐怖组织对非营利组织的滥用情况得到正式承认已有十年，但恐怖主义对这些组织的威胁至今仍然存在，而恐怖组织仍在继续通过各种手段滥用和恶意利用这类组织。

以下特征使得慈善组织或非营利组织特别容易成为恐怖融资活动所利用的对象：

- 享有公众信任。
- 掌握大量资金来源。
- 多使用现金。
- 通常在全球范围内运作，且经常位于或靠近恐怖活动多发地区。
- 活动通常很少或不受监管，且 / 或者设立几乎没有障碍。

为了帮助合法非营利组织避免与涉及恐怖主义的组织发生联系，重新获得公众的信任，金融行动特别工作组在 2002 年首次发布了打击滥用非营利组织最佳实践指南。2015 年，金融行动特别工作组更新了这份最佳实践指南，以便帮助各国根据风险为本的方法，落实第 8 项建议；帮助非营利组织减轻受到的恐怖融资威胁，并协助金融机构在向非营利组织提供金融服务时，适当采取风险为本的方法。

第 8 项建议的目的是确保非营利组织不受恐怖组织滥用，恐怖组织可能采取以下伪装：

- 恐怖组织伪装成合法公司。
- 恶意利用合法公司作为恐怖融资通道。
- 秘密将用于合法目的的资金转移给恐怖组织，掩藏或模糊此行迹。

最佳实践包括：各国及非营利组织等机构识别并缓释风险，非营利组织实行自我监管，非营利组织保障获取金融服务的途径。金融行动特别工作组建议非营利组织采取以下措施：

- 维护并展示完整的项目预算，说明所有花费的用途。
- 开展独立的内部审计和外部现场审计，后者的任务是确保资金被用于预期目的。

金融行动特别工作组建议慈善组织使用正规银行账户进行储蓄和转账，以便接受银行的监管和控制。反之，开户银行也能像对待其他客户一样对待非营利组织，对其开展“了解您的客户”工作，并报告可疑交易。

慈善委员会是监管英国英格兰及威尔士地区慈善组织的独立机构，旨在保护慈善组织中的公共利益，确保慈善组织践行造福公众的既定目标，并与私人利益、政府利益或政治利益保持独立。该委员会发布的《反恐战略报告》提出了一种四管齐下的方法，用以防止恐怖融资者滥用慈善组织，包括：

- 与国内外政府监管部门和执法机关合作。
- 就恐怖主义对慈善组织造成的风险提高行业意识。
- 积极开展行业监控，监管督查风险较高的领域。
- 在慈善组织明显受到恐怖活动滥用或存在滥用风险时实施干预。

案例分析

2013 年 5 月，美国明尼苏达州两名当地妇女因向美国认定的恐怖组织索马里青年党提供重大支持，被联邦法院判刑。Amina Farah Ali 和 Hawo Mohamed Hassan 均来自索马里，后入美国国籍，她们因向有关部门提供虚假口供、向恐怖集团提供重大支持等罪名分别被判处在联邦监狱服刑 20 年和 10 年。根据法庭上出示的证据，两名被告从 2008 年 9 月至 2009 年 7 月，向索马里青年党提供支持。索马里的青年党成员要求她们向组织提供金融支持，收到此要求后，她们在他人的帮助下，在美国明尼苏达州、其他州市以及加拿大的索马里人群体中寻求资金支持，为青年党筹款。她们谎称要资助不幸的人，骗取他人捐赠善款。她们安排人在电话会议中演讲，鼓动他人捐款，利用这些钱为青年党提供直接支持。一旦收到捐款，Ali 和其他人使用多种汇款服务，将超过十二笔资金汇出，收款人姓名均为虚构，以便隐藏这些资金的真实受益人——索马里青年党。

案例分析

圣地基金会 (Holy Land Foundation) 是一家伊斯兰教慈善机构，在美国多个地点开展业务，总部位于德克萨斯州理查森。2001 年，美国财政部关闭圣地基金会，认定其向美国指定的海外恐怖组织哈马斯提供支持，包括向约旦河西岸和加沙地带附属于哈马斯的圣地基金会办事处提供直接资金转账，向归哈马斯所有或由其成员控制的伊斯兰教慈善委员会等慈善组织提供转账。2008 年 11 月，圣地基金会及其五名主管因向恐怖主义提供重大支持，被美国政府处以刑罚。2014 年 4 月，另一家与圣地基金会类似的组织——困苦人群国际救助基金加拿大分

会，被加拿大公共安全局根据《刑法》认定并公布为恐怖主义组织。加拿大政府指控该组织于 2005 年至 2009 年向哈马斯输送了 1460 万美元，并宣称部分资金来源于圣地基金会，后转移给一家位于英国的非营利组织，再由该组织转账给位于加沙地带和约旦河西岸的几家巴勒斯坦救助组织，据了解，这些救助组织受哈马斯或其领头人物的控制。据信，圣地基金会和困苦人群国际救助基金加拿大分会的成立完全是为了向哈马斯提供金融及其他方面的支持。

恐怖融资的新风险

金融行动特别工作组发布的《2015 年恐怖融资新风险》详细列举了该领域的全新风险，包括：

- **外国恐怖主义分子 (FTF) 自行融资**

  随着社交媒体、智能手机应用程序以及互联网共享网站的发展，使恐怖组织如今能以低成本甚至零成本触抵世界各地。一种前所未见的新情况是，外国恐怖主义分子 (FTF) 和恐怖主义同情者可以激化自己的思想，或与恐怖组织联系。对“软弱的目标”（即平民，非军事人员的自保能力相对较低，因而易受到恐怖袭击）发动恐怖主义罪行的成本往往很低，因而这些罪行可自行资助。自行融资的资金来源包括工资、社会补贴、家庭支持、银行贷款等，如果不采取其他加强型恐怖融资指标，这些资金来源几乎不可能被侦测。

  2015 年 12 月 9 日，美国联邦调查局局长 James Comey 在美国参议院司法听证会上表示：“恐怖分子在无政府管辖地区散播毒害思想和训练材料，煽动全世界被毒害的灵魂加入他们。他们鼓动他人离开家乡，但如果这些人不出走，恐怖分子就会发动他们在家乡施暴。这是恐怖主义与十年前最大的不同之处。”

  案例分析

  2015 年 12 月 2 日，Syed Rizwan Farook 与其妻子 Tashfeen Malik 在美国加州圣贝纳迪诺开枪射杀了参加聚会的同事，致使 14 人遇难，22 人受伤。这对夫妇随后被警方击毙。联邦政府机关表示，Farook 生前的几年间变得越来越激进和暴力，其部分原因是他观看了宣扬圣战的视频。行凶当日，他的妻子在脸书上发布了对恐怖组织 ISIS (Islamic State in Syria) 效忠的誓词。这场袭击与大多数恐怖主义活动类似，均只需较少的资金即可实施。Farook 生前受雇于加州政府，是一名卫生巡视员，他在袭击中使用的部分武器便是利用工资收入购得（他曾委托他人购买武器）。他还通过互联网上的某个将投资者和借款人对接的点到点借贷平台，借贷 2.85 万美元。该借贷平台未观察到任何能引起其警惕的迹象，因而无从得知 Farook 的图谋，且 Farook 的工作和信用情况均证明其有能力偿还贷款。

- **利用社交媒体募资**

  社交媒体具有人类历史上从未出现过的强大能力，可搭建社交和信息共享网络。这一非凡的技术进步为恐怖组织提供了独特机会，他们可通过社交媒体宣传自己的活动并募集资金，且有可能几乎同时触抵每个国家的每个家庭。恐怖分子利用社交媒体募资的方式有很多，包括众筹以及分享虚拟或预付账户信息。这为执法机关带来特殊挑战，不仅因为活动涉及的范围更广，也因为执法活动需要得到金融机构和社交媒体平台的配合。

  案例分析

  Shafi Sultan Mohammad al-Ajmi 是利用社交媒体募资的典型案例，2014 年 8 月，美国财政部将其认定为叙利亚和伊拉克恐怖分子的支持者。Al-Ajmi 在社交媒体上定期开展宣传活动，为叙利亚战斗人员募集资金，是为努斯拉阵线 (ANF) 募资的人员中最活跃的科威特人。他曾公开承认自己以慈善的名义筹集资金，亲自将资金送给努斯拉阵线，还为该组织购买和走私武器。

- **新型支付产品及服务***（参见新型支付产品及服务的风险）*

- **恶意利用自然资源**

  一些恐怖组织已占领了某片土地，或在政府管制薄弱的国家组织活动，它们可能会控制当地的自然资源，例如天然气、石油、木材、钻石、金（及其他贵金属）、野生动物（如象牙交易），以及历史文物，或者勒索那些开发以上资源的公司，利用得来的资金发动恐怖袭击，维持组织的日常活动。这些资源可能在黑市上交易，或者被卖给同谋企业，以便融入全球贸易体系。这种恐怖融资方式可能为恐怖分子带来大量资金，为了打击这种活动，应关注恐怖组织活动或者恐怖分子控制的区域，了解大宗货物的当前价格，并加强跨司法管辖区的合作。

备注：

第 2 章

国际反洗钱和反恐融资活动标准

金融行动特别工作组 (Financial Action Task Force; FATF)

1989 年，七国集团在巴黎召开年度经济峰会时，联合成立了金融行动特别工作组 (FATF)，自此，反洗钱 (AML) 领域的国际行动力度大大加强。法国是工作组的第一任主席国，这一国际组织协调一致，并致力于打击国际洗钱犯罪活动。

金融行动特别工作组最初被称为七国集团金融行动特别工作组，现已成为为世界各国提供反洗钱指导的先锋力量。国际货币基金组织 (IMF) 和世界银行也为这一领域提供了重要的观点。

金融行动特别工作组给全球银行与企业的经营模式带来了巨大变革。同时，它也推动各国法律和政府运行模式不断的调整。

作为一个政府间组织，金融行动特别工作组的秘书处与经济合作与发展组织 (OECD) 联署办公，总部位于巴黎。金融行动特别工作组的官方网站为 http://www.fatf-gafi.org/。

金融行动特别工作组的宗旨

金融行动特别工作组的目标为“制定标准，推动有效落实法律、监管和业务手段，实施打击洗钱、恐怖融资和其他国际金融体系诚信的威胁。金融行动特别工作组要求成员国落实反洗钱相关建议；研究洗钱和恐怖融资手法及应对措施；推动各国采纳和落实其建议。”

为了实现这些目标，金融行动特别工作组重点关注以下任务：

1. 在全球范围内传播反洗钱信息：该组织基于成员国的扩展来推动在全球建立打击洗钱和反恐怖融资活动网络，促进世界各地区域性反洗钱组织发展，加强与其他国际组织的合作。
2. 监督成员对金融行动特别工作组建议的执行情况。

2011 年，金融行动特别工作组完成第三轮成员国互评估。互评估工作始于 2004 年。2014 年金融行动特别工作组开始第四轮互评估，并采用一种全新的评估方式，以评估各成员国在技术层面上的合规性及反洗钱 / 反恐融资体系的有效性。

新评估方法于 2013 年发布，其制定基础是金融行动特别工作组、类区域组织 (FSRB)、国际货币基金组织 (IMF) 和世界银行等国际组织对旧版 FATF 建议遵守情况的工作经验。通过评估一国反洗钱技术合规性和有效性，可综合分析该国对金融行动特别工作组建议的遵守情况，以及该国反洗钱 / 反恐怖融资体系运行在多大程度上是有效的。互评估包括以下内容：

- 技术合规性评估：评估金融行动特别工作组建议中的具体要求，包括成员国如何将这些建议纳入相关法律和制度框架，以及有关部门的权力和工作流程。评估的重点是各国反洗钱 / 反恐融资体系的构建基础。

  评估方将逐一对照每条建议，确定受评估国是否遵守金融行动特别工作组标准。技术合规程度分为五个等级，包括：

  - 合规
  - 基本合规
  - 部分合规
  - 不合规
  - 不适用

- 有效性评估：旨在评估成员对金融行动特别工作组建议的落实情况，了解成员在建立健全的反洗钱 / 反恐融资制度方面取得的重要成效。评估的重点是各国法律和制度框架取得了多大的成效。

  在 2013 年发布的评估方法中，金融行动特别工作组将有效性定义为“预设成果的实现程度”。有效性评估包括 11 条直接目标：

  1. 受评估国理解洗钱 / 恐怖融资风险，并采取协调措施打击洗钱 / 恐怖融资和扩散融资。
  2. 通过国际合作，传递有用信息，推动对犯罪及犯罪资产的打击行动。
  3. 监管机构对金融机构和非银行金融机构采取风险为本的反洗钱 / 反恐融资监管措施。
  4. 金融机构和非银行金融机构采取预防性措施，报告可疑交易。

5. 防止滥用法人进行洗钱 / 恐怖融资，主管部门无障碍地获取其受益所有权信息。
6. 主管部门利用金融情报信息开展洗钱或恐怖融资调查。
7. 洗钱犯罪活动得到调查、刑事起诉和制裁。
8. 犯罪所得充公。
9. 恐怖融资犯罪活动得到调查、刑事起诉和制裁。
10. 恐怖分子和恐怖组织的募集、转移和使用资金活动得到遏制，且其无法滥用非营利组织 (NPO)。
11. 涉及大规模杀伤性武器扩散的个人和组织的募集、转移和使用资金活动得到遏制。

11 条直接目标均为有效的反洗钱 / 反恐融资体系的核心目标。11 条直接目标中还包括 3 条体现反洗钱 / 反恐融资措施主要专项目标，分别为：

1. 旨在减少洗钱和恐怖融资活动的政策、合作与协作。
2. 防止犯罪所得进入金融系统，并在出现此类现象时报告。
3. 侦测并扰乱洗钱 / 恐怖融资威胁。评估方将逐一对照每条直接目标，确定受评估国是否有效，并根据受评估国对核心问题和特征的解决程度，提供有效性评级：

- 高度有效
- 基本有效
- 中等有效
- 低度有效

如果受评估国未能达到高度有效，评估方应说明原因，并提出建议措施，以便其增强自身能力，实现上述目标。

金融行动特别工作组对不合作成员国没有罚款或处罚权。然而在 1996 年，金融行动特别工作组针对不遵守建议的成员国制定了一项处理政策，即“同伴压力渐进递增法”。这一渐进递增法轻则要求成员国在全体会议上提交改进报告，重则中止成员国资格。

1996 年 9 月，土耳其成为首个受到“同伴压力渐进递增法”处理的成员。虽然土耳其早在 1990 年就已成为金融行动特别工作组成员国，但它尚未将洗钱定为犯罪。金融行动特别工作组向全球金融机构发出警示，要求它们在与土耳其人员和实体开展业务和交易时保持警惕，因为土耳其对洗钱缺乏监控。一个月后，土耳其颁布了反洗钱法。

3. 研究洗钱趋势及对策。

面对几乎没有地域限制、在各个时区不停运作并与全球电子高速公路保持同步的金融体系，犯罪分子总能不断找出新的薄弱环节，进而调整其洗钱手段，以应对金融行动特别工作组成员国和其他国家所采用的各项防范措施。因此，金融行动特别工作组成员国不断搜集洗钱趋势信息，确保提出的建议与时俱进。例如，2013 年 10 月，金融行动特别工作组与金融情报机构埃格蒙特集团联合发布一项关于钻石交易洗钱和恐怖融资风险的研究报告，研究了“钻石交易通道”的漏洞和风险，报告涉及钻石交易的方方面面，包括生产、钻石原石买卖、切割与抛光、珠宝制作以及珠宝零售。

自 1989 年创立以来，金融行动特别工作组一直采用五年制的委托权限。2004 年 5 月，成员国将该组织的委托权限延长至八年，达到历史最高，这预示着它可能成为全球打击洗钱和恐怖融资活动方面的永久性机构。2012 年 4 月，委托权限延长至 2020 年 12 月 31 日。

自成立之日起，金融行动特别工作组始终专注于以下三大主要工作：(1) 制定标准，(2) 促进标准的有效实施，(3) 识别洗钱和恐怖融资威胁。

在余下的委托期限内，这些仍是金融行动特别工作组的工作重心。展望未来，金融行动特别工作组将加强这些工作，应对全新威胁，如资助大规模杀伤性武器扩散融资、新技术漏洞等可能动摇国际金融体系安全的威胁。

金融行动特别工作组 (FATF) 40 项建议

金融行动特别工作组在反洗钱方面的一项关键工作是详细列举恰当标准，以便各国依照清单一一落实。“40 项建议”对这些措施进行汇总，于 1990 年首次发布，并分别于 1996 年、2003 年和 2012 年进行修订。此外还发布了一系列解释性说明，旨在明确建议的适用方式并提供额外指导。

2001 年，“9·11”恐怖袭击发生后，金融行动特别工作组通过了《反恐融资活动 9 项特别建议》。前 8 项特别建议于 2001 年 10 月 31 日通过，第 9 项则于 2004 年 10 月 22 日通过。2012 年的修订版本将 9 项特别建议纳入 40 项建议当中。

金融行动特别工作组的这些建议已成为世界各国打击国内和国际洗钱和恐怖融资活动的重要指引。国际货币基金组织和世界银行将金融行动特别工作组的建议视为打击洗钱和恐怖融资活动的国际标准。2002 年，国际货币基金组织、世界银行和金融行动特别工作组通过了一套评估建议合规情况的通用方法。

40 项建议提供了一套完整的反洗钱和反恐融资活动措施，其中包括：

- 风险的识别以及适当政策的制定。
- 刑事司法制度和执法。
- 金融体系及其监管。
- 法人和法律安排的透明度。
- 国际合作。

金融行动特别工作组认为，由于各国的法律和金融体系各异，它们不能使用完全相同的措施来打击洗钱和恐怖融资活动。建议根据各国的特殊国情和宪法框架设定了最低行动标准。在 2012 年的修订中，金融行动特别工作组将风险评估定为第 1 项建议，认为风险评估是打击洗钱和恐怖融资活动的首个步骤。

在 2003 年发布的修订版 40 项建议中，金融行动特别工作组将范围扩展至打击资金的非法流动方面。为了增强打击洗钱和恐怖融资活动的措施，金融行动特别工作组对建议进行了实质性的修改，进一步提高设定标准，以便各国能够更好地打击洗钱和恐怖融资活动。

2003 年，金融行动特别工作组对建议进行重大修改，具体如下：

- 将恐怖融资活动纳入覆盖范围。
- 拓宽了各国法律所应涵盖的业务种类，包含房地产经纪商、贵金属经销商、会计师、律师以及信托服务提供商。
- 就客户身份识别和尽职调查等问题规定了具体的合规程序，包括适用于高风险客户和交易的强化身份识别措施。
- 对洗钱的上游犯罪进行了更为明确的定义。
- 鼓励各国禁止一般设立在离岸保密庇护所且仅有名称招牌和邮箱的“空壳银行”，并致力提高法人和法律安排的透明度。
- 包含了更严格的保护性条款，特别是诸如针对恐怖融资活动调查的国际合作条款。

2012 年，金融行动特别工作组再次修订建议，将 9 项关于恐怖融资的特别建议纳入 40 项建议之中。此次修订最为重要的内容为：

- 针对所有反洗钱 / 反恐融资活动中的风险评估和以风险为本的方法实施情况制定了一项建议。
- 针对大规模杀伤性武器的扩散进行金融制裁制定了一项建议。
- 更为关注国内政治公众人物 (PEP) 以及在国际组织中担任重要职务的人员。
- 提出在推出新产品前对新产品的风险进行识别和评估的新要求。
- 新增一项要求，即要求金融机构在全集团内实施反洗钱和反恐融资制度并制定团体内的信息共享程序。
- 将涉税犯罪列入洗钱上游犯罪类别。

组织	主题	建议
I	**反洗钱和反恐融资活动政策和协调** • 评估风险并采用风险为本的方法 • 国家层面的合作和协调	1-2
II	**洗钱和没收** • 洗钱犯罪 • 没收或临时措施	3-4
III	**恐怖融资活动和扩散融资** • 恐怖融资犯罪 • 对恐怖主义和恐怖融资活动执行金融制裁 • 对大规模杀伤性武器的扩散执行有针对性的金融制裁 • 非营利组织	5-8
IV	**金融和非金融机构防范措施** • 金融机构保密法律 • 客户尽职调查和记录 • 针对特定客户和活动的额外措施 • 信赖、控制措施和金融集团 • 报告可疑交易 • 特定非金融行业	9-23
V	**法人和法律安排的透明度和受益所有权** • 法人的透明度和受益所有权 • 法律安排的透明度和受益所有权	24-25

组织	主题	建议
VI	**主管部门的权力、职责以及其他制度性措施** • 监管和监督 • 行动和执法措施 • 一般要求 • 制裁	26-35
VII	**国际合作** • 国际公约 • 司法互助 • 冻结和没收方面的司法互助 • 引渡 • 其他形式的国际合作	36-40

2012 年对 40 项建议的修订中最为重要的修改为:

- **风险为本的方法:** 各国应首先对其面临的洗钱以及恐怖融资活动的风险进行识别、评估和了解，之后应采取恰当的措施来降低已识别的风险。风险为本的方法允许各国根据自身的国情，有针对性地利用有限的资源，提高防范措施的有效性。金融机构也应使用风险为本的方法识别和减轻其面临的风险。

- **指定的犯罪类型:** 该建议明确了应被视为洗钱上游犯罪的“指定犯罪类型”（犯罪分子企图通过金融诡计隐藏的犯罪即构成洗钱上游犯罪）。各国还应制定与没收犯罪所得相关的法律或以其他方式阻止犯罪分子获得犯罪所得。

- **恐怖融资活动和扩散融资:** 各国应将恐怖融资活动定为犯罪，包括资助恐怖行为、组织和恐怖分子，即使该笔资金并不直接指向恐怖活动。各国应建立制裁机制，支持冻结联合国安理会指定的参与恐怖活动或大规模杀伤性武器扩散的个人的资产。各国还应采取充分的措施来减轻非盈利组织被恐怖分子滥用的现象。

- **明知和刑事责任:** 该建议包括了这样一个概念: 可从客观事实情况推断出确定洗钱罪所需的“明知”。这与一些国家所定义的“有意忽视”或“有意回避明知的事实”类似。此外，建议还敦促各国对法人适用刑事责任（如不适用刑事责任，则适用民事或行政责任）。

- **客户尽职调查 (CDD) 措施:** 金融机构应在以下情形下进行客户尽职调查:

  — 建立业务关系。

  — 进行超过特定限额的一次性交易或电汇。

  — 怀疑存在洗钱或恐怖融资活动。

— 对先前获得的客户身份识别信息的真实性或充分性存在质疑。

金融机构必须使用风险为本的方法，采取以下措施：

— 确认客户身份，并利用可靠、独立来源的文件、数据或信息核实该客户的身份。禁止匿名或使用明显的假名开立账户。

— 采取合理措施核实受益所有人的身份，使金融机构确信了解受益所有人。对于法人和法律安排，则应包括了解客户的所有权和控制结构。

— 了解并在适当情形下获取关于业务关系目的和意图的信息。

— 对业务关系进行持续的尽职调查并仔细审查该关系进程中进行的交易，以确保交易与机构对客户、客户业务和风险状况（在必要时还包括资金来源）的认知相符。

— 保留上述客户信息以及所有交易的记录，确保其符合相关主管当局的要求。

— 特定情况下依托第三方开展客户尽职调查；然而，该第三方机构仍有责任完成必需的客户尽职调查。

— 在全集团内建立反洗钱制度。

- **针对特定客户和交易的额外尽职调查：**某些类型的客户和交易具有较高的风险，特别是：

  — **政治公众人物 (PEP)：**必须采取恰当措施识别政治公众人物，包括建立业务关系时获得高级管理层的批准，采取措施识别财富和资金的来源以及进行持续的监控。

  — **跨境代理行业务：**必须采取适当措施，以便了解代理行的业务、声誉、监管和反洗钱管控情况；建立代理行关系需经管理层批准；明确规定每个机构的职责；降低通汇账户的风险；确保账户并非由空壳银行开设。

  — **资金或价值转移服务 (MVTS)：**各国应确保资金或价值转移服务已获得许可或经过登记，并已满足适当的反洗钱要求。

  — **新技术：**各国和金融机构应评估与新产品的开发、商业实践、交割机制和技术相关的风险。金融机构应在推出新产品前评估这些风险；它们还应采取恰当的措施来降低已识别的风险。

  — **电汇：**各国应要求金融机构在办理电汇时获得所需的汇出方、中介方和受益人的准确信息。金融机构应监控电汇中的不完整信息并采取恰当的措施。金融机构还应监控电汇交易是否涉及联合国安理会指定个人或实体，并采取冻结措施，禁止交易进行。

- **可疑交易 / 活动报告：**金融机构如果怀疑或有合理的理由怀疑资金与犯罪活动所得或与恐怖融资活动相关，则必须向相关金融情报机构报告。在依法报告可疑交易时，金融机构及其员工应受到法律保护，严禁向外泄露其报告可疑活动的行为。

- **行业覆盖范围的扩大：**为加大打击洗钱的力度，建议将一些新的非金融行业纳入到金融机构的范畴中来，以作为反洗钱工作的重点环节。扩大反洗钱审查范围是许多政府为应对日益增加的非法资金流通而在反洗钱工作中着重加强的一个关键领域。这些特定非金融行业 (DNFBP) 包括：

  — 赌场，当客户从事的金融交易金额等同或超过指定限额。赌场至少应持有许可执照；相关机构应防止犯罪分子参与赌场运营并应对赌场进行监管，以确保其遵守反洗钱和反恐融资活动的要求。

  — 房地产中介商，当其为客户进行房地产买卖交易时。

  — 贵金属和宝石经销商，当其与客户进行的任何现金交易超过指定限额。

  — 律师、公证员以及独立法律专业人员和会计师，当他们为客户准备或执行以下交易，包括买卖房地产；管理客户资金、证券或其他资产；开立或管理银行、储蓄或证券账户；为创办或管理公司筹集资金；创建、运作或管理法人或法律安排；买卖企业。

  — 信托和公司服务提供商，当其为客户准备或执行与某些特定交易相关活动时（如担任创建法人的代理机构；担任公司的董事或秘书；担任明示信托受托人；或担任第三人的代名股东）。

  金融行动特别工作组还明确规定了引发反洗钱审查的限额。例如，金融机构对一次性客户的监控限额为 15,000；对赌场（包括网上赌场）的监控限额为 3,000；对贵金属交易商的现金交易活动的监控限额为 15,000。

- **法人和法律安排的透明度和受益所有权：**各国应采取恰当措施防范法人被洗钱或恐怖融资活动所滥用，包括确保向相关主管当局提供关于受益所有权和此等法人控制权的信息，特别是与可以发行不记名股票或拥有代名股东或董事的法人相关的信息。

- **主管当局的权力和责任：**各国应监督金融机构，确保金融机构正在执行金融行动特别工作组建议，且拥有或控制该机构的人员并非犯罪分子。监管者应获得充分的资源和权力，以便在其司法管辖区内有效地监管金融机构。在参与某些金融活动时，特定非金融行业和个人也应接受监管。各国应建立金融情报机构并向执法和调查当局提供充分的资源和权力，以便调查

洗钱和恐怖融资活动并查扣或冻结调查发现的犯罪所得。各国应采取措施监测货币和不记名可转让票据的实际跨境转移。各国应提供与反洗钱和反恐融资活动相关的有用数据、指南和反馈。

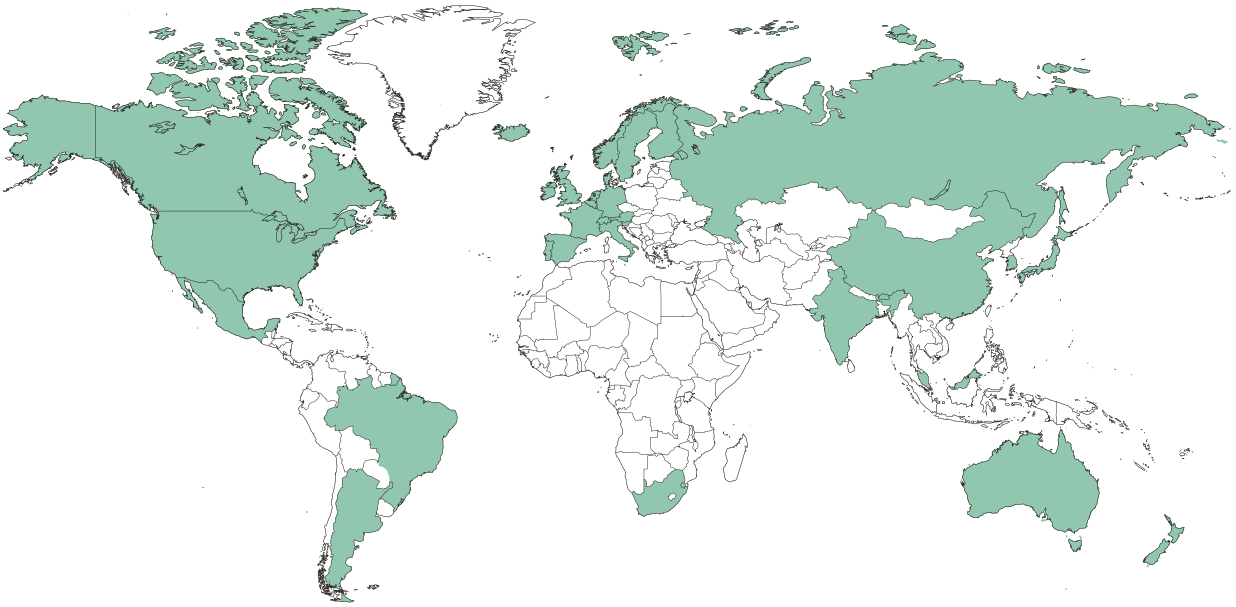
- **国际合作：**部分建议涉及国际合作的加强。各国在洗钱和恐怖融资活动调查、冻结和没收犯罪所得、引渡以及其他事项方面，应迅速、积极且高效地提供尽可能广泛的司法互助。各国应批准涉及打击重大犯罪和恐怖主义的联合国公约。

金融行动特别工作组 (FATF) 成员及观察员

金融行动特别工作组现有 37 个成员，其中包括 35 个司法管辖区和 2 个区域性组织（海湾合作委员会[1]和欧洲委员会）。另有 31 个准成员参与该组织的工作，或称金融行动特别工作组的观察员（多为国际或区域组织）。虽然海湾合作委员会 (GCC) 是金融行动特别工作组的正式成员，但海湾合作委员会的各个成员国（巴林、科威特、阿曼、卡塔尔、沙特阿拉伯和阿联酋）却并非金融行动特别工作组的成员。

金融行动特别工作组成员中的 35 个司法管辖区包括：阿根廷、澳大利亚、奥地利、比利时、巴西、加拿大、中国大陆、丹麦、芬兰、法国、德国、希腊、中国香港、冰岛、印度、爱尔兰、意大利、日本、韩国、卢森堡、马来西亚、墨西哥、荷兰、新西兰、挪威、葡萄牙、俄罗斯、新加坡、南非、西班牙、瑞典、瑞士、土耳其、英国和美国。

[1] 虽然海湾合作委员会 (GCC) 是金融行动特别工作组的正式成员，但海湾合作委员会的各个成员国（巴林、科威特、阿曼、卡塔尔、沙特阿拉伯和阿联酋）却并非金融行动特别工作组的成员。



金融行动特别工作组 (FATF) 成员

阿根廷	中国	香港（中国）	韩国	挪威	瑞典
澳大利亚	丹麦	冰岛	卢森堡	葡萄牙	瑞士
奥地利	芬兰	印度	马来西亚	俄罗斯联邦	土耳其
比利时	法国	爱尔兰	墨西哥	新加坡	英国
巴西	德国	意大利	荷兰	南非	美国
加拿大	希腊	日本	新西兰	西班牙	

金融行动特别工作组成员遴选标准

在考虑将某个国家或地区作为金融行动特别工作组成员候选对象时，会采用以下标准：

a) 根据以下量化指标、定性指标和其他考量，该司法管辖区应具有战略重要性：

— *量化指标：*
  > 国内生产总值 (GDP) 的规模。
  > 银行业、保险业和证券业的规模。
  > 人口

— *定性指标：*
  > 对国际金融体系的影响，包括金融部门的开放程度及其与国际市场的相互作用。
  > 积极参加与金融行动特别工作组类似的区域性组织 (FSRB)，以及反洗钱 / 反恐融资活动工作中的区域性声望。
  > 对反洗钱和反恐融资活动工作的投入程度。
  > 反洗钱和反恐融资活动的风险程度以及打击风险的投入程度。

— *其他考虑因素：*
  > 对金融部门标准的遵守程度。
  > 参与相关的其他国际组织。

b) 该司法管辖区加入金融行动特别工作组后，应能提高该组织的地域平衡。

金融行动特别工作组成员申请过程

第 1 步——与该国或地区接触，授予观察员身份

a) 该国或地区应提供政治 / 部长级的书面承诺：

i. 通过并支持金融行动特别工作组 2012 年度建议和金融行动特别工作组 2013 年度反洗钱 / 反恐融资方法（以及未来的修订版）。
ii. 同意在成员资格申请流程中完成互评以评估其符合金融行动特别工作组成员资格标准的程度，使用当时可用的反洗钱和反恐融资活动方法，同意提交后续跟踪报告。
iii. 同意积极参与金融行动特别工作组并实现金融行动特别工作组成员的其他所有承诺，包括支持金融行动特别工作组在所有相关论坛中的职能和工作。

b) 全体会议决定安排对该国或地区的高层访问活动，以便与相关部长、国会代表和合格机构验证书面承诺，确定该国或地区是否具备成功实施互评并在 3 年内取得满意的技术合规水平的条件，包括对建立有力反洗钱 / 反恐融资制度必不可少的建议的合规情况，比如第 3、5、10、11 和 20 条建议。同时还要考虑该国或地区必要建议的实施水平，以及其应第 1 条建议的要求，在评估和处理其洗钱 / 恐怖融资风险方面的进度。高层访问团应包括金融行动特别工作组组长、指导小组部分成员以及代表团团长。访问团由金融行动特别工作组秘书陪同。高层访问报告将在下一次全体会议上宣读。

c) 根据高层访问报告结果，全体会议可以决定邀请该国或地区从下一次全体会议开始，以观察员身份参加金融行动特别工作组的活动。如果全体会议决定不邀请该国或地区以观察员身份参加金融行动特别工作组会议，则可以指定一个联络小组，就向该国或地区发出此邀请的合适时间提出建议。此后，联络小组应与该国或地区的合格机构接触，确定该国或地区何时能具备成功实施第 2 步所述互评的条件。联络小组向所有金融行动特别工作组成员和准成员开放，应至少包括指导小组的一名成员。联络小组由金融行动特别工作组秘书处协助开展工作。联络小组将定期召开会议，并在每次全体会议上报告该国或地区取得的进步。

第 2 步——实施互评，就行动计划达成一致，授予成员资格

该国或地区受邀成为金融行动特别工作组观察员后的三年内，必须开启互评活动。在此期间，可以由一个新的联络小组帮助该国或地区确保已经做到互评准备。

如果互评结果令人满意，则金融行动特别工作组将向该国授予会籍。如果该国或地区有以下表现，则互评结果不理想，包括：

- 在技术合规方面有 8 个或以上不合规或部分合规的评级；
- 第 3、5、10、11 和 20 条建议中的任何一条或多条被评定为不合规或部分合规；
- 在 11 项有效性效果中，有 7 项或以上的有效性评级为低或中等；
- 在 11 项有效性效果中，有 4 项或以上的有效性评级为低；
- 在 11 项有效性效果中，有 4 项或以上的有效性评级为低。

如果互评结果达不到但接近满意程度，则该国或地区应在政治 / 部长级明确承诺将在合理时间内（不超过 4 年）达到预期结果。该国或地区准备一份详细的行动计划，规定好要采取的措施及时间框架，并在经第二联络小组审核后交由金融行动特别工作组全体会议表决。

在每次金融行动特别工作组会议上，全体会议会密切监控该国或地区行动计划的实施情况：

- 如果对进步的节奏或程度不满意，全体会议可以决定对该国或地区采取“金融行动特别工作组第四轮反洗钱 / 反恐融资互评程序”第 77 段里列出的强化措施
- 只要第 3、5、10、11 或 20 条建议中的任意一条或多条的评定结果为不合规或部分合规，都不会授予某国或地区正式成员资格
- 除此以外，在该国或地区实施行动计划的过程中，在行动计划实施完毕之前，全体会议可以根据该国或地区的进度，随时决定授予正式成员资格。

不合作国家

金融行动特别工作组自成立之日起，针对反洗钱控制措施持续不力或拒不配合全球反洗钱 / 反恐融资工作的国家，采用“点名批评”的做法。多年以来，金融行动特别工作组一直致力于识别全球反洗钱斗争中的“不合作国家和地区”(NCCT)。金融行动特别工作组通过其所制定的流程来寻找特定司法管辖区在反洗钱制度上存在的严重缺陷，正是这些缺陷妨碍了该领域的国际合作。

2000 年 2 月 14 日，金融行动特别工作组发布首份《不合作国家和地区》报告，公布了 25 条有助于识别相关有害规则与做法的标准，这些标准与 40 项建议保持一致。通过程序能识别使用这类规则和实践的司法管辖区，并鼓励它们在这一领域执行国际标准。

25 项标准涵盖了以下四大领域：

1. 金融监管中的漏洞：

   — 缺乏对金融机构的监管或监管不充分。

   — 许可和建立金融机构的规则不充分，包括对管理层和受益所有人背景的评估。

— 金融机构的客户身份识别要求不充分。

— 金融机构保密规定过多。

— 缺乏有效的可疑交易报告制度。

2. 因其他监管要求而引起的障碍：

— 企业和法律实体注册方面的商法要求不充分。

— 缺乏对法人和企业实体受益所有人的身份识别。

3. 国际合作方面的阻碍：

— 来自行政管理当局对合作的阻碍。

— 来自司法机关对合作的阻碍。

4. 防范和侦测洗钱活动的资源不充分：

— 公共和私营机构的资源缺乏。

— 缺少金融情报机构或同类机制。

“不合作国家和地区程序”的目标是：通过确保所有金融中心根据国际公认标准制定并实施防范、侦测和惩罚洗钱的措施，以降低金融体系在洗钱方面的脆弱性。随后，金融行动特别工作组继续推进不合作国家和地区行动，于 2000 年 6 月发布首份审查报告，指出 15 个不合作国家和地区。受到不合作国家和地区行动点名批评的司法管辖区共有 24 个，最多曾一次性点名 19 个司法管辖区，这些成员采取必要改善措施后，才被金融行动特别工作组从名单中删除。名单清空后，金融行动特别工作组才中止该行动。

金融行动特别工作组如果再次发现有司法管辖区的反洗钱 / 反恐融资体系存在缺陷，会重新启动不合作国家和地区行动，制定不合作国家和地区名单。金融行动特别工作组的这一新流程响应了二十国集团公开识别高风险司法管辖区并对存在战略缺陷的司法管辖区发布定时更新的努力。如今，金融行动特别工作组在以下两份每三年公布一次的文件中点名这些司法管辖区。

1. 金融行动特别工作组公开声明公布的国家或司法管辖区：

- 或存在重大战略缺陷，须实施应对措施，此类国家或司法管辖区可为金融行动特别工作组的成员或非成员。
- 或须根据本国缺陷引发的风险，实行增强尽职调查措施，此类国家或司法管辖区为金融行动特别工作组的成员。

2. *改善全球反洗钱 / 反恐融资活动合规情况的持续性流程*识别那些反洗钱 / 反恐融资措施存在战略漏洞，但高度落实金融行动特别工作组制定的行动计划的国家或司法管辖区。

   - 金融行动特别工作组鼓励成员根据这些司法管辖区的战略缺陷进行自省。
   - 如果某国未能及时进步，或进步程度不足，则金融行动特别工作组可对该国施加更大压力，通过在《公开声明》中点名，迫使其进步。
   - 这份文件还公布无需加入全球反洗钱 / 反恐融资活动合规情况持续性流程的司法管辖区。通常，如果某国针对以往识别的战略缺陷，建立法律或监管框架，兑现其对行动计划的承诺，则可认定该国已在改善反洗钱 / 反恐融资体系方面做出重大进步。然而，该国必须继续和适当的与金融行动特别工作组类似的区域性组织合作，解决互评报告指出的问题。

巴塞尔银行监管委员会

巴塞尔银行监管委员会由十国集团的中央银行行长于 1974 年组建，旨在全球范围内推行完善的银行监管标准。委员会是银行业审慎监管标准的全球首要制定机构，也是银行业监管事务的合作平台。委员会的宗旨是以提高金融稳定性为目标，加强对全球银行的监管、监督和实践。委员会的秘书处设于瑞士巴塞尔，与国际清算银行联署办公，其员工大多为专业监管人员，是成员机构派遣的临时员工。

巴塞尔银行监管委员会成员	
国家	**机构**
阿根廷	阿根廷中央银行
澳大利亚	澳大利亚储备银行 澳大利亚审慎监管局
比利时	比利时国家银行
巴西	巴西中央银行
加拿大	加拿大银行 加拿大金融机构监管办公室
中国大陆	中国人民银行 中国银行业监督管理委员会
欧洲联盟	欧洲中央银行 欧洲中央银行单一监督机制
法国	法国银行 法国审慎监督管理局
德国	德意志联邦银行 德国联邦金融监管局 (BaFin)
香港特别行政区	香港金融管理局
印度	印度储备银行

巴塞尔银行监管委员会成员	
国家	**机构**
印度尼西亚	印度尼西亚银行 印度尼西亚金融服务管理局
意大利	意大利银行
日本	日本银行 日本金融监管厅
韩国	韩国银行 韩国金融监督院
卢森堡	卢森堡金融监管委员会
墨西哥	墨西哥银行 墨西哥银行与证券委员会
荷兰	荷兰银行
俄罗斯	俄罗斯联邦中央银行
沙特阿拉伯	沙特阿拉伯货币管理局
新加坡	新加坡金融监管局
南非	南非储备银行
西班牙	西班牙银行
瑞典	瑞典中央银行
瑞士	瑞士国家银行 瑞士金融市场监督管理局 (FINMA)
土耳其	土耳其共和国中央银行 土耳其银行监管署
英国	英格兰银行 英国审慎监管局
美国	联邦储备银行理事会 纽约联邦储备银行 货币监理署办公室
巴塞尔银行监管委员会观察员	
国家	**机构**
智利	阿根廷中央银行
马来西亚	马来西亚中央银行
阿联酋	阿联酋中央银行

巴塞尔委员会历史

银行监管机构通常并不负责各自国内的洗钱刑事指控。但他们有极大责任确保银行制定一定程序，例如严格的反洗钱政策，以避免卷入毒贩和其他犯罪分子的非法活动，并促进金融部门道德与职业标准的提升。20 世纪 90 年代早期的国际商业信贷银行 (BCCI) 丑闻、1992 年对意大利 Banca Nazionale del Lavoro 亚特兰大分支机构前任官员的起诉及其认罪答辩，以及其他国际银行业丑闻，促使最富有国家的银行监管机构就跨国银行监管和运营的基本规则达成一致。

1988 年，巴塞尔委员会发布了名为《防止犯罪分子利用银行系统洗钱》的原则声明，承认金融部门可能被犯罪分子滥用。这是防止洗钱犯罪分子滥用银行业洗钱的一大进步。声明就以下问题制定了原则：

- 客户身份识别。
- 法律合规。
- 遵守严格的道德标准和当地法律法规。
- 在不违反客户保密规定的前提下，在允许的范围内与国内执法机构全力合作。
- 员工培训。
- 记录保存和审计。

这些原则制定后，一些反洗钱法规才相继出台，这些法规规定，必须向执法机关披露客户信息，并防止执法机关因违反客户保密规定而被客户提起民事诉讼。因此，这些原则强调合作应局限在遵守保密规定的范围之内。

1997 年，巴塞尔委员会发布了《有效银行业监管的核心原则》，为全球监管当局提供了基本的参考依据。该文件指出：“银行业监管机构必须确定银行制定了充分的政策、实践措施和各种程序，其中包括严格的‘了解您的客户’规则，从而提高金融行业的道德和职业标准，并防范银行有意或无意被犯罪因素所利用。”该文件还敦促各国采纳金融行动特别工作组 40 项建议。该核心原则在 15 个非十国集团国家和地区的协助下编写完成，这些国家和地区包括巴西、智利、中国香港、墨西哥、俄罗斯、新加坡和泰国。

为了推动执行和评估，委员会于 1999 年 10 月制定了“核心原则方法”。然而，自 1997 年起，银行业的监管方面发生了重大变化，各国在执行核心原则时积累了丰富的经验，在监管方面的新颖见解也日益突出。鉴于这些发展趋势，有必要更新核心原则以及相关评估方法。

基于 1999 年对跨境银行业的内部调查结果，委员会发现，不少国家的“了解您的客户”(KYC) 政策存在缺陷。2001 年 10 月，委员会发布《银行客户尽职调查》白皮书，指出：“一些国家的了解您的客户政策严重不达标，而一些国家根本没有了解您的客户政策。即使在金融市场高度发达的国家，了解您的客户的完善程度也不尽相同。”这份白皮书跟着 2001 年 1 月的一份咨询文件之后发布。

委员会对了解您的客户的关注主要围绕着如何使用尽职调查要求来减轻不良客户的危害。没有尽职调查，银行可能面临声誉、经营、法律和集中风险，从而蒙受重大的财务损失。完善的了解您的客户政策和程序对保护银行的安全与稳定以及银行系统的完整性具有重要作用。以国际商业信

贷银行 (BCCI) 丑闻为例，1988 年，9 名国际商业信贷银行官员因涉嫌清洗毒资在美国的佛罗里达州被捕，该丑闻开始浮出水面。随后，事态的严重性不断升级，至 1991 年，国际商业信贷银行被监管部门关闭，7 万多名客户已获得的及正在索赔的赔偿金额价值 90 亿美元。

委员会 2001 年发布的白皮书就了解您的客户标准及其落实提供了更为准确的指引，从而强调了委员会在先前的白皮书中制定的原则。在制作指南的过程中，编制白皮书的工作组充分借鉴了成员国的实践经验并兼顾了监管工作的发展变化。白皮书涉及的关键因素是对所有银行应该在全球范围内执行的最低标准提供指南。然而，这些标准还需要通过针对特定机构和个别国家银行系统风险的措施得到补充和加强。例如，具有更高风险的账户和寻求高净值客户的银行需要接受强化尽职调查。这份白皮书的一些特定章节提出了对银行内风险较高的领域实施更为严格的客户尽职调查标准的建议。

白皮书讨论的内容包括：

1. 了解您的客户标准对监管机构和银行的重要性。
2. 了解您的客户标准的关键因素。
3. 监管机构的作用。
4. 跨国背景下了解您的客户标准的执行。

白皮书重点强调的具体问题包括：

- 了解您的客户制度的四大关键因素：
    1. 客户身份识别。
    2. 风险管理。
    3. 客户接纳。
    4. 监控。
- 银行不仅应识别其客户身份，还应监控账户活动以识别不符合该客户或该类账户通常或预期交易的交易活动。“为了确保记录的相关性，银行有必要对既有记录进行定期审查。发生重要交易、客户文件标准发生实质性改变或账户运作方式发生重大变化时是进行审查的合适时间。”
- 不具名账户不应被禁止，而应该实行与其他账户完全一样的了解您的客户程序。了解您的客户测试可由选定的员工完成，但如果银行要做到足够尽职，则必须安排足够数量的员工调查客户的身份。“这类账户绝不能用来隐瞒客户身份，以逃避银行合规部门或监管机构的监管。”

- 涉及高风险客户的特定身份识别问题，例如：
  - 信托、代名人和受托人账户。
  - 公司工具，特别是设有无记名股东的公司或发行不记名股票的实体。
  - 经第三方介绍的业务。
  - 由专业中介机构开立的客户账户，如由专业中介机构代表诸如共同基金、养老基金和货币基金等实体管理的“公共”账户。
  - 政治公众人物。
  - 非面对面的客户，即未进行当面访谈的客户。
  - 代理银行业务。
- 银行应制定客户接纳政策和描述客户的背景、母国、业务活动及其他风险指标的客户接纳程序，并应清晰明确地描述哪些是可接纳的客户。
- 私人银行账户“必须”接受了解您的客户政策的监管。
- 在涉及专业中介机构时，银行应尽一切可能识别运作账户的公司身份，并核实账户所有者与中介的真实关系。
- 在处理非无法面谈的客户时，银行应使用标准身份识别程序，且决不允许给坚持匿名的人士开户。
- 培训应面向银行的全体员工，阐明了解您的客户政策和反洗钱要求的重要性。
- 内部审计师或合规专员应定期监控员工表现并检查了解您的客户程序的执行情况。
- 合规专员应持续监控高风险账户，以便提高对客户“常规活动”的理解，及时更新客户身份识别文件以及侦测可疑交易模式。
- 银行监管机构应确保银行员工遵循了解您的客户程序，审查客户文件和账户抽样情况，并强调其会采取“合理措施”来处理未能遵循了解您的客户程序的员工。

客户身份识别是客户尽职调查程序有效的关键因素，银行需要利用客户尽职调查来防范声誉、经营、法律和集中风险。客户身份识别也是遵守反洗钱法律要求的必要措施，识别与恐怖主义相关的银行账户的先决条件。2003 年 2 月，委员会发布了《账户开立和客户身份识别指南》，以及根据委

员会发布的银行客户尽职调查白皮书原则制定的最佳实践基本指导。这份由跨境银行业工作小组起草的文件并未涵盖每种可能出现的情况，而是着重关注了一些机制，这些机制可供银行用来制定有效的客户身份识别制度。

需要严格的客户尽职调查标准的机构并不局限于银行。巴塞尔委员会坚信，非银行金融机构和律师、会计师等专业金融服务中介也需要类似的指南。

2004 年 10 月，委员会发布了另一个关于了解您的客户的重要文件：《一体化了解您的客户风险管理》，是对 2001 年 10 月发布的《银行客户尽职调查》的补充。该白皮书审视了整个银行业内有效管理了解您的客户风险的关键因素，指出银行需要有一个全球统一的方法，并将实现完善的了解您的客户制度所需的要素应用于母行或总部以及所有分支机构和子公司。这些要素包括：风险管理、客户接纳和识别政策以及对高风险账户的持续监控。

2016 年 2 月，巴塞尔委员会发布*《洗钱和恐怖融资风险健全管理》*和修订版*《账户开立通用指南》*。

针对洗钱和恐怖融资风险管理的指南介绍了银行应如何将这些风险纳入整体风险管理框架。这些指南指出，对这些风险的审慎管理以及有效的监管至关重要，有助于保护银行业的安全和稳健发展，以及金融系统的诚信。如果这些风险未能得到有效管理，则银行将面临严重的声誉风险、经营风险、合规风险等。这些指南主要围绕以下方面：

- **风险分析与治理：**为管理洗钱风险，首先须识别并分析风险，这是设计并有效落实适当管控措施的基础。风险分析应涵盖国家、行业、银行和业务关系层面的适当固有风险与剩余风险。风险评估应记录在案，以便监管机构等政府部门查阅。风险分析还有助于安排与银行其他部门的讨论，帮助他们识别风险，设计适当的管控措施以降低风险。

  另一重要内容是适当的治理措施，这些措施可自上而下形成合规文化。董事会肩负关键的监督职责；作为银行的最高管理层，他们应审批和监督风险政策、风险管理政策及合规政策。董事会还应清晰认识洗钱风险，包括及时了解全面准确的风险评估信息，以便做出明智的决策。董事会应与高级管理层共同任命合格的首席反洗钱官，令其负责整个反洗钱职能部门，并赋予其充足的权力，一旦出现问题，即可得到董事会、高级管理层和业务部门的注意。首席反洗钱官代表董事会推动日常反洗钱工作，保障银行安全，因此，董事会应为首席反洗钱官提供充足的资源，方便其履行自己的职责，负责管理银行反洗钱制度的合规情况。

- **三条防线：**委员会阐释了银行反洗钱工作的三条防线；一是业务条线，二是合规和内部控制职能部门，三是内部审计。

1. **业务条线**负责制定、落实并维护政策与流程，并将其告知所有人员。他们还须建立员工筛选程序，确保实行较高的职业道德和专业标准，并根据员工的作用和职能，推出适当的反洗钱政策和流程培训，使其明确自己的责任。为此，员工应在入职后尽快接受最新的培训。

2. **反洗钱合规职能部门，**以及更广义的合规职能部门、人力资源部门和科技部门共同构成第二条防线。在任何情况下，首席反洗钱官均负责持续监控以确保反洗钱合规，具体包括抽样检验、复查例外报告等，以便加快识别不合规等问题，并向高级管理层报告，如有必要，还需向董事会报告。首席反洗钱官应在所有反洗钱事务方面担任银行内外有关部门的联络人，且有责任报告可疑交易。为确保成功监管反洗钱制度，首席反洗钱官必须具备充分独立性，不受业务条线干扰，谨防存在利益冲突或受到不公正意见或顾问的影响。首席反洗钱官不应负责数据保护或内部审计工作。

3. **审计职能部门**应向董事会审计委员会（或相同级别的管理部门）报告，并通过定期评估，独立评估银行的洗钱风险管理和控制情况，包括：银行控制措施是否足以降低已识别的风险，银行职员落实的控制措施是否有效，合规监管和质量控制是否有效，以及培训的有效性。审计职能部门必须具有知识渊博、审计专业知识充足的员工。审计的频率应根据风险大小而定；银行应定期对整个机构进行审计。审计应设定适当的范围，以便评估制度的有效性，包括适时使用外部审计机构。审计应积极跟进其结论和建议。

- **客户尽职调查和接纳：**银行应制定客户接纳政策，明确可能造成较高洗钱风险的客户（例如政治公众人物），以及银行拒不接纳的客户关系（例如空壳银行，或受到美国海外资产控制办公室等机关施加的经济制裁的机构）。银行应对所有客户执行基本尽职调查，并根据风险等级调整尽职调查程度。根据相关法律，一些洗钱风险低的客户可能仅需接受简化尽职调查。

  银行的客户尽职调查政策应旨在确定和核实客户和受益所有人，并建立风险档案。为此，银行应识别客户及受益所有人，并核实他们的身份。在核实客户身份前，银行不应与该客户建立业务关系，也不应开展交易，除非这一操作顺序会扰乱正常的业务开展（在此情况下，银行应一边执行身份核实和客户尽职调查，一边采取适当的管控措施）。为开展身份核实，银行应采取可靠的手段。确定受益所有权时，银行可要求客户填写书面声明，但不可仅依靠此声明。

  如无法执行客户尽职调查，或无法核实客户身份，银行不应开立账户（如此等账户已开立，则银行应予以关闭），并考虑向相关部门报告此等可疑活动。这也适用于匿名账户；匿名账户本不应开立。如果银行允许开立数字账户，则这种账户不应用作匿名账户；银行应安排充足的工作人员完全掌控此类账户的信息，确保对其执行适当程度的客户尽职调查和交易监控。

- **交易监控系统和持续监控：**由于交易监控系统是降低银行内洗钱风险的关键因素，委员会认为，反洗钱风险不仅要求制定适当的政策和流程；还要求银行必须建立有效的适当监控系统。对大多数银行而言，为做到这一点，需建立 IT 监控系统。如果某家银行不认为自己需要建立 IT 监控系统，则该银行须书面说明其理由。监控系统应覆盖银行客户的所有账户和交易，生成客户活动趋势分析，识别异常业务关系和交易，尤其是客户交易资料发生变动的情况。IT 系统应能为银行获得集中化的信息知识，例如按客户、较大集团内的法律实体或业务部门分类的信息。尽管指南指出银行必须建设 IT 监控系统，但这并不意味着仅采用一种 IT 工具即可一劳永逸；相反，多种工具应互相配合，使银行了解企业层面的全行洗钱风险。

  一种降低洗钱风险的重要方法是，根据风险评估和客户资料提供的信息，利用交易监控系统对客户的活动开展持续监控。通过这种方法，银行可履行识别和报告可疑活动的职责。银行应根据其面临的风险，调整监控系统，例如，如果银行发现其司法管辖区内存在某个洗钱计划，应调整其监控系统。

- **信息管理：**由于反洗钱法规的一大重要目标是创建记录，使执法部门能够据此追溯金融交易的操作人，因此，银行应保留其记录。一方面，银行应记录在核实客户或受益所有人身份时获得的资料，可为资料复印件，也可为对档案或非档案来源的信息记录，另一方面，银行还应将所有客户尽职调查信息录入 IT 系统。客户尽职调查信息应及时更新，准确无误，这要求银行定期评估信息，评估频率依据风险大小而定。

  银行还应记录其在异常活动调查过程中所做的决定，无论银行最终是否创建可疑活动报告，此类决定均应记录在案。银行应根据法律规定，保留所有记录，直至账户关闭五年后，方可自行决定是否继续保留相关记录。如果某账户正在接受调查，即使该账户的记录保留期限已满，银行仍不可销毁客户尽职调查记录。

- **报告可疑交易和资产冻结：**银行通过持续监控账户和交易，可识别异常活动，将异常活动交由内部审核职能部门处理，删除误报，并及时秘密地报告可疑活动。银行应在其政策和流程中明确规定以上程序，并告知相关职员。

  银行报告某客户的可疑活动后，应对该客户采取适当措施，包括提高该客户的风险评级，或决定是否继续维持业务关系（无论是某个账户，还是与该客户的所有业务关系）。某些情况下，银行可关闭客户的某个账户，但不终止与该客户的其他业务关系，例如该客户既有活期存款账户，也借贷了大额款项。银行应筛查新客户是否为某项制裁的对象，并应持续关注受制裁对象名单，了解客户是否成为受制裁对象，以便确定是否应该冻结某个客户关系。银行应有方法适当冻结任何被认定为受到制裁的资产。

欧洲联盟反洗钱指令

第 1 号指令

1991 年 6 月，欧洲理事会通过了“欧盟关于防止利用金融系统进行洗钱”的第 1 号指令（91/308/EEC 号指令）。

与理事会通过的所有其他指令一样，该指令要求欧盟成员国取得具体的成果（必要时须修改国内法律）。第 1 号指令要求成员国通过立法来防止其国内金融系统被用于洗钱活动。

欧盟作为“国家共同体”的独特性使其与其他国际组织存在本质区别。欧盟可制定具有法律效力的措施，甚至无须获得各成员国议会的批准。此外，欧盟指令的法律效力优于各成员国的国内法律。在这一点上，欧盟指令比由巴塞尔委员会或 FATF 等组织发布的自愿性标准更具分量。当然，欧盟指令仅适用于欧盟成员国，不适用于其他国家。

1991 年发布的第 1 号指令针对的上游犯罪活动仅为 1988 年《维也纳公约》定义的毒品走私相关洗钱活动。不过，该指令鼓励成员国将上游犯罪扩展到其他形式的犯罪。

第 2 号指令

2001 年 12 月，欧盟通过第 2 号指令（2001/97/EEC 号指令），该指令对第 1 号指令进行了修订，要求各成员国在辖内实施更为严格的反洗钱控制措施。

成员国同意在 2003 年 6 月 15 日前将此指令作为国家律法实施；然而，只有丹麦、德国、荷兰和芬兰按时实施第 2 指令，爱尔兰和西班牙于截止日期后不久实施。此后，其他成员国才纷纷开始行动。

第 2 号指令的主要特征为：

- 该指令将第 1 号指令的范围进行延伸，而不再局限于涉毒犯罪。“刑事犯罪活动”的定义得以扩大，除毒品走私外，还涉及包括违背欧洲共同体金融利益的腐败和诈骗犯罪在内的一切重罪。
- 该指令明确将货币兑换所和汇款机构纳入反洗钱监管范围。
- 该指令指出，对犯罪行为的“明知”可从客观实际情况进行推定。

- 该指令对洗钱进行了更为准确的定义，包括：
  - 明知财产为犯罪所得或参与犯罪活动所得，为隐瞒或掩饰该财产的非法来源，或为协助任何参与实施犯罪的人员逃避其行为的法律后果而转换或转让财产。
  - 明知财产为犯罪所得或参与犯罪活动所得而隐瞒或掩饰该财产的性质、来源、所在地、处置、转移、相关权利或所有权。
  - 明知财产为犯罪所得或参与犯罪活动所得而仍获取、使用或使用该财产。
  - 参与实施、共同实施、企图实施以及协助、教唆、帮助或指导实施上述任何犯罪行为。
- 该指令拓宽了接受其约束的行业与职业范围。根据要求，包括参与客户资金转移的律师在内的特定人员必须向当局报告任何可能牵涉洗钱的事实。这些特定人员包括：审计师、外部会计师、税务顾问、房地产经纪商、公证员以及法律专业人员。

由于第 2 号指令适用于全球许多重要的金融中心，它无疑是反洗钱领域的一大飞跃，其影响远远超越了联合国甚至 FATF 等组织所发布的类似标准。

第 3 号指令

2005 年，在 FATF 修订后的 40 项建议的基础上，欧盟通过了关于防止利用金融系统进行洗钱和恐怖融资活动的第 3 号指令（2005/60/EC 指令）。

成员国必须在 2007 年 12 月 15 日前实施第 3 号指令。虽然部分成员国并未按时完成任务，但该指令最终得到所有成员国的落实。

根据 FATF 反洗钱建议的要求，欧盟第 3 号指令通过以下措施扩展了洗钱犯罪的范围：

- 将“洗钱”和“恐怖融资活动”定义为两个不同的犯罪。指令中的措施有所增加，除操纵犯罪所得外，还包括为恐怖活动筹集资金或财产。
- 将客户身份识别以及可疑交易报告义务扩展至信托和公司服务提供商、人寿保险中介以及商品现金交易额超过 15,000 欧元的经销商。
- 详细规定了用于客户尽职调查的以风险为本的方法。客户尽职调查（无论简化或是强化）的范围应依据其洗钱或恐怖融资活动的风险而定。
- 对报告可疑洗钱活动或恐怖融资活动的员工进行保护。这项规定要求成员国“尽其所能保护员工免遭威胁”。

- 规定成员国必须保留有关可疑交易报告的使用及其结果的全面统计数据，如：创建的可疑活动报告数量；对这些报告的跟进情况；每年调查的案件数量，起诉和判决的人员数量。
- 要求所有金融机构识别并验证所有由法律实体或个人持有的账户的“受益所有人”。“受益所有人”指对某法律实体或法人拥有 25% 以上的直接或间接控制权的自然人。

第 3 号指令适用于：

- 信贷机构。
- 金融机构。
- 审计师、外部会计师和税务顾问。
- 法律专业人员。
- 信托与公司服务提供商。
- 房地产经纪商。
- 现金交易额超过 15,000 欧元的高价值商品经销商。
- 赌场。

第 3 号指令的适用范围与第 2 号指令不同，具体表现为：

- 明确包括了信托和公司服务提供商；
- 涵盖了所有现金交易额超过 15,000 欧元的商品经销商；
- 将某些保险中介纳入金融机构的定义之中。

第 3 号指令的三个争议焦点为：

1. 对政治公众人物 (PEP) 的定义。根据第 3 号指令的定义，政治公众人物指“被赋予或曾被赋予重要公共职能的自然人、其直系亲属或已知亲信”。只有当某人与政治公众人物的关系为公众所知或机构怀疑存在这一关系时，方可将此人认定为关系密切人员。最后，委员会认为，在卸任要职一年之后，相关人员不再被认定为政治公众人物。
2. 将律师纳入需要报告可疑交易的群体。
3. “综合事务委员会”(comitology committee) 的确切职能。欧盟委员会新造了“comitology”这一术语，意指监督欧盟体系执行欧盟委员会所提交法案的情况。

第 4 号指令

欧洲议会和欧洲委员会于 2015 年 5 月 20 日通过关于防范将金融系统用于洗钱或恐怖融资的欧盟第 2015/849 号指令，并于当年 6 月 26 日生效。成员国须在生效之日起两年内，根据该指令修改本国立法。这份指令废除了之前通过的第 1、2、3 号指令。

第四号反洗钱指令作出的更改包括：

- 义务主体报送可疑交易（即商品经销商或交易商）的限额从 15,000 欧元降至 10,000 欧元。
- 义务主体的范围从单纯的赌场扩大至所有“博彩服务供应商”。
- 转账金额如果超过 1,000 欧元，须进行客户尽职调查。
- 指令还提出了一些新定义，包括：
  - — 代理关系。
  - — 政治公众人物的家属及关系密切人员。
  - — 高级管理层及其他。
- 根据第四指令，直接或间接与纳税相关的犯罪均属于广义上的“刑事犯罪活动”，与修订版 FATF 建议一致。
- 新指令还解释了“偶然性或有限金融活动”。
- 欧洲委员会必须每两年提交一份报告，汇报对影响欧盟市场的洗钱和恐怖融资活动的风险评估结果。
- 欧盟执行委员会还负责识别在反洗钱和反恐融资方面具有战略缺陷的第三国司法管辖区（即“高风险第三国家”）。
- 第四指令重点关注政治公众人物。在此方面，应对欧盟内部及第三国家的每个政治公众人物实行增强尽职调查 (EDD)。将这类人士的风险潜伏期延长至 12 个月，且对他们实行的管控措施也必须同样适用于他们的家属和已知亲信。
- 针对集团（及其分支机构和子公司）对第三方实施客户尽职调查方面，这份指令制定了充分合规的标准。

- 指令还增加了有关受益所有人信息的新规定，尤其适用于信托及类似法律安排。在不违反数据保护法规的情况下，该信息必须由各成员国的集中注册处保管，且相关部门、金融情报机构 (FIU)、责任主体及任何有合法利益的人士必须有访问权。
- 考察反洗钱和反恐融资系统有效性的统计数据采集范围扩大，新增的信息种类包括产业的规模和重要性、FIU 接到的跨境信息请求数量等。
- 隶属某集团的责任主体必须落实集团层面的政策和流程，并根据风险程度采取适当措施。此举可防止在其他领域被判刑的犯罪分子及其亲信在集团内担任管理职务，或间接控制某些责任主体。
- 关于违反规定的罚款，行政制裁和惩治措施轻则“点名批评”，重则取消授权。对自然人的罚款不少于 500 万欧元，或不少于公司年营业额的 10%。
- 第四指令有一节专门规定各成员国 FIU、欧洲监管机关联合委员会 (ESA) 和欧盟委员会的合作规范。
- 由于第四指令并非监管条例，各成员国可自行决定对各条款的适用情况。
- 从国家层面看，该指令要求各成员国执行洗钱 / 恐怖融资风险评估，并指定主管部门。此外，各成员国必须确保责任主体采取适当措施，识别并评估各自面临的风险。指令提供了潜在的较高和较低风险的非详尽清单，为各国的风险评估提供指导，这些清单的依据包括：
  - 客户风险因素，例如公共管理机构与使用大量现金的企业。
  - 产品 / 服务、交易或销售渠道风险因素，例如保费较低的保单与私人银行业务。
  - 地理风险因素，例如成员国与受制裁国家。

相关法律文件

除以上法规外，欧盟出台的反洗钱和反恐融资法规还包括：

- 有关洗钱以及识别、追踪、冻结、扣押、没收票据和犯罪所得的《联合法案》（1998 年）及其后续修正案。
- 《框架决议》（2001 年）。
- 关于欧洲金融情报机构合作的《框架决议》（2000 年）。
- 关于打击恐怖主义的限制措施的《监管条例》（2001 年）及其修正案（2003 年）。

- 《现金控制监管条例》（2005 年）。
- 《电汇监管条例》（2015 年）。

与金融行动特别工作组 (FATF) 类似的区域性组织

与金融行动特别工作组 (FATF) 类似的区域性组织和准成员

全球共有 9 个与金融行动特别工作组类似的区域性组织 (FSRB)，其形式与职能和金融行动特别工作组相似。它们也被视为金融行动特别工作组的准成员。金融行动特别工作组制定标准的依据不仅来源于其成员国，也来源于这些金融行动特别工作组类区域性组织 (FSRBs)；然而，金融行动特别工作组始终是唯一的标准制定机构。

以下高标准原则既适用于金融行动特别工作组也适用于金融行动特别工作组类区域性组织，包括：

- **职责：** 金融行动特别工作组类区域性组织负责识别和满足其成员国的反洗钱 / 反恐融资技术支持需求。对于开展此类协调工作的组织，技术支持可帮助司法管辖区落实金融行动特别工作组的标准，是对互评和跟进流程的必要补充。
- **自主权：** 金融行动特别工作组与其同类区域性组织均为独立机构，它们肩负共同的目标，即打击洗钱、恐怖融资和扩散融资活动，构建有效的反洗钱 / 反恐融资系统。
- **互惠：** 金融行动特别工作组与其同类区域性组织的工作基础是（互相、共同或普遍）认同各组织的工作，这意味着二者采取相似的机制，因而可有效参与对方的活动。
- 由于金融行动特别工作组与其同类区域性组织共同构成一个更大的整体，而一个组织的成败关系到所有组织的工作成效，因此，保护金融行动特别工作组品牌符合其与其同类区域性组织的**共同利益**。

不少金融行动特别工作组的成员国也加入了以下九个金融行动特别工作组类区域性组织之一：

— 亚太反洗钱工作组 (APG)。

— 加勒比地区金融行动特别工作组 (CFATF)。

— 欧洲理事会评估反洗钱措施和恐怖融资活动专家委员会 (MONEYVAL)（前身为 PC-R-EV）。

— 欧亚反洗钱与反恐融资活动工作组 (EAG)。

— 东南非反洗钱工作组 (ESAAMLG）。

— 拉丁美洲金融行动特别工作组 (GAFILAT)（旧称南美反洗钱金融行动特别工作组，即 GAFISUD）。

— 西非政府间反洗钱行动工作组 (GIABA)。

— 中东与北非金融行动特别工作组 (MENAFATF)。

— 中非反洗钱特别工作组 (GABAC)。

亚太反洗钱工作组 (APG)

亚太反洗钱工作组 (APG) 是一个区域性反洗钱自治组织，于 1997 年 2 月在曼谷召开的第四届亚太反洗钱研讨会上成立，此次会议通过了该工作组的“参照条款”。

2012 年 7 月，亚太反洗钱工作组对“参照条款”进行重大修改，承认修订后的金融行动特别工作组 40 项建议为打击洗钱、恐怖融资和扩散融资活动的国际新标准。“参照条款”包含了亚太反洗钱工作组成员国将根据其特定文化价值观和宪法框架执行这些建议的承诺。条款还指出，为了确保全球性方法的制定，亚太反洗钱工作组成员必须与金融行动特别工作组紧密协作。

亚太反洗钱工作组：

- 聚焦在亚太地区合作开展反洗钱 / 反恐融资活动。
- 提供论坛，以便：
  - — 探讨区域性问题并分享经验。
  - — 鼓励各成员司法管辖区在行动中开展合作。
- 促进各成员司法管辖区制定并执行被国际社会所接受的反洗钱 / 反恐融资活动措施。
- 在实施国际反洗钱 / 反恐融资活动措施时考虑区域和司法管辖区的因素。
- 鼓励各司法管辖区执行反洗钱 / 反恐融资活动倡议，包含更为有效的司法互助。
- 在可能时进行协调，并根据要求向所在地区的成员和司法观察员提供实际支持。

亚太反洗钱工作组本质上是自愿的合作型组织。亚太反洗钱工作组的工作内容与工作流程是根据成员间的共同协商确定的。亚太反洗钱工作组根据成员之间的协议建立并实行自我管理，并非国际协定的产物，也不是任何国际机构的附属机构。

亚太反洗钱工作组也采用与金融行动特别工作组类似的机制来监控并促进其进程。两者彼此享有出席对方会议并共享文件的权利。但与其他自主管理的反洗钱组织一样，亚太反洗钱工作组独立决定其政策和做法。颁布反洗钱 / 反恐融资活动法律并非加入亚太反洗钱工作组的先决条件。

自成立以来，亚太反洗钱工作组的规模不断壮大，其成员国数量从 1997 年成立之初的 13 个增加至 2015 年 7 月的 41 个。亚太反洗钱工作组成员包括：阿富汗、澳大利亚、孟加拉国、不丹、文莱、达鲁萨兰国、柬埔寨、加拿大、中国大陆、库克群岛、斐济、中国香港、印度、印度尼西亚、韩国、日本、老挝、中国澳门、马来西亚、马尔代夫、马绍尔群岛、蒙古、缅甸、瑙鲁、尼泊尔、新西兰、纽埃岛、巴基斯坦、帕劳、巴布亚新几内亚、菲律宾、萨摩亚、新加坡、所罗门群岛、斯里兰卡、中国台北、泰国、东帝汶、汤加、美国、瓦努阿图和越南。

亚太反洗钱工作组的秘书处设于澳大利亚悉尼。亚太反洗钱工作组的官方网站为 www.apgml.org。

加勒比地区金融行动特别工作组 (CFATF)

由于毗邻世界上最大的可卡因生产地和出口地南美洲安第斯山脉地区，以及世界上最大的毒品市场之一的美国，加勒比海盆地长久以来一直被包括毒贩在内的众多国际犯罪分子视为便捷的银行中心。

加勒比地区金融行动特别工作组共有 27 个成员国，分别位于加勒比海盆地、中美和南美地区，各成员国同意实施共同的对策来解决洗钱、恐怖融资、大规模杀伤性武器扩散融资等问题。加勒比地区金融行动特别工作组是 1990 年 5 月阿鲁巴会议和 1992 年 11 月牙买加会议的共同产物。

加勒比地区金融行动特别工作组的主要目标是确保各成员国有效地落实并遵守其建议，以防范和控制洗钱活动，打击恐怖融资活动。加勒比地区金融行动特别工作组的秘书处的设立宗旨是监控和推动各成员国充分落实《金斯敦部长宣言》（*详见下文*）。

1990 年 5 月，西半球国家（尤其是加勒比和中美国家）的代表在阿鲁巴岛召开会议，制定打击洗钱犯罪所得的共同方法。此次会议最终制定了 19 条建议。这些建议具有明显的地域特点，被认为是对金融行动特别工作组 40 项建议的补充。

牙买加部长级会议于 1992 年 11 月在金斯敦召开。各国部长联合发布《金斯敦部长宣言》，同意并确认其政府执行金融行动特别工作组建议、阿鲁巴建议、美洲国家组织 (OAS) 规范条例以及 1988 年联合国《禁止非法贩运麻醉药品和精神药物公约》。各国部长还授权建立秘书处，令其负责协调各成员国对以上条例的落实工作。

该宣言建议了以下法律措施：

- 基于美洲国家组织发布的法律范本对洗钱进行定义。
- 考虑查封和没收毒品所得以及相关资产从而确保可对应查封财产进行识别、追踪和评估，并认可资产冻结命令。
- 允许对行政机关的查封令提出司法质疑。
- 允许在定罪后没收财产。
- 允许法院决定“毒贩在特定时间内获得的所有财产均为此类刑事犯罪活动所得”。

加勒比国家同意签署在洗钱调查方面的互助协议。各国还一致同意，洗钱应是可依照简化程序进行引渡的犯罪，并且被没收资产应由合作国家共享。

加勒比地区金融行动特别工作组成员包括：安圭拉岛、安提瓜岛和巴布达、阿鲁巴岛、巴哈马、巴巴多斯、伯利兹、百慕大群岛、英属维尔京群岛、开曼群岛、库拉索、多米尼加、多米尼加共和国、萨尔瓦多、格林纳达、危地马拉、圭亚那、海地、牙买加、蒙特塞拉特、圣基茨和尼维斯、圣卢西亚、圣马丁、圣文森特和格林纳丁斯、苏里南、特立尼达和多巴哥、特克斯和凯科斯群岛，以及委内瑞拉。

加勒比地区金融行动特别工作组负责监控成员国对反洗钱建议的执行情况。加勒比地区金融行动特别工作组秘书处与特立尼达和多巴哥政府联署办公。加勒比地区金融行动特别工作组的官方网站为 https://www.cfatf-gafic.org/。

评估反洗钱措施专家委员会 (MONEYVAL)

1997 年 9 月，评估反洗钱措施专家委员会由欧洲理事会部长委员会成立，负责引导欧洲理事会成员国中未加入金融行动特别工作组的国家开展反洗钱措施自评和互评。2006 年，评估反洗钱措施专家委员会成为金融行动特别工作组准成员。

2010 年 10 月 13 日，部长委员会通过“关于评估反洗钱措施专家委员会 (MONEYVAL) 法规”的第 CM/Res (2010)12 号决议。这部法规提升了评估反洗钱措施专家委员会的级别，自 2011 年 1 月 1 日起，该组织正式升级为欧洲理事会的独立监控机构，直接向部长委员会报告。2013 年通过的第 CM/ Res (2013)13 号决议进一步修订了《MONEYVAL 法规》。

评估反洗钱措施专家委员会 (MONEYVAL) 成员包括：阿尔巴尼亚、安道尔、亚美尼亚、阿塞拜疆、波斯尼亚和黑塞哥维那、保加利亚、克罗地亚、塞浦路斯、捷克共和国、爱沙尼亚、直布罗陀 *、格鲁吉亚、根西岛 *、匈牙利、梵蒂冈（2011 年 4 月加入）*、马恩岛 *、以色列（2006 年 1 月加入）*、

泽西岛 *、拉脱维亚、列支敦士登、立陶宛、马耳他、摩尔多瓦、摩纳哥、黑山共和国、波兰、罗马尼亚、俄罗斯联邦（2003 年也加入 FATF）、圣马力诺、塞尔维亚、斯洛伐克共和国、斯洛文尼亚、前南斯拉夫马其顿共和国和乌克兰。

** 非欧洲理事会成员。*

评估反洗钱措施专家委员会与欧洲理事会联署办公，位于法国斯特拉斯堡。评估反洗钱措施专家委员会的官方网站为 www.coe.int/t/dghl/monitoring/moneyval/。

拉丁美洲金融行动特别工作组 (GAFILAT)

拉丁美洲金融行动特别工作组 (GAFILAT) 旧称南美反洗钱金融行动特别工作组 (GAFISUD)，于 2000 年 12 月成立于哥伦比亚喀他赫纳港，9 个成员国的政府代表签署了谅解备忘录，这些国家分别为：阿根廷、玻利维亚、巴西、智利、哥伦比亚、厄瓜多尔、巴拉圭、秘鲁和乌拉圭。随后，墨西哥（2006 年）、哥斯达黎加和巴拿马（2010 年）、古巴（2012 年）、危地马拉、洪都拉斯和尼加拉瓜（2013 年）先后加入该组织。

拉丁美洲金融行动特别工作组依照金融行动特别工作组的形式组建，将 其 40 项建议视为国际反洗钱 / 反恐融资标准。拉丁美洲金融行动特别工作组还制定了增强建议，完善打击此类犯罪的国家政策。

拉丁美洲金融行动特别工作组支持成员国将 40 项建议作为国家法律来落实，还支持它们针对洗钱和恐怖融资活动建立区域防范系统。该组织的两大主要工具为培训措施和互评。

拉丁美洲金融行动特别工作组成员包括：阿根廷、玻利维亚、巴西、智利、哥伦比亚、哥斯达黎加、古巴、厄瓜多尔、危地马拉、洪都拉斯、墨西哥、尼加拉瓜、巴拿马、巴拉圭、秘鲁和乌拉圭。

拉丁美洲金融行动特别工作组秘书处位于阿根廷共和国，在该国具有法律能力和外交地位。拉丁美洲金融行动特别工作组的官方网站为 http://www.gafilat.org/index.php。

西非政府间反洗钱行动工作组 (GIABA)

西非政府间反洗钱行动工作组由西非国家经济共同体 (ECOWAS) 的国家政府首脑决定 于 1999 年 12 月 10 日成立。2006 年 1 月，GIABA 修改其委托权限，以便全面纳入并适当反映其反恐融资工作。

西非政府间反洗钱行动工作组的宗旨为：

- 保护签署国的国家经济和金融及银行系统不受犯罪所得及恐怖融资活动侵害。

- 改善打击犯罪所得的措施，并加强此项工作。
- 巩固各成员国之间的合作。

西非政府间反洗钱行动工作组成员包括：贝宁、布基纳法索、佛得角、科特迪瓦、冈比亚、加纳、几内亚比绍、几内亚科纳克里、利比里亚、马里、尼日尔、尼日利亚、塞内加尔、塞拉利昂和多哥。

西非政府间反洗钱行动工作组秘书处位于西非塞内加尔，官方网站为 www.giaba.org。

中东与北非金融行动特别工作组 (MENAFATF)

2004 年 11 月，在巴林首都麦纳麦召开的首届部长级会议上，14 个国家的政府决定在中东和北非建立一个与金融行动特别工作组类似的区域性组织。中东与北非金融行动特别工作组本质上是自愿参与的组织，由各成员国协议建立，而不是国际条约的产物。它独立于任何其他国际组织，并以成员协商一致的方式确定自身的工作任务、规则和程序。该组织通过与其他国际组织（特别是金融行动特别工作组）开展合作来实现其目标。

中东与北非金融行动特别工作组的成员国同意并致力于实现以下目标：

- 采纳并实施金融行动特别工作组打击洗钱、恐怖融资和扩散融资活动的 40 项建议、被视为该领域国际标准的相关联合国公约和联合国安全理事会决议，以及阿拉伯国家为加强该地区的反洗钱、反恐融资和反扩散融资工作而制定的标准。
- 实施与打击洗钱和恐怖融资活动相关的联合国协定、协议以及联合国安理会的决议。
- 合作提高中东与北非区域内部的标准和措施的合规性并与其他国际组织合作提升世界范围内的合规性。
- 合作识别区域性洗钱和恐怖融资活动问题，共享应对这些问题的经验并制定区域性解决方案。
- 在整个地区建立有效的安排与制度体系，以打击洗钱和恐怖融资活动，这些安排与制度不能和各成员国的特定文化价值观、宪法框架和法律体系相抵触。

中东与北非金融行动特别工作组成员包括：阿尔及利亚、巴林、埃及、毛里塔尼亚伊斯兰共和国、约旦、科威特、黎巴嫩、利比亚、摩洛哥、阿曼、巴勒斯坦权力机构、卡塔尔、伊拉克共和国、沙特阿拉伯、苏丹、叙利亚、突尼斯、阿拉伯联合酋长国和也门。

中东与北非金融行动特别工作组总部位于巴林，官方网站为 www.menafatf.org。

欧亚反洗钱与反恐融资活动工作组 (EAG)

2004 年 10 月，欧亚反洗钱与反恐融资活动工作组 (EAG) 于莫斯科成立。该组织专为未加入与金融行动特别工作组类似的区域性组织的欧亚国家而设。

欧亚反洗钱与反恐融资活动工作组的主要目标为，确保各成员国开展区域层面的有效互动与合作，并依照金融行动特别工作组 40 项建议和它们加入的其他国际组织的标准，融入国际反洗钱 / 反恐融资系统。

欧亚反洗钱与反恐融资活动工作组的主要任务包括：

- 协助成员国落实金融行动特别工作组建议。
- 制定并开展旨在打击洗钱和恐怖融资活动的联合行动。
- 实施以金融行动特别工作组建议为基础的成员国互评制度，包括评估各国采取的反洗钱 / 反恐融资法律及其他措施的有效性。
- 协调成员国与国际专门组织、机构和利益相关国之间的国际合作和技术支持项目。
- 在认识到区域特殊性的基础上，分析洗钱和恐怖融资活动变化趋势（类型），交流打击此类犯罪的最佳实践。

欧亚反洗钱与反恐融资活动工作组成员包括：白俄罗斯、中国、印度、哈萨克斯坦、吉尔吉斯斯坦、俄罗斯、塔吉克斯坦、土库曼斯坦和乌兹别克斯坦。

欧亚反洗钱与反恐融资活动工作组总部位于俄罗斯联邦莫斯科，官方网站为 http://www.eurasian-group.org/。

东南非反洗钱工作组 (ESAAMLG)

东南非反洗钱工作组 (ESAAMLG) 这一政府间机构负责推动有效落实法律、监管和业务手段，打击洗钱、恐怖融资等危害国际金融体系诚信的威胁。

该组织于 1999 年在坦桑尼亚成立，目前共有 18 个成员国，分别为：安哥拉、博茨瓦纳、科摩罗、埃塞俄比亚、肯尼亚、莱索托、马拉维、毛里求斯、莫桑比克、纳米比亚、卢旺达、塞舌尔、南非、斯威士兰、坦桑尼亚、乌干达、赞比亚和津巴布韦。

东南非反洗钱工作组的主要决策机构为部长理事会，由各成员国主管金融相关事务的部长组成。

各成员国签署了谅解备忘录，同意：

- 采纳并执行金融行动特别工作组 40 项建议。
- 将反洗钱措施应用于所有重罪。
- 实施反恐融资措施。
- 执行在成员国为防范并控制清洗所有严重犯罪所得和恐怖融资活动而签署的多边协定和倡议中有所提及的其他各项措施。

东南非反洗钱工作组还开展区域专项活动和研究。例如，2014 年，ESAAMLG 发起一项活动，旨在获取野生动物偷猎、野生动物制品非法交易和相关洗钱活动的信息、数据和变化趋势。

东南非反洗钱工作组总部位于坦桑尼亚，官方网站为 www.esaamlg.org。

中非反洗钱特别工作组 (GABAC)

中非反洗钱特别工作组 (GABAC) 是中非国家经济共同体的下属机构，按照其法语名称 *(Groupe d'Action contre le blanchiment d'Argent en Afrique Centrale)* 的首字母缩写命名。该组织于 2000 年成立，旨在打击洗钱和恐怖融资活动，评估各成员国对金融行动特别工作组标准的遵守情况，为成员国提供技术支持，并推动国际合作。2012 年 2 月，中非反洗钱特别工作组在金融行动特别工作组获得观察员地位。2015 年 10 月，金融行动特别工作组认可中非反洗钱特别工作组为与金融行动特别工作组类似的区域性组织，并承认其为准成员。

中非反洗钱特别工作组成员包括喀麦隆、中非共和国、乍得、刚果共和国、赤道几内亚和加蓬。

中非反洗钱特别工作组总部位于中非班吉，官方网站为 www.spgabac.org。

美洲国家组织：美洲药物滥用管制委员会 (Comision Interamericana Para El Control Del Abuso De Drogas)

1992 年 5 月，美洲国家组织 (OAS) 就专门针对洗钱的立法范本达成协议，并成为首个开展此类行动的永久性国际组织。在巴哈马首都拿骚举行的年度全体会议上，美洲国家组织一致通过了以法律语言撰写的由 19 个条款组成的法律范本，并推荐成员国颁布实施。

美洲国家组织 (OAS) 的行动成果来之不易。法律范本的表决通过是美洲药物滥用管制委员会 (CICAD) 经过 2 年努力的成果。美洲药物滥用管制委员会是美洲国家组织旗下的一个实体，按照其西班牙语名称 (Comisión Interamericana para el Control del Abuso de Drogas) 的首字母缩写命名。1990 年，美洲药物滥用管制委员会组建来自 14 个国家的“专家组”，委托其起草法律范本。

美洲药物滥用管制委员会的任务包括：

- 担任西半球毒品问题方面的政策论坛。
- 推动美洲国家在毒品问题上的多边合作。
- 执行行动方案，以加强成员国防范和应对毒品滥用的能力，打击非法药物的生产和贩卖，并拒绝给予毒贩其非法所得。
- 推进与毒品相关的研究、信息交流、专业培训以及技术协助。
- 就毒品相关立法、治疗、毒品消费和毒品社会成本的测量以及毒品控制措施等方面制定最低标准并加以推广。
- 定期开展多边评估，检验各成员国打击毒品工作的进展。

美洲药物滥用管制委员会的核心使命是增强人员和制度两方面的能力，并利用成员国的集体力量，减少美洲国家的非法毒品生产、走私和滥用，解决毒品交易带来的健康卫生、社会和犯罪问题。

美洲药物滥用管制委员会内设的反洗钱机构 (CICAD-AMLU) 成立于 1999 年。该反洗钱机构主要致力于在司法、金融措施以及执法方面为所有成员国提供技术协助与培训。它还是美洲药物滥用管制委员会控制洗钱专家组的秘书处。

通过专家组的努力，美洲药物滥用管制委员会针对涉及毒品走私的洗钱犯罪和恐怖融资等其他犯罪制定了示范规章。作为永久性法律文件，这些规章为成员国提供了法律框架。这些规章受到金融行动特别工作组 40 项建议的影响并与其保持一致。

如需查看示范规章的完整文本，请访问：http://www.cicad.oas.org。

1999 年，美洲开发银行 (IADB) 和美洲药物滥用管制委员会在 8 个南美国家启动了一项计划，对来自金融机构和负责反洗钱监管的金融监管机构的员工进行培训。2001 年，它们针对这 8 个国家的法官和检察官制定并实施了另一项计划。2002 年，它们又开始实施在阿根廷、智利、厄瓜多尔、巴西、秘鲁、乌拉圭和委内瑞拉建立金融情报机构的长期计划。

美洲药物滥用管制委员会的官方网站为 http://www.cicad.oas.org。

金融情报机构埃格蒙特集团

1995 年，多个国家的金融情报机构 (FIU) 开始在被称为埃格蒙特集团的非正式组织框架下开展合作，该名称取自首次会议召开地，即布鲁塞尔的埃格蒙特 - 艾伦贝格宫殿 (Egmont-Arenberg Palace)。该集团的目标是为全球的金融情报机构提供论坛，以促进在打击洗钱和恐怖融资活动领域的合作并推动该领域国内项目的实施。

支持措施包括：

- 使相互信息交换的合作得以扩大并系统化。
- 通过提供培训和促进人员交流来提高金融情报机构员工的专业知识与能力，从而增加金融情报机构的有效性。
- 通过诸如埃格蒙特安全网站 (ESW) 等技术的应用，促进金融情报机构间更为顺畅和安全的沟通。
- 提升金融情报机构的运作自主权。
- 促进在已经拥有反洗钱和反恐融资活动制度的司法管辖区或该制度尚处发展初期阶段的区域建立金融情报机构。

埃格蒙特集团包含多个机构，包括：金融情报机构主管联合会 (HoFIUs)、埃格蒙特委员会、多个工作组、多个区域工作组，以及埃格蒙特集团秘书处。该集团的 5 个工作组定期召开会议，直接向金融情报机构主管联合会汇报，分别是：信息技术工作组 (ITWG)、法务工作组 (LWG)、行动工作组 (OpWG)、外联工作组 (OWG) 和培训工作组 (TWG)。

2013 年，埃格蒙特集团修订了一系列统筹文件，为集团未来的工作奠定了基础，也将促进金融情报机构之间更广泛的国际合作和信息交流。这些文件包括：《埃格蒙特宪章》和《埃格蒙特关于金融情报机构进行信息交流和行动指导的原则》。

埃格蒙特集团还提供案例研究，涵盖洗钱、恐怖融资、欺诈及其他形式的金融犯罪。这些案例研究的素材通常是各司法管辖区内金融情报机构提交的案例，研究结果可帮助反洗钱专业人员识别可疑活动，决定是否上报。

1999 年，培训工作组开展的一项活动最终为埃格蒙特出版了题为《金融情报机构在行动：100 个洗钱案例》的报告。据埃格蒙特集团表示，这份出版物为识别洗钱案例要素提供了宝贵支持。这份报告不仅分析了 100 个洗钱案例，还总结了洗钱活动中最常见的六大信号：

1. 大额现金交易。

2. 非典型或非经济的跨司法管辖区资金转账。

3. 罕见的商业活动或交易。

4. 大额或快速资金流动。

5. 不符合客户资料的巨额财富。

6. 抵抗询问。

截至 2015 年，共有 151 个金融情报机构成为埃格蒙特的成员，另有 19 个机构拥有观察员地位。由于 2012 版金融行动特别工作组建议鼓励金融情报机构加入埃格蒙特，故该集团预期将继续壮大。埃格蒙特集团的官方网站为 http://www.egmontgroup.org/。

沃尔夫斯堡集团

沃尔夫斯堡集团是由 13 家全球性银行组成的协会，旨在制定金融服务行业标准，并为了解您的客户、反洗钱和反恐融资政策提供指引。沃尔夫斯堡集团没有强制执行权，但其通过发布指引来管理成员国自身的风险，帮助健全有关客户的决策机制并避免其操作系统被犯罪分子滥用。

该集团于 2000 年在瑞士沃尔夫斯堡城堡召开首次会议，与会的还有来自透明国际的代表。会议起草了私人银行反洗钱指引，该指引一经实施将对清洗腐败所得的打击将到达前所未有的水平。

《沃尔夫斯堡私人银行反洗钱准则》于 2000 年 10 月发布，随后分别于 2002 年 5 月和 2012 年 6 月进行修订。这些原则建议对私人银行采取广泛的控制措施，如客户身份识别这一基础性措施以及对“拥有或曾经拥有公共信托身份”的个人进行强化审查的增强尽职调查。与透明国际共同发布这些准则的银行表示，这些准则将“增加腐败人员将其非法所得存入世界银行体系的难度”。

这些准则指出，银行必须“仅接受财富和资金来源具有合法性（经合理判断）的客户”。准则还强调，在账户受益人并非客户本人时，必须识别“所有账户”的资金受益人身份，并要求私人银行家就“资金管理人和类似中介”开展尽职调查，以确定该中间人的客户尽职调查流程“令人满意”或对其执行尽职调查负有监管责任。准则建议“除私人银行经理外还应至少有一人”批准所有的新增客户和账户。

准则列举了需要增强尽职调查的情形，其中包括涉及以下事项的活动：

- 政治公众人物，例如公务人员，当前正担任或曾担任“高级、显要或重要公共职位，在政策、行动或对政府资源分配使用方面握有重大权力，例如高级政府官员、国有企业高管、高级政客、重要政党官员以及他们的家属和亲信”。
- 居住在或资金来源于高风险国家，包括“根据可靠信息来源被确认为反洗钱标准不充分或犯罪和腐败风险极高”的国家。
- 参与“公认的涉嫌洗钱的经济或商业活动或行业”的个人。

以下信息决定客户可能需要接受更细致的审查，包括：

- 通过监控他们的活动获取的信息。
- 外部问讯。
- 毁誉信息，例如负面新闻报道。
- 可能给银行造成声誉风险的其他因素。

沃尔夫斯堡准则认为，银行应制定书面政策，“对异常和可疑活动进行识别和跟踪调查”，并应对“可疑活动”进行定义，同时给出范例。建议利用私人银行经理对特定客户可疑活动类型的了解来建立“完善”的监控系统。同时，沃尔夫斯堡还概括了可以用来识别可疑活动的各种机制（其中包括会议、讨论以及拜访国内客户等）以及发现可疑活动时需采取的步骤。

准则还对以下事项作了规定：

- 向管理层报告洗钱问题。
- 反洗钱培训。
- 保存相关文档。
- 对政策的违背。
- 建立反洗钱部门并制定反洗钱政策。

2001 年 5 月，沃尔夫斯堡准则作出修订，其中一项重大修订是禁止使用内部非客户账户（有时称为“集中账户”）来隔离客户与其资金流动的关联。新规定指出，银行对内部账户的使用不得阻碍相关官员对客户资金动向进行适当监控。

2002 年初，沃尔夫斯堡集团还发布了《抑制恐怖融资活动》指引，对金融机构在打击洗钱和恐怖融资活动方面所发挥的作用进行了概括性的阐述。

沃尔夫斯堡建议包括：

- 在全球协作的基础上，由相关当局发布疑似恐怖分子的官方名单。
- 该名单包含信息应足以帮助各机构有效地对客户数据库进行检索。
- 该官方名单发布后及时向各机构提供信息反馈。
- 提供有关恐怖分子采用的方式、手段和方法的信息。
- 为被认为具有恐怖融资高风险的企业部门及其活动制定政府指引。
- 制定全球统一的资金转账模式来协助侦测恐怖融资活动。
- 为金融机构提供免责的安全保护，从而鼓励金融机构分享信息并向当局报告有关情况。
- 对“与汇款企业、货币兑换所和转账代理等机构之间的业务关系”实施增强尽职调查，并对高风险客户或处于高风险行业的客户以及类似“地下钱庄业务或替代性汇款体系”的活动实施增强尽职调查。

2002 年，沃尔夫斯堡集团发布了《代理银行业务反洗钱准则指引》，该文件概述了金融机构在打击通过代理银行业务进行洗钱和恐怖融资活动时应采取的步骤。代理账户指由一家金融机构在另一金融机构开立并用于存款、付款及处理其他交易的账户*（详情请见第二章）*。

该指引于 2014 年更新，强调这些准则是为了防范外国代理关系带来的风险，而非针对本国代理关系。更新后的指引全面覆盖机构建立或维持的所有代理银行服务关系，包括该机构的附属机构、子公司或分支机构的代理银行服务关系。

以下建议更加值得关注：

- 尽职调查应以风险为本持续进行，视地点、业务类型、所有权关系、客户群、监管状况以及对代理银行客户或业务的反洗钱控制措施而定。开展尽职调查时，建议考虑以下因素：
  - — 地域风险。
  - — 代理银行服务客户及机构的分支机构、子公司和附属机构。
  - — 代理银行服务客户的所有权和管理架构。
  - — 客户的客户基础和业务。
  - — 客户的产品和服务。
  - — 客户的监管现状和历史表现。

— 客户的反洗钱控制。

— 客户与空壳银行的往来。

— 考察客户业务。

— 对政治公众人物与代理银行服务客户的关系，以及代理服务衍生的下游代理（连环）关系增强尽职调查。

— 金融机构应在其反洗钱制度中融入这些准则，此外还应包括反贿赂、反腐败、反欺诈、反躲避制裁等内容。

2004 年，沃尔夫斯堡集团开始与《银行家年鉴》合作，为金融机构建立了国际尽职调查数据库。数据库的具体内容包括公司章程副本、相关许可证、商业注册或企业登记的摘录、最新的年度报告、持股比例超过 5% 的股东信息、董事会成员和高级管理人员的简历、与各金融机构的反洗钱政策和程序相关的信息等。该倡议是尽职调查信息标准化过程中的一大进展，它能够在查询多种来源的信息时缩短时间，从而节省成本。自启动以来，《银行家年鉴》进一步增加了数据库的功能，其中包括向用户告知文档或机构状态变动的警示服务。

2003 年 9 月，沃尔夫斯堡集团发布了《关于监控、筛选和搜索的沃尔夫斯堡声明》，随后于 2009 年更新，进一步指导“交易监控框架的设计、落实和持续维护，以便进行实时筛选、交易监控和反向搜索”。该文件探讨了对交易和客户进行适当监控以识别潜在的异常或可疑活动和交易以及向主管当局报告此等活动和交易的必要性。声明特别涵盖了与建立风险为本的流程相关的问题，该流程可用于监控、筛选和搜索交易和客户。

该集团的所有出版物均可在其网站上查看，网址为：www.wolfsberg-principles.com/standards.html。

截至 2016 年 6 月 30 日，网站上所列的沃尔夫斯堡集团标准包括：

- 《沃尔夫斯堡代理银行准则》（2014 年）
- 《沃尔夫斯堡集团 MIPS 白皮书》（2014 年）
- 《沃尔夫斯堡私人银行准则》（2012 年 5 月）
- 《沃尔夫斯堡预付卡及储值卡指引》（2011 年 10 月 14 日）
- 《沃尔夫斯堡反腐指引》（2011 年）
- 《关于发布“沃尔夫斯堡反腐指引”的声明》（2011 年 8 月）
- 《沃尔夫斯堡贸易金融准则》（2011 年）

- 《沃尔夫斯堡关于监控、筛选和搜索的白皮书》—— 2009 年 11 月 9 日
- 《沃尔夫斯堡集团关于信用卡和签账卡发行以及商业收购活动的反洗钱指引》—— 2009 年 5 月
- 《沃尔夫斯堡集团清算中心关于支付信息标准的声明》—— 2007 年 4 月
- 《沃尔夫斯堡集团向代理银行客户发布的通告》—— 2007 年 4 月
- 《沃尔夫斯堡关于使用风险为本的方法管理洗钱风险的指引声明》—— 2006 年 3 月
- 《沃尔夫斯堡关于共同基金和其他公共投资工具的反洗钱指引声明》—— 2006 年 3 月
- 《沃尔夫斯堡抑制恐怖融资活动的声明》—— 2002 年 1 月

世界银行和国际货币基金组织

国际货币基金组织 (IMF) 和世界银行共同协助金融行动特别工作组处理某些国家对参与国际反洗钱斗争持抵制态度的问题。自 2001 年以来，这两大机构一直要求受益于金融和结构援助项目的国家实施有效的反洗钱控制措施。

2001 年 4 月，在题为《加大对反洗钱工作的投入》的联合政策文件中，这两大机构详细阐述了将针对洗钱行为所采取的全球性措施。

2001 年 9 月，国际货币基金组织和世界银行开始将打击洗钱及其他金融犯罪全面融入其监控行为和程序。当月，国际货币基金组织理事会的顾问机构，即国际货币与金融委员会 (IMFC) 发布了一份公报，宣称其将“尝试把金融滥用问题方面、尤其是国际打击洗钱的工作，整合到各种相关且适宜的工作中去”。

2001 年 2 月，国际货币与金融委员会、国际货币基金组织和世界银行联合发布《金融系统的滥用、金融犯罪和洗钱》文件，其中探讨了机构在利用自身的影响力推进国家的反腐进程，从而“保护国际金融体系的诚信度免受滥用”中如何扮演自己的角色。

此后，国际货币基金组织和世界银行更加积极地开展打击洗钱活动，具体表现如下：

- 相比其他形式的金融滥用，更加关注洗钱。
- 帮助各国加强金融监管。
- 加强与经济合作与发展组织 (OECD) 和巴塞尔银行监管委员会的互动。
- 对请求金融援助的国家坚持执行国际反洗钱标准。

在 2004 年 4 月的联席会议上，这两大机构同意永久性地采纳试点法案，即使用统一的国际反洗钱和反恐融资标准对一国的合规状况进行评估。该法案为金融行动特别工作组发布“不合作国家和地区”(NCCT) 名单的做法画上句号。

世界银行和国际货币基金组织与金融行动特别工作组共同建立合作框架，采用全球统一的方法，全面评估各国对金融行动特别工作组 40 项建议的合规情况。这一评估是金融部门评估制度的一部分，并最终发布了《关于遵守标准与守则报告》(ROSC)。这份报告总结了各国在多大程度上遵守国际货币基金组织和世界银行的 12 个领域及相关标准。这 12 个领域分别为：会计；审计；反洗钱 / 反恐融资；银行业监管；公司治理；数据传输；财政透明；破产和债权人权利；保险业监管；货币和金融政策透明度；支付系统；证券监管。《关于遵守标准与守则报告》依照成员国的要求制作并发布，其中总结了国家对标准的遵守情况。报告可帮助各国政府机构制定机构的政策，在私人领域，还可供评级机构进行风险评估。《关于遵守标准与守则报告》会定期修订，但每隔几年便会制作并发布新报告。

2002 年，世界银行和国际货币基金组织制定了《反洗钱及反恐融资活动参考指南》，为各国根据国际标准贯彻执行反洗钱 / 反恐融资制度提供了切实可行的步骤。2006 年，第二版和第 9 项特别建议补充内容发布。该指南对个别国家和地区在发展过程中存在的全球性洗钱和恐怖融资活动问题进行了描述。该指南解释了建立有效反洗钱和反恐融资活动的法律及制度框架所需的基本要素，同时还概述了世界银行和国际货币基金组织在其中所发挥的作用。

组织	性质	主要文件
金融行动特别工作组	• 由 34 个成员和 2 个国际组织组成的政府间组织 • 制定反洗钱和反恐融资活动标准	• 40 项打击洗钱和恐怖融资活动建议（2012 年 2 月最新修订）
巴塞尔银行监管委员会	• 由十国集团的中央银行行长组成 • 在全球范围内推广健全的监管标准	• 《银行客户尽职调查白皮书》（2001 年） • 《各司法管辖区共享与反恐融资活动有关的金融记录》（2002 年） • 《账户开立和客户身份识别通用指南》（2003 年）（2016 年修订） • 《一体化了解您的客户风险管理白皮书》（2004 年）（2016 年修订）

组织	性质	主要文件
欧洲联盟	• 由 28 个欧洲国家组成的政治经济联盟 • 针对成员国出台法律发布反洗钱 / 反恐融资指令，要求各国必须防范本国金融系统受到洗钱和恐怖融资活动的滥用	• 欧盟关于防止利用金融系统进行洗钱活动的第 1 号指令（1991 年） • 第 2 号指令（2001 年） • 第 3 号指令（2005 年） • 第 4 号指令（2015 年）
沃尔夫斯堡集团	• 由 13 家全球性银行组成的协会 • 旨在制定银行反洗钱控制措施的标准	• 《沃尔夫斯堡私人银行反洗钱原则》（2002 年最新修订） • 《抑制恐怖融资活动指南》（2002 年） • 《代理银行业务反洗钱原则》（2002 年）
亚太反洗钱工作组、加勒比地区金融行动特别工作组、欧亚反洗钱与反恐融资活动工作组、中非反洗钱特别工作组、西非政府间反洗钱行动工作组、拉丁美洲金融行动特别工作组、中东与北非金融行动特别工作组、关于评估反洗钱措施专家委员会、东南非反洗钱工作组	• 与金融行动特别工作组 (FAFT) 类似的区域性组织，形式及职能与金融行动特别工作组相似 • 为金融行动特别工作组制定标准和类型做出贡献	• 洗钱类型等
埃格蒙特集团	• 金融情报机构非正式网络组织	• 宗旨声明（2004 年最新修订） • 《金融情报机构间洗钱案件信息交换原则》（2001 年） • 《金融情报机构间信息交换最佳实践》（2004 年）
美洲药物滥用管制委员会	• 美洲国家组织内处理涉毒问题（包括洗钱）的委员会	• 示范规章
世界银行和国际货币基金组织	• 这两大机构相互合作并与金融行动特别工作组共同努力，鼓励国家制定充分的反洗钱法律并对金融行动特别工作组成员国的反洗钱法律和程序进行审查	• 2002 年反洗钱和反恐融资活动参考指南：帮助国家建立和改进其制度框架的手册（2007 年最新修订）

重要的美国立法和监管举措适用于国际性的交易

本节概述了适用于国际交易和司法管辖的美国反洗钱和反恐融资活动法律的基本要素。

美国《爱国者法》

2001 年 9 月 11 日的恐怖袭击使美国国会深刻意识到识别并破坏恐怖融资活动机制的迫切需求。为此，美国国会于 2001 年 10 月颁布了《使用适当之手段来阻止或避免恐怖主义以团结并强化美国的法律》（即《爱国者法》），继 1970 年通过《银行保密法》和 1986 年颁布世界首部将洗钱定罪的《洗钱控制法》（美国公法 99-570）以来，该法将反洗钱法律和《银行保密法》(BSA) 提高到了全新水平。

该法案第 3 篇（美国公法 107-56）题为“2001 年国际反洗钱、反恐融资法案”，涵盖了大多数与反洗钱相关的法律条款。第 3 篇的目的是“巩固美国为防范、侦测、起诉国际洗钱和恐怖融资活动采取的措施，以国家名义授权机构特别审查外国司法管辖区、在美国国外运营的金融机构、对犯罪分子形成可乘之机的国际交易级别或账户类型，确保金融服务行业的所有适当要素均符合相关要求，以便向有关部门报告潜在的洗钱交易”。

在用途声明中，美国《爱国者法》将美国机构和在美国经营的非美国机构纳入覆盖范围。值得关注的是，美国财政部根据美国《爱国者法》颁布的法规规定了金融组织在遵守该法条款时需要遵循的详细要求。这些法规收录在《联邦法规汇编》第 31 篇第 10 章。

美国《爱国者法》的关键条款建立在这样的大前提下，即: 美国金融系统的国际接入点必须得到控制。因此，该法涵盖了大量影响外国企业的反洗钱和反恐融资活动条款。其中包括:

第 311 条：针对主要洗钱问题的特别措施（美国法典第 31 篇第 5318A 条）。该条款授权美国财政部针对被其部长认定为“首要洗钱关注对象”的海外司法管辖区、外国金融机构、某类国际交易或某类型账户可采取渐进、适度的措施。在将某国或某一金融机构认定为“首要洗钱关注对象”后，美国政府可强令美国银行中止与被认定对象的多项金融交易。一旦作出认定，财政部就可要求美国金融机构采取下述五项特别措施中的任何或所有措施:

1. 对特定金融交易的记录进行保存并 / 或提交报告，其中包括对交易的描述、参与交易各方的身份和住址以及所涉资金的受益所有人身份。
2. 获取与由某外国人员或其代表在美国开设或持有的任何账户的受益所有权相关的信息。

3. 对获得允许使用外国银行通汇账户或通过其进行交易的客户进行身份识别并获取有关信息。

4. 对获得允许使用外国银行“代理”账户或通过其进行交易的客户进行身份识别并获取有关信息。

5. 关闭某些通汇账户或代理账户。

为确保考虑周全，在将某一司法管辖区、机构、特定交易类型或特定账户类型认定为“首要洗钱关注对象”前，财政部长必须与国务卿和总检察长进行磋商。

第 311 条的措施与海外资产控制办公室 (OFAC) 的任命不同，这条法律规定的措施应用范围更广，可提出冻结资产的要求。

第 312 条：代理账户和私人银行账户（美国法典第 31 篇第 5318(i) 条）。要求对非美国人员的外国代理（几乎包括一家机构与外国金融机构所能产生的所有账户关系）账户和私人银行账户实施尽职调查，并在特定情形下实施增强尽职调查。

代理银行服务的规定适用于美国银行、信用合作社、储蓄机构、信托银行、经纪自营商、期货经纪商、商品和共同基金的中介经济商以及外国银行在美国的代理机构和分支机构。

该条款所指的外国金融机构包括外国银行、美国银行在国外的分支机构、担任经纪自营商的外国企业、期货经纪商、商品中介经纪商或在美国经营的共同基金的经纪商以及在国外组建的汇款经纪商或货币兑换所。

在必要时，尽职调查制度必须包括“合适、具体并以风险为本的”合理性强化政策、程序和控制措施，以便识别并报告在美国的代理账户中存在的可疑洗钱活动。这一尽职调查制度还应纳入机构的反洗钱制度。

尽职调查制度必须涵盖三大措施：

1. 确定强化尽职调查是否必要。

2. 评估代理账户的洗钱风险。

3. 适用风险为本的程序和控制措施来侦测和报告可疑洗钱活动。

根据实施条例的规定，持以下许可证的外国银行所开立的代理账户必须适用增强尽职调查流程：

- 离岸银行业务许可证。
- 由被国际组织认定且美财政部长对这一认定表示同意的不合作国家和地区所签发的许可证。
- 由美国财政部部长根据上述《爱国者法》第 311 条认定需要采取特别措施的国家签发的许可证。

在以下情形下，必须进行增强尽职调查：

- 对可能存在的洗钱和可疑交易开展强化审查，包括：
  - — 获得与外国银行反洗钱制度相关的信息。
  - — 采用合理措施监控代理账户的进出交易，以侦测可能的洗钱和可疑活动。
  - — 获得与充当通汇账户的代理账户相关的信息。
- 确定与外国银行（开立代理账户的银行）存在代理关系的其他外国银行是否使用代理账户，并采取合理措施评估并减轻与此等账户相关的洗钱风险。
- 对于股份无法公开交易的外国银行，识别在该外国银行中拥有 10% 及以上投票权的各类银行证券所有人的身份以及各所有人所有者权益的性质和程度。

私人银行业务规定的适用对象与代理银行业务规定的适用对象相同。此等机构必须制定适用于私人银行账户的尽职调查制度并对外国高级政要及其直系亲属和关系密切人员的私人银行账户进行强化审查。

根据这一规定，私人银行账户指：一名或多名非美国人员的累积存款金额达到或超过 100 万美元并指定银行员工作为非美国人员联络人的账户。

对于需要尽职调查的私人银行账户，美国机构必须采取合理步骤以：

- 确认识别账户所有名义和受益所有人的身份。
- 确认这些所有人是否为“高级外国政要”。
- 确认账户的资金来源以及账户的目的和预期用途。
- 监控账户，确保账户活动与账户资金来以及账户目的和预期用途的信息相符，以便防范洗钱犯罪并报告任何可疑的洗钱行为或可疑活动。

在确认账户所有人是否为“高级外国政要”时，机构应采取合理步骤用以确认此人是否为“外国政府行政、立法、管理、军事或司法部门的现任或前任高级官员”。此外，国外政党和政府所有制商业企业的官员也在定义的涵盖范围内。定义还包含直系亲属以及“广泛公认”的关系密切人员。

为这些人员持有账户的机构必须执行合理的“强化详细审查”来侦测其资金是否“涉及外国腐败所得”，包括任何“通过侵吞、盗用或挪用公共资金，非法侵占外国政府财产，或受贿或勒索等手段”而获得的资产或财产。

第 313 条：禁止为外国空壳银行开立代理账户（美国法典第 31 篇第 5318(j) 条）。禁止美国银行、证券经纪商和经销商为外国不受监管且没有实体经营活动的空壳银行持有代理账户。“实体经营”指外国银行拥有开展银行业务活动的固定经营场所（相对于仅有一个电子地址），其特点包括：取得开展银行业务活动的授权；拥有一名以上的全职员工；保存经营记录；接受签发许可证的银行业监管当局的检查。空壳银行一词不包括拥有实体经营的银行所管理的附属机构。

该法条还要求金融机构采取合理措施，确保拥有代理账户的外国银行不向外国空壳银行发出使用此等账户的许可。银行和证券经纪商可以使用认证表来执行该规定。该流程要求外国银行至少每三年进行一次确认，证明其自身不是空壳银行，且其不允许空壳银行通过连环代理关系使用美国的代理账户。

第 314(A) 条和第 314(B) 条：“通过推动执法机关、监管部门、机融机构开展合作，分享涉嫌参与恐怖主义或洗钱活动的人员的信息”，帮助“执法机关识别、扰乱、防范恐怖主义活动和洗钱活动”。

- **第 314(a) 条：**美国金融犯罪执法网络的第 314(a) 条规定令美国联邦、州级、地方和外国（欧盟）执法机关可通过金融犯罪执法网络，与 2.2 万多个金融机构内的 4.3 万多个联络点对接，从而确定涉嫌参与恐怖主义或洗钱活动的人员的账户和交易地点。金融机构报告可疑活动后，执法机关在获取相关文件时，必须遵守适用于其选定的调查工具的法律标准。
- **第 314(b) 条：**允许金融机构在提供免责保护的安全港进行信息共享，以便更好地识别并报告洗钱或恐怖活动。314(b) 信息共享为自愿制度。可能参与 314(b) 的机构包括受美国金融犯罪执法网络规定的反洗钱制度监管的美国金融机构，以及这些机构的所有关联机构。314(b) 目前涵盖的美国金融机构类型包括：
  - 银行
  - 赌场和纸牌俱乐部
  - 货币服务企业
  - 证券经纪 / 经销商
  - 共同基金
  - 保险公司
  - 期货经纪商和商品中介经纪商
  - 贵金属、宝石或珠宝交易商

— 信用卡系统运营商

— 贷款或金融公司

第 319(a) 条：从美国代理账户中没收（美国法典第 18 篇第 981(k) 条）。当资金已被存入外国银行时，本法条允许美国政府从该外国银行在美国开立并维护的代理银行账户中查封同等数额的资金。由于该资金被视为代理账户中的存款，所以美国政府无需追踪资金。但资金所有人可以就查封令提出异议。

第 319(b) 条：与外国银行代理账户相关的记录（美国法典第 31 篇第 5318(k) 条）。允许相应的联邦银行业监管机构要求金融机构在 120 小时（5 天）内提供与该机构的反洗钱合规制度，或其客户又或其在美国境内开立、维护、管理的账户相关的记录或信息。

该法条还允许财政部长或司法部长使用作证传票向在美国境内拥有代理账户的外国银行索要记录。只要与该代理账户有关，包括在美国境外产生的任何记录均可索要。如果外国银行无法服从作证传票要求或提出异议，财政部长或司法部长可以命令美国金融机构在收到此等命令后的十天之内关闭代理账户。

此外，该法条还要求外国银行指定美国境内的注册代理人根据法条规定接受作证传票的送达。另外，为外国银行维护代理账户的美国银行、证券经纪商和经销商必须保留在外国银行拥有 25% 控股权的所有人的身份记录（除非股份公开交易）以及该代理银行在美国的注册代理人名称。

一般来说，这一信息收集在遵守上述第 313 条所需的认证表上，且必须至少每三年更新一次，或在信息有误的情形下进行更为频繁的更新。

美国犯罪资金的到达
洗钱犯罪刑事及民事财产没收法律的适用范围

1986 年，美国颁布全球首个将洗钱活动定为刑事犯罪的法律——《洗钱控制法》，这是一个强大的法律武器，适用于金融交易所涉及的资产来源于至少一种“特定非法活动”(SUA) 的情形。特定非法活动几乎包含美国所有可能产生经济收益的犯罪，包括劫持航空器、电信欺诈、银行欺诈、侵犯版权、挪用公款、出口违规、非法赌博、毒品犯罪、敲诈勒索甚至是环境犯罪。（美国法典第 18 篇第 1956 条和第 1957 条。）

如果金融交易的全部或部分发生在美国境内或外国金融机构在美国金融机构中持有银行账户，则该反洗钱法还适用于外国个人和外国金融机构。

虽然洗钱指控必须证明特定非法活动收益的存在，但却无须证明被告“明知”资金的确切来源。洗钱指控只需证明被告知道资金“来源于该州、联邦或外国法律规定为重罪的某种活动”，但该活动是否为“特定非法活动”在所不论（美国法典第 18 篇第 1956(c)(1) 条）。法院经常将“有意忽视”（即“有意回避明知的事实”）视为切实明知。“有意忽视”可根据交易与被告行为的客观情况进行推定。

上述美国《爱国者法》的第 319(a) 条极大地加强了没收外国人员和机构资金的权力。如果美国政府追查的资金存于外国银行，而该外国银行又在某一美国银行开设了“跨行账户”，则美国政府可通过法律途径没收存放在美国账户内的涉罪资金。

案例分析

2012 年 4 月，美国纽约南区检察院收缴 Wegelin & Co. 公司在瑞士银行康涅狄格州斯坦福德市分行的代理账户中存储的 1630 万美元。Wegelin 成立于 1741 年，是瑞士最古老的银行，主要向全球客户提供私人银行业务、资产管理等服务，其客户也包括美国纳税人。这起民事财产没收控诉指控 Wegelin 利用其代理账户，帮助美国纳税人逃税。截至 2010 年，Wegelin 共持有 15 亿美元的未经申报的美国纳税人的资金。2013 年 1 月，Wegelin 银行向某法院认罪，承认在 2000 至 2001 年期间图谋欺诈美国国税局，伪造联邦所得税收据，躲避联邦所得税，因而被判向美国缴纳近 5800 万美元。此判罚及 2012 年 4 月的民事财产没收的总金额近 7400 万美元。

美国财政部海外资产控制办公室

除上述法律法规外，其他国家的金融机构与企业必须了解由美国财政部海外资产控制办公室 (OFAC) 颁布的法规的治外法权。

美国财政部海外资产控制办公室根据美国外交政策和国土安全目标制定和实施针对特定国家、恐怖分子、跨国毒贩和大规模杀伤性武器扩散有关人员的经济贸易制裁措施。美国财政部海外资产控制办公室根据战时总统权利、国家紧急权力以及经专项法律的授权对美国司法管辖区内的交易实行管制并对海外资产进行冻结。很多制裁是以联合国和其他国际委托为基础的多边制裁，需要与盟国政府紧密合作。

美国财政部海外资产控制办公室定期发布受制裁的个人和组织的名单，美国财政部海外资产控制办公室制裁计划禁止这些个人和组织的交易，并要求冻结其资产。对于违反制裁计划冻结命令的个人和组织，美国财政部海外资产控制办公室有权对其进行重罚。

所有美国人员和机构都必须遵守美国财政部海外资产控制办公室的法规。这里所说的美国人员和机构包括所有美国公民和永久居民（不论其身居何处）；美国境内的所有个人和实体；以及所有在美国成立的实体及其海外分支机构。对于某些制裁方案，例如针对朝鲜、叙利亚和古巴的制裁，由美国公司拥有或控制的所有外国附属机构也必须遵守。然而，值得注意的是，美国正在修订古巴制裁计划的规定。有些制裁方案还要求拥有原产于美国的商品的外国人遵守。

案例分析

2014 年，法国巴黎银行为与美国财政部海外资产控制办公室 (OFAC) 达成和解，支付 9.63 亿美元，创下历史新高，此前该银行还因明显违反美国制裁法规，被处以 89 亿美元的罚款。法国巴黎银行采用系统性做法，对 2005 年至 2012 年间发送给或经由美国各银行机构的近 4000 笔涉及美国制裁对象的金融交易相关信息进行隐匿、移除、删除或模糊处理，明显违反了美国对苏丹、伊朗、古巴和缅甸的制裁措施。法国巴黎银行对发送至或经由美国的制裁相关支付的处理方法包括，移除有关受制裁对象的信息，用银行的名字或代码代替受制裁对象，或对支付进行拆分，使监管部门无法识别交易涉及受制裁对象。

备注：

第 3 章

反洗钱 / 反恐融资合规制度

反洗钱 / 反恐融资制度（AML/CFT 制度）是金融机构合规体系必不可少的组成部分。反洗钱 / 反恐融资制度的首要目标是保护机构不受洗钱、恐怖融资及其他金融犯罪的滥用，确保机构完全符合相关法律法规的要求。因此，设计、构建并实施反洗钱制度是所有金融机构的当务之急。

反洗钱 / 反恐融资制度应以风险为本。金融机构的某些业务面临更大的洗钱风险，也就需要更多的控制措施来缓释风险，而其他业务的风险则相对较低，无需相同级别的关注。

根据机构规模不同，反洗钱职能可由专设或独立部门行使，可由法务部门等企业其他部门管辖，也可由负有其他合规义务的人员行使。无论机构的规模如何，反洗钱 / 反恐融资制度应从企业级层面防范此类犯罪。

反洗钱 / 反恐融资制度必须为企业设定最低标准，确保其符合所有适用法律法规的要求。各业务或针对特定领域（如私人银行业务、贸易金融、现金处理、机构银行业务、资产管理或调查）的法律实体所制定的政策和程序可以构成对整个机构反洗钱 / 反恐融资制度的补充。合规制度还应包括有洗钱和恐怖融资风险的公司治理和整体管理。

金融机构在设计反洗钱 / 反恐融资制度之前，务必弄清其业务及客户所在的司法管辖区对该金融机构及其员工和客户有何法律规定。金融机构还必须把内部政策和业务风险管理标准考虑在内。在制定反洗钱 / 反恐融资制度之前，如需就复杂的反洗钱 / 反恐融资法律法规获得指导，应咨询专业顾问，包括咨询外部顾问。

本章主要阐述了下列内容：设计合规制度时应考虑哪些因素；如何评估风险；如何识别、处理、记录和追踪可疑活动；如何了解您的客户及员工；如何有效地审计项目；以及在培训和筛选员工方面应了解哪些知识。

评估反洗钱 / 反恐融资风险

引言

了解法律对您的机构、员工和客户的要求是建立有效制度的必备条件。同样需要了解的是反洗钱 / 反恐融资监管部门或监督部门的期望。

金融行动特别工作组 (FATF) 及其众多成员国（如英国和美国）都推动建立以风险为本的控制措施。根据金融行动特别工作组的要求，如果洗钱或恐怖融资风险较高，应采取增强客户尽职调查 (CDD) 措施。

风险为本的方法要求金融机构根据其面临的特定洗钱和恐怖融资风险制定相应的系统和控制措施。因此，风险评估是创建有效反洗钱 / 反恐融资合规制度的最重要步骤之一。随着洗钱风险的增加，强化控制措施已成必要。然而，如需识别并减轻各类风险（无论是低风险、中等风险还是高风险），必须采取一定的控制措施，如客户身份验证、客户尽职调查政策、可疑交易监控和经济制裁筛查等。

大多数政府认为，在反洗钱 / 反恐融资活动领域，风险为本的方法比规范性方法更为可取，因为前者：

- **更灵活**——因为洗钱和恐怖融资活动的风险因所在司法管辖区、客户、产品、交付渠道以及时间的不同而各异。
- **更有效**——因为与立法者相比，机构有更好的条件来有效地评估并降低其所面临的特定洗钱及恐怖融资活动风险。
- **更配套**——因为风险为本的方法促使人们形成共识。推动了反洗钱和反恐融资活动的智能化方法，而不是采用所谓的“照章办事”方法。此外，它还能使机构最大限度地降低反洗钱程序对低风险客户的不利影响。

原因在于，根据合理预期，没有一家金融机构可以侦测到客户的所有不法行为，包括洗钱。但如果金融机构制定了用于侦测、监控和上报危险客户和交易的系统和程序，那么其免遭犯罪分子侵害和免受政府制裁与处罚的可能性就会大大提高。

金融机构面临的风险取决于多个因素，包括地理区域、客户类型以及产品和提供的服务等等。

评估风险时，金融行动特别工作组建议从以下方面考虑：

- 客户风险因素包括非本地居民客户、资金密集型企业、企业的所有权结构复杂，以及企业使用不记名股票。

- 国家或地域风险包括反洗钱 / 反恐融资系统不充分，受到制裁或禁运，为恐怖主义活动提供资金或支持，或腐败程度较为严重的国家。
- 产品、服务、交易或销售渠道风险因素包括私人银行业务、匿名交易、来自未知第三方的付款等。

尽管一些司法管辖区的反洗钱 / 反恐融资法律法规未要求机构建立洗钱 / 恐怖融资 (ML/TF) 风险模型，但许多机构发现此举有利于评估企业层面的风险，其中的客户元素可提供客户类型（如个人、企业、信托）层面的洗钱 / 恐怖融资风险评估，并使机构能够评估特定客户的风险（即对某位客户与该机构的所有关系进行洗钱 / 恐怖融资风险评估）。此外，一些司法管辖区还对报送机构进行单独的制裁评估。

维护反洗钱 / 反恐融资风险模型

风险为本的方法旨在识别、控制和分析反洗钱 / 反恐融资风险，以便设计并有效落实适当的管控措施。因此，至关重要的是风险评级能准确反映目前的风险；提供有价值的评估结论，帮助制定有效的措施以降低风险；并确保定期核查评级结果，必要时予以更新。

风险为本的分析应涵盖国家、行业、法律实体和业务关系层面的适当固有风险与剩余风险。综合上述分析，金融机构应充分认识其客户基础、产品、销售渠道、服务及业务或客户所在司法管辖区的固有风险。机构应根据其收集的业务、交易或其他内部信息和外部信息，充分认识上述风险。

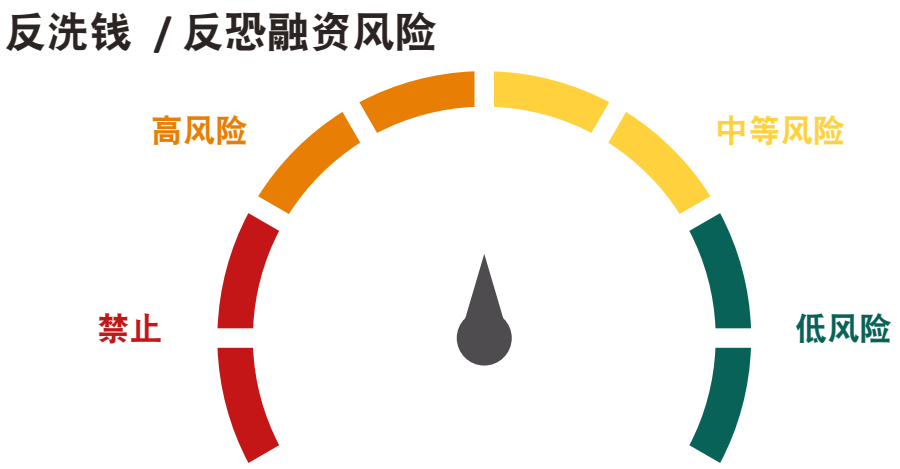
为识别所有的洗钱 / 恐怖融资相关风险，必须全面考虑所有信息。这通常要求业务、风险管理、合规和法务部门的专家参与，有时可能还需听取外部专家的建议。新的商业产品或服务尤其需要进行洗钱和制裁漏洞方面的评估，在进入市场前事先采取适当的管控措施。此外，机构还应考虑有关洗钱 / 恐怖融资风险评估的公开指南，此类指南数量越来越多，且非常有用。这些指南由金融行动特别工作组、金融行动特别工作组类区域性组织、监管机构和联合国毒品与犯罪问题办公室 (UNODC)、国际货币基金组织 (IMF)、世界银行、某司法管辖区的信息、指导和监管机构等其他组织定期发布。

风险是动态变化的，需要持续进行管理。每个机构的营业环境不断变化，这一点也应注意。从机构外部来看，某司法管辖区的政治局势变化或是否对其施加或取消经济制裁可能影响一国的风险评级。从机构内部来看，机构需要根据市场和客户的需求变化，引入新产品、新服务，实施新的销售系统。这些变化共同决定了对审查洗钱 / 恐怖融资风险模型进行定期审查是非常关键的。某些国家出台相关法律法规，强制机构定期审查风险模型（通常一年一次），或在新产品、新销售渠道或新客户类型出现时进行审查。

认识反洗钱 / 反恐融资风险

反洗钱 / 反恐融资风险类别可分为以下等级：

- **禁止类**——机构不得进行涉及这一风险的任何类型的任何交易。遭受经济制裁或被认定为资助恐怖主义活动的国家或地区均为禁止交易的对象，例如被联合国或美国海外资产控制办公室列入制裁名单的国家或 OFAC 名单。
- **高风险**——交易面临极大的风险，但不一定被禁止。为了缓释交易中的高度风险，金融机构应适用更严格的控制措施来降低洗钱 / 恐怖融资风险，例如进行增强尽职调查和更严格的交易监控。以腐败或贩毒闻名的国家或地区一般都视为具有高风险。高风险客户包括政治公众人物 (PEP)，或特定类型的货币服务企业或资金密集型企业；高风险产品和服务包括代理银行业务和私人银行业务。
- **中等风险**——需要进行额外审查，但尚未达到高风险的级别。例如零售企业，虽然接收低或中等资金，但尚不属于资金密集型类别。
- **低风险**——这一级别是洗钱风险的基线。低风险一般指某项活动正常、可预期。



反洗钱 / 反恐融资风险评分

风险评分模型用数值来表现各类风险（地理区域、客户类型以及产品和服务）以及整体客户风险的等级。例如，每个类别的得分在 1 - 10 分之间，10 分代表最高的风险。对于各个类别来说，1 - 3 分为标准风险，4 - 8 分为中等风险，而 9 - 10 分则为高风险。评估产品风险时，这一模型有助于确定适合产品的控制措施，因而特别有效。

随后将这三个类别加以综合，得出总分。简单的模型仅需将各个类别的得分相加即可，总分在 3 - 30 分之间。更为复杂的模型则可以为不同因素设置不同的比重，如更加强调客户类型，而非产品、国家或地区。此外，模型还可以更加复杂，例如，创建可以体现综合评级的组合因素。使用模型的机构可自行设计模型的复杂程度；模型越复杂，评级越有可能反映客户的整体风险情况。

如果采用上述简单的三要素模型，必须特别注意避免无意中认为某个与其他要素相异的异常值不重要。例如，如果某个要素的风险得分为 3，那么综合或总得分将为 9。然而，如果三个要素中，有两个要素的得分为 1，另一个的得分为 7，则综合得分也为 9。在此情况下，应了解如何缓释得分为 7 的要素。这意味着实施更严格的管控或增加限制。

值得注意的是，将各类风险进行综合考量后，客户的风险等级才会变得清晰。比如，当您把产品和客户类型结合起来时，风险等级可能会发生根本改变。例一：国外一家小型私企欲在您处开立活期存款账户，并开通在线电汇业务，而您对该公司了解甚少。客户快速转移资金的能力可能增加其风险等级。地理区域、客户类型以及产品和服务等因素也可能提高客户的风险等级。例二：国内一家在主要股市上市的公司欲在您处开设员工退休计划。公司在主要股市上市时必须提供大量信息。此外，退休计划账户不易受洗钱活动滥用。因此，该客户和账户的风险比前一个外国私企小。

下一个步骤是建立每个风险类别所适用的阈值。机构应留意到，高风险客户不得在所有关系中占过大比重；这并不意味着机构需要调整得分来适应客户构成，而是因为高风险客户确实需要更多的注意。此外，如果客户构成过多地倾向于高风险客户，机构的整体风险等级可能变得难以承受。

评估反洗钱 / 反恐融资风险是反洗钱 / 反恐融资合规制度的一个持续而不断发展的组成部分。机构还须适时评估风险评分模型，风险自评估需要每年或每 18 到 24 个月，每次推出新产品前，以及并购其他金融机构时进行。

机构可通过定期复查风险评级标准，了解被评为高风险的客户是否真的更可能参与可疑活动。如果不是，则需要对风险评分模型进行重新评估。

评估客户的动态风险

风险评估的另一大关键组成部分是重新评估风险，确定是否应该调高或降低客户的风险等级。为了有效地分配有限的资源，有必要识别触发此类复查工作的重要因素。

除了对客户固有风险的初次评估，还需考虑客户与机构的关系及其风险评级随时间的变化。决定客户风险评级的最重要因素也许是客户的实际活动。例如：一个学生活期存款账户的风险一开始可能很低。然而，如果记录显示该账户多次将大笔资金转至高风险司法管辖区，这对该客户类型而言是异常活动，则该账户的风险等级应调高。同样，货币服务企业 (MSB) 或代理银行等潜在的高风险客户可能只从事其分内活动。这种客户的实际风险可能低于仅根据固有风险做出的判断。因此，仅根据固有风险被判断为风险“低”或“标准”的学生客户实际上给机构带来的风险高于固有风险“高”的货币服务企业。

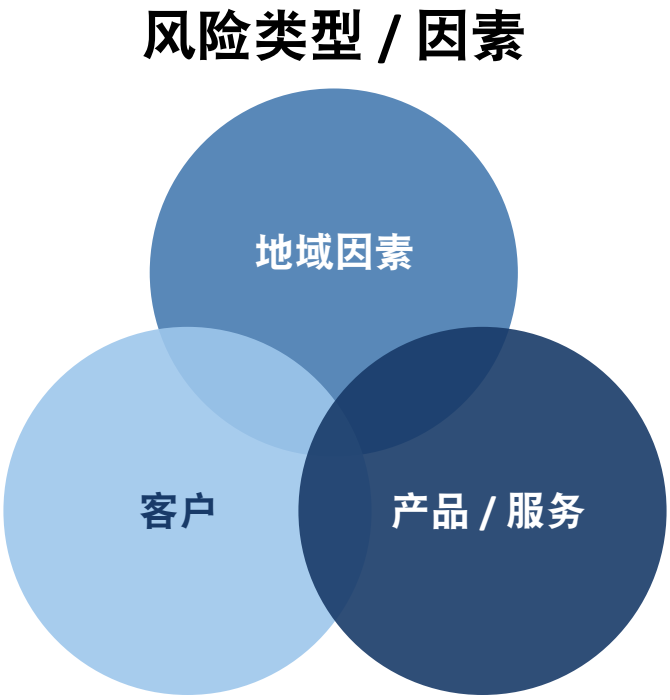
由于每个金融机构都会建立客户交易记录，机构应考虑根据以下因素调整客户的风险评级：

- 日常活动，例如警报、案例和可疑交易报告 (STR) 等记录。
- 收到执法机关问讯，如作证传票。
- 违反经济制裁制度的交易。
- 其他因素，例如客户进行大量出乎意料之外的活动，如国内慈善机构开展大规模国际交易，或正常情况下不需大量现金的企业接触大笔现金。

机构了解客户的活动后，可更好地确定该客户的实际风险。正如之前所述，高风险客户以及风险评级因活动而调高的客户应接受增强尽职调查 (EDD)，以便缓释风险。这种调查可能最终确定客户的活动是否可疑。如果可疑，客户记录应能反映此活动造成的变化。

反洗钱 / 反恐融资风险识别

风险为本的方法的核心目的是评估金融机构的客户、地域和产品或服务。下文将进一步分析这三大重要的风险因素。



客户类型

风险评估中一个至关重要的步骤，是对机构或企业所提供产品和服务的用户进行分析。客户类型包括个人、上市公司、私营企业、合资企业、合伙企业和金融机构，基本包含任何希望与金融机构建立业务关系的客户。

有犯罪历史的客户会被评定为最高风险等级。对政治人物或政治组织成员的评分也趋于最高。

跨国上市公司的风险评分一般低于非上市公司，因为在主要证交所上市的公司已经提供了大量公开信息，也进行了一定的尽职调查。如果洗钱分子隐藏在公司组织形式之后，如信托、慈善组织、有限责任公司或很难识别受益所有人的机构，风险通常更高。如果客户公司位于缺少反洗钱要求或有严格公司保密法规保护的国家或地区，则风险将会进一步增加。

各国监管机构均表示，一些客户类型本身即具有较高的洗钱风险。这些客户类型包括：

- 银行
- 赌场
- 位于避税 / 金融庇护所的离岸公司和银行
- 大使馆

- 货币服务企业，包括货币兑换所、汇款经纪公司和支票兑现所
- 虚拟货币交易所
- 汽车、船舶和飞机经销商
- 二手车、二手卡车经销商和机械零部件生产商
- 专业服务供应商（律师、会计、投资经纪商，以及为客户提供金融联络服务的第三方）
- 旅行社
- 证券经纪 / 经销商
- 珠宝、宝石和贵金属经销商
- 进出口公司
- 现金密集型企业（如餐馆、零售商店、停车场等）

以上为高风险行业的不完全名单。值得注意的是，行业并非决定风险大小的唯一因素。许多未出现在名单中的企业也能被用于洗钱，因此审视风险时应结合其他因素。

在接纳客户时，以及开展业务关系期间，应落实严格有效的筛查程序，这是识别高风险客户类型的重要环节。

案例分析

2014 年 11 月，美国佛罗里达州的北郡社区发展联邦储蓄互助社因客户中包含大量货币服务企业等反洗钱缺陷，被金融犯罪执法网络 (FinCEN) 处以 30 万美金的罚款。该储蓄互助社共有 400 万美元资产和 5 名员工，其客户中包含 56 个位于中美洲、中东地区和墨西哥等高风险司法管辖区的货币服务企业，均与该互助社的会员领域相距甚远。互助社的年收入有 90% 来自货币服务企业，为这些企业处理的交易总价值约 20 亿美元。金融犯罪执法网络发布的指令显示，该互助社的一大失误是未开展风险评估，否则可能识别这些风险。此外，该互助社还依靠某客户对这些货币服务企业开展尽职调查。正是这位客户最初为互助社推荐了这些货币服务企业。由于互助社未独立评估该客户的尽职调查工作，这加剧了互助社面临的风险。

地理位置

制定风险评分模型的关键步骤之一是设定司法管辖区风险。个人客户的居住国或司法管辖区在哪？客户的国籍国又在哪？企业客户的总部在哪？它们的业务主营地又在哪？

由于没有明确且独立的系统对不同区域和国家存在的洗钱风险进行评估，一些企业自行设计评估方法；其他企业则选择外部解决方案。无论选择何种途径，对风险评级方法进行记录至关重要。在较大的机构内，整体风险管理战略可能要求执行人员审查，并由高级管理层签批洗钱 / 恐怖融资风险评估结果。

在对洗钱风险进行有针对性的关注时，由政府和国际组织公布的恐怖主义和制裁名单都是有用的参考。其中包括英国金融服务监管局 (FCA)、美国海外资产控制办公室 (OFAC)、美国金融犯罪执法网络 (FinCEN)、欧盟 (EU)、世界银行、联合国安理会，以及印度尼西亚国家反恐局 (BNPT) 等各司法管辖区的监管和执法机关发布的名单。模型还应考虑该国是否为金融行动特别工作组成员国或其同类区域性组织成员，且是否符合与国际最佳实践相当的反洗钱 / 反恐融资要求。

机构还可以考虑国家或地区的整体声誉。在某些国家或地区，现金可能是标准的交易工具。有些国家或地区可能存在政治不稳定因素，公共或私营机构腐败猖獗。有些国家或地区则是公认的银行保密庇护所。还有一些国家或地区可能是众所周知的毒品产地或者毒品过境地。怎样才能识别这些国家呢？

- 美国国务院发布的年度《国际毒品控制战略报告》对 100 多个国家和地区的洗钱控制措施进行了评级
- 透明国际发布的“年度清廉指数”对 100 多个国家和地区的清廉度进行了测评
- 金融行动特别工作组识别反洗钱 / 反恐融资制度薄弱的司法管辖区并发布国家互评报告
- 美国国内司法管辖区的评估标准是其是否成为政府认定的高风险地域，例如高密度毒品贩卖区 (HIDTA) 或金融犯罪高发地区 (HIFCA)

机构还可以密切关注主流新闻媒体的报道，并定期追踪所有国家和地区名单中的变化。

产品 / 服务

评估反洗钱 / 反恐融资风险的一个重要因素是审查机构或企业所提供的全新和现有产品和服务，确定它们可能以何种方式被用于洗钱或恐怖融资活动。合规专员应积极参与到项目小组中，为全新产品和系统确定适当的控制框架。

您所在的机构所提供的哪些产品和服务可能会面临洗钱和恐怖融资活动风险？互联网账户？私人银行业务？汇款业务？股票经纪业务？年金？保险产品？离岸服务？汇票？代理银行业务？

这种风险评级基于客户寻求的产品类型，在计算时考虑了若干与产品相关的因素。最值得注意的是，风险评级的结果取决于该产品被用于洗钱或恐怖融资活动的可能性。利率掉期不太可能被用于恐怖融资活动，但这一点在证券上可能就不适用。产品评分并非普遍一致，因为不同的金融机构面临着不同的风险程度。

某一特定产品或服务（无论全新或现有）：

- 是否允许在短时间内进行大量交易？
- 是否允许客户在机构监管程度极低的情况下参与交易？
- 是否允许用户享有极高的匿名等级？
- 是否具有极高的交易或投资价值？
- 是否允许向第三方支付？
- 是否存在异常的复杂性？
- 是否需要政府核实客户资格？

此外，某些银行的特定业务或产品也被视为具有高风险。其中包括：

- 私人银行业务
- 离岸国际活动
- 吸纳存款业务
- 电汇和现金管理业务
- 未披露主要受益人身份的交易
- 贷款担保计划
- 旅行支票
- 正式银行本票
- 汇票
- 外汇交易

- 跨国汇款
- 支付处理方等支付服务；预付产品、自动清算中心 (ACH)
- 远程储蓄
- 有不确定定价特征的贸易融资交易
- 通汇账户 (PTA)

反洗钱 / 反恐融资制度

反洗钱 / 反恐融资制度的要素

反洗钱 / 反恐融资制度有四个必需要素，通常被成为反洗钱 / 反恐融资制度的“四大支柱”，分别为:

- 包括内部政策、程序和控制措施的反洗钱制度体系（第一道防线）
- 指定合规职能部门及合规专员（第二道防线）
- 持续的员工培训项目
- 检验反洗钱制度整体有效性的独立审计职能部门（第三道防线）

有关客户尽职调查 (CDD) 的要求通常包含在内部控制制度中，金融行动特别工作组着重将客户尽职调查作为缓释反洗钱 / 反恐融资风险的关键手段。美国金融犯罪执法网络 (FinCEN) 在 2016 年的规定中提出了第五大支柱，要求采取适当的风险为本程序来开展持续的客户尽职调查，将这一关键问题升级为反洗钱 / 反恐融资制度的支柱性内容。这些程序包括:

- 了解客户关系的本质及建立客户关系的目的，以便制定客户风险状况档案
- 开展持续监控工作，识别并报告可疑交易
- 保存并更新客户信息

许多国家的反洗钱 / 反恐融资法律提出了一些必须纳入反洗钱 / 反恐融资制度的要素。机构应确保已满足业务所在司法管辖区的法律法规对全部要素的规定。

包括内部政策、程序和控制措施的反洗钱制度系统体系

金融机构应制定并持续改进其政策、程序和控制措施，这是建立成功的反洗钱 / 反恐融资制度的基础。政策、程序和控制措施共同定义并支撑整个反洗钱 / 反恐融资制度，同时也是概括机构如何满足监管部门规定的蓝图。这三项内容的设计应旨在缓释已识别的反洗钱 / 反恐融资风险，还应考虑金融机构必须遵守的反洗钱 / 反恐融资法律法规。政策、程序和控制措施应清楚反映机构的风险偏好——即机构准备好承受的风险和不能承受的风险。

尽管这些控制措施通常用于第一道防线（负责接纳新客户的员工），下文将介绍金融机构所有各级员工必须为创建和维护反洗钱 / 反恐融资制度、推动其取得全面成功做出贡献。

在较大的金融机构，采取企业级层面的措施非常关键，这能使整个金融机构的洗钱 / 恐怖融资风险管理方法保持一致。此外，金融机构还须满足对区域或具体业务的要求。例如，对于在多个区域或国家开展业务的金融机构，其企业级层面洗钱 / 恐怖融资风险模型必须反映当地的监管要求。为此，机构可在其全球反洗钱 / 反恐融资制度以外提供另一个制度，或附上针对某个国家的附录。

案例分析

2012 年 12 月，汇丰控股有限公司和汇丰美国银行因违反规定，同意向多个美国政府部门交付 12 亿美元罚金，其中包括未能从企业级层面认识其全球机构的合规情况。在一个案例中，汇丰的伦敦总部意识到墨西哥业务部门存在薄弱环节。美国业务部门为墨西哥业务部门处理了大量交易，但从未被集团的任何人员告知对方的薄弱环节。另一案例中，美国以外的业务部门故意隐瞒经由美国业务部门汇向受制裁对象的电汇信息。有关如何解决这些问题的争议未得到妥善解决，导致汇丰内部的痼疾持续多年。如果当时汇丰设有强大的集中监管制度，而非采用基于地方的模型，则这些薄弱环节可能得到有效缓释，可能也就不会导致随后的重量级处罚。

内部反洗钱 / 反恐融资政策应由执行管理层和董事会制定并审批通过，应确定机构在反洗钱方面的总基调。虽然机构的政策可能是高级别的原则声明，但它也是相关程序和控制措施的基础，这些程序和控制措施所提供的具体内容确定了业务条线应如何满足法律法规以及机构反洗钱 / 反恐融资政策的规定。

标准的反洗钱 / 反恐融资运作程序应由金融机构的业务部门起草。这些程序必须根据法律法规的变化、产品和机构的变动进行修订和更新。这些程序比相应的反洗钱 / 反恐融资政策更加详细；它们将政策转化成可接受、可操作的实践。这些程序还构成了反洗钱 / 反恐融资培训的重要组成部分，也为合规监控制度奠定基础。除了政策和程序外，还应该制定一个流程来支持和促进相关程序的有效执行，并定期审查和更新该流程。

在政策和程序提供重要指导的同时，反洗钱 / 反恐融资制度还依赖于各种不同的内部控制措施，包括管理报告和其他内设的保障措施，以保证制度的正常运转。这些内部控制措施应确保合规部门能识别标准程序和安全协议之间的偏差。诸如要求企业主管对超过规定数额的交易进行批准或者两人会签，如此简单的事情也能成为关键的内部控制要素，一旦被忽略，将严重削弱机构的反洗钱 / 反恐融资制度，引起监管部门的调查。

同样，如果发现后续问题，对之前认为偏离政策的情形进行二次审查和批准流程就会非常有用。其他有效控制措施涉及技术的使用，如要求输入所需信息的账户开立系统，侦测需要上报的现金交易的集合系统以及自动账户监控程序。

反洗钱政策、程序和控制措施

反洗钱 / 反恐融资合规制度应以书面形式呈现，包含为防范、侦测和防止洗钱和恐怖融资活动而制定的政策、程序和控制措施，指导金融机构：

- 识别高风险业务（产品、服务、销售渠道、客户及地理位置）；定期更新机构的风险状况信息；制定完全符合风险管理需求的反洗钱 / 反恐融资合规制度。
- 及时向董事会（或其下设委员会）及高级管理层汇报合规计划、已知合规制度缺陷、已提交的可疑交易报告以及已采取的纠正措施等情况。
- 制定和维护指标报告系统，以便及时提供有关反洗钱 / 反恐融资制度状况的准确信息，包括制度关键要素数据，例如受监控交易、产生的警报、创建的调查、报送的可疑交易报告 (STR) 的数量。
- 明确反洗钱 / 反恐融资制度责任人的责任。
- 确保管理层或员工人事变动时的制度连续性。
- 遵循所有反洗钱 / 反恐融资合规监管要求与建议。
- 定期审查并根据法律法规的变化及时更新（至少每年一次）。
- 实施以风险为本的客户尽职调查政策、程序和流程。
- 双重管控、职责分离。
- 遵守所有的记录保存要求，包括记录的留存和检索要求。

- 上线完善的控制和监控系统，以便及时监测、报告潜在可疑活动和大额交易。此外，还应制定程序，记录根据调查结果决定不报告某项活动的理由。
- 制定明确的问责制和职责，确保对参与反洗钱 / 反恐融资风险较大活动的员工实行适当而有效的监督。
- 制定培训要求和标准，确保员工了解并有效认识应遵守的程序，以及这些程序与缓释其所在部门或职责领域的反洗钱 / 反恐融资风险存在的关系。
- 清晰解释报告可疑活动的重要性，包括阐述应如何以及对何人进行关注，合规官的职责，以及“保密”限制在实践中的意义。
- 在所有职位描述和工作审查流程中增加始终遵守反洗钱政策和程序规定的要求。对于未遵守这些要求的员工，机构应根据现有纪律予以处理。
- 制定并实施人才筛选制度，确保在员工招聘中采用高标准。对始终未能按照反洗钱 / 反恐融资框架履行职责的员工进行适当的处罚。
- 制定并实施质量保证测试方案，以评估反洗钱 / 反恐融资制度的实施和执行效果。这一功能有别于独立审计要求，但目的相似，即评估制度的持续有效性。

金融机构的政策、程序和控制措施的完善程度与其规模、结构、风险和产品复杂程度等因素直接相关。机构如果未能建立、落实、遵守或保持充分的政策、程序或控制措施，可能会引起针对该机构或特定参与人的严厉执法行动。

案例分析

2014 年 1 月，标准银行公司（简称标准银行）因在其反洗钱 / 反恐融资政策、程序和控制措施方面存在诸多问题，被英国金融市场行为监管局 (FCA) 处以 764 万英镑罚金。具体而言，标准银行未能妥当管控与政治公众人物 (PEP) 相关的客户带来的风险。英国金融市场行为监管局表示，“涉案期间，标准银行共与 5,339 个企业客户保持业务关系，其中有 282 家企业与一名或多名政治公众人物存在联系。”标准银行此前曾意识到自身在持续监控这些账户方面的能力不足，但却未采取充分措施，解决这一问题。最终，英国金融市场行为监管局 (FCA) 认定标准银行，未能 (1) 在为与政治公众人物有关的机构开立新账户时实施妥当的增强尽职调查措施，也 (2) 未能对现有账户进行充分的持续监控。

反洗钱 / 反恐融资政策、程序和控制措施的要点和差异	
政策	• 在全机构内发布的统一、清晰、简洁的高级别声明（确定自上而下的基调）。 • 经高级管理层或董事会批准。 • 反映整个机构利益相关者的高级别职责。
程序	• 将反洗钱 / 反恐融资政策转化为可为大家所接受且切实可行的做法，为利益相关者分配职责。 • 可在金融机构的业务（非执行）层级建立。指导机构如何达成目标。 • 比反洗钱政策更为详尽。 • 定期审查和更新。
控制措施	• 金融机构为确保反洗钱 / 反恐融资制度按预期在预设参数范围内运作而采取的内部技术或工具。 • 提示可能需要审查的潜在异常情况或偏离正常政策的情况。 • 包括管理层报告、自动审查系统或动用多个审查方。

合规职能部门

合规职能部门通常被称为第二道防线。负责监控业务，也就是第一道防线的控制措施。该职能部门很明显不能按照“一刀切”的想法设计，详见下文。然而，无论第二道防线采用何种结构，必须确保该防线能够有效发挥作用。

合规职能部门的完善程度必须以机构的性质、规模、复杂程度、监管环境以及与产品、服务及客户有关的具体风险为依据。任何两个机构的合规结构都不可能完全一致，因为各个机构的风险评估显示其面临的风险不尽相同。

合规官的任命和职责

多数情况下，董事会负责任命具有资质的人员担任本机构的反洗钱 / 反恐融资合规官。合规官负责管理反洗钱 / 反恐融资合规制度的方方面面，包括但不限于设计并实施合规制度、对制度进行必要的修改和更新、向核心员工传达制度实施的成功经验与失败教训、为员工培训方案设计反洗钱 / 反恐融资相关内容、保持机构遵守适用的反洗钱 / 反恐融资法律法规（包括随时关注和跟踪该领域法律法规的最新动态）。

沟通

合规官以书面和口头方式进行有效沟通的能力是机构反洗钱 / 反恐融资制度成功实施的关键。合规官必须掌握与机构所有层级员工沟通的方法，下至一线员工，上至首席执行官和董事会。

对合规官而言，至关重要的一点是能够清楚地向高级和执行管理层汇报重要事务，尤其是可能给机构带来风险的重要变化，例如可疑交易报告 (STRs) 或现金交易报告 (CTRs) 的数量突然或大量增加。其他需要上报管理层的事务包括可能需要立即采取行动的法律法规变动。合规官必须具备必要的技能，能够分析、解释不断发生的变化，确定它们对机构的影响，适时提出行动计划建议。

许多国家的反洗钱 / 反恐融资官还必须直接向董事会或同等地位的组织汇报工作。直通董事的汇报通道使其能够有效发挥监督作用。其他一些国家可能存在不同的汇报机制。

委派反洗钱职责

各个机构反洗钱 / 反恐融资部门的任务和职责分配有所不同。该部门可能分成不同的小组，例如安排一人负责制度的战略事务，另一人负责操作事务，包括监控可疑洗钱活动，报告可疑行为。

反洗钱 / 反恐融资部门下设小组示例：

- **制度管理**
  - 管理和协调监管检查。
  - 对制度进行定期审查和更新。
  - 与业务条线支持小组共同开展活动以确保业务程序已根据制度变动进行更新。
  - 监控监管环境以便对制度进行相应调整。
  - 可能参与编制培训材料，就业务条线支持小组无法解决的复杂反洗钱 / 反恐融资问题提供指导和建议。
- **了解您的客户**
  - 根据客户尽职调查风险评估得分为所有客户分配风险代码。
  - 对客户尽职调查流程中所确定的中等或高风险客户或要求金融机构提供特定产品或服务的客户进行额外尽职调查。
  - 第一时间提供业务联系人员对反洗钱 / 反恐融资事务相关业务问题进行解答。

- **制裁筛查**
  - — 管理制裁筛查软件应用或流程。
  - — 监控和协调各资料来源系统收到的数据。
  - — 根据机构的风险情况变化微调筛查阈值。
  - — 审查名单报警信息，向有关监管部门报告确认命中的情况。
- **交易监控**
  - — 管理交易监控软件应用。
  - — 监控和协调各资料来源系统收到的数据。
  - — 根据机构的风险情况变化微调监控阈值。
  - — 参与设计交易监控类型和保存必要的多种文件。
- **金融调查**
  - — 监控客户交易产生的预警，如来自系统的预警以及业务员工的汇报。
  - — 调查此类预警和汇报，按要求向有关金融情报机构 (FIU) 提交可疑交易报告。

除上述小组外，其他反洗钱/反恐融资工作任务通常贯穿在所有涉及客户联络的业务条线上。例如，客户尽职调查表格通常由前台主管和其他人员在新账户开立时填写，分支机构的工作人员则参与对高风险客户的定期审查并根据要求提供额外的信息或解释来支持潜在可疑活动的调查。有时，可疑活动可能需要先上报至安全小组，该小组认定此项交易可能引发反洗钱 / 反恐融资风险后，才会将其转送金融调查小组。

合规部门还可根据监管机构的指示或其他调查结果，指导与反洗钱 / 反恐融资相关的合规工作。业务和合规职能部门可能建立风险为本的质量保证审查，开展监控和监测活动，确保恰当履行职责。为此，可能需要审查已采集的客户尽职调查以确保完整性，监控客户尽职调查完整性或缺陷以确保系统按照预期运作，开展检测工作以评估监控和业务履职是否足以衡量和确保合规情况。

合规官问责制

无论机构如何分派反洗钱 / 反恐融资任务，机构指定的合规官应对机构的整体反洗钱合规性负责。各监管部门开展的执法活动越来越密集，不仅针对违反反洗钱 / 反恐融资规定的机构、执行管理层和董事会，还针对合规官。

案例分析

2016 年 3 月，Thriftway 食品超市（货币服务企业）及其企业主和合规官因故意多次违反《银行保密法》，金融犯罪执法网络 (FinCEN) 对其进行了民事罚款。这项罚款源于 2009 年开展的调查，结果显示该食品超市违反有关反洗钱、记录保存和报告的规定。合规官承认操作不当，接受 1 万美元的罚款。

案例分析

2014 年 12 月，MoneyGram 前首席合规官因未能确保公司遵守反洗钱法律和《银行保密法》，被金融犯罪执法网络 (FinCEN) 处以 100 万美元的民事罚款。这名首席合规官曾拒不接受罚款，希望撤销其对违规事件负有责任的指控，但 2016 年 1 月，美国地区法院拒绝了他的诉求。

反洗钱 / 反恐融资培训

有效的培训项目组成部分

大多数反洗钱 / 反恐融资法律法规要求金融机构为“专门”或“相关”员工提供培训项目，作为其正式反洗钱 / 反恐融资合规制度的一部分。培训是强调反洗钱 / 反恐融资工作重要性的重要方法，也是培训员工正确应对潜在洗钱风险的有效途径。培训也是缓释金融机构可能面临的洗钱风险的一大重要控制措施。

有效的培训项目不仅应解释相关的反洗钱 / 反恐融资法律法规，还应覆盖机构为缓释洗钱风险而采取的政策和程序。本节中，“培训”一词既包括正式的培训课程，也包括持续开展的沟通工作，以便让员工了解并始终注意反洗钱 / 反恐融资要求，沟通手段包括电子邮件、新闻资讯、定期团队会议、内联网网站及其他信息共享途径。下文将简要介绍反洗钱 / 反恐融资培训的对象、构成培训项目基础的话题、以及开展培训的方式、时间和地点。

培训对象

明确培训对象是设计有效反洗钱 / 反恐融资培训项目的第一步。金融机构的大多数部门都应接受反洗钱 / 反恐融资培训。在某些国家，不仅全职或兼职员工须接受培训，承包商、顾问、学生或学徒以及来自分支机构或子公司的借调员工均需接受培训。各个部门都应就反洗钱 / 反恐融资话题和与其活动相关的问题接受培训。

比如：培训范围

- **面向客户的员工：**这些员工是金融机构的第一道防线——他们需要对反洗钱 / 反恐融资工作的重要性以及如何对洗钱活动保持警惕有着最为深刻的实际认知。虽然一般课程通常能够说明反洗钱的重要性并提供一些基本知识，但还应就与业务部门提供的产品和服务有关的特定程序进行额外的培训。例如，贷款和信贷操作员工还需要就洗钱犯罪分子如何滥用信贷产品、员工如何识别潜在的洗钱活动以及在面对洗钱活动时应采取的措施等内容接受培训。由于现金引发的风险日益增加，很多司法管辖区均就此提出了更高的要求，因此现金处理人员通常需要专门的培训。这些员工需要了解如何正确处理现金交易，尤其是符合报告要求的现金交易，包括如果客户试图拆分交易以规避报告要求，应在何时报告。为新客户建立贷款和账户的员工应了解适用的监管要求，以及机构为客户接纳阶段的识别和尽职调查工作制定的政策和程序。

- **业务操作人员：**机构的业务部门内不面向客户的员工也属于第一道防线，机构在开展专门的培训活动时不应忽视这一群体。例如，负责金库、电汇、贸易金融、贷款审批、贷款收回、资金管理等业务的员工常常需要识别非法、欺诈或异常账户活动。因此，机构应考虑为这些员工提供专门培训，指导他们识别反洗钱 / 反恐融资危险信号，将异常活动报告给合规人员。

- **反洗钱 / 反恐融资合规人员：**这一职能部门由指定合规官领导，负责协调和监督机构反洗钱 / 反恐融资合规制度的日常情况。这是机构的第二道防线。鉴于该部门负责确保机构遵守反洗钱 / 反恐融资监管要求，机构应为该部门的员工提供更先进的持续培训，让他们了解监管要求和最新趋势，这一点非常重要。通常，这要求员工参加行业会议或反洗钱 / 反恐融资主题展示等更专业的交流活动。

- **独立测试员工：**独立测试员工是机构的第三道防线。由于该部门负责独立评估机构的反洗钱 / 反恐融资合规制度是否充分，这些员工应接受定期培训，学习监管要求、法规、洗钱手段和执法行动的变化及其对机构的影响。

- **高级管理层和董事会：**董事会和高级管理层无需接受与第一、二、三道防线的员工同等程度的培训。专门针对机构领导层的培训应介绍反洗钱 / 反恐融资监管要求的重要性、违规的惩罚措施、个人责任和机构的独有风险。如果高级管理层和董事会不了解上述信息，就无法充分监督反洗钱 / 反恐融资工作，审批反洗钱 / 反恐融资政策，或提供充足的资源保障。

培训内容

确定培训主题是设计有效反洗钱 / 反恐融资培训项目的下一个要素。这会随着机构及其提供的具体产品与服务的不同而有所变化。

反洗钱 / 反恐融资培训应该考虑以下几个基本事项：

- 有关反洗钱控制措施的大致背景和历史，包括洗钱和恐怖融资活动的定义、犯罪分子从事该活动的动机以及阻止这些活动的重要性。
- 介绍适用于机构及其员工的反洗钱 / 反恐融资法律框架。
- 违反反洗钱 / 反恐融资法律法规的处罚，包括刑事和民事处罚、罚金、监禁和内部处罚（如包括直至解聘在内的纪律处分）。
- 内部政策，如客户身份识别及验证程序和政策，包括客户尽职调查 (CDD)、增强尽职调查 (EDD) 和持续尽职调查。
- 对内部反洗钱 / 反恐融资及制裁风险评估的审核。
- 法定记录保留要求。
- 可疑交易监控和报告要求。
- 现金交易报告要求。
- 如何应对可疑客户或交易。
- 如何应对希望规避报告要求的客户。
- 员工的职责和问责。
- 反洗钱相关事务保密工作。
- 反洗钱趋势及与犯罪活动、恐怖融资和监管要求有关的新问题。

- 现实生活中的洗钱手法（最好选取那些发生在本机构或类似机构的案例），包括最初被发现时的行为模式，其对机构的影响以及最终如何解决等。

负责设计培训方案的人员必须确定上述哪些主题与培训对象相关。

2015 年 4 月，英国金融市场行为监管局 (FCA) 针对持续存在重大反洗钱缺陷的小型银行发布了一份改进指南。这份指南的编制基础是英国金融市场行为监管局及其前身在两项主题审查中发现的优秀实践案例。在发现问题中，英国金融市场行为监管局指出了培训项目的有效性问题，认为培训项目对其独有风险的针对性往往不强。指南公布的培训最佳实践包括：

- 根据培训对象的具体岗位确定适当的培训。如下领域的人员缺乏具体培训：离岸中心、抵押借贷、服务政治公众人物及其他高风险客户的领域、投资银行和贸易金融等。对具体业务部门或部门内具体岗位的培训，专门培训配合实践应用的培训方式较受欢迎。
- 为现有员工提供定期复训（通常为一年一次）。
- 银行应评估是否需要让第三方或外包部门的员工参与专门的反洗钱培训。

  案例分析

  2016 年 2 月 25 日，金融犯罪执法网络 (FinCEN) 和美国货币监理署 (OCC) 联合开展执法行动，以故意反洗钱违规的名义对美国佛罗里达州科勒尔盖布尔斯的 Gibraltar 私人银行和信托公司进行了处理。该银行严重违反反洗钱制度，包括未能妥当培训合规人员，因此分别被美国货币监理署和金融犯罪执法网络处以 250 万美元和 400 万美元的罚款。从 2009 年至 2014 年，该银行的反洗钱培训工作不充分，未按照特定岗位、部门、董事及其他员工的需求制定具体的培训项目。例如，2009 年，高级银行官员接受的基本反洗钱课程是专为柜员设计的，与他们的职责不匹配。2013 年 5 月，管理层开展的培训评估结果显示，银行需要开展重大培训项目，以便充分落实反洗钱制度。一年后（2014 年），监管部门发现该银行仍不满足 2013 年评估中提出的培训需求。

培训方式

培训师可以采取下列步骤制定有效的反洗钱 / 反恐融资培训项目：

- 明确必须进行沟通的议题，并确定最佳的沟通方式。有时，无需正式的现场培训，通过备忘录或者电子邮件即可完成培训。有时，利用网络教学可以有效地完成培训。有时，课堂培训才是最好的选择。

- 根据职能领域和员工或管理者的等级来确定培训对象。这应该与“他们为什么参加培训？”的快速评估同步进行。新员工还应该接受与老员工不同的培训。
- 确定培训需求。可能是审计或监管检查发现的问题，或者系统、产品或规章的变化产生的问题。
- 确定制定并实施培训项目的最佳人选。
- 确定采用分散式培训（例如通过较大的分支网络）的“培训师培训”课程是否必要。
- 制定课程摘要或课程大纲，其中应包括课程目标、目的和预期结果。务必明确培训对象以及相关资料的讲解方式。
- 在可能的情况下，制定培训日程表，明确培训主题和每门课程的培训频次。
- 考虑是否提供讲义。大多数培训讲义的目的或是强化培训要点，以及作为课后参考资料。
- 测试应作为评估培训效果的手段，测试应设定及格线，并保存测试分数。同样，如果用案例研究来阐释某一个知识点，则应提供关于“较为可取的行动方案”的详细讨论。
- 注意力持续时间也是需要考虑的因素。重点关注易于领会且便于分类的小问题。
- 做好出勤记录。要求参加培训者签到，如果需要补课，则发出提醒通知。可对无故缺席者予以纪律处分并记录在员工档案中。

培训时间

机构的培训应具有常规性和持续性。现有员工至少应参加年度培训课程。新员工应在入职或转入新岗位后的合理期限内，接受与其职务相关的培训。但也可能出现需要立即展开培训的紧急情况。例如，在检查或审计中发现洗钱控制措施存在严重缺陷之后，机构可能就有必要进行紧急培训。如果新闻提到本机构的名称或近期的监管活动，例如处罚决定，机构也应进行快速响应培训。软件、系统、程序或规章的变化也是促成临时培训的因素。

培训地点

有些机构设有培训中心，培训学员可以避免日常工作的干扰。有些培训（如洗钱案例评析）更适合以小组的形式进行。角色扮演练习是有课堂讲解或小组讨论的有益补充，同样采用小组的形式效果更佳。规模较大的机构可开展网络培训课程，设计自动记录出勤和测试等功能（设定及格线，确保学员对材料的最低掌握度）。

独立的审计

评估反洗钱 / 反恐融资制度

仅仅实施反洗钱 / 反恐融资合规制度是不够的，还必须对制度进行监控和评估。机构应该定期评估反洗钱 / 反恐融资合规制度，以确保其有效性并及时发现新的风险因素。

审计必须独立进行（即审计人员不应由机构内部的反洗钱 / 反恐融资合规部门员工担任），且审计人员应直接向董事会报告，或者直接向指定的董事委员会（主要或全部由外部董事组成）报告。进行审计的人员必须具有充分的资质，以确保审计发现和结论的可靠性。各个司法管辖区可能会以独立测试或独立审查的形式开展独立审计。

独立审计应:

- 评估反洗钱 / 反恐融资合规制度的整体完整性和有效性，包括政策、程序和流程。
- 评估反洗钱 / 反恐融资风险评估的充分性。
- 评估客户尽职调查政策、程序和流程的充分性和与监管要求的符合程度。
- 确定工作人员是否遵循机构的反洗钱 / 反恐融资政策、程序和流程。
- 进行适当的交易测试，重点关注高风险业务（产品、服务、客户和地理位置）。
- 评估培训的充分性，包括其全面性、材料的准确性、培训日程、出勤记录和出勤率低的上报流程。
- 评估制度是否符合机构业务所在司法管辖区的适用法律法规。
- 审查反洗钱 / 反恐融资合规制度中所用管理信息系统的完整性和准确性。如果适用，审查应包括相关第三方独立系统的充分性验证和涉及人员的资质。
- 审查每个外包给第三方的反洗钱 / 反恐融资合规职能部门的方方面面，包括人员资质、合同、表现以及公司声誉。
- 通过以下措施，评估用于识别异常活动的交易监控软件应用的能力:
  - 审查与可疑活动监控相关的政策、程序和流程。
  - 审查用于确保源交易处理系统提供的数据是否完整、准确、及时的流程。
  - 评估用于建立和分析预期行为或筛选标准的方法。

  — 评估监控报告是否恰当。

  — 对比交易监控类型与反洗钱 / 反恐融资风险评估，以确保合理性。

- 审查案件管理和可疑交易报告系统，包括评估对异常交易的调查和移交，审核将异常或可疑活动从业务部门移交给负责调查异常活动人员的政策、程序和流程。
- 评估机构对生成多次可疑交易报告的账户进行审查的政策的有效性，包括账户关闭流程。
- 评估记录保管和记录留存流程是否充分。
- 跟踪之前已经发现的缺陷，确保管理层已及时进行纠正。
- 确定审计的总体覆盖面和频率是否与机构的风险状况相匹配。
- 在董事会或指定董事委员会的协调下，确保总体的审计范围和频率与机构的风险状况相匹配。
- 考虑董事会是否对之前的审计发现作出反应。
- 确定以下培训项目和培训材料相关事项的充分性：

  — 董事会和高级管理层对持续教育、培训与合规的重视程度。

  — 有确保反洗钱 / 反恐融资合规制度得以实施的员工问责机制，包括员工业绩管理流程。

  — 针对每一业务条线的风险评估进行全面的培训。

  — 对来自机构所有适用领域的人员进行的培训。

  — 培训频率，包括向新员工和调任员工提供培训的及时性

  — 内部政策、程序、流程以及新的规章条例的覆盖程度。

  — 对不同形式涉及洗钱和恐怖融资活动的可疑活动识别的覆盖范围。

  — 对违反内部政策和监管要求行为的纪律处分。

一个有效的内部审计部门会建立并维护审计风险评估，以便确定审计优先事项。它同时还会针对每个领域建立并维护详细的审计测试制度。

所有对照审计和监管意见的改进措施必须得到跟踪，并明确完成时间和负责人。应定期向高级管理层和董事会提供状况报告。监管部门可能要求查看这些文件。审计问题处理不妥经常招致问责及监管部门对机构的罚金。

案例分析

2015 年 6 月 15 日，金融犯罪执法网络宣布美国西弗尼吉亚州威廉姆森的 Mingo 银行故意违反《银行保密法》，并对其处以 450 万美元的民事罚款。该银行与美国西弗吉尼亚州南区检察长办公室达成 220 万美元的暂缓起诉协议和没收诉讼，美国联邦存款保险公司责令其缴纳 350 万美元的民事罚款。据指，该银行的反洗钱 / 反恐融资制度在多个方面存在重大系统性缺陷，包括独立测试不充分等。该银行的独立测试未能确定银行是否为识别、监控、报告可疑活动和大额现金交易而采取适当的控制措施。银行最近一次于 2011 年 12 月实施的独立合规性测试没有涉及某些高风险活动，因此导致在 2008 年至 2012 年间超过 920 万美元的拆分交易和其他可疑现金交易未被报告。

建立合规文化

在金融机构的整体结构中建立合规文化是制定并持续管理有效的反洗钱 / 反恐融资制度的关键。通常，反洗钱 / 反恐融资合规制度的最终责任在于金融机构的董事会。董事会和高级管理层必须公开表达他们对实施反洗钱 / 反恐融资制度的承诺，从而确定自上而下的基调，确保其承诺贯穿于所有服务领域和业务条线，并且敦促责任方对合规制度负责。

尽管建立合规文化可能无法解决现在或将来的所有问题，但注重识别和控制风险的有效反洗钱 / 反恐融资合规制度是机构取得全面成功的关键。所有业务部门的关系方必须明确其按规办事的职责。采用合规文化是预防可识别的简单问题发展成系统性问题的最有效方式。

一套完善的反洗钱 / 反恐融资制度需要资金支持，而管理层可能不愿支出这笔费用。合规专员面临的挑战在于说服管理层：实施反洗钱 / 反恐融资制度的支出是为了保护机构并使机构规避法律问题和声誉受损，因而这笔开支必不可少。

金融犯罪执法网络根据其调查发现了多家金融机构存在反洗钱 / 反恐融资合规缺陷，其中包括董事会和高级管理层的未勤勉尽责，这一调查结果发表在 2014 年 8 月的一份咨询文件中。金融犯罪执法网络提出了六条加强金融机构反洗钱 / 反恐融资合规文化的建议，包括：

1. 领导层必须积极支持和了解合规工作。

   董事会在反洗钱 / 反恐融资合规中的作用包括审查和批准整个反洗钱 / 反恐融资制度以及确保制度得到持续的监管。董事自身不必成为反洗钱 / 反恐融资专家，也无须负责日常的制度管理。当然，他们应该足够了解并正式批准机构的反洗钱 / 反恐融资合规制度，确保制度得到员工的充分落实和维护。

董事会的监督作用还延伸到监管部门的检查过程中。检查人员在现场检查前和检查过程中与董事会和管理层进行例行沟通，以便评估董事会对合规制度的承诺、对法律的理解和对机构运作的了解。在监管部门或审计师完成检查后，董事会也有责任确保采取必要的整改措施。具体职责可以授权他人行使，但如果检查人员或审计师指出的问题没有得到整改，董事会将对此负责。

2. 机构不得为了营收利益而放松对反洗钱 / 反恐融资缺陷和风险的管控和缓释。

   合规人员应掌握适当权力以便落实机构的反洗钱 / 反恐融资政策。不应无视合规工作，背离机构风险偏好，而一味追求收益。最重要的是，合规工作不得位居盈利目标之后。

3. 机构各部门的相关信息必须与合规人员共享，以便进一步推进反洗钱 / 反恐融资工作。

   业务部门不应局限于自身孤岛之内。机构内不应存在沟通界限或障碍。相关信息应与反洗钱 / 反恐融资合规人员共享。

4. 机构必须向合规职能部门投入足够的资源。

   领导层除了必须指定人员负责依照法规协调和监控日常的反洗钱 / 反恐融资合规事务，还要根据机构的风险情况，提供科技资源和合适的人员支持。

5. 合规制度必须行之有效。确保制度有效的方法之一是有独立、合格的制度测试方。

   有效的反洗钱 / 反恐融资制度必须包含持续的风险评估记录、风险为本的客户尽职调查，并由独立、公正、合格的测试方对其进行测试。

6. 领导层和员工必须清楚反洗钱 / 反恐融资的目的及可疑交易报告的用途。

   领导层和反洗钱 / 反恐融资岗位员工应了解上报监管报告的重要性。对于金融犯罪执法网络而言，正确上报的报告会用于“应对严重的威胁，包括恐怖主义组织的威胁、激进国家的威胁、大规模杀伤性武器 (WMD) 的扩散威胁、境外贪污，以及日益频发的网络威胁”。

2016 年 6 月 30 日，美国纽约州金融服务局 (DFS) 发布《最终规定第 504 部分》，进一步强调了合规文化的必要性。这份《规定》要求受监管的机构持续实行设计合理的“交易监控和过滤制度”(TMPs)，以便：

- 在交易完成后监控交易是否遵守《银行保密法》和反洗钱法律法规，包括有关可疑活动报告的要求。
- 防范流向美国财政部海外资产控制办公室 (OFAC) 经济制裁对象的非法交易。

2017 年 1 月 1 日生效的最终规定还要求受监管机构的董事会或高管（们）每年向纽约州金融服务局提交证明，证明机构已采取所有必要的措施以满足“交易监控过滤制度”的要求。

尽管该法案表面上仅适用于纽约州，但许多外国银行因为在纽约州运营也适用该法案。具体而言，本法律适用于银行、信托公司、私人银行家、储蓄银行、根据《纽约银行法》设立的储蓄和信贷协会，以及依照《纽约银行法》在纽约提供银行业务的外国银行业公司分支机构。此外，本法律还适用于持有《纽约银行法》许可证的非银行金融机构 (NBFIs)，包括支票兑现公司和货币转移服务商。不合规行为将受到《纽约银行法》下相关条例的处罚。

重要的是，本法律除了明确金融机构必须遵照制定和维护的制度的核心要素外，还制定了交易监控和过滤的八项基本要求，包括：

1. 识别所有数据来源。
2. 核验数据的完整性、准确性和质量。
3. 数据提取和加载流程应确保完整、精确地传递数据。
4. 治理和管理监督。
5. 如有第三方供应商，需要供应商筛选流程。
6. 为设计、实施和维护制度提供资金。
7. 合格人员或外部顾问。
8. 定期培训。

使反洗钱 / 反恐融资部门作用最大化的关键方法在于，除执法机构、监管机构和高级管理层外，反洗钱部门还可以与机构其他领域的部门共享有价值的数据。由于反洗钱 / 反恐融资部门会建立客户尽职调查文件，其他部门能利用他们确认的信息，去销售产品和扩大利润。例如，如果营销部门能够更好地了解某些零售或企业客户的活动，就可以更有效地发现营销其他产品、深化总体客户关系的机会。

在发布客户信息之前，请务必查看适用的隐私权法律和公司的隐私权政策，以便了解相关的限制规定。同一法律实体的不同部门间共享客户信息通常不存在监管问题；但是，一个大型机构内不同附属公司间共享信息可能受到限制。有些机构限制在本机构之外共享客户信息，客户可能要求机构不得向第三方提供其信息。

合规人员应充分独立于其支持的业务线，以便最大程度避免潜在的利益冲突——机构不应向合规人员提供与业务部门盈利挂钩的激励措施。这并不意味着合规人员不应获得奖金；而是激励措施的设置不应引发利益冲突。

虽然合规人员可能在业务部门办公并向业务部门经理报告，但他们应具备向业务部门外的合规或风险管理职能部门报告问题的能力，无需畏惧受到反责。这并不意味着合规人员不能与业务部门保持密切关系；相反，这种密切工作关系是成功执行反洗钱 / 反恐融资制度的关键。最终，合规人员应被业务部门视为值得信赖的顾问，业务部门员工在遇到问题时会向合规人员请教并遵循其提供的建议。

案例分析

2016 年 5 月 24 日，新加坡金融管理局 (MAS) 宣布，由于瑞士瑞意银行严重违反反洗钱法规，管理层对银行业务监管不力，且某些员工恶劣的违规操作，责令该银行停止在新加坡的商业银行业务。新加坡金融监管局还通知瑞意银行，由于该银行违反预防洗钱和反恐融资规定，将对其处以 1,330 万新加坡元罚金。瑞意银行的违规行为包括未能对高风险账户实行增强客户尽职调查、未能持续开展可疑交易监控。

该银行的首席执行官、副首席执行官、理财主管等六名高管和员工因涉嫌刑事犯罪，被移送至公诉机关。

了解您的客户

客户尽职调查

健全的客户尽职调查 (CDD) 程序是防范洗钱及其他金融犯罪活动的最佳手段之一。认知是整个反洗钱 / 反恐融资合规制度的基础。机构对客户了解越深，成功防范洗钱活动的几率就越大。事实上，联邦金融机构检查委员会 (FFIEC) 在 2014 年 11 月发布的《银行保密法 / 反洗钱检查手册》修订版中指出，一个健全的反洗钱合规制度的基础是针对所有客户，尤其是洗钱和恐怖融资风险较高的客户，采纳和落实全面的客户尽职调查政策、程序和流程。大多数情况下，正常的基础性客户尽职调查已足够。在少数情况下，机构必须采取进一步尽职调查，调查范围可能更广泛。机构的客户尽职调查程序必须设置必要的流程，确保能够提供现实所需的不同程度尽职调查。

联邦金融机构检查委员会认为，客户尽职调查的目的是帮助银行（或任何金融机构）较为准确地预测客户可能参与的交易类型。这些流程帮助金融机构明确交易是否可疑。

金融行动特别工作组 (FATF) 于 2012 年 2 月发布的修订版建议第 10 条即为客户尽职调查。金融行动特别工作组建议，金融机构在下列情况中必须进行客户尽职调查：

- 建立业务关系。
- 在特定情况下开展一次性交易。
- 怀疑存在洗钱或恐怖融资活动。
- 金融机构对先前获得的客户身份识别信息的真实性或充分性存疑。

客户尽职调查程序的主要元素

金融行动特别工作组建议金融机构在其客户尽职调查程序中采用以下四项措施：

- 确定客户身份，并利用可靠、独立来源的原始文件、数据或信息核实该客户的身份。
- 查明受益所有人，并采取合理措施验证受益所有人的身份。
- 了解并在适当情形下获取关于业务关系目的和意图的信息。
- 对业务关系进行持续的尽职调查并仔细审查该关系进程中进行的交易，以确保交易与机构对客户、客户业务和风险状况（在必要时还包括资金来源）的认知相符。

健全的客户尽职调查程序应包含以下七大要素：

要素	说明
客户身份识别	适时充分了解客户和业务实体，包括资金和财富来源。机构应确保实行更新和保存现有客户信息的流程。
概况	创建每位客户的交易和活动概况。概况应包含充足的信息，以便审查预期与实际账户活动，或帮助机构通过对比客户信息与活动识别可疑活动。
客户接纳	根据客户使用的具体产品和服务来界定并确定是否接纳客户，标准针对不同客户和市场的标准可能各异。
风险评级	对客户账户关系呈现的风险进行评估和定级。确定风险时应考虑多种因素（例如：客户类型、产品与服务、交易活动以及地理位置）。确定风险时不应只考虑单一因素（除非该单一因素即构成非法活动，例如违反经济制裁或参与非法活动）。

监控	根据呈现的风险进行账户和交易监控。
调查	调查和检查异常客户或账户活动，此类活动不符合担任某种职务或开展某类业务的客户预期可能开展的活动。
归档	将调查发现归档以留作证据，或作为行动记录。俗话说得好，“没有记录的事情等于未发生过。”

增强尽职调查

金融行动特别工作组在第 10 项建议的解释性说明中指出，如果洗钱或恐怖融资风险较高，则应采取增强客户尽职调查措施。必须采取增强尽职调查的风险因素包括：

客户风险因素：

- 业务关系是在异常条件下开展的，例如金融机构和客户的地理位置相距甚远且无合理解释。
- 非本地居民客户。
- 作为个人资产持有工具的法人或法律安排。
- 设有无记名股东或发行不记名股票的公司。
- 现金密集型企业。
- 从公司业务性质来看，公司的所有权结构似乎不正常或过度复杂。

国家或地域风险因素：

- 根据可靠信息来源（例如金融行动特别工作组的互评结果或详细的评估报告）被确认为反洗钱 / 反恐融资体系不完善的国家。
- 受到联合国等实施的制裁、禁运或类似惩戒措施的国家。
- 根据可靠信息来源被确认为贩毒、腐败、金融犯罪或其他犯罪活动猖獗的国家。
- 根据可靠信息来源被确认为资助或支持恐怖活动的国家，或已表明有恐怖组织在其境内运作的国家或地区。
- 共享边境线、据知存在实际跨境交易活动的国家。
- 洗钱或金融犯罪活动风险较高的地区，例如美国的金融犯罪高发地区 (HIFCA) 和贩毒高发地区 (HIDTA)。

产品、服务、交易或交付渠道风险因素：

- 私人银行业务。
- 匿名交易（可能涉及现金）。
- 非面对面商业关系或交易。
- 从未知或无关联第三方收到的付款。

巴塞尔委员会在《对反洗钱和反恐融资风险的有效管理》中指出，对于计划在账户中持有大量余额或定期进行跨境电汇的个人，或政治公众人物，应该采取增强尽职调查。

对高风险客户进行增强尽职调查

洗钱或恐怖融资风险较高的客户会给金融机构带来更大风险。机构应在开立账户前更加密切地审核高风险客户，并在账户关系存续期间更频繁地审核其交易。

金融机构应考虑获取高风险客户的以下附加信息：

- 资金和财富来源。
- 控制账户的人员（如签署人或保证人）的身份信息。
- 职务或业务类型。
- 财务报表。
- 银行征信。
- 住所。
- 客户居住地、工作地点或营业地点与银行的距离。
- 对客户的首要贸易范围以及是否可能定期开展国际交易的描述。
- 对业务活动、预期的现金量和总交易量的描述，以及主要客户和供应商的名单。
- 对账户活动变动的解释。

针对高风险客户，金融行动特别工作组还建议在建立或继续开展业务时应获得高级管理层的批准，并建议要求客户在进行第一笔付款时使用以自己名义开立的账户与采用类似客户尽职调查标准的银行进行交易。

开户、客户身份识别与核实

健全的客户尽职调查程序应包含可靠的客户身份识别和开户流程，以便金融机构确定客户的真实身份。机构还应根据特定客户可能的风险来设定相应的身份识别标准。在某些国家或地区，有关当局发布了具体的法律法规来明确机构在客户身份识别方面应采取的措施。

巴塞尔委员会在其 2014 年 1 月发布的《对反洗钱和反恐融资风险的有效管理》中指出，银行应建立系统的客户身份识别与核实流程，包括客户代理人和受益人所有人的身份。尽管巴塞尔委员会着重关注银行，但其建议适用于任何开立账户的金融机构。

银行在建立银行业务关系或开展任何交易前必须按照金融行动特别工作组第 10 项建议充分确认并核实客户身份。机构必须利用可靠、独立来源的文件、数据或信息，核实客户、受益所有人或其代理人的身份。银行应该意识到某些身份文件更容易伪造。如果遇到易伪造文件或客户提交的文件信息存在不确定性，机构应提高核实要求并采取更多的问询或参考其他信息来源核实客户提供的信息。

2016 年 2 月，作为《对反洗钱和反恐融资风险的有效管理》的附件，巴塞尔委员会发布了《客户尽职调查》白皮书。其中附录四为《账户开立和客户身份识别通用指南》，内容如下：这份文件并未涵盖每种可能出现的情况；而是着重关注了一些机制，这些机制可供银行用来制定有效的客户身份识别与核实制度。

这份附录将客户分为两类，一类为欲开立账户的自然人，一类为法人和法律安排。附录还涵盖了针对两类客户分别应该收集和核实哪些类型的信息。

欲开设个人账户的自然人新客户应该提供以下信息：

- 法定姓名（姓和名）及其他曾用名（如女性结婚之前的姓名、曾用法定姓名或化名）。
- 完整的居住地址，视风险等级提供公司地址或邮编。
- 固定电话或移动电话和电子邮件地址。
- 出生日期和出生地和性别。
- 国籍和居民身份。
- 职业、职位和单位名称。
- 官方指定的个人身份证号或者其他的唯一身份识别号。
- 账户类型以及银行业务关系的性质。

- 签字。

机构应利用可靠、独立来源的文件、数据或信息核实该信息。

文件核实流程包括：

- 根据具有客户照片且在有效期内的官方文件确认客户身份。
- 根据官方文件确认客户的出生日期和出生地。
- 通过获得授权人士的认证确认官方文件的有效性。
- 确认居住地址。

非文件核实流程包括：

- 在账户开立后通过电话或信件联系客户，确认客户提供的信息。
- 调查其他金融机构的征信。
- 使用独立的信息核实流程，例如评估上市登记处、私人数据库或其他可靠的独立信息来源。

在有些司法管辖区，其他具有同等性质的文件也可作为证明客户身份的可信证据。

机构应特别关注高风险客户。额外的信息来源和增强核实流程可能包括：

- 根据官方文件、信用征信机构调查或通过家访，确认客户的居住地址。
- 获得此前的银行征信（包括银行业组织征信），联系此类银行来了解客户。
- 通过适当措施核实收入来源、资金和财富。
- 核实客户的雇用情况或公职。
- 从金融机构的现有客户获得个人征信。

如果国家法律允许非面对面账户开立，银行应考虑这种方法的特殊风险。客户身份识别与核实流程应与面对面采访类似和同样有效。作为更广泛的客户尽职调查手段之一，银行还应根据风险敏感度考虑证实财富和资金来源或资金去向信息。

对于非自然人或法律安排的法人，机构应获取以下信息：

- 该法人的名称、法律形式、状态及注册证明。
- 该法人主要活动场所的永久地址。

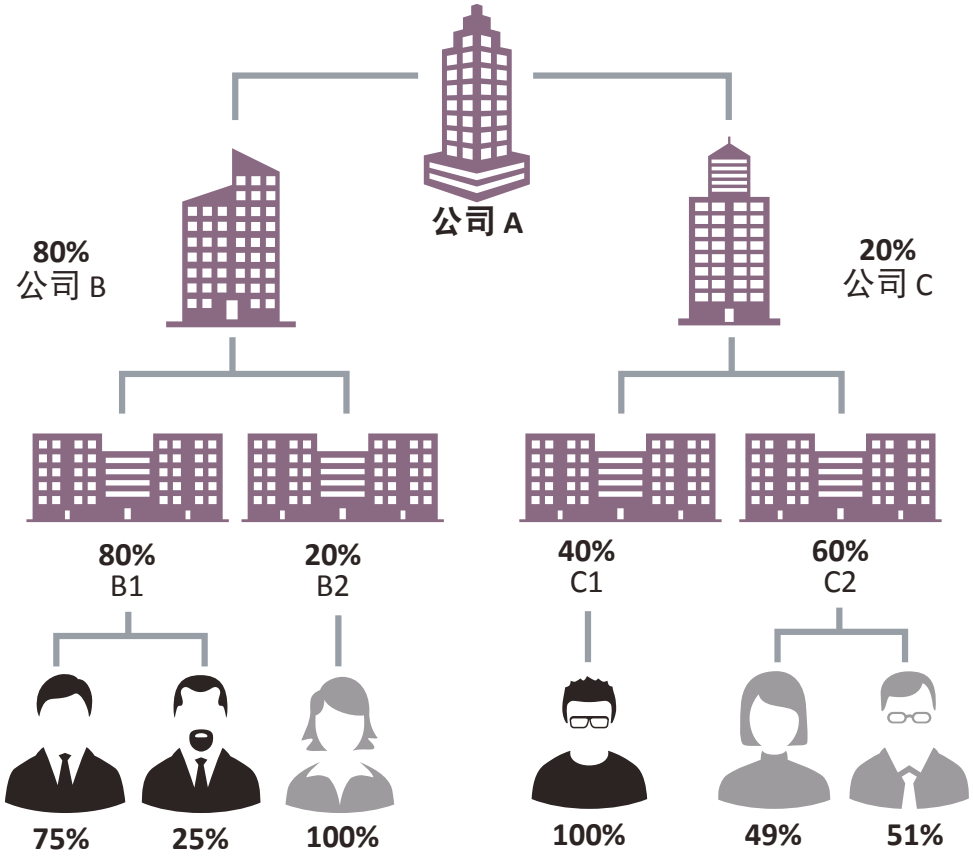
- 法人的邮寄和注册地址。
- 获得授权操作账户的自然人身份信息；如果没有获得授权的操作人，则应获取高级管理层人员的身份信息。
- 联系电话号码。
- 官方身份号码。
- 监管和约束法人的权力机关。
- 受益所有人的身份。
- 法律实体的活动的性质和目的及其合法性。
- 实体的财务状况。
- 从风险角度了解账户的预期用途，包括预期交易的金额、数量、类型、目的和频率；账户可能收到的资金来源；经由该账户的资金去向。

银行应利用可靠、独立来源的文件、数据或信息核实客户的身份。

- 文件核实流程包括：
  - 获取企业登记、备忘录、组织章程、合作协议或其他证明机构存在的文件的副本。
  - 对于已成立的公司，审核财务报表（优先查看已审计的报表）副本。
- 非文件核实流程包括：
  - 通过公司调查或其他商业查询确保该法人未解散或终止，也未进入解散或终止程序。
  - 使用独立的信息核实流程，例如评估上市公司登记处、私人数据库或其他可靠的独立信息来源（例如律师、会计）。
  - 利用公开服务核实法律实体身份识别号和相关数据。
  - 获得此前的银行征信。
  - 如果可行，实地拜访公司。
  - 通过电话、信件或电子邮件联系公司。

机构应核实代表法人进行操作的人员是否获得授权。如是，银行也应核实该名人员的身份。银行还应采取合理步骤，核实受益所有人的身份。然而，具体的开户程序和客户接纳政策取决于客户类型、风险以及当地法规。

受益所有人离析案例



案例分析

2011 年，美国金融犯罪执法网络对佛罗里达州最大的特许银行海洋银行处以 1,090 万美元民事罚款。金融犯罪执法网络判定海洋银行未能按照规定制定并实施有效的反洗钱制度。例如，海洋银行的客户中有 28% 居住在美国境外洗钱高风险地区，如委内瑞拉。该银行为政治公众人物、领事馆和发行不记名股票的公司开立美国账户。但海洋银行并未对这些高风险的账户执行相应的政策、流程和有效的内部控制措施以评估和缓释贩毒相关的洗钱风险，并确保及时发现并汇报可疑交易。

美国金融犯罪执法网络发现：

- 海洋银行没有对外籍客户的身份和账户开立文件进行验证，这些文件通过信件寄送至该银行。

- 未经面对面交流即为在委内瑞拉的客户开立账户。
- 识别客户身份的文件不符合质量控制要求，因此无从保证信息的准确性。
- 没有所需的完整文件，海洋银行也无法建立适当的客户档案。
- 海洋银行的政策、流程和控制手段不能保证其获取并审查外国和境内客户的必要信息，因而也不能充分评估洗钱风险和可能性。
- 在对国内外零售客户文件的抽查中发现了多处关于客户具体信息的错误和遗漏，包括客户所从事行业的性质、对所有者 / 运营者身份的验证以及账户的预期活动。

一体化客户尽职调查

如果金融机构执行的客户尽职调查制度过于分散，将导致其面临的洗钱和恐怖融资风险大幅上升。为确保执行有效的客户尽职调查制度，金融机构可以采取的措施为：在机构层面统一并简化账户开立程序并对交易流程进行持续监控。如果可行，该方法应在国内和国外同时应用。

政府间组织已经意识到实施一体化的客户尽职调查的重要性，也已为金融机构制定了专门的指导意见。根据巴塞尔委员会的要求，全球客户尽职调查风险管理制度应包括：在全球范围内对客户账户进行跨越业务领域和地理区位的持续识别和监控，同时在母公司层面进行监管，以便发现那些在其他情况下可能无法侦测的异常交易事例和模式。该委员会表示，对客户信息进行此等全面处理可以侦测潜在的有害活动并大大提高银行的整体声誉风险、集中风险、操作风险和法律风险管理水平。

金融机构应努力将一体化的客户接纳政策、客户身份识别程序、高风险账户监控流程和风险管理框架运用到其所有办事处、分支机构和附属机构。机构应通过持续的培训活动、定期交流明确传达这些政策和流程，以及监控和测试来确保符合政策和流程的要求。

机构的每个办事处、分支机构或附属机构都应遵守母公司实施的最低客户身份识别和接受标准。但是，为了符合当地监管要求或相关风险因素（如：某些地区的洗钱、恐怖融资和腐败风险较高），不同司法管辖区的信息收集和保存方式可存在差别。

如果母国和东道国在客户尽职调查的最低标准上存在差异，那么位于东道国司法管辖区的办事处应该采用两者之中较高的标准。如果上述要求不可能达到，则机构应与母国和律师协商以执行适当且有效的客户尽职调查标准。

经济制裁

经济制裁是从经济方面孤立制裁目标的一种方式。与军事打击相比，各国越来越倾向于使用经济制裁作为一种对外政策。一般，经济制裁可分为以下几类：

- **针对性制裁措施**——针对特定人员，如某国或某地区的重要领导人、特定恐怖分子、重大毒品走私犯罪分子和大规模杀伤性武器扩散分子。制裁措施包括冻结资产和实施旅行禁令。
- **行业制裁**——针对经济环节中某些重要产业，禁止进行某类金融交易以阻止这些产业进一步发展。
- **全面制裁**——禁止对大部分商品、技术和服务所有直接或间接的进出口交易、贸易代理、金融或其他促进手段。主要用于制裁有重大违反人权行为和核武器扩散行为的国家或地区。

多数司法管辖区根据联合国或欧盟（如果是成员国的情况下）的制裁要求实施相应的制裁法案。因为有着相似的目标，所以他们实施的制裁可能会有所重叠。

联合国

联合国的制裁由联合国安理会负责。安理会可根据《联合国宪章》第七章采取相应措施，维持或修复国际和平与安全状况。第 41 条详细列出了多种制裁执行措施，但不包括使用武力。制裁形式因目标不同而有所差异。手段包括全方位经济和贸易制裁以及更具针对性制裁措施，如武器禁运、旅行禁令、金融或商品限制。安理会实施制裁旨在鼓励和平转变、阻止非宪法性变革、遏制恐怖主义、保护人权以及防止核武器扩散。

欧盟

《欧盟运行条约》(TFEU) 第 215 条规定欧盟可以与第三方国家（如非欧盟国家）中断或减少部分或全部经济和金融关系，以实现《欧盟共同外交与安全政策》中制定的目标。概括地说，欧盟实施限制性措施以令目标国家或国家部分地区、政府、机构或个人对政策或活动做出改变。这些措施具有防范作用，而非惩罚工具，有助于欧盟迅速应对政治性改变和发展。这些措施有助于实现人权和民主目标，并在阻止伊朗和朝鲜的核武器扩散问题上对联合国制裁措施进行了补充。

美国

美国财政部海外资产控制办公室 (OFAC) 发布的制裁名单 (SDN) 是最为有名的名单之一。这份名单时常更新，名单中包含了 150 多个国家的数千名个人、企业以及飞机和船舶（“轮船”）。名单所列出的均为受美国外交政策及贸易制裁的恐怖分子、国际毒品走私犯或其他类型的受制裁对象。

海外资产控制办公室实施的制裁法案规定金融机构不得向制裁目标（即某一制裁项目中受制裁的主体等）提供财产或财产权益。各项目的制裁方式也有所不同，可能是封锁（或冻结）交易，也可能是拒绝（或驳回）交易。制裁法案由一系列的法律、法规组成，有可能会发生变化，因此，为遵守制裁法案，需要掌握专业技能并时刻关注其变化。

海外资产控制办公室并非监管机构，但与联邦及各州的监管机构均关系密切。监管机构在检查金融机构时会检查其对海外资产控制办公室合规方面的措施，包括政策和流程、培训及筛选系统的检测和调整，以判定该机构是否遵守了海外资产控制办公室 (OFAC) 的制裁法案，能有效监测制裁名单上列出的机构和其他被海外资产控制办公室制裁的机构，甚至包括一些不在特别指定名单上的机构。如果发现一金融机构对海外资产控制办公室 (OFAC) 规范的管控措施薄弱，或与制裁名单上的机构或海外资产控制办公室 (OFAC) 其他制裁下的机构有交易往来，联邦和各州的检察人员和海外资产控制办公室 (OFAC) 将采取行动，包括但不限于罚款、刑事处罚和监管行动（如书面协议和注意事项）。

制裁名单筛查

金融机构在与新客户进行交易或参与某些交易（如国际电汇支付）前，应参考该国的各项制裁制度规定和公布的已知或疑似恐怖分子、毒品走私贩等犯罪分子的名单进行比对。

要遵守制裁规定，机构应根据定期更新的名单审查客户和交易记录。名单中包括了政府机构禁止交易的指定或确定的人员和机构。制裁名单可以识别恐怖分子、恐怖主义组织、恐怖主义支持者，以及上文所列三种类型制裁所针对的制裁目标。

对于制裁名单上的人员或团体参与的交易，金融机构应加以警惕。要做到这一点有时并不容易，尤其是当所需审查的名单上的名字原本并非罗马字母时，难度则更大，如出现在制裁名单上的中东国家或亚洲国家恐怖分子嫌疑人。例如，海外资产控制办公室的制裁名单上列出的“指定恐怖分子”上的多数名字还附带了多个“别名”的信息。虽然有些名字可能是假名，但其他人困扰是因为不了解他们的起名习惯。了解阿拉伯的起名习惯和礼仪可以帮助我们更好地理解。下列是一些建议：

- 在从阿拉伯文字转写而来的名字中，短辅音省略常常可见。所以“Mohammed”这个名字在金融账户上可能被写成“Mohamed”或“Mohamad”。
- 阿拉伯人的姓名通常特别长。姓名中的第二个名字是其父亲的名字。如果名字前出现“bin”或“ibn”，则表示此人是“……的儿子”。如果名字最后有家族姓氏，则家族姓氏前有时会出现“al”。
- 有些名字被广泛使用，如“Mohamed”、“Ahmed”、“Ali”或带有前缀“Abd-”或者“Abdul”（意为“……的仆人”）的名字，后接真主的 99 个尊名之一。
- 许多阿拉伯名字以单词“Abu”开头。如果它位于名字的开头，那它可能不是这个人的本名，因为“Abu”意为“……的父亲”。“Abu”后接名词表示“自由”或“斗争”的意思，恐怖分子与合法的政治领袖均使用此类姓名。只有当“Abu”作为姓氏的前缀时，才应被看作是本名。

政治公众人物筛选

尽管金融机构千方百计制定强有力的措施和审查程序，以遵守制裁或其他客户审查规定，这些管控措施也不一定总能发现应该避免交易的可疑的高风险个人或企业。例如，政府间机构，如金融行动特别工作组 (FATF) 在其 40 项建议中明确地提到了政治公众人物 (PEP)。政府发布的规定，特别是欧盟第四号反洗钱指令也针对政治公众人物做出了明确且详细的规定。但如何确定政治公众人物及其相关人员仍是个难题。

问题在于全世界都缺少可用且有效的政治公众人物的身份信息。目前，有数十家政治公众人物数据库私人供应商。但这些数据库提供的政治公众人物信息能否与客户匹配仍是一大问题。此外，需接受额外检查的政治公众人物躲避检查的方式也是花样百出，如以公司（如空壳公司）名义在离岸司法管辖区开立账户，而非以自己或近亲的名义。另一方面，从地理问题、账户的规模和性质以及账户的目的就可以看出与政治公众人物相关的问题。

可以利用一些公共信息识别政治公众人物及其相关人。透明国际发布的“清廉指数”在关注高风险司法管辖区时非常有用，该机构是一个致力于打击腐败的非政府间国际组织。一些政府机构（如美国中央情报局）也发布了外国国家元首和内阁成员名单。但这些名单未能提供识别政治公众人物的全部信息。例如缺少出生日期或出生地等唯一识别信息。这就造成了严重的操作限制，在大型零售金融机构中尤为如此。

在美国，洗钱交易的来源之一是政治公众人物收受的贪污收益。在某些国家法律下，这可能违法其制裁条款。识别这些政治公众人物确有难度。因此，为了更有效地识别政治公众人物，应制定严格的客户尽职调查和监控措施。

同时应持续审查并更新客户筛选和制裁制度。这些措施包括更新流程、调整并检测筛选工具以及开展员工培训。

了解您的员工

金融机构和企业在付出了巨大的代价后才懂得，内部人员可以带来与客户相同的洗钱威胁。反洗钱 / 反恐融资领域逐渐形成了一个共识：制定类似的合规制度以了解您的客户和员工至关重要。

“了解您的员工”(KYE) 制度的建立意味着机构已制定适当的制度来了解员工的背景、利益冲突情况以及成为洗钱共犯的可能性。同时，政策、程序、内部控制措施、职位说明、行为和道德准则、权力级别、合乎人事法律法规的规定、问责制、监控、双重管控以及其他威慑措施都应坚决到位。

对潜在员工和现有员工进行背景调查（特别是犯罪记录的筛查），对于将不需要的员工拒之门外以及识别需要予以辞退的员工来说非常重要。美国联邦存款保险公司 (FDIC) 在于 2005 年 6 月发布的题为《聘用前背景调查：建立有效的聘用前背景调查流程指南》中规定了员工背景调查的指导性意见。

背景调查是一个有效的风险管理工具，它能协助管理层确定求职者提供的信息为真实信息且拟聘用员工没有犯罪记录。如果使用得当，聘用前的背景调查可通过核查拟聘用员工是否拥有某一职位所需要的必要技能、资格认证、执照或学位，来减少员工流动；遏制盗窃和贪污；防止因聘用操作引发诉讼。机构还应对承包商也进行类似的背景调查程序。

制定和执行有效的调查程序会产生成本。但是如果缺少这一流程，银行可能会在招聘、聘用、培训以及最终解聘不合格人员方面支出大笔费用。

有时，法规禁止被判欺诈或洗钱罪的人成为或继续作为机构的关联方；直接或间接拥有或控制一个机构；或者在没有事先获得监管机关书面同意的情况下，直接或间接地参与机构事务。参与金融机构事务的顾问也可能受这一要求限制。

因此，所有的金融机构都应该建立聘用前背景调查制度，以至少核查求职者的犯罪记录。有时，应提高背景调查的强度。根据 FDIC 的建议，某些职位的敏感性或个别员工的权限级别可能决定了需要进行额外的背景调查，其中应包括推荐信、工作经历、教育背景和职业资格等方面的核查。新加坡金融管理局员工聘用指南中还提到应对洗钱 / 恐怖融资信息进行筛选、开展破产调查和信用历史检查。

管理层还需像核查客户身份一样核查求职者的身份。一旦录用该员工，应该根据情况的变化，或者根据在一段时间内对部门全体员工进行全面审查的需求，考虑对具体职位人员实施持续的背景调查。管理层还应该制定相关政策来说明，在调查发现的信息与求职者或员工提供的信息不符时应采取的措施。

机构可以对身处敏感职位的员工定期进行指纹检查，当考虑将某位员工晋升至高级职位时，机构还可以聘请服务供应方对该员工进行详尽的背景调查。如果没有适当的调查程序，金融机构可能承担违规聘用法定失格人员的风险。员工调查的程度视具体情况而定，以合理为标准。

在英国，国家基础设施保护中心 (Centre of Protection of National Infrastructure) 在“了解您的员工”方面做了进一步规定，围绕内部威胁和风险管理制定了一些内容丰富的指导意见。该机构还提供了多个因内部威胁或数据泄漏对机构造成毁灭性影响的案例。对金融机构而言，风险可能包括滥用仅限内部人员所知的内幕信息。如今，许多银行对员工进行培训，使其在处理数据时做到透明、合法且以客户为中心。

对员工的定期反复培训，使其了解机构对员工的期望，应作为常规在岗培训的一部分。社交媒体已成为个人和机构日常交流沟通的重要形式。“了解您的员工”制度可能也需要机构监测员工或内部人员在社交媒体上提及的事项或者喜欢的内容。社交媒体账户涉及的信息及发帖的内容可能会提供给机构大量关于员工行为表现的信息。

案例分析

2015 年 10 月，在加州圣地亚哥的联邦法院里，一名银行职员承认犯下银行贪污重罪，导致花旗银行未能报告可疑交易，也未能执行有效的反洗钱 / 反恐融资合规制度。该职员承认，他在工作中利用其金融知识和职位之便，帮助客户规避花旗银行的反洗钱 / 反恐融资审查。为了获得金钱和实物报酬，他明知多位花旗银行客户曾屡次参与可疑高风险活动却并未就此进行汇报，导致银行违反法定义务，并将内部反洗钱 / 反恐融资指南提供给客户，透露银行在反洗钱 / 反恐融资方面的检查参数。此外，他还建议客户开立、持有无风险行业的空壳银行账户，以便进行高额现金交易，避免触发银行的反洗钱 / 反恐融资报告义务。本教材出版时，该案尚未判决。

可疑或异常交易监控与报告

适当的尽职调查可能要求合规专员在确定交易可疑并提交可疑交易报告前，进一步收集客户信息或交易信息。虽然没有关于可疑活动构成要件的硬性规定，但金融机构的员工应该关注与客户的收入来源或常规业务不相符的活动。

由于金融机构每天必须整理数以千计的交易，因此，机构的可疑活动监控和报告系统应基于风险进行设置，并由机构规模、业务性质、地理位置、交易频率和规模以及客户的类型和地理位置来决定。

金融机构的核心操作系统一般都需维护大量客户数据，可利用该系统制作内部报告，以检查是否存在可疑的洗钱和恐怖融资活动。这些报告包括以下内容：

- 超过该国报告限额的日常现金活动。
- 略低于该国报告限额的日常现金活动，以此识别可能的拆分交易行为。
- 一段时间内累计的现金活动（如超过一定数额的个人交易，或者以 30 天为周期，交易总额超过一定数额），以此识别可能的拆分交易行为。
- 用数额和地理因素进行筛选的电汇报告或记录。
- 金融票据的记录或报告。
- 有重大借记 / 贷记资金流动的空头支票或未收款的资金汇票。
- 重大变动报告。
- 新开账户活动报告。

虽然不同国家或地区的报告程序有所差异，但作为金融机构反洗钱 / 反恐融资制度的一部分，其内部常见的可疑或异常交易报告流程一般包括以下内容：

- 通过员工观察或识别、执法部门调查和交易监控系统警报等多种渠道，识别可疑或异常交易或活动的流程。
- 对异常交易或活动的每一个个案及其后续情形的正式评估。
- 可疑交易报告的决策记录（即，是否向有关当局提交了报告的记录）。
- 定期向高级管理层或董事会通报可疑交易报告情况的程序。
- 关于侦测可疑交易或活动的员工培训。

大多数要求提交可疑交易报告的国家或地区都禁止向报告所涉及的主体披露有关报告的事宜（即“泄漏信息”）。在美国，金融机构及其董事、管理人员、员工和经纪人均不得向报告交易涉及的任何个人泄露信息。大多数国家或地区的法律还规定了报告机构及其员工的民事责任豁免（安全港）。

美国甚至规定如泄露信息，令他人知道有此可疑活动报告的，也属于违法行为。这不仅包括禁止泄露可疑活动报告本身，还包括曾经提交或未提交报告这一事实。例如，如果一个金融机构被问及是否曾提交过可疑活动报告时，不作回答可能会间接意味着该机构曾提交过一份可疑活动报告。可疑活动报告的保密性是整个报告制度的一个关键方面，可以保护金融系统避免因提交报告而受到威胁。报告旨在为执法部门提供有效信息，犯罪分子的诉讼威胁不应成为金融机构履行报告职责的绊脚石。

严格的记录保存程序是防止报告带来的任何监管或者法律后果的关键。国家的法律或法规通常规定了金融机构和企业的记录保存期限、必须保存的记录类型以及应要求这些记录应该如何提供给监管或执法人员。

目前尚未建立用于保存可疑交易报告的国际清算所，但很多国家的金融情报机构 (FIU) 经常发布报告，公布每年提交的可疑交易报告数量、哪些领域提交的报告数量最多、可疑活动或种类的发展趋势以及案例分析。这些信息为各司法管辖区的金融机构履行反洗钱 / 反恐融资职责提供了额外的指导。

自动化反洗钱 / 反恐融资解决方案

落实反洗钱法规涉及大量人员、制度和数据，单纯依靠人工开展反洗钱 / 反恐融资工作变得异常艰难。大部分机构采用专门的信息系统实现合规活动的自动化，仍有一小部分机构采用人工操作。

切实有效的技术可以提高金融机构防范金融犯罪风险的能力，具体体现在：

- **自动化客户验证：**使用第三方数据库，将客户提供的信息与源数据进行比较。
- **监控名单过滤：**根据针对恐怖分子、罪犯和其他禁止往来人员的监控名单，对新开账户、现有客户、受益人和交易对手进行筛查。
- **交易监控：**扫描和分析交易数据以发现潜在的洗钱活动。
- **自动提交监管报告：**向政府当局提交可疑交易报告 (STR)、现金交易报告 (CTR) 及其他监管报告。

- **案例管理：**提供仪表板功能，用以查看客户信息（“了解您的客户”）、交易历史以及对客户展开的任何调查或针对其的监管报告。
- **审计线索：**记录旨在向审计师和监管机构证明合规成果而采取的措施。

自动化技术的广泛范围不仅仅提高了反洗钱工作效率和控制水平。它也反映出机构对达到或超过合规要求的承诺。这一承诺的又一益处是，监管机构可以得到即时、简洁且标准格式的信息。

很多软件公司提供用于打击洗钱活动的信息系统，但有些机构自己设计开发反洗钱信息系统。在设计反洗钱 / 反恐融资合规制度或购买新技术之前，金融机构应审查每个行动步骤的可行性、成本和收益。

有些金融机构选择外购反洗钱 / 反恐融资信息系统。许多机构采用招标书 (RPF) 的方式。金融机构将招标书发送给那些被认为有资格参与竞标的软件供应商。招标书中列出了项目需求以及应用流程。招标书的目的在于选择一个系统，可以帮助金融机构履行反洗钱法规中所规定的反洗钱义务。系统可以帮助机构识别潜在的高风险客户、账户以及交易，并协助执行、管理和记录后续调查，也可以对可疑交易报告甄别和提交流程进行优化完善。

大多数机构都希望其寻求的合作伙伴能够承诺其在快速变化的监管环境下始终处于领先地位，并阐明其软件在客户交易监控、客户调查方面所体现的适应性、灵活性和紧迫性。理想的信息系统应具备灵活、快速和高效等特点。系统将使机构能够跨越一系列不同的产品线与业务系统，包括存款、电汇、转账、贷款、信托、经纪、信用证以及支票成像应用系统等，在客户关系、账户、交易等方面实现无缝操作。在提供高效、可靠、实时的信息服务方面，对客户关系达成一致认识具有极其重要的意义。每一个机构都应挑选能最好地满足其需求的供应商。在招标过程中，大多数机构都会组建由合规、运营、技术和业务部门的管理人员组成的评估团队。这个团队由项目经理牵头，负责审查和评估招标书的回应。

对于一家金融机构来说，最适用的系统取决于其客户基础、规模和提供的服务。一般地，在评估过程中，金融机构应考虑系统的下列能力：

- 监控交易并识别可疑活动异常情况的能力。
- 采集新老客户的客户尽职调查 (CDD) 信息，对客户回应进行打分并存储客户尽职调查数据以备后续使用的能力。
- 根据各个客户的风险状况和同类客户群的风险特征，由监控系统识别可疑或异常交易并进行高级评估和分析的能力。

- 结合客户在本机构内的所有活动在较广范围内审视个别警示信号的能力。
- 工作流程特征，包括根据一次或者一系列警示信号创建案例的能力，多个利益集团之间（同步或连续）合作审查和更新信息以及在监控和调查部门以及整个银行（必要时）共享反洗钱 / 反恐融资信息的能力。
- 利用该机构核心客户和交易系统以及数据库数据通告或更新监控及案例管理活动的能力。
- 储存并调集至少 12 个月的数据以供趋势分析之用的能力。
- 管理可疑活动甄别的任务分配、上报路径、批准和持续监管等事项的能力。
- 自动生成并向金融情报机构提交可疑交易报告。
- 为管理层以及其他群体准备标准和特别报告，说明可疑活动调查的性质和数量以及调查者的工作效率水平。
- 对每一个反洗钱调查人员的业务量进行计划、分配和监控的强化能力。
- 全面、准确地报告机构反洗钱合规工作的能力，包括向管理层的报告、向监管机关报告、工作效率报告和特别报告。
- 用户友好型的风险参数设置更新，无需专门的计算机技术和技能即可完成设置。
- 为用户、经理和审计师提供分级用户访问权限。

除上述特性外，金融机构应对自动化系统的以下几个方面进行评估：

- 应用的便捷性，以及经变动的全新交易监控规则设置的简便性。
- 数据整合、系统执行和配置的简便性。
- 应用的可扩展性，即系统功能随着机构要求的变化而增强的能力。
- 机构的内部资源能够支撑系统运行的程度。
- 用户对硬件和软件支持的满意度。
- 价格，包括维护系统或扩充系统能力的初始成本和持续费用。上述费用均体现为供应商收取的费用以及机构在财力、人力和技术能力方面的费用。

除了提供可能的监管合规解决方案外，自动化工具还可以帮助机构分析客户和用户使用其产品和服务的方式。出于营销目的，不同类型客户和不同业务领域的活动方式可以通过图表和统计报告来表示。根据机构的需求，从标准的分析系统到精密的人工智能等各种软件产品可以自动完成这些任务。

自动化工具还有助于文档管理，对很多金融机构来说是一大负担。一直以来，影像系统逐步采用快速的无纸化记录方式。随着技术的进步，不能仅限于系统的便捷性。新系统可以跟踪和报告所有文档的情况，包括丢失或过期的文档。一站式的接入系统既可以提供图片，也可以提供文档的标准化和控制措施，而这些在实现合规目标时都必须加以考虑并实施。

洗钱和恐怖融资活动的危险信号

虽然在经过实践验证的可疑交易信号方面，目前还没有一份针对企业的详尽清单，但还是有许多具有共性的金融犯罪、洗钱和恐怖融资行为标志可供您所在的机构参考。

随着金融关系的日益复杂以及资金通过金融机构在全球流动的路径的多样化，洗钱的手法也愈加复杂。同时人们还对世界各地的恐怖主义威胁深感担忧。在打击用于支持和实施恐怖主义袭击的资金运作方面，金融机构和非银行金融机构发挥着至关重要的作用。虽然发现恐怖融资交易活动可能并不容易，但众多权威机构都对此提供了很有价值的指导意见。在开发或调整交易监控程序时，可以使用关于危险信号标志的指导意见。

下列情况可能需要额外审查，因为它们可能是洗钱或恐怖融资活动的迹象。这些清单虽未穷尽所有情况，但应该有助于判定活动是否可疑，或判定活动是否缺乏合理的业务或法律目的。

异常客户行为表现

- 客户举止异常或过于紧张。
- 客户在讨论金融机构的交易记录保存制度或报告制度时表现出明显的规避意图。
- 客户威胁员工，极力阻止银行履行交易记录保存或可疑交易报告义务。
- 客户在被告知某交易必须上报后，不愿意继续进行该交易。
- 客户暗示向员工支付小费。
- 客户似乎有隐秘的事项或行为异常，如拒绝利用大量账户余额获得更高的利率。

- 公职人员以家庭成员的名义开立账户，后者存入的巨额存款与其公开的家庭合法收入不匹配。
- 学生客户大量转移资金或兑换货币，与其身份不符。
- 账户资金的流动速率快，但日初和日终的余额很少。
- 交易涉及离岸机构，其名称与知名的合法金融机构相似。
- 交易涉及很难在地图上找到的陌生国家、地区或岛屿。
- 代理人、律师或财务顾问的代理行为没有相应的授权委托书，如委任状。

异常客户身份情况

- 客户提供异常或可疑的身份证明文件或不愿提供原件进行核查。
- 客户在开户时不愿意提供个人背景信息。
- 客户试图在未进行身份识别，也未提供推荐信或完整本地住址的情况下开立账户。
- 客户的永久地址在机构的服务区域之外。
- 客户的家庭或公司电话无法接通。
- 客户不愿接收账单或邮件。
- 客户询问许多关于金融机构如何披露客户身份信息的问题。
- 企业客户不愿提供完整的业务性质和目的信息，不愿透露预期账户活动及其他业务相关细节，或不愿提供与关联企业实体相关的财务报表或其他文件。
- 客户在申请贷款时未能提供过去或当前的就业记录。
- 客户的互联网协议 (IP) 地址与网上注册时提供的身份识别信息不符。

异常现金交易

- 客户存入大笔现金时不进行清点。
- 客户频繁使用小面额纸币兑换大面额纸币。
- 客户存入的现金中常常出现伪钞、发霉或污渍严重的纸币。
- 两名一起进入营业大厅的客户分别在不同的窗口办理低于报告限额的现金交易。

- 客户在进行大额现金存款时存入大量大面额纸币。
- 客户使用一个或多个姓名开立多个账户，之后多次存入低于报告限额的现金。
- 客户提取低于报告限额的现金。
- 客户从一个账户中取款并将现金存入另一个账户，这两个账户都由该客户所有。
- 客户夜间通过存款机进行与其业务不相符的大额现金交易。
- 客户频繁存取大量现金且没有明显的业务目的，或该企业通常不会产生大量现金。
- 客户在同一天内在不同的分支机构进行大额现金交易，或指使他人以其名义进行此类交易。
- 客户以低于报告限额的金额将现金分散存入多个账户，之后汇总到一个账户并汇往国外。
- 客户在得知自己的交易将被提交现金交易报告后，试图取回超过报告限额的那部分现金。
- 客户多次在 ATM 上进行低于报告限额的现金存款。
- 企业账户主要以现金方式进行存取款交易，而不是采用支票转账的形式。
- 客户从他行提取现金后未经拆包即存入本行，金额巨大且频繁发生。
- 客户频繁使用现金购买金融票据，且交易金额低于报告限额。
- 客户进行外汇兑换交易的次数过多。
- 客户频繁开展外汇交易或货币互换，但从不关心利润。
- 非银行客户将现金存入客户账户，存款随后在不同地点被提取。

异常非现金存款

- 客户存入大量旅行支票，这些旅行支票通常面额相等且连续编号。
- 客户存入大量连号汇票。
- 客户存入与该账户的目的或业务性质不相符的支票或汇票。
- 客户存入大量第三方支票。
- 存入账户的资金通过与账户开立目的不相符的支付方式迅速转移出去。

异常电汇交易

- 同一个人与不同的账户进行电汇交易。
- 非账户持有人通过电汇转出资金，资金包括大量金融票据，且单笔金额低于报告限额。
- 电汇来账指示将资金转换成银行本票并邮寄给非账户持有人。
- 进出保密天堂或高风险地区的电汇活动没有明显的业务理由，或者与客户的历史交易情况不符。
- 受益人收到电汇来账后迅速购买金融票据，用于向其他方支付。
- 账户中的国际电汇交易增多，该账户之前没有过此类交易或此类交易与客户所声称的业务目的不符。
- 客户频繁地通过电汇将所谓的国际业务利润转移到境外。
- 客户收到多笔小金额汇款，然后通过电汇将一大笔资金一次性转往其他国家或地区。
- 客户存入无记名票据，然后根据指示将资金汇给第三方。
- 以货币兑换所名义开立的账户接收电汇入账或现金存款，交易金额低于报告限额。

异常保险箱活动

- 客户在保险箱服务区长时间逗留，可能表明保险箱内存有大量现金。
- 客户经常在使用保险箱后立即办理低于报告限额的现金存款。
- 客户租用多个保险箱。

异常信用交易

- 客户财务报表的某些列报项目不符合会计准则。
- 使用一些引人注目但没有意义的术语，如发行率、银行优惠债券、余额包销、套利合约或对冲合约等，故意把交易变得复杂难懂。
- 客户要求信贷资金转给离岸公司，或者由离岸银行对贷款进行担保。
- 客户突然偿还历史坏账，且用来偿还贷款的资金来源不明。

- 客户购买定期存单并作为质押申请贷款。
- 客户用现金存款作为质押申请贷款。
- 客户用离岸公司的现金作为质押申请贷款。
- 客户的贷款收益意外转移出境。

异常商业账户活动

- 企业客户提供的财务报表明显不同于其他同类企业。
- 大型企业提供的财务报表不是由会计师所编制。
- 提供支票兑现服务的零售企业并未针对支票而提取大量现金，表明其可能另有现金来源。
- 客户为据称正在进行的业务持有过多账户。
- 企业账户显示很少或几乎没有规律的定期活动。
- 交易涉及的情形可能导致工作人员对其质押担保产生怀疑，从而拒绝其贷款申请。
- 空壳公司之间进行的多笔高额付款或转帐，但无明显的合法商业目的。
- 参与交易的企业拥有相同的地址，只提供注册代理公司的地址，或者存在与地址相关的其他不一致问题。

异常贸易融资交易

- 客户寻求进出口商品的贸易融资，但其所申报的价格大大高于或低于类似市场情况或环境下的商品价格。
- 客户请求将收益支付给不相关的第三方。
- 在不提供合理依据的情况下，对信用证进行大幅修改；或者在付款前临时更改付款地点或受益人。
- 客户改变信用证中的付款地点，改为向非受益人所在地的某国账户支付。
- 客户的备用信用证被用作投标或履约保函，但未说明标的项目或合同，或其受益人情况异常。
- 信用证与客户业务不符。

- 信用证所载货物在进口国的需求量极小。
- 信用证所载货物在出口国的产量极低。
- 文件中缺少产权证书。
- 信用证来自洗钱风险极高的国家或地区。
- 商品和服务定价明显过高或过低。
- 交易结构过于复杂，以期掩盖交易的真正性质。
- 商品通过一个或多个没有明显经济或物流原因的司法管辖区进行运输。
- 交易使用重复修改或频繁延长的信用证。
- 装运规模与出口国或进口国的正常业务量不符。

异常投资活动

- 客户使用投资账户作为转账工具将资金电汇至离岸地区。
- 投资者似乎对关于投资账户的常规决策（如风险、佣金、手续费或投资工具的适宜性问题）不感兴趣。
- 客户希望通过一系列的小额交易来清算一笔大额头寸。
- 客户存入低于报告限额的现金、汇票、旅行支票或银行本票，以便向投资账户注入资金。
- 客户在“保单撤销期”提取年金或提早退出年金计划。

其他异常客户活动

- 客户通过互联网或电话进行大量异常交易。
- 客户购买若干与其正常业务活动不符的大额开放式预付卡。
- 从账户提取的资金与账户持有人的正常业务或个人活动不符，或包含向可疑国际司法管辖区的转账。
- 客户将个人账户用于商业目的。
- 客户在没有充分商业目的的情况下，经常在远离客户家庭或办公室的银行或分行办理业务。

异常员工活动

- 员工在银行要求提交的书面报告中夸大客户的资质、背景或经济实力和财力。
- 员工频繁涉及未解决的例外情况。
- 员工奢华的生活方式与其薪水不相符。
- 员工经常无视内部控制措施或已确认的核准权限或规避政策。
- 员工利用公司资源牟取私人利益。
- 员工协助未披露最终受益人身份或交易对手的交易。
- 员工规避定期休假。

涉及货币汇款机构 / 外汇兑换所的异常活动

- 汇票、旅行支票或资金转账的异常使用。
- 两人或多人共同参与交易。
- 改变交易以规避现金交易报告 (CTR) 的提交。
- 客户频繁前来购买金融票据，但每次金额均少于 3,000 美元（或当地记录保存限额）。
- 改变交易以规避银行对 3,000 美元及以上金额（或当地记录保存限额）的转账、汇票或旅行支票进行记录。
- 同一人在短时期内利用多个地点进行交易。
- 两人或多人使用同一个身份。
- 同一人使用多份身份证明文件。

异常虚拟货币活动

- 经常收到来自虚拟货币交易所的资金转账，与客户档案不符。
- 多笔转账流向同一最终用户。
- 在涉及虚拟货币交易所的交易完成后不久，即有资金转入高风险地区，或在高风险地区的 ATM 上取出。

- 收到来自不相关第三方的资金转账后不久即购买虚拟货币。
- 利用多个账户收集资金并将资金转入少数几个虚拟货币账户。
- 多次购买虚拟货币，每笔金额等于或低于 3,000 美元的记录保存限额。
- 录入的交易关键词可能涉及可疑产品销售。

涉及保险公司的异常活动

- 现金支付保单。
- 利用不同来源的现金等价物（如银行本票或汇票）支付保单或年金。
- 产品购买金额超出客户正常财力或财产规划需求。
- 在保险单规定的“法定取消期”或“保单撤销期”内要求退款。
- 从国外支付保险费，特别是从离岸金融中心支付。
- 要求定期缴付大额保费的保单。
- 更改保单指定的受益人，新受益人与投保人之间的关系不明确。
- 撤销保单时不顾及巨额税金或其他罚款。
- 赎回保险债券，但最初登记购买的个人和赎回的企业实体位于不同的国家或地区。

涉及经纪自营商的异常活动

全美证券交易商协会 (NASD) 是根据美国证券交易委员会的授权负责监管纳斯达克 (NASDAQ) 股票市场的一个自律性组织。2002 年，该协会在《全美证券交易商协会致全体成员的特别通知》中指出了证券领域可疑洗钱活动的迹象特征：

- 客户似乎在充当未披露姓名的委托人的代理人，但在没有正当商业理由的情况下，拒绝或不愿意提供信息或回避谈论被代理的个人或实体。
- 在没有任何明显理由的情况下，客户拥有以一人或多人名义开立的多个账户，并拥有大量的账户间转账或第三方转账。
- 客户的账户有原因不明或突然增多的电汇，特别是以往很少有或几乎没有此类交易活动的账户。
- 客户存入资金的目的是购买长线投资工具，但不久后即要求清算头寸并将收益转出。

- 客户在没有任何明显商业目的的情况下，在无关账户之间涉及大量的日记账分录。
- 客户要求交易以特定方式进行以规避银行的正常记录要求。
- 客户在没有任何明显的理由或出现其他“危险信号”的情况下，从事涉及某些类型证券的交易，如低价股票、“S”规则股票、无记名债券等，这些证券虽然合法，但曾被用于与诈骗和洗钱等相关的活动。
- 客户账户存在原因不明的大量交易活动，但证券交易量很小。

涉及房地产的异常活动

- 借款人 / 买家提交无效文件，以撤销抵押债券或付清其贷款余额。
- 同一公证员或其他“授权代表”与数量异常的借款人合作并 / 或收取他们支付的款项。
- 伪造以借款人 / 买家账户而非金融机构账户为担保的保付支票、银行本票或“非现金项目支票”。
- 借款人 / 买家为主要住所申请贷款，但并不住在贷款申请上填写的新主要住所；其他个人占用借款人 / 买家的新主要住所，表明该物业目前为次要住所或创收物业。
- 在公共文件和个人文件显示借款人 / 买家实住地与贷款申请上填写的地址不同的情况下，借款人 / 买家提出“主要住所”再融资申请。
- 评估价值低，卖空买家和卖家之间存在不公平关系，或者以前的做空交易中存在欺诈性抛卖行为。
- 买家或卖家在抵押贷款交易中的代理人未取得经营执照。
- 借款人 / 买家过去做出过虚假陈述，试图获取资金、物业、再融资或实施卖空。
- 文件手续不当 / 不完整，包括借款人 / 买家不愿提供更多信息并且 / 或者未兑现提供更多信息的承诺。
- 重新提交的贷款申请明显是被拒绝过的申请，其中的关键借款人 / 买家明细信息从个人借款人改成了公司 / 企业；此项活动可能表明，同一人试图以虚假手段，通过“虚拟借款人”取得贷款。
- 借款人 / 买家试图拆分现金存款 / 取款，或以其他方式隐瞒或掩盖资产的真正价值，以达到面向存在经济困难的业主的贷款修改计划的要求。
- 代表存在经济困难的业主的第三方关联机构要求接受抵押贷款咨询、止赎规避、贷款修改或其他相关服务的业主提前付费。

- 第三方诱使存在经济困难的业主接受所谓的抵押贷款咨询、止赎规避、贷款修改或其他相关服务；这些第三方也可能自称是合法抵押贷款人、美国政府或美国政府计划的关联方。

贵金属和贵重物品交易商的异常活动

据金融行动特别工作组 2013 年 10 月发布的报告《钻石交易中的洗钱和恐怖融资活动》，以下是与交易实务相关的交易性和其他危险信号标志。

- 钻石来源国的钻石产量有限，或者根本没有钻石矿。
- 与“钻石渠道”以外的国家进行大量交易。
- 购买量或进口量远远超过预期销量。
- 珠宝店（零售）出售金条、钱币和散钻。
- 在全行业成交量大幅下降的情况下，钻石交易商账户活动量增加。
- 两家当地公司通过境外中间人买卖钻石 [缺乏商业依据或不确定双方之间是否真正存在商品交易行为]。
- 付款涉及在已知交易程序以外的国际市场上出现的稀有钻石或特有钻石（如多色菱形粉钻出现在年度拍卖程序以外的国际市场上）。
- 多家企业使用同一银行账户。
- 同一银行账户有多个存款管理人（零售和批发）。
- 通过第三方将资金存入同一个或多个钻石交易商账户。
- 金融活动与钻石贸易实务不一致。
- 在将来自国外公司的款项存入或转入钻石交易商账户之后，立即将金额类似的款项转到另一司法管辖区。
- 通过第三方对冲或从第三方收款的方式结算未结清的出口交易。
- 在进口 / 出口资金收款 / 转账中，订购客户 / 受益人为货币服务企业。
- 钻石交易商付款的收款人名称不是出口商 / 供应商。

关于贸易洗钱的异常活动

- 由与往来交易无关的第三方以任何方式（现金、电汇、支票、银行汇票等）进行的付款。
- 以拆分交易的方式向个人活期存款账户存入资金，在一天之内多次向同一家银行不同分支机构的多个账户存入款项。
- 发票中描述的商品与装运的实物商品有差异。
- 无故修改信用证。
- 双方和交易之间无明显的业务关系。
- 经常进行舍入金额或整数金额的交易。
- 转入账户的资金被等额转移到高风险国家。
- 公司在其商业目的未得到全面理解并且难以确定所有权的司法管辖区开展业务。
- 交易缺少相应的支撑文件。
- 用不记名金融票据支付连号交易或无付款人信息的交易的款项。

关于人口走私的异常活动

据金融犯罪执法网络 2014 年发布的《识别可能与偷渡和人口走私有关的活动指南——金融危险信号》，以下是关于人口走私的危险信号：

- 多笔电汇（通常低于 3,000 美元报告限额）从美国各地流向西南边境沿线的美国或墨西哥城市的同一受益人。
- 同一日或连续几日在同一金融机构的不同分行，有多笔电汇转入或转出西南边境沿线的美国或墨西哥城市。
- 不符合常见汇款规律的资金流动：
  - 源于高移民比例国家（如墨西哥、危地马拉、萨尔瓦多、洪都拉斯）的电汇流向西南边境沿线的美国或墨西哥城市的受益人。
  - 从高移民比例国家（如墨西哥、危地马拉、萨尔瓦多、洪都拉斯）收到电汇的受益人并不是这些国家的国民。

- 巨额现金存入美国金融机构，然后以电汇方式转移到高移民比例国家（如墨西哥、危地马拉、萨尔瓦多、洪都拉斯），与预期客户活动不相符。这可能包括现金存款突然增加，资金快速周转，资金来源不明的大额现金存款。
- 显然没有关系的多位客户向同一受益人电汇资金，该受益人可能位于西南边境沿线的美国或墨西哥城市。这些电汇发送人也可能使用相似的交易信息，包括但不限于相同的金额、地址和电话号码。在条件允许的情况下进行询问时，电汇发送人可能与收款人没有明显的关系，或者不知道电汇的目的。
- 客户账户似乎是流入账户，办理现金存款（通常低于 10,000 美元的报告限额）的城市 / 州不是客户居住地或业务所在地。在流入账户的情况下，资金通常在存入后被迅速取出（同一日）。
- 从可能的流入账户存入的支票似乎是预签，签字栏和付款人栏的笔迹不同。
- 不在现金密集型行业工作的客户经常用小面额纸币兑换大面额纸币。这类活动可能表明，走私贩在为大批量运输现金准备收益。
- 在西南边境附近的客户账户因可疑活动被注销时，新客户可能以账户已被注销的客户的名义开展交易；这可能是继续非法活动的一种手段。在这种情况下，新账户往往反映出与已注销账户相似的活动特点，交易频率可能很高，涉及大量现金，参与的个人过去经常与因可疑活动被注销的账户进行资金往来。
- 生活方式与工作或岗位不符，且无正当理由 / 依据；利润 / 存款显著多于类似职业 / 工作岗位的同行。
- 流入的资金多为现金，而大规模现金流与客户业务不相符；大量使用现金购买资产、进行交易。

关于人口贩卖的异常活动

据金融犯罪执法网络 2014 年发布的《识别可能与偷渡和人口走私有关的活动指南——金融危险信号》，以下是关于人口贩卖的危险信号：

- 企业客户没有正常的工资支出（如工资、工资税、社保缴费）；相对于客户声称的运营规模、员工人数或业务 / 商业模式，工资成本可能不存在或者极低。
- 工资大幅扣减。在金融机构可以观察的范围内，企业客户可能从员工工资中扣除大笔费用（如食宿费），员工只收到很少一部分工资；这种情况可能发生在工资支付前后。

- 将工资支票兑换成现金，其中大部分资金由雇主保留或存回雇主账户；那些可以取得工资单和其他工资记录的金融机构可以发现这种活动。
- 经常在没有商业目的或明显合法目的的情况下汇出电汇，汇入高风险人口贩卖国家或与客户预期活动不相符的国家。
- 客户账户似乎是流入账户，办理现金存款的城市 / 州不是客户居住地或业务所在地。在流入账户的情况下，资金通常在存入后被迅速取出（同一日）。
- 显然没有关系的多位客户向同一受益人电汇资金。这些电汇发送人也可能使用相似的交易信息，包括但不限于相同的地址和电话号码。在条件允许的情况下进行询问时，电汇发送人可能与收款人没有明显的关系，或者不知道电汇的目的。
- 个人在第三方陪同下（以需要翻译的名义）办理交易，向其他国家转账（表面看像是他们的工资）。
- 经常向网上伴游服务公司支付广告费，包括向网上分类广告公司、更昂贵的高端广告公司和网络托管公司支付小额发帖费。
- 企业客户以帮扶个人的名义（如支付住房费用、住宿费、定期车辆租赁费、购买大量食物等）经常进行交易，与预期活动或业务不相符。
- 向无营业执照 / 未注册或曾违反劳动法的职业介绍所或学生招聘机构支付款项。
- 客户在第三方的陪同下（以需要翻译的名义）开户或到分行办理交易。陪同客户的第三方可能持有客户的身份证。
- 明显不相关的企业账户或个人账户有着相同的签字人 / 保管人；类似地，以不同名称开立的多个账户使用相同的信息（如地址、电话号码、就业信息）。
- 外国工人或学生账户的保管人为雇主或职业介绍所。
- 生活方式与工作或岗位不符，且无正当理由 / 依据；利润 / 存款显著多于类似职业 / 工作岗位的同行。
- 流入的资金多为现金，而大规模现金流与客户业务不相符；大量使用现金购买资产、进行交易。

以下两个危险信号可能显示存在异常客户活动；然而，在确定交易是否与人口贩卖相关时，必须与其他迹象结合考虑：

- 交易活动（贷方或借方）与客户声称的职业、业务或预期活动不相符，或者交易缺少商业目的或明确的合法目的。
- 现金存款或电汇金额分别保持在 3,000 美元或 10,000 美元以下，其目的明显是为了规避记录保存或提交现金交易报告。

关于潜在恐怖融资的异常活动

埃格蒙特集团对金融情报机构 (FIU) 提交的 22 份恐怖融资案例进行了评估，归纳出下列金融和行为标志，这些标志是通常与恐怖融资相关的活动中最常见的标志：

行为标志：

- 交易各方（所有人、受益人等）来自因支持恐怖活动和恐怖组织而著称的国家。
- 使用虚假公司，包括空壳公司。
- 包括联合国第 1267 号制裁清单里的个人。
- 媒体报道称，账户持有人与已知恐怖组织有关联，或者参与了恐怖活动。
- 账户受益所有人身份不明。
- 使用名义持有人、信托公司、家人或第三方账户。
- 使用虚假身份。
- 滥用非营利组织。

与金融交易相关的标志：

- 非营利组织的资金运用行为与其成立宗旨不符。
- 考虑到账户持有人的业务或职业，交易缺乏经济依据。
- 通过一系列复杂的转账交易将资金从一个人转到另一个人，以此掩盖资金来源和预期用途。
- 交易与账户正常活动不相符。
- 故意拆分存款，使存款金额低于报告要求以免被发现。
- 多次存入和取出现金，证明人可疑。
- 在国内外 ATM 上频繁操作。

- 交易缺乏商业理由或经济依据。
- 外国银行账户出现异常现金活动。
- 向账户中存入多笔小额现金存款，随后以大额电汇方式汇入另一个国家。
- 使用多个外国银行账户。

备注：

第 4 章

开展调查和回应调查

本章将讨论帮助金融机构获取信息、发起调查的各种渠道，并探讨金融机构应采取哪些措施以确保调查透彻且有效。

金融机构发起的调查

调查的缘由

对潜在可疑活动的积极监控，或为处理监管调查结果、移交的线索或其他建议而采取的应对措施都可能引发调查。常见的调查缘由包括：

- 监管建议或官方调查发现。
- 旨在识别潜在可疑活动的交易监控规则。
- 直接面对客户的员工移交的涉嫌可疑活动的线索。
- 内部热线收到的信息。
- 负面新闻。
- 收到政府作证传票或搜查令。

监管建议或官方调查发现

金融机构可能因监管部门的调查发现或建议发起调查。此类调查工作可能导致新的持续监控或者一次性审查，以便解决具体问题或建议。最重要的是，金融机构应清晰记录和设计因监管部门的调查发现而开展的内部调查，以确保在监管机构规定的时间范围内（如有）解决该发现涉及的各方面问题。此外，应让高级管理层或更高级别的领导层知晓监管审查中提及的事项、金融机构的应对情况以及最终处置措施，以确保金融机构适当地补救监管发现或建议中提到的问题。

交易监控

金融机构应建立制度，定期监控交易，积极识别潜在可疑活动。常见的交易监控方法包括根据机构具体情况建立相应的内部交易监控规则，或委托第三方协助制定和实施自动化规则。金融机构应采取风险为本的交易监控方法，还应在设计交易监控规则时考虑机构的规模、提供的产品以及这些产品的特点。

机构还应制定可疑活动监控政策和程序，应清楚界定触发调查的参数和阈值。机构应定期审查和更新这些政策，以反映监控制度的变化和改进。

沃尔夫斯堡集团在其 2009 年《沃尔夫斯堡声明 - 监察、审查及搜寻》中指出，机构的交易监控框架应与其业务模式风险、产品和服务及其客户群匹配，并应根植在机构的反洗钱制度中。该声明还探讨了监控类型、类型审查以及员工培训。

交易监测规则应定期进行审查，并进行调整，确保其继续按照设计运作。调整工作可能包括评估监控规则的效果，检查特定阈值，进行基准线上下检测，从而确定是否有必要调整规则。

直接面对客户的员工移交的线索

除了持续运行的自动交易监控机制，金融机构还应为面向客户的员工建立线索移交机制，方便他们将发现的问题提交调查，以确定是否存在潜在可疑活动。根据机构规模，可以建立人工移交程序，通过电子邮件、电话或者内部报告系统将线索移交给适当的调查团队。例如，金融机构可设定一个特定的内部在线表格，供分支机构的员工在发现异常情况，如客户进行拆分交易，可能存在受管制的货币流动，或客户对大额现金存款的来源解释前后不一致时填写。分支机构员工完成此表格后发送至指定的反洗钱 / 反恐融资合规电子邮箱。随后，反洗钱 / 反恐融资团队将按照正常的调查流程审查可疑活动。员工培训项目应介绍线索移交制度和应当移交的活动类型，尤其是针对第一道防线员工的培训。

内部热线

内部热线又称道德、合规或举报热线。通过内部热线，员工可以举报广泛的活动，包括员工欺诈、骚扰和歧视，违反行为准则的行为，盗取公司财产和不当礼物。内部热线可能要求员工提供身份信息，但是大部分允许员工匿名举报。不管哪种情况，大多数司法管辖区禁止金融机构对通过内部热线举报的人员进行报复，且金融机构必须制定政策、程序和流程，对通过内部热线获得的信息开展保密调查。金融机构的规模和层级决定了举报信息的处理部门，如法务部门、合规部门、人力资源部门或公司安全部门。

负面新闻

调查可能是为了回应一些值得关注的新闻报道。这些新闻可能与金融机构的某一客户、产品在市场上的使用情况、机构开展业务的地域或者洗钱或恐怖主义事件有关。因此，金融机构应建立接收、核查和升级处理这些潜在高优先级触发事件类型的机制。确定负面新闻是否与金融机构在经济上具有风险相关性非常关键。某些情况下，金融机构可以积极监控新闻报道，进而开展调查，确定是否需要提交可疑活动报告或可疑交易报告（SAR 或 STR），或者是否应采取后续措施。

负面新闻案例

收到政府作证传票或搜查令

金融机构可能会因为收到政府的作证传票或搜查令而开展调查。无论何种情况，金融机构应履行以下两项独立的义务：(1) 依法满足作证传票或搜查令的要求，(2) 判断是否就作证传票或搜查令中涉及的客户的活动提交可疑交易报告。

值得注意的是，银行业监管机构通常无需使用作证传票或搜查令，或者其他司法管辖区特有的法律工具。它们有权直接进行检查，可以检查被监管机构的所有账簿和记录。

作证传票

作证传票通常由大陪审团签发，在法院的权限内运作，授权执法部门强制获得文件和证词。文件和证词旨在允许执法部门调查可疑交易，发现证据并形成案件提交公诉。

如果金融机构收到作证传票，要求其提供与客户有关的特定的文件或人员，应由机构高级管理层和/或顾问审查该作证传票。如果没有理由对作证传票提出异议，机构应采取所有适当的措施，及时、完整地遵守传唤或作证传票的要求。否则，金融机构可能遭受不利行动或处罚。金融机构不得向客户泄露谁正在被调查。

准备政府机构要求的文件时，金融机构应该首先确定一名熟悉机构文件的员工，由其负责文件的搜集。应建立文件保管系统以确保能找到所有文件，无论它们是位于机构档案、部门档案还是个人档案中。此外，不同人员手中持有的相同文件的副本也应收回。这样做之所以非常重要，是因为某些副本上可能有收件员工手写的备注。

如果政府要求机构保持某些账户处于开立状态，该要求应以书面的形式提出，并印有适当的抬头和经政府适当授权。

案例分析

2010 年 3 月，美国美联银行因未能落实设计合理有效的反洗钱制度以便识别和报告涉嫌洗钱或其他可疑活动的交易，被金融犯罪执法网络处以 1.43 亿美元的民事罚款。金融犯罪执法网络指出，“刑事作证传票或大陪审团作证传票如果显示涉及洗钱或特定非法活动，则需要对该可疑活动进行报告，这对不参与作证传票流程的执法部门有一定价值。该银行未能及时审查积压的 6,700 多份作证传票对可疑活动报告流程造成的潜在影响。”因而，美联银行未能及时提交数千份可疑活动报告和现金交易报告，从而大大削弱了这些报告对执法部门和监管机构的价值。

搜查令

搜查令是法院授权执法部门搜查指定场所以及扣押特定类别物品或文件的法律文书。一般来说，需要执法部门证明有理由相信能找到犯罪证据。法院根据执法人员提供的宣誓书中的信息签发搜查令。

执法部门持搜查令前来搜查时，在场的每个人都应该保持冷静，这一点非常重要。每名员工都应知道，搜查令通常不是无限制的命令。相反，搜查令仅授予执法人员进入公司以及搜寻和扣押特定物品或文件的权利。此外，搜查令也不能强制要求作证。

在接到搜查令后，机构应考虑采取以下步骤：

- 致电金融机构内部法务或外部法律顾问，或者指定负责安全、风险管理或类似领域的专员。
- 查看搜查令，以了解授权范围。
- 要求并获得一份搜查令的副本。
- 要求获得一份支持搜查令的宣誓书的副本。执法人员没有提供宣誓书副本的义务，但如果金融机构被允许查看宣誓书，就可以更好地了解调查的目的。
- 在执法人员制作扣押物品清单时，金融机构应派人在场。记录并保存执法人员带走的物品清单。

- 要求获得一份执法人员制作的扣押物品清单的副本。
- 记下搜查人员的名字和所属机构。

享受律师和客户特权或者其他法律特权保护的文件和计算机记录应明确标记享受特权，并与其他一般文件分开单独保存。受特权保护的文件应存放在一个标有“律师 - 客户特权”的区域（如，文件柜）。

如果执法人员希望扣押这些文件，机构代表可以拒绝并建议，作为替代方案，将文件交由法院保管。所有员工都应接受如何应对搜查的培训，金融机构还应指定专人与执法部门沟通。

司法冻结

如果执法部门或检察官获得冻结账户或防止提取或转移资金的法院指令，金融机构应获得一份指令副本并全力遵照执行。一般来说，指令通常根据宣誓书签发。该宣誓书有时会包含在指令中。如果指令没有包含宣誓书的内容，金融机构可以要求查看该宣誓书，从中可以了解执法部门为何要获得某一客户的信息。执法部门是否有提供宣誓书的义务视各国的法律法规而定。在某些司法管辖区，执法人员也可凭扣押令下达冻结命令。

案例分析

2013 年 5 月 9 日，美国发布扣押令，扣押 Mutum Sigillum LLC 公司以及 Mt. Gox 公司所有人 Mark Karpeles 在富国银行账户内的 210 万美元。当时，Mt. Gox 公司在日本开展业务，是全球最大的比特币交易商。根据扣押令，Mt. Gox 公司未能按照美国法律注册为货币服务企业。2013 年 5 月 14 日，美国发布扣押令，扣押一个电子商务在线支付处理商 在 Dwolla 的 账户内的约 290 万美元。该账户是以 Mutum Sigillum LLC 之名在 Veridian 储蓄互助社开立的。当时，消费者为了购买比特币，可以先在 Dwolla 存钱，资金随后转给 Mt. Gox，用于真实的购买过程。美国表示，Mt. Gox 和 Mutum Sigillum 是未经许可的汇款经纪机构，因此扣押其账户内的 500 万美元。

执行调查

要对潜在可疑活动实施有效的金融调查，需要采取几个关键步骤：(a) 审核内部交易、从客户取得的信息以及其他相关内部文件；(b) 查找并审核外部信息以了解客户、相关实体和相关媒体；(c) 联系负责客户关系的业务线员工；以及 (d) 准备一份书面报告，记录相关发现。

金融调查人员的主要目标是追踪资金的走向，即资金是否通过银行、经纪自营商、货币服务企业、赌场或其他金融机构进行转移。金融机构很容易获取大量信息，因为他们从事收取、支付、说明和记录资金走向的业务。例如，银行会保留在账户开立、账单、存款单、支票、收款凭证以及贷方和借方通知单上的预留印签。金融机构也保存着贷款、银行本票、保付支票、旅行支票和汇票的交易记录。银行以及大部分金融服务企业从事货币兑换、第三方支票兑现和电汇等业务。金融机构还提供保险箱服务并发行信用卡。互联网金融机构会保留登录活动日志、IP 地址和地理位置信息。

通常情况下，金融机构需要将客户的账户资料保存 5 年。上述规定在不同国家会存在差异，金融机构的合规人员必须了解相关的法律要求，这一点非常重要。账户记录和其他非账户活动记录对追踪可能的洗钱活动至关重要。其他金融机构会保存类似的交易记录并维持对账户进行控制的能力，比如通过经纪账户进行股票交易的能力。

金融机构可以知悉内情，其制定和遵照金融调查的政策和程序是非常重要的。一般情况下，由金融机构明确需要采取的程序步骤、完成调查所需的信息以及后续建议步骤。以下是两个例子：

1. 分行柜台发现有一名新客户连续几天在三个不同分行办理大额现金存款业务，并且存款金额刚好低于监管现金报告限额，于是启动了调查。随后，该客户将 95% 的资金电汇到一个不相干的、居住于历来以毒品走私门户著称的高风险司法管辖区的个人。据该金融机构的调查政策和程序，必须采取下列措施：对该客户账户最近一年的情况进行审核与记录，包括所有交易、“了解您的客户”信息等，并在社交媒体上搜索任何相关负面媒体报道。报告必须分析审查过的信息，并确定是否需要提交可疑交易报告，是否需要采取任何额外的补救措施。

2. 交易监控警示系统发现，有大额整数资金从高风险司法管辖区采用通用名称的进出口公司汇到其商业客户，由此启动了调查。在审核“了解您的客户”信息时发现，该客户在多个零售点从事家具销售工作。另外发现，有大量的转入支票和信用交易，但没有转入电汇交易；然而，该客户却向低风险管辖区电汇资金，用于采购家具。在这次调查过程中，联系了公关经理，要求其解释客户活动，协助解释发现的异常情况。如果没有解释，下一步调查工作则是确定此类活动是否需要提交可疑交易报告。

利用互联网进行金融调查

有效的调查要求既要取得金融机构保存的信息，也要从外部来源取得信息。必须谨慎处理，确保发现的信息可靠、可验证，如有必要，还需取得外部专家的协助。确保调查中依赖的信息准确可靠至关重要，尤其是其可能成为关闭账户或终止商业关系的决定性因素时。

在内部调查中，互联网越来越多地被当作信息来源。集中搜索可靠、信誉良好的信息来源，可以提供有用的第三方信息，为金融机构保存的档案提供额外的背景材料。结合对内部文件和记录的审核，互联网来源有助于全面了解问题，确定是否需要采取进一步措施以降低与客户相关的可能金融犯罪风险。

当明确知道哪些网络来源可靠时，利用互联网进行调查才能发挥最大的效用。例如，虽然 Facebook、LinkedIn 等社交媒体可能对验证部分信息有用，但博客或这些网站上的评论可能无法作为关于个人声誉的可靠来源。独立标准机构（如金融行动特别工作组、沃尔夫斯堡、经济合作与发展组织和海外资产控制办公室）和监管机构（国家级或州级监管机构、企业注册处、选民民册 / 登记名单）维护的独立网站可以在被调查方可能涉及或参与的监管状态、制裁、罚款、业务活动和广泛商业活动等方面提供有价值的信息。另外，这些来源普遍被认为具有很高的可靠性。

在有些国家或地区，法院名单、法庭判决、地方法官、行政法庭和具有纪律惩戒权的专业监督机构（如律师协会）也可以作为提供有用信息的信息来源。

通过互联网搜集客户声誉相关信息时，在调查新闻或准新闻性质的网站时必须谨慎。必须采取措施，从一个以上的来源验证负面新闻报道的准确性，降低完全依赖新闻记者观点的风险。记者有自己的偏见，其雇主亦是如此，这些偏见可能不知不觉地体现在新闻报道里。另外，在言论自由和新闻自由制度不成熟的国家或地区，记者不能自由地表达自己想写的内容。这种情况的具体表现通常是极力宣传不受政府青睐的某个人的负面新闻（包括可能存在政治意图的刑事或民事指控），或是有意淡化受政府赏识的某个人的负面新闻。虽然并非所有媒体都腐败不堪，但有时候，新闻来源存在的风险不亚于新闻主题。这正是调查者必须密切审核新闻来源和新闻本身的原因，也是取得多个来源对全面了解情况至关重要的原因。有些来源可能只体现了整个事情的有限部分，只有当调查者找到其他信息片段时，整个事情的全貌才会显现出来。

在涉及到严格限制互联网发布内容并限制公众可访问信息量的国家或地区时，可能需要寻求额外帮助。尤其是面对值得付出额外费用的高价值客户时，机构可能需要委托在该领域拥有深厚专业知识的服务供应商，由其验证关于某位客户的严重不利信息是否有独立来源的支持。

互联网搜索技巧：在开始搜索互联网之前，调查者应制定一份计划，突出调查主题和所需信息的类别。这样可以在搜索时提高效率、突出重点。

调查人员首先应使用多种不同的搜索引擎进行元搜索，然后再使用具有不同功能的特定搜索引擎。调查人员还可以通过使用关键词从元搜索中缩小参数。提前制定计划有助于在调查中选择应重点关注的关键词和领域。例如，如果调查客户的交易活动会引起顾虑，则在搜索时可以从客户的个人和专业背景开始，然后重点关注客户所进行商业活动的性质。这样有助于调查者评估这些交易是否与客户提供的开户理由以及账户的预期商业用途相符。

网上有一些很好的教程，可供希望提高搜索技能的人使用。还有些网站向您介绍面向专业搜索人员的搜索引擎。提高搜索技能最简便也最有效的方法就是阅读主要搜索引擎的“帮助”菜单并尝试使用其高级搜索功能。

以下是有关搜索引擎的建议：

- 由于单个搜索引擎无法涵盖整个网络的内容，使用多个搜索引擎是明智之举。
- 如果您在外国搜索，请使用当地的搜索引擎。
- 使用元搜索引擎。

您也可以访问商业数据库。虽然这些数据库需要付费，但公共记录收集人员可以从中交叉查询大量记录，支付此笔费用也是非常值得。此外，这些数据库可能有互联网上找不到的某些个人身份信息，如出生日期、政府身份证号码等。

案例研究

在对客户进行正常的交易监控时，有家银行在一名客户的交易中发现了可能的异常情况。这位客户是一家货币服务企业，在开户时告知银行，其核心客户来自欧洲，估计该账户每月会有 10 到 20 笔交易。银行对这家公司进行了内部调查。经搜索互联网，调查者发现，这家公司在中东和东非推广其资金转账服务，故意淡化提供“了解您的客户”信息的必要性。这家银行迅速采取行动，在向金融情报机构通报发现的问题后，冻结并在之后关闭了这个账户。

搜索场景：大额资金。以一位加油站老板为例，他每周在银行存入 5 万美元现金，这是洗钱吗？许多人只会简单地把该老板的名字输入谷歌进行查询并认为这样的尽职调查足矣。但更好的方法是思考以下问题：规模和地理位置与其相似的加油站一般每周存储多少现金？这会引出一条很不一样的调查线索。互联网来源可能会披露营销案例、商业评估网站或待售企业等信息来源，这些都可能提供关于类似加油站现金流的有用线索。

互联网还可能提供加油站所在地区的有用信息，如：人口统计数据、收入水平、种族状况、犯罪率等。它是否地处交通要道？附近是否有竞争对手？是否有附属的洗车场或者便利店？

把该公司与其他公司进行对比并分析其所处的环境，就可能得出这样的结论："……大量的现金存款与该企业的预期业务状况不符"，而这就是典型的洗钱标志。

搜索场景：不了解的企业。本案例涉及的一位银行客户在其私人账户里存入了大量现金。银行怀疑该客户在其餐馆的掩护下经营未经许可的货币汇兑业务。正当他们准备提交可疑交易报告时，他们意识到自己忽略了一条关键信息，即客户餐馆的名称。这一谜团如何破解？他们一开始就假定该客户的餐馆位于银行附近。借助简单的在线电话簿，他们就能够生成距离银行 1 英里范围内的所有餐馆列表。

但哪家餐馆才是这位客户的呢？他们需要查询已经掌握的每一家企业的注册登记信息。由于不想使用商业服务，他们便访问了一个免费的在线公共记录提供商。点击司法管辖区和公司链接后，他们找到了相应的政府部门网站。他们把该地餐馆的名称一一输入，直到发现其中一家餐馆的老板正是他们的客户为止。

这个案例很好地展示了以下做法的好处：即在开始调查之后缩小关注范围，从而取得对受调查客户的全面认识。

搜索场景：异常银行账户活动。哪些技术技能对"了解您的客户"(KYC) 和尽职调查有用？我们将通过这个简单的场景来思考如何进行调查。您需要对美国新墨西哥州中部城市阿尔布开克一位名叫 Cynthia Jenkins 的客户展开调查。交易监控系统发出警示，Cynthia 似乎在利用其账户开展与其开户预期不相符的活动，或者，该账户已经休眠一段时间，但突然被重新激活了。交易监控系统显示，Cynthia 的账户在过去两个星期从不同来源收到了大量的电汇。每笔转账金额为 9,900 美元。在 Cynthia 起初开户时，她声称账户是用于"家庭开支"。首先您可能要确认 Cynthia 的身份，然后搜索互联网以确认账户用途是否合法。

- 电话号码簿或选民民册上有她的名字吗？
- Cynthia 住在哪里？是否有证据表明该账户被用于任何商业活动从而为所收款项提供正当的理由？
- 是否有任何其他公开记录提到她？试试公开记录搜索引擎。
- 她在社交媒体上提供了哪些职业、位置等信息？

- 是否有证据表明有人在滥用 Cynthia 的账户，比如，她是否是老人或者可能已经去世？这会是身份窃取案件吗？骗子经常盗用死者的社会保障号码。在美国，可以查询“社保人员死亡名录”。

通过互联网搜索取得的信息应与公司保存的内部文件和记录结合使用。转账来自谁？来自哪家银行？转账是否注明了付款理由？是否可以搜索互联网，确认网上是否有关于付款人的任何信息？

可疑交易报告决策过程

在作出是否提交可疑交易报告（在美国也称为可疑活动报告，简称“SAR”）的决定时，通常需要权衡在调查过程中发现的各种定罪因素和正向因素。金融机构应起草相应的程序，记录在决定是否需要提交可疑交易报告 (STR) 时要考虑的各种因素。接受过有效培训的可疑活动调查和报告负责人应执行明确、简洁的上报程序，将发现的问题上报合规官、经理或有决定权的其他职员。最终决定应记录在案并给出用于作出决定的理由。通常情况下，不提交可疑交易报告的理由与提交可疑交易报告的理由同等重要。

在作出提交决定之后，金融机构应向其监管机构或执法机构或者同时向二者报告可疑活动，具体根据所在司法管辖区的适用制度执行。许多司法管辖区要求在发现潜在可疑活动之后特定天数之内提交可疑交易报告。

在许多司法管辖区，要求向高级管理层或董事会报告关于可疑交易报告的特定信息。这些信息可能局限于所交报告数量、涉及的金额和合规人员观察到的重要趋向。在某些情况下，如果该活动对金融机构构成重大风险或潜在持续风险，机构领导应知情，以便高层就可能对制度、人员配备、产品、服务或机构维持的特定关系进行的调整作出决策。

提交可疑交易报告

提交可疑交易报告的决定应该是定罪因素不断累积而缺乏正向因素的结果，同时还应结合考虑该机构的客户、产品和服务地区做出预期判定。提交的可疑交易报告不但应该包括可疑活动详情和相关客户特征信息，还应包括机构认为活动可疑的原因。可疑交易报告的接收人对机构特定客户和产品的预期活动并没有深刻了解，因而只能从包含这些信息的推论中了解有用信息。另外，还要审核时发现的任何确切的类型判定信息也应包含在内。

如果在调查后，机构决定应提交可疑交易报告，则应尽快通知调查员或检察官。然而，由于可疑交易报告流程具有连续性并且报告机构提交的报告数量巨大，因而在某些司法管辖区，这样做并不实际。依据国别制定报告提交时间表对于避免机构受到处罚或罚款也至关重要。对金融机构采取的监管行动通常将未及时提交报告作为理由之一。反洗钱 / 反恐融资官或被指定人员应实时向管理层和董事会汇报可疑交易报告指标以及这些报告带来的任何重要问题，尤其是会对金融机构造成监管或声誉风险的事项。

质量保证

所有金融机构都必须及时、完整地提交可疑交易报告，可疑交易报告的质量可以体现金融机构反洗钱 / 反恐融资制度的质量。可疑交易报告决策过程的质量和一致性是确保在调查过程中采取适当监督的关键。质量保证 (QA) 审查有助于确保可疑交易报告的内部一致性，确保决定的正确性，确保发现了重点事项且已向领导汇报。对于大型金融机构，其员工和所在地都可能对质量保证流程造成影响。因此，实施质量保证流程的金融机构应规定质量保证审查员的要求和资质，定期审核质量保证审查结果，评估员工素质、培训要求和制度的整体运行状况。

可疑交易报告的监督 / 升级

机构应制定可靠的政策和程序，规定适当的调查过程监督制度和监管报告要求。其中包括要采取的具体措施，比如，在面向客户的员工或反洗钱 / 反恐融资指挥链中的个人串通一气或故意对可疑金融活动视而不见的情况下，向高级管理层上报。

案例研究

2016 年 3 月，美国货币监理署 (OCC) 颁布了一项处罚决定，对美国科勒尔盖布尔斯市直布罗陀私营信托银行 (Gibraltar Private Bank and Trust Co.) 的前首席合规官和首席风险官处以 2,500 美元的罚款，惩处其在督促银行提交可疑活动报告方面的失职行为。在这项处罚决定中，美国货币监理署指出，该银行的银行保密法专员对与该行一起庞氏骗局案相关的活动进行了调查，并准备了可疑活动报告。Sanders 先生赞同报告的内容，但未能督促银行及时提交报告。

案例研究

2009 年，佛罗里达州的律师 Scott Rothstein 承认策划了一个涉案金额为 12 亿美元的庞氏骗局，诱使投资者参与纯属杜撰的保密庭外和解。据称，本应在结构化和解中兑现的当事人卷入了性骚扰和告密案件，被告希望对这些案件保密。虽然其前提是可行的，但 Rothstein 提供的回报远远高于那类投资的合理回报水平，有些情况下，90 天回报超过 20%。Rothstein 最初

在直布罗陀私营信托银行开立了账户，他还对这家银行进行了个人投资；后来在 2016 年，该行因故意违反反洗钱合规要求而被金融犯罪执法网络 (FinCEN) 处以 400 万美元的罚款。直布罗陀私营信托银行受到处罚是因为其制度存在缺陷，导致该行错过了与 Rothstein 账户相关的警示信息。Rothstein 作为投资人的身份可能是导致银行未对其账户提交监管报告的部分原因；他后来也辩解称，直布罗陀私营信托银行的一名副总裁曾协助他在账户之间转移资金以避开合规工作人员。

在部分投资者告诉他更喜欢与大型机构交易之后，Rothstein 在加拿大多伦多道明银行 (TD Bank) 开立了账户以继续操纵庞氏骗局。Rothstein 后来指出，他曾向多伦多道明银行的联系人提供现金，以便此人继续为骗局提供方便；Rothstein 同时提到，此人“处理了银行合规官员就账户提出的”与骗局相关的“所有疑虑”。2013 年 9 月，金融犯罪执法网络决定，对多伦多道明银行处以 3,750 万美元的罚款，因为该行未能提交与这起特大庞氏骗局相关的可疑活动报告。

销户

根据内部调查的结果，金融机构应该就是否销户这一问题作出独立的判断。着重考虑以下因素：

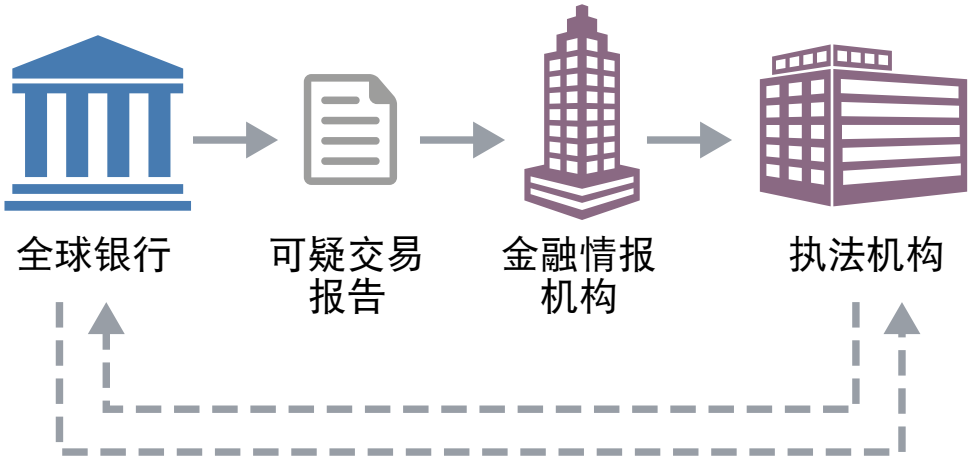
- 销户的法律依据。
- 机构关于销户所规定的政策和程序，可能包括提交指定次数的可疑交易报告之后的自动销户建议。
- 行为的严重程度。如果行为达到销户要求，则应该考虑销户。
- 保留账户给金融机构带来的声誉风险。
- 遵从执法机构的销户或保有账户要求。

与执法机构就可疑交易报告进行沟通

在金融机构提交可疑交易报告时，报告细节可能上升到需要向执法机构发出额外通知的程度。可疑交易报告代表着向一个国家或地区的金融情报机构提交的金融情报；根据在特定国家或地区提交的报告数量，值得优先关注的报告可能隐藏在提交的大量报告之中。在提交可疑交易报告之后，负责的合规官或被指定人员可以联系特定的执法部门，告知他们最近提交的报告，让他们获悉与

其责任范围或地理位置相关的活动。另外，执法机构可以联系提交该可疑交易报告的金融机构，要求其提供在开展可疑交易报告调查中使用的基本信息。因此，每个金融机构都要在就可疑交易报告与执法机构进行沟通方面，制定自己的政策和程序，这一点至关重要。

与执法机构就可疑交易报告进行沟通的示例



执法机构发起的调查

执法机构可以对金融机构发起调查，也可以在涉及金融机构的客户的调查中联系金融机构。执法机构在执行反洗钱调查时可能或应该采取的步骤包括：

- 以资金为线索。如果执法机构掌握了“黑钱”的来源或最终去向，则通过资金的流入和流出串联出一条完整的资金链。
- 利用金融机构掌握的金融知识和尽职调查信息。通过信息共享和交易审查，金融机构可以协助执法机构发现嫌疑人资金的来源或最终目的地。另外，在许多司法管辖区，用于编写可疑交易报告或客户尽职调查文件的支撑文件可以作为证据，而实际可疑交易报告却不能作为证据。
- 识别非法活动。大多数国家或地区都从上游犯罪或“特定非法活动”的角度来定义洗钱。在通常情况下，洗钱活动涉及的上游犯罪很广泛且往往牵扯到很多重罪，包括贿赂、勒索、诈骗、毒品走私和人口贩卖。要为洗钱案件定罪，检察官需要明确资金流转的过程并确定上游犯罪类型。

- 查看数据库。金融情报机构数据库和商业数据库可以提供非常有用和广泛的金融信息，还能就向哪些金融机构求助提供一些线索。此外，美国的“社保”信息（即与税务相关的信息）等记录可以用来进一步核实嫌疑人的身份。
- 查看公共记录。法院记录、公司档案和信用报告都能提供有用的背景信息。
- 查看许可和注册文件。这些文件（如由机动车管理部门和其他注册数据库保存的记录）可以提供背景信息以及有用的引导。
- 分析调查对象的金融交易和账户活动。根据背景相似的人员的自我披露、收入和典型资金流动来判断正常且符合预期的交易。金融机构有可能帮助发现这些事项。对于超出标准或声称的额度范围的交易，则需要分析额外资金的来源以及异常活动的原因。
- 查看可能涉及与调查目标、交易或活动相关的潜在个人可疑交易报告。
- 在跨境案件中可以寻求国际援助。

决定对洗钱违规的金融机构提起诉讼

在决定是否（或在什么程度上）对涉及洗钱嫌疑的机构提起诉讼时，检察官会考虑很多因素，包括:

- 该机构有无犯罪历史。
- 该机构是否配合调查。
- 该机构是否发现并自行报告了与洗钱相关的问题。
- 该机构是否具备完整有效的反洗钱 / 反恐融资制度。
- 该机构是否采取了及时有效的补救措施。
- 是否可以用民事补偿作为惩罚措施。
- 是否需要通过他人来阻止犯罪或者需要通过公诉机关来达到此目的。
- 是否有来自该司法管辖区的监管机构或金融情报机构的意见和建议。

如果案情复杂或者影响恶劣，检察官对机构可疑活动意图的认定通常是决定是否起诉的关键。

对针对金融机构的执法调查的回应

在面对执法调查时，金融机构要对所有要求快速、全面的回应。否则可能给机构造成不必要的风险或损失。如果司法机关的调查要求过于宽泛或欠妥，机构可以尝试缩小要求的范围，甚至可在法庭上对该调查的全部或部分要求提出异议。但是，机构绝对不能忽视或推迟对执法调查或文件提供要求的回应。

在收到执法质询时，金融机构应通知相关高级管理层并指定专人负责回应，掌握调查的进程并将调查的性质和进程告知高级管理层（包括董事会）。当然，不得向任何可能牵涉调查的员工、主管或董事提供关于调查的报告或相关信息。

金融机构应考虑聘请符合要求、经验丰富的法律顾问。该法律顾问可以指导机构应对质询，对不当要求提出异议并协助机构商议处理方案（如需要）。

如下所述，在收到作证传票、搜查令或类似执法命令，或知晓涉及机构的政府调查时，金融机构应通过开展自我调查确定基本事实、本机构的风险以及应采取的措施（如有）。

对针对金融机构的执法调查进行监控

金融机构还应确保所有提供给大陪审团的作证传票以及其他政府机构的信息都经过高级管理层、调查小组或顾问的审查，从而确定对质询的最佳回应方式以及质询或潜在活动是否会对本机构产生风险。此外，金融机构应对所有要求或回应保持统一管理，以此确保得到及时完整的反馈结果并予以登记。这份集中记录还有助于金融机构的内部调查。

内部备忘录、交易凭证、日志、电子邮件、财务记录、出行记录、电话记录、预留印签、存款单、支票、取款凭证、借方和贷方凭证和贷款记录中都隐含着重要信息。因此，金融机构必须确保相关文件未被篡改、遗失或损毁且所有员工都已知晓这一规定。这一规定可以通过备忘录向所有相关人员传达。但是，如果备忘录可能会提醒某些别有用心的员工去篡改或损毁文件，则必须另当别论。

机构还应建立文档销毁制度，确保根据这一政策，任何文件不得在调查期间被销毁。如果与政府调查有关的文件在收到调查通知或作证传票前已经按照规定被销毁，则不会产生严重的影响。但如果这些文档在机构接到调查通知后被销毁，即使机构尚未收到作证传票且无论出于什么原因（甚至是根据合法的政策），这都将成为严重的问题。

金融机构应确保原始文件的完整性，同时尽量不要影响业务开展。金融机构还必须建立有效的文件保管系统，用于文件的整理、维护、编号、保护和复制以及向政府的提交（或向民事诉讼中的对方当事人提供）。为方便寻找，文件应该建立索引。

文件收集完成后，还要制定使用和查看权限。为避免不慎泄密，有查看权限要求的文件应与其他文件分开存放。

在针对金融机构的调查期间与执法机关合作

向调查人员提供有助于得出结论的信息可能是终止调查最为有效的方法，以避免给本机构的资源和声誉造成破坏性影响。配合的内容包括：安排包括公司主管在内的员工接受面谈，在不要求作证传票的情况下提供文件，以及主动披露相关信息并向调查人员提供由专业顾问书写的关于调查对象的报告。

金融机构应尽量与调查人员和检察官保持良好的关系。至少，良好的工作关系有助于金融机构有效开展相应的内部调查，从而更加有效地回应调查或检察质询。

充分了解调查人员和检察官对事件的看法对金融机构来说也非常重要。如果调查人员和检察官恰巧对部分事实存在误解，金融机构就有机会进行纠正。如果金融机构了解调查人员和检察官的关注点，它至少能够使自己的回应更有针对性。

为针对金融机构的调查聘请顾问

聘请顾问

对于特别重大、重要或严重的调查，金融机构可能需要聘请专业顾问提供协助或建议。包括大型银行和证 经销商在内的很多金融机构都聘有内部法律顾问。但很多小型金融服务企业却不一定拥有内部法律顾问。在政府对本金融机构展开调查时，上述两类金融机构最好都聘请或咨询外部资深法律顾问。如果金融机构面临紧迫的刑事起诉或诉讼，则需聘请资深律师，专门负责在这些事务中为金融机构进行辩护。

使用内部顾问成本相对较低，且内部顾问对本机构及其人员、政策和程序都非常熟悉。但是，如果被调查的行为可能涉及或导致刑事调查或起诉，外部顾问可能更为合适。

如果金融机构认为确实需要聘请内部或外部顾问，则应采取适当措施以确保顾问有足够的经验和知识来处理相关的问题。此外，金融机构应确定顾问的性质和职责范围并确保高级管理层知晓及认可。

律师 - 委托人特免权适用于企业和个人

在内部调查中，所有相关方都应知晓，本机构律师代表的是企业，而非员工。顾问应了解这些问题并据此开展内部调查。根据律师 - 委托人特免权，工作成果和通讯可能受到保护。如果企业的利益和员工的利益发生冲突，或者是员工牵连了企业或企业牵连了员工，都有可能造成严重的后果。在这样的案例中，就需要聘请独立的顾问。

顾问书面报告的分发

如果顾问为金融机构准备调查的书面报告，金融机构应采取措施，防止因向不应接收报告的人员分发报告而不慎放弃律师 - 委托人特免权。报告的每一页上都应包含“本文件保密”以及“本文件受律师 - 委托人特免权和工作成果特权保护”的声明。

金融机构应对报告副本进行编号，并留存副本接收人的名单。在一段时间后，所有副本都应收回。副本接收人不得在副本上留下笔记。为了进一步确保最高级别的保护，所有副本都应保存在区别于普通机构档案的独立档案中。

将金融机构受到调查之事通知员工

在面对政府调查时，金融机构应告知员工并指示其不要直接提供公司文件，同时将所有检查要求告知高级管理层或顾问，由高级管理层或顾问提供相应资料。这样，金融机构才能知道政府部门要求的内容以及提供的资料。此外，金融机构还能决定对哪些要求（如有）提出异议。与员工面谈的要求也按照相同的规则来处理。

因金融机构受到执法调查造成的员工面谈

除了保护和审查相关文件外，与知情的员工进行面谈也是重要的环节。一旦可行，应立即与员工进行面谈，确保其记忆处于最为清晰的状态以有效指引管理层或顾问及时获取相关的文件、了解相关的人。

此外，金融机构（通常是顾问）应帮助需要接受执法部门调查人员面谈的员工做好准备，并在面谈结束后了解面谈的具体情况。前者可以帮助员工了解具体的流程和处理方法，后者则可以协助本机构更好地了解政府调查的范围和方向。如上所述，执法部门调查人员提出的所有与员工面谈的要求都应在单独或统一的地点进行。

无论是执法部门调查人员或是有本机构顾问参与的面谈，大部分员工都不愿接受。因此，金融机构应尽可能地帮助员工放松心情。

此外，尽可能减少面谈的争议性也将大有帮助。在面谈开始时应介绍调查的背景和谈论一些开放性的问题，且避开对抗性的信息。如有必要，较有争议的问题应稍后提出。

媒体关系

人们常常错误地忽视了公共舆论和媒体关系在保护机构时的重要性。在维持公共信任方面，公共舆论对机构的成功与否至关重要。如果事实对本机构不利，“不予置评”可能是最佳的回应方式。试图表明金融机构不存在问题或者没有过错的误导性或虚假陈述可能会使情况恶化。如果上市公司发表这样的言论，还可能招致监管部门和执法部门的额外审查。

案例研究

当受到美国当局调查的金融机构积极配合调查时，结果通常会使当局感到满意，从而暂缓对金融机构的起诉，降低处罚力度，或者取消针对此次诉讼的监管审查。2007 年 8 月 6 日，美国运通银行国际部 (AEBI) 同意向美国当局缴纳 6,500 万美元的罚款，并与美国司法部达成暂缓起诉协议；此前，美国司法部对美国运通银行国际部提起诉讼的罪名是未建立有效的反洗钱 / 反恐融资制度，导致在发现和报告黑市比索交易 (BMPE) 方面存在严重的缺陷。当时，美国运通银行国际部发言人表示，“我们全面配合政府调查，我们理解有必要在我们的制度中保持绝对的警惕性，有效防范洗钱行为。我们已经采取了有力措施，补充和加强我们的合规制度，并将一直持续下去。我们将坚定不移地执行我们达成的协议，以最高的诚信、合规和控制标准开展工作。”

国家或地区间的反洗钱 / 反恐融资合作

金融行动特别工作组关于国家或地区间合作的建议

监管当局或金融情报机构 (FIU) 在分析和调查可疑交易或洗钱犯罪、没收资产、引渡被控洗钱犯罪分子等领域进行国际合作会受到限制，这是反洗钱领域的严重障碍。

金融行动特别工作组 40 项建议中关于建立和维护有效反洗钱 / 恐怖融资机制的第 36 - 40 项专门阐述了洗钱与恐怖融资活动调查中国际合作的问题。包括双边司法协助、引渡、资产没收和国际信息交换机制等。

国际洗钱信息网

国际洗钱信息网 (IMoLIN) 是洗钱信息的交换场所，对国际和国内反洗钱机构大有裨益。该网络由联合国毒品与犯罪问题办公室 (UNODC) 下辖的全球反洗钱计划，代表联合国和其他包括国际刑警组织 (Interpol) 在内的国际组织进行开发和管理。国际洗钱信息网有五个主要模块，除一个模块外，其余四个均可接受公众访问：

- **国际反洗钱数据库：** 国际反洗钱数据库 (AMLID)——美国反洗钱法律规章的概要与分析，以及国家联络机关和当局的信息。此数据库须凭密码登录。
- **参考资料：** 研究与分析、参考文献、公约、法律文书和示范法律。
- **国家或地区页面：** 包括反洗钱立法的全文（如可用）以及指向国家或地区金融情报机构 (FIU) 的链接。
- **大事纪要：** 按时间顺序罗列反洗钱领域的培训活动、会议、研讨会、专题讨论会和其他会议。
- **当前事件：** 最近发生的反洗钱新闻事件。

司法互助协定

当要求另一司法管辖区提供证据时，需要发挥司法互助的作用。司法互助协定 (MLAT) 为相互间传递可用于起诉和司法程序的证据提供了一个法律平台。

例如，1995 年 3 月 3 日开始生效的《加拿大与西班牙刑事事件互助协定》将刑事事件定义为与税收、关税和资本或款项的国际转移相关的调查或诉讼。另外，该协定将互助定义为“取得证据和个人口供；提供信息、文件和其他记录，包括犯罪记录、司法记录和政府记录；查找个人和物品，包括其身份；搜查和扣押；移交财产，包括出借物证；允许被逮捕的个人和其他人作证或协助调查；传送文件，包括需要个人出庭的文件；查找、限制和没收犯罪所得的措施；以及符合本协定目的的其他互助方式。”

虽然具体程序不尽相同，但典型流程如下：

- 申请国的中央政府向另一个国家的中央政府发出“调查委托书”。委托书的内容包括要求提供的信息、请求的性质、申请国的刑事指控以及提出请求所依据的法律规定等。
- 收到委托书的中央政府将委托书转发给当地的金融调查人员，由其确定信息是否可以提供。
- 申请国的调查人员造访信息提供国，在其来访期间或录取口供时由当地调查官陪同。
- 调查人员请求中央政府将证据移交给申请国。
- 中央政府将证据交给申请国的中央政府，至此就完成了司法互助请求。当地证人可能需要出席在申请国进行的庭审。

金融情报机构

金融情报机构 (FIUs) 是处理金融情报的合法国家机构。金融情报机构负责接收和分析个人、金融机构及其他实体提交的可疑交易报告，并把由此获得的情报分发给地方执法机关和外国金融情报机构，用以打击洗钱活动。

最早的一批金融情报机构成立于 20 世纪 90 年代初期，因反洗钱需要一个集中的机构接收、分析和分发金融信息应运而生。当前，金融情报机构的数量不断增加。作为金融情报机构的非官方国际协会，埃格蒙特集团已拥有 150 多个成员。

20 世纪 90 年代末成立的欧洲各国金融情报机构主要在国内开展工作，工作内容以国内事务为主。但是，为了应对犯罪分子和恐怖分子利用欧盟边境开放政策所带来的威胁，卢森堡、英国、意大利和法国的金融情报机构响应荷兰金融情报机构的号召，建立了分散型金融情报网络，以便通过一种更成熟的方式交换信息。2004 年，随着试点项目的启动，FIU.net 由此诞生。自 2006 年起，原来的欧盟委员会司法、自由和安全总司 (DG JLS)，后来的移民和内部事务总司 (DG HOME)，荷兰国家安全司法部以及其他一些参与的金融情报机构共同为欧盟 FIU.net 项目提供资金，该项目至今已持续逾十年。

在此期间，专门负责开展 FIU.net 项目的荷兰司法部下属 FIU.net 署、项目支持团队以及一些金融情报机构携手将 FIU.NET 打造成了一个用于打击洗钱和恐怖融资活动的成熟有效的工具。多年来，项目参与者为 FIU.net 新增了多项功能，如具有颠覆性的 Ma3tch 技术，该技术可在对一般当事人进行匹配及侦测的同时，不向他人暴露当事人相关信息；以及，Templates 功能，该功能使得项目参与者可根据各金融情报机构的的需求，对其系统进行相应调整。

2012 年，金融行动特别工作组修订了针对打击洗钱活动的一系列建议，首次就金融情报机构的组建和职能提出了明确建议。尽管埃格蒙特集团的金融情报机构成员拥有共同的核心职能，即为打击洗钱和恐怖融资活动而接收、分析和分发金融信息，但它们在组建方式和运作模式上却存在差异。2016 年，欧盟在实施全面反恐行动计划时，采取了大量措施，以强化金融情报机构的作用，并提升这些机构在欧洲各国间分享信息的能力。

金融情报机构的三个基本职能

金融情报机构在反洗钱和反恐融资活动事业中发挥着重要作用。金融行动特别工作组于 2012 年发布了 40 项建议，其中第 29 项建议为，各国应组建国家级金融情报机构，以便接收和分析以下信息，并将对这些信息的分析结果进行分发：(a) 可疑交易报告；(b) 与洗钱、相关上游犯罪及恐怖融资活动有关的其他信息。金融情报机构应具备从报送机构获取额外信息的能力，且为有效履行其职能，其应具备及时获取所需相关金融、行政和执法信息的能力。

金融行动特别工作组 40 项建议中的第 30 和 31 条阐述了金融情报机构和其他主管当局的多种职权，其中包括：

1. 在国家反洗钱 / 反恐融资政策框架内，负责对洗钱和反恐融资活动开展调查。
2. 至少在与产生收益的重大犯罪活动相关的所有案件中，应在追查洗钱、相关上游犯罪及恐怖融资活动（包括在司法管辖区外发生的相关上游犯罪活动）的同时，开展积极的金融犯罪调查。
3. 对于应予没收或可能需予以没收，或疑为犯罪所得的财产，应迅速地加以识别、追踪，并采取行动予以冻结和扣押。

4. 可获取上述调查、刑事诉讼及相关行动所需的一切文件和信息。金融情报机构和其他主管当局的其中一项职权是，采取强制性措施要求金融机构、特定非金融行业以及其他自然人或法人出示其持有的记录，用于搜查个人或房屋、获取证人陈述书以及扣押和获取证据。

5. 运用适用于洗钱、相关上游犯罪及恐怖融资活动调查的各种调查技巧。这些调查技巧包括：开展卧底行动、截获通讯信息、访问计算机系统和实施控制下交付。

澳大利亚交易报告和分析中心成立于 1989 年，是澳大利亚打击重大有组织犯罪和恐怖融资活动所需金融情报的主要来源。英国的金融情报机构隶属于英国国家犯罪局。该局于 2013 开始运作，负责带领英国执法机关打击严重的有组织犯罪。美国金融犯罪执法网络成立于 1990 年，通过接收、分析和分发金融情报以及有策略地使用金融情报机构等手段履行其职责，即保护金融系统免遭不法分子利用，打击洗钱活动以及推动国家安全的发展。

金融情报机构肩负着以下职责：接收和分析可疑交易报告，与警方和海关保持密切联系，调查期间在机构内部非正式地共享信息，这些通常都是以谅解备忘录的形式进行。金融情报机构埃格蒙特集团已经制定了谅解备忘录的模板。与司法互助协定不同的是，这一途径通常不是用来获取证据，而是用来获取可能指向证据的信息。

2001 年 6 月，集团成员签署了《金融情报机构间信息交换原则》文件，并将其作为集团宗旨声明的一部分。有些国家或地区可能会限制与其他金融情报机构间的情报交换或者限制其他金融情报机构获取信息。该文件描述了金融情报机构之间实现最大限度合作的实践方法，对政府部门在考虑反洗钱立法时有所帮助。

此外，为了解决妨碍司法互助的现实问题，该文件为实现金融情报机构间信息交换提供了最佳实践范例。该文件力主金融情报机构在处理国际信息交换请求时，充分考虑采用这些最佳实践。

以下是文件中列举的一些原则：

- 埃格蒙特集团关于在金融情报机构层面上免费交换信息的原则应该建立在对等的基础上，包括信息的自动交换。
- 金融情报机构管辖范围内对罪名定义的差异不应成为在金融情报机构层面免费交换信息的障碍。为此，金融情报机构的管辖范围应予以扩展至涵盖洗钱和恐怖融资活动的所有上游犯罪。
- 金融情报机构之间的信息交换应该尽可能地采用非官方和便捷的方式，不得附加过多形式上的先决条件，同时要保证对隐私的保护以及共享数据的保密性。

- 如果金融情报机构需要通过谅解备忘录进行信息交换，则应进行谈判并签署谅解备忘录，不得无故拖延。为了实现这一目标，金融情报机构有权独立签署谅解备忘录。
- 金融情报机构之间的沟通可以直接进行，毋须通过中介。
- 出于执法或司法目的，金融情报机构应该及时且最大限度地批准信息的分发。提供信息的金融情报机构不得拒绝信息的分发，除非此举超越了反洗钱和反恐融资活动的规定范围，妨碍刑事调查，与个人、法人或金融情报机构所在国的合法利益发生冲突，或者不符合所在国家法律的基本原则。任何拒绝批准的行为都应该给予适当的解释。

以下是要求获得信息的金融情报机构应该遵循的做法：

- 所有金融情报机构都应该根据埃格蒙特集团制定的信息交换原则提交信息请求。在可能的情况下，金融情报机构间信息共享协议的规定也应该予以遵守。
- 一旦准确界定了需要协助的内容，就应该尽快提出信息请求。
- 当一个金融情报机构掌握了对另一个金融情报机构可能有用的信息时，一旦信息共享的相关性得到证实，该机构就应该考虑主动移交信息。
- 埃格蒙特集团金融情报机构之间应该采用安全的方式进行信息交换。为了实现这一目标，埃格蒙特集团金融情报机构应该在适当的时候使用埃格蒙特安全网站 (ESW)。

金融情报机构通过谅解备忘录交换信息的一个例子发生在 2013 年 10 月。美国金融犯罪执法网络与墨西哥国家银行和证券委员会签署了金融情报机构间信息交换史上的首个谅解备忘录，以期促进双方监管信息的交换，为对方机构开展的反洗钱和反恐融资活动提供支持。另外，该谅解备忘录还制定了严格的控制和保护措施，从而确保共享的信息得到妥善保护，并确保双方以保密和经授权的方式将信息仅用于对反洗钱和反恐融资活动的监管。

备注：

第 5 章

术语表

A

宣誓书 (Affidavit)

在法庭官员、公证员或其他获授权人面前经宣誓后所立的书面声明。宣誓书被广泛用作申请搜查令、逮捕令或扣押令的事实依据。

替代性汇款体系 (Alternative Remittance System; ARS)

地下钱庄或非正规价值转移体系。通常与中东、非洲或亚洲的族群相关，且通常涉及银行体系以外的跨国价值转移。汇款实体可以是与另一国家或地区代理企业有协议关系的从事商品销售的普通商店。该体系通常不存在货币的实际转移且缺少关于身份验证和记录保存方面的正规手续。货币转移采用加密信息（通过便条、快递、信件、传真、电子邮件、短信或者在线聊天系统发送）的形式，随后再经某种电信方式确认。

国际反洗钱数据库 (Anti-Money Laundering International Database; AMLID)

反洗钱法律法规的集成分析资料库，包括国内法律和国际合作这两大类型的洗钱控制措施以及国内联系部门和当局的信息。作为一个安全的多语种数据库，AMLID 是执法官员调查跨司法管辖区案件时的重要参考工具。

反洗钱制度 (Anti-Money Laundering Program)

旨在协助机构打击洗钱和恐怖融资活动的制度。在很多司法管辖区中，政府法规要求包括银行、证券交易商和货币服务企业在内的金融机构建立该制度。反洗钱制度至少应包括：

1. 书面的内部政策、程序和控制措施；
2. 指定的反洗钱合规专员；

3. 持续的员工培训项目；以及

4. 对制度进行的独立性测试

反洗钱和反恐融资制度 (Anti-Money Laundering and Counter-Financing of Terrorism Program)

参见“反洗钱制度 (Anti-Money Laundering Program)”

逮捕令 (Arrest Warrant)

指示执法官员逮捕并拘留某一特定人员并要求其对一指控作出答辩或出庭的法庭命令。

亚太反洗钱工作组 (Asia/Pacific Group on Money Laundering; APG)

与金融行动特别工作组 (FATF) 类似的区域性组织，由亚太地区的司法管辖区组成。

资产保护 (Asset Protection)

包括重组所持资产在内的流程，旨在减少个人遭索赔时对资产的影响。资产保护还是税务筹划人员使用的一个术语，用来描述为保护资产免受其他司法管辖区的税收政策影响而采取的各项措施。

资产保护信托 (Asset Protection Trusts; APT)

不可撤销信托的特殊形式，通常在海外创立（设立），主要目的是保留和保护个人财产不受其债权人追索。资产所有权转移给指定的受托人。资产保护信托 (APT) 通常用来保护资产且往往呈税收中性，其最终功能是为受益人服务。有些支持者宣称，资产保护信托允许外国受托人无视美国法庭命令并方便地将信托资产转移至另一司法管辖区，以应对威胁信托资产安全的法律诉讼。

自动清算中心 (Automated Clearing House; ACH)

批量处理大量贷记和借记交易的电子银行网络。自动清算中心的贷记转账功能包括直接储蓄薪酬支付和对承包人及供应商的支付。自动清算中心的借记转账功能包括保险费、按揭贷款和其他费用的消费者支付款项。

自动柜员机 (Automated Teller Machine; ATM)

一种电子银行设备，可让顾客在无银行员工协助的情况下完成基本的交易。自动柜员机的功能一般包括：现金提取、支票存款、现金存款、转账以及账户余额查询。

B

银行汇票 (Bank Draft)

银行汇票是由信誉良好的机构签发的规范性国际金融票据，通常在见票后即可从签发机构在另一国家开立的账户中进行现金支付，因此易被用于洗钱。

银行保密规定 (Bank Secrecy)

指某些国家或地区禁止银行在未经账户持有人同意的情况下泄露账户信息、甚至披露该账户存在的法律法规。这类规定阻止信息在金融机构及其监管者之间的跨国流动。FATF 在 40 项建议中指出，各国应确保金融机构的保密法律不得阻碍 FATF 建议的执行。

银行保密法 (Bank Secrecy Act; BSA)

美国主要的反洗钱监管法规（美国法典第 31 篇第 53115355 章），于 1970 年颁布实施，其最为著名的修正案为 2001 年颁布的美国《爱国者法》。该法规定了多项措施，其中就要求金融机构以及许多其他企业实施反洗钱控制措施，包括报告各种金融交易并保存记录的规定。

银行保密法合规制度 (Bank Secrecy Act (BSA) Compliance Program)

总部设在美国的金融机构（根据美国《银行保密法》的定义来确定）为控制洗钱及相关金融犯罪而制定和执行的有关制度。该制度最基本的内容应包括：内部政策、程序和控制措施的制定；合规专员的指定；持续的员工培训项目；对制度进行测试的独立审计部门。

巴塞尔银行监管委员会（巴塞尔委员会）(Basel Committee on Banking Supervision; Basel Committee)

巴塞尔委员会由 G10 国家中央银行行长于 1974 年组建，旨在促进监管标准在全球范围内的建立健全。委员会秘书处由位于瑞士巴塞尔的国际清算银行任命。该委员会已经发布了关于银行客户尽职调查、一体化里了解您的客户风险管理、支付信息透明化、跨境电汇支付信息的尽职调查和透明化以及各司法管辖区共享与反恐融资活动有关的金融记录等各个方面的文件。*参见 www.bis.org/bcbs。*

批量处理 (Batch Processing)

将相关交易汇集在一起进行传输并处理的一种数据处理和数据交互程序，通常由同一台计算机在同样的应用程序下运行。

不记名形式 (Bearer Form)

对于证券、股权转让或其他文件来说，不记名形式无需进一步的书面指令就可出售、转让、放弃或以其他任何方式处理指定的投资或储蓄。

不记名可转让票据 (Bearer Negotiable Instruments)

包括以不记名形式持有、无限制背书、开给收款人或所有权在票据交付时即告转移的可转让票据（包括支票、本票和汇票）等在内的金融票据。

不记名股票 (Bearer Share)

将公司所有权赋予实质占有（开给“持有人”、未载明个人姓名或机构名称的）不记名股票证书之个人的可转让票据。

贝纳米账户 (Benami Account)

也称为代理人账户。贝纳米账户由某一个人或实体代表他人持有，通常与印度次大陆的哈瓦拉地下钱庄体系相关。如果处于某一司法管辖区的个人希望通过哈瓦拉经纪人将资金转到另一司法管辖区，此人可利用贝纳米账户或贝纳米交易来掩饰其真实身份或资金接收方的真实身份。

受益所有人 (Beneficial Owner)

受益所有人一词有两种不同的定义，具体取决于以下情况：

- 最终拥有或控制某一账户并通过账户开展交易的自然人。
- 对法人或法律安排拥有重要所有权或可行使最终有效控制权的自然人。

受益人 (Beneficiary)

根据不同的情况，受益人一词有两种不同的定义：

- 从一笔交易中获益的自然人或法人，例如接收电汇款额或保险赔偿金的一方。
- 信托关系中，所有的信托（慈善信托或法律允许设立的非慈善信托除外）都必须有受益人，信托人也可以成为受益人。信托关系必须确定信托的最长时限，即“永续期”，这一期限通常可长达 100 年。尽管信托关系必须拥有最终确定的受益人，但当下可以没有确定的受益人。

以钱换钱 (Bill Stuffing)

赌场顾客先后将现金塞入多台老虎机中并换取领款券，但并不参与赌博活动，而是使用这些领款券在赌场柜台兑换现金或支票。

黑市比索交易 (Black Market Peso Exchange; BMPE)

黑市比索交易 (BMPE) 是一种基于交易的复杂洗钱手段。哥伦比亚限制性货币兑换政策是推动 BMPE 发展的最初因素。为了规避这些政策，哥伦比亚企业通过与黑市或平行金融市场上的比索经纪人进行交易来逃避政府课税。哥伦比亚毒贩利用这一方法将来源于美国的贩毒所得美金兑换成哥伦比亚比索并在哥伦比亚境内接收。

C

持卡人 (Cardholder)

金融交易卡的发卡对象，或者获得授权使用该卡的其他个人。

加勒比地区金融行动特别工作组 (Caribbean Financial Action Task Force; CFATF)

由阿鲁巴、巴哈马、英属维尔京群岛、开曼群岛和牙买加这些加勒比国家（地区）组成的类似 FATF 的区域性组织。

货币兑换处 (Casa de Cambio)

也称为货币兑换所 (Bureau de Change)、外币兑换所 (exchange office)。货币兑换处提供的一系列服务对洗钱者非常具有吸引力，其中包括：货币兑换和零票换整；兑换旅行支票、汇票和私人支票等金融票据；以及电汇服务。

现金密集型企业 (Cash-Intensive Business)

客户通常支付现金购买其产品或服务的任何企业，如餐馆、比萨外卖店、出租车公司、投币机或洗车行。有些洗钱者通过经营或利用现金交易型企业，将其非法所得资金与合法经营所得资金进行混合。

现金抵押贷款 (Cash Collateralized Loans)

现金抵押贷款是指将现金存款作为抵押物的贷款。而现金存款有时可能位于另一个司法管辖区内。

现金存款 (Cash Deposits)

存放在一家金融机构的一个或多个账户内的货币总额。易被用于洗钱的“处置阶段”，犯罪分子可通过在金融机构账户中存入现金这一方式将现金转移至非现金经济体中。

银行本票 (Cashier's Check)

一种常见的以现金购买的金融票据。银行本票是金融机构签发的金融票据，可用于洗钱。

美洲药物滥用管制委员会（西班牙语：Comisión Interamericana para el Control del Abuso de Drogas; CICAD）

参见“美洲国家组织：美洲药物滥用管制委员会 (Comision Interamericana Para El Control Del Abuso De Drogas)”。

集中账户 (Concentration Account)

也称为“综合账户”。清算账户由金融机构以自己的名义持有，主要用于内部管理或银行间交易，无需识别汇出方的个人身份就能进行资金的转账和混合。

托收账户 (Collection Accounts)

外国移民在其居住地的一个账户中存入多笔小额现金，托收总额将被转移至其母国的账户，且无需对其资金来源进行记录。亚洲或非洲的某些民族可能会利用托收账户从事洗钱活动。

调查委托书 (Commission Rogatoire)

也称为调查委托函 (letters rogatory)，是一国中央政府为寻求司法管辖区外的证据而向另一国的中央政府发出的法律或司法协助书面请求。通常来说，该委托书会明确请求的性质、在请求国国内的有关刑事指控、作出请求所依据的法律规定以及所希望寻求的信息。

集中风险 (Concentration Risk)

集中风险主要是存在于资产负债表中的资产一栏。通常的做法是，监管机构不仅要求金融机构建立识别信贷集中的信息系统，而且还要对银行对某一借款人或某一相关借款人团体的借款额度作出限定。在负债方面，集中风险与融资风险有关，特别是大额储户忽然提前提取现金从而影响机构流动性的风险。

保密 (Confidentiality)

不向公众或未授权方公开特定的事实、数据和信息。在大多数司法管辖区，提交可疑交易或活动报告时需要保密，即报告提交机构的员工不得告知客户其交易情况已被报告。在另一种情形下，机构违反当地的银行保密法而向执法机关或金融情报机构披露客户信息可能会构成对保密规定的违反。

没收 (Confiscation)

没收在适用的情况下还包括充公，是指根据相关部门或法院的命令永久性剥夺资金或其他资产。充公或没收通过司法或行政程序将特定资金或其他资产的所有权转移给政府。所有权转移后，原则上，在充公或没收时对特定资金或其他资产享有利益的个人或实体丧失了对被充公或没收资产的所有权利。

公司组织形式 (Corporate Vehicles)

可能遭到滥用的各种法律实体包括：私人有限公司和股票未在股票交易所交易的公共有限公司、信托、非营利组织、有限合伙企业和有限责任合伙企业以及私人投资公司。有时，因为识别这些法律实体的最终受益所有人以及实际控制人存在相当的难度，所以它们才极易被用来洗钱。

代理银行业务 (Correspondent Banking)

由一家银行（“代理银行”）向另一家银行（“委托银行”）提供的银行服务。大型国际银行往往同时充当全球成千上万家其他银行的代理银行。委托银行可获得广泛的服务，包括现金管理（如各种货币的利息存款账户）、国际资金电汇、支票清算、账户支付和外汇兑换等服务。

信用卡 (Credit Cards)

一种设定信用限额用来购买商品和服务并可预支现金的塑料卡片。发卡人在消费完成后向持卡人寄送账单，要求其按信用期限偿付账单数额。如果还款金额由犯罪所得资金进行偿付，则信用卡就成了洗钱的工具。

犯罪所得 (Criminal Proceeds)

直接或间接通过犯罪活动获得的任何财产。

跨境 (Cross Border)

用于涉及两个或两个以上国家的活动，如跨境电汇或跨境携带货币。

货币 (Currency)

流通中作为交换媒介的钞票和硬币。

货币走私 (Currency Smuggling)

大量现金的非法跨境转移，通常是将现金转入未实施严格银行保密制度、外汇控制措施混乱或缺乏反洗钱法规的国家或地区。

现金交易报告 (Currency Transaction Report; CTR)

记录某一笔超过一定金额上限的现金交易的报告。如果同一天内多笔现金交易的累积金额超过某一限额，也可以提交现金交易报告。包括美国在内的一些国家针对何时应向政府部门提交现金交易报告进行了规定。

保管人 (Custodian)

负责为他人或机构管理、经营或保管资产的银行、金融机构或其他实体。保管人保管资产是为了尽可能降低失窃或遗失的风险，保管人并不主动交易或处理资产。

保管 (Custody)

保护和管理客户投资或资产的行为或授权。

客户尽职调查 (Customer Due Diligence; CDD)

在洗钱控制措施领域，客户尽职调查要求制定相应的政策、惯例和程序，从而使得金融机构能大致预测客户可能会进行的交易的类型。客户尽职调查要求，金融机构不仅需要明确客户身份，而且应设定账户活动的基准，以便识别那些与该客户的正常或预期交易不符的交易活动。

D

借记卡 (Debit Card)

允许账户持有人从其已有账户中提取资金的银行卡。借记卡可用于偿付债务或购物，并可在包括互联网在内的多种场所中使用。借记卡通常通过刷卡现金返还交易或自动柜员机提现实现现金流动。

特定犯罪类型 (Designated Categories of Offense)

金融行动特别工作组 (FATF) 认定为洗钱的上游犯罪的犯罪活动。各国可依照其国内法律自行决定特定犯罪的认定标准和要素。许多国家或地区并没有具体列明哪些犯罪可作为洗钱的上游犯罪，而只是声明所有重罪都可能是洗钱的上游犯罪。

特定非金融行业 (Designated Non-Financial Businesses and Professions)

金融行动特别工作组 (FATF) 建议，下列特定非金融行业应采用特定标准：

- 赌场（包括网络赌博）。
- 房地产经纪商。
- 贵金属和宝石交易商。
- 律师、公证员、其他独立的法律专业人士和会计人员。（请注意，此类人员是指代表客户准备或开展特定工作的人员。）
- 代表其客户准备或开展特定工作的信托公司和公司服务提供商。

境内转账 (Domestic Transfer)

汇出方与受益机构处于同一个司法管辖区的电子资金转账业务。因此，境内转账是指完全发生在同一个司法管辖区的任何电汇环节，即使发出电汇的实际系统位于另一个司法管辖区或互联网。

E

东南非反洗钱工作组 (Eastern and Southern African Anti-Money Laundering Group; ESAAMLG)

成立于 1999 年，由非洲东部和南部国家或地区组成的类似 金融行动特别工作组 (FATF) 的区域性组织。

金融情报机构埃格蒙特集团 (Egmont Group of Financial Intelligence Units)

埃格蒙特集团由多个国家的金融情报机构组成，各成员定期举行会晤，以期寻找促进金融情报机构自身发展和相互间协作的方式，尤其是在信息交换、培训和经验交流方面的协作。该集团的宗旨是为各国金融情报机构提供交流平台，以便促进反洗钱和反恐融资合作，推动各成员在其国内实施反洗钱和反恐融资制度。

电子资金转账 (Electronic Funds Transfer; EFT)

金融机构间的电子化资金转移。美国最常用的两个电子资金转账系统是 FedWire（联邦电子资金转账系统）和 CHIPS（纽约清算所银行间支付系统）。SWIFT（环球银行金融电讯系统）通常被视为美国第三大电子资金转账系统，但实际上，它只是在银行间传输汇款指令的国际信息交换系统，本身并非电汇系统。

电子货币 (Electronic Money; E-Money)

电子现金是指以电子形式存储于例如互联网、设备硬盘或塑料卡片微芯片中的一系列货币价值单位。

增强尽职调查 (Enhanced Due Diligence; EDD)

增强尽职调查是指，金融机构为识别和规避高风险客户所带来的风险，须在开展常规客户尽职调查之余采取的额外措施。相比常规或低风险客户，增强尽职调查要求金融机构对高风险客户的性质、业务及账户交易活动进行更加深入的了解。金融机构应确保掌握高风险客户的全面的账户情况，并对这类账户采取风险为本的方法加以监控。

欧亚反洗钱与反恐融资活动工作组 (Eurasian Group on Combating Money Laundering and Financing of Terrorism; EAG)

金融行动特别工作组类区域性组织，2004 年 10 月成立于莫斯科。

欧洲联盟 (European Union; EU)

1992 年，欧洲共同体于马斯特里赫特通过《马斯特里赫特条约》。1993 年，该条约正式生效，欧洲联盟（简称“欧盟”）正式诞生。欧盟主要由欧洲国家组成，是一个政治经济联盟。成员国组建了三个共同机构，即欧洲议会、欧盟委员会和欧盟理事会，并赋予其部分主权。当出现涉及集体利益的具体问题时，成员国便可通过民主的方式从整个欧洲层面作出决策。因此，欧盟各成员国间实现了人员、商品、服务和资金的自由流动。

欧盟关于防止利用金融系统进行洗钱和恐怖融资活动的指令 (European Union Directive on Prevention of the Use of the Financial System for the Purpose of Money Laundering and Terrorist Financing)

欧盟于 1991 年 6 月通过了这一指令，并分别于 1997、2005 及 2015 年对其进行修订。该指令要求欧盟各成员国禁止洗钱和恐怖融资活动。该指令适用于各种类型的实体，其中包括：金融机构、会计、公证员、信托公司、房地产经纪商以及赌博服务提供者。根据该指令的要求，成员国需要适当地识别并缓释风险。成员国需要监督金融机构和其他有责任实体，其中包括：设定客户尽职调查标准；杜绝与空壳银行有所关联；组建金融情报机构 (FIU)；制定文件保留标准；以及要求在违规时承担后果。

欧洲刑警组织 (Europol)

欧洲刑警组织是欧盟的执法机构，主要使命是协助欧盟为其公民打造更加安全的欧洲。在反洗钱领域，欧洲刑警组织通过欧洲刑警组织联络官 (ELO) 及其分析员不仅为欧盟成员国的执法机构提供运作和分析方面的支持，还为其提供先进的数据库和沟通渠道。

书面信托 (Express Trust)

通常以书面信托契约等文件形式，由信托人创建的明文规定的信托关系。一些信托公司的设立并非信托人特定意图或决定的结果（例如，为处置未申报财产，根据法律要求设立的推定信托），而书面信托不同于此类信托公司。

引渡 (Extradition)

根据协议由一司法管辖区向另一司法管辖区交出被指控或被判刑人员的行为。该协议应就此类交换的条件做出明确规定。

域外管辖权 (Extraterritorial Reach)

一国政策和法律的效力向他国个人和机构的延伸。反洗钱法的禁令和制裁可能延伸至其他司法管辖区，具体视各司法管辖区而定。

F

金融行动特别工作组 (Financial Action Task Force; FATF)

1989 年由七个工业化国家为推进国家和全球性反洗钱措施的制定而组建的机构。是全球范围内反洗钱标准和反恐融资活动措施的国际政策制定机构。不过其建议并不具有法律效力。金融行动特别工作组的成员包括 35 个国家和 2 个国际组织。2012 年，金融行动特别工作组大幅修订了 40 + 9 项建议并将其缩减为 40 项建议。该组织发布年度洗钱类型报告，列述当前洗钱和恐怖融资活动的发展趋势和方法。*参见 www.fatf-gafi.org*。

拉美反洗钱金融行动特别工作组 (Financial Action Task Force on Money Laundering in Latin America; GAFILAT)

与金融行动特别工作组类似的拉丁美洲区域性组织，成立于 2000 年。

金融行动特别工作组类区域性组织 (Financial Action Task Force-Style Regional Body; FSRB)

该组织具有与金融行动特别工作组类似的形式和职能，但它们的工作主要针对特定地区。该组织与金融行动特别工作组共同构筑成反洗钱和反恐融资相关的全球网络。

金融情报机构 (Financial Intelligence Unit; FIU)

一个负责接收、分析和向主管当局披露可疑交易的中央国家机关。

没收 (Forfeiture)

因法律诉讼而产生的财产或资产非自愿损失。没收的原因通常是，财产所有人未能遵守法律或该财产与某类刑事犯罪活动相关。

冻结 (Freeze)

阻止或限制资产或银行账户的交换、提取、清偿或使用。与没收不同的是，在冻结期间，被冻结财产、设备、资金或其他资产仍属于对其享有权益的自然人或法人的财产，并可由第三方继续管理。为防止资产的流失，法院可能会实施资产冻结。

前台公司 (Front Company)

由另一个机构成立并控制的公司。虽无确切违法行为，但犯罪分子利用前台公司洗钱，使非法所得获得表面的合法性。前台公司可利用大量非法资金来补贴其产品和服务，从而使其产品价格远低于市场价，甚至低于制造成本。

G

南美金融行动特别工作组（西班牙语：Grupo de Acción Financiera de Sudamérica; GAFISUD）

参见“拉美反洗钱金融行动特别工作组 (Financial Action Task Force on Money Laundering in Latin America)”。

守门人 (Gatekeepers)

律师、公证员、会计师、投资顾问、信托与公司服务提供商等协助涉及资金流动的交易并被认为在识别、防范和报告洗钱活动中具有特殊作用的专业人员。有些国家和地区对守门人和金融机构工作人员提出了相似的客户尽职调查要求。

让与人 (Grantor)

转让财产或资产的产权或所有权的一方。就信托而言，让与人通常指信托的设立者或资助者。

海湾合作委员会 (Gulf Cooperation Council; GCC)

海湾合作委员会成立于 1981 年，旨在促进成员国在经济和工业领域的合作。成员国包括科威特、巴林、卡塔尔、沙特阿拉伯、阿曼和阿联酋。海湾合作委员会是金融行动特别工作组成员，但其成员国并非金融行动特别工作组成员。

H

哈瓦拉 (Hawala)

常见于中东、北非及印度次大陆的非正规价值转移体系，这一体系独立于传统银行系统运营。基本运作模式为，汇款人联系哈瓦拉经纪人 A，把需要转移的资金交给他。A 将联系收款人所在国家或地区相应的人员 B，由 B 向收款人交付资金。A 和 B 将记录交易流水帐，明确 A 欠 B 的净款额。*参见“替代性汇款体系 (Alternative Remittance System)”*。

哈瓦拉经纪人 (Hawaladar)

在哈瓦拉交易中，负责利用哈瓦拉体系帮助客户转移资金的人员。

人口走私 (Human Smuggling)

人口走私指违反一国或多国法律帮助人们实现跨国运输或非法入境。与人口贩卖不同的是，人口走私主要指相关人员的运输和非法入境，而非对他们的剥削。

人口贩卖 (Human Trafficking)

也称为“人口贩运”。人口贩卖的目的通常是开展性奴役、强制劳动或商业性剥削活动。人口贩卖几乎存在于全球各国，常被称为世界第二大犯罪形式。

非正规价值转移体系 (Informal Value Transfer System; IVTS)

参见“替代性汇款体系 (Alternative Remittance System)”。

融合 (Integration)

融合阶段通常指典型洗钱过程的第三个阶段，也是最后一个阶段。通过重新将资金注入金融体系并使其获得表面合法性，清洗后的资金可以在该阶段重新投入经济体。

国际商业公司 (International Business Company; IBC)

国际商业公司指仅可在其组建地之外的司法管辖区开展业务的各种离岸公司。此类公司组建迅捷，保密严格，权力宽泛，成本低廉，税率极低甚至为零且承担极少的记录和报告要求。

国际货币基金组织 (International Monetary Fund; IMF)

国际货币基金组织是一个拥有 180 多个成员国的国际组织，其宗旨在于促进全球货币合作、保持金融稳定、促进国际贸易、实现较高的就业率水平、推动经济持续增长以及减少全球贫困。自成立以来，该组织的这些目标一直保持不变。包括监督、金融援助和技术支持在内的业务都已作出调整，以便适应成员国不断变化的需求。

K

明知故犯 (Knowledge)

进行禁止行为的心理状态。2012 年 FATF 40 项建议第 3 项的解释性说明指出，各国应确保：证明洗钱犯罪所需的意图和认识应该与《维也纳公约》和《巴勒莫公约》所设定的标准一致，包括可从客观事实情况推测此等心理状态。反洗钱法律对“明知”的准确定义因国家而异。在某些情况下，“明知”可认为包括有意忽视；即“有意避免对事实的认识”，正如有些法院对这一术语的定义。

了解您的客户 (Know Your Customer; KYC)

用以确定客户真实身份及其“正常和预期”活动类型并侦测特定客户的“异常”活动的反洗钱政策和流程。

了解您的员工 (Know Your Employee; KYE)

用以更好地了解机构员工以便侦测利益冲突、洗钱活动、过往犯罪活动以及可疑活动的反洗钱政策和流程。

L

离析 (Layering)

离析阶段是典型的洗钱三步流程中的第二阶段，位于放置和融合之间。这一阶段通过建立层次复杂的金融交易来掩饰审计线索并隐匿身份，从而使非法所得与其来源分离。

法律风险 (Legal Risk)

根据 2001 年巴塞尔银行客户尽职调查白皮书的定义，法律风险是指因诉讼、不利判决或无法执行的合同而干扰或危害金融机构的可能性。此外，银行可能受到政府的行政或刑事处罚。涉及银行的诉讼案件可能给机构造成超出司法成本的重大影响。如果银行在识别客户身份和了解并管理其洗钱风险时没有进行尽职调查，那它就无法有效地避免此类法律风险。

信用证 (Letter of Credit; L/C)

由银行签发的保证在某些条件得到满足时代表其客户向第三方付款的信用票据。

调查委托函 (Letter Rogatory)

参见“调查委托书 (Commission Rogatoire)”。

M

谅解备忘录 (Memorandum of Understanding; MOU)

双方就制定一系列原则来处理双方在特定事项上的关系而达成的协议。谅解备忘录通常被各国用来管理国际资产没收案件中的资产共享事宜或者确定各自在反洗钱工作中的义务。金融情报机构肩负着以下职责：不间断的接收和分析可疑交易报告，与警方和海关保持密切联系，调查期间在内部非正式地共享信息，这些通常都是以谅解备忘录的形式进行。

中东与北非反洗钱金融行动特别工作组 (Middle East and North Africa Financial Action Task Force; MENAFATF)

中东和北非地区于 2004 年建立的与金融行动特别工作组类似的机构。

金融票据 (Monetary Instruments)

旅行支票、包括个人支票和商业支票在内的可流转票据、正式银行本票、银行本票、期票、汇票、不记名证券或股票。金融票据与货币被绝大多数国家纳入反洗钱法规的管辖范围，金融机构必须就涉及金融票据的客户活动提交报告并保存相关记录。

洗钱 (Money Laundering)

对非法所得财产或资金的存在、来源、移动、目的地或非法使用进行隐藏或掩饰以使其具有表面合法性的过程。洗钱通常包含三个阶段：将资金注入金融系统，通过离析交易掩饰资金来源、所有权和所在地，并以表面合法的持有形式使资金融入社会。在将洗钱认定为犯罪的国家或地区中，各国 / 地区对洗钱的定义也不尽相同。

洗钱报告专员 (Money Laundering Reporting Officer; MLRO)

多项国际规则中使用的术语，指负责监管公司反洗钱活动和制度并向国内金融情报机构提交可疑交易报告的人员。洗钱报告专员是实施反洗钱战略和政策的关键人员。

汇票 (Money Order)

通常以小额现金购买（往往低于 500 欧元 / 美元）的金融票据。汇票通常被没有活期存款账户的人用来支付账单或在卖方不接受个人支票的情况下支付所购物品款项。因为汇票是由机构签发而非从个人账户取钱的票据，所以可能被用于洗钱。

货币服务企业 (Money Services Business; MSB)

开展下列活动且超过适用监管限额的个人（自然人或法人），在此情况下，这个人通常被视为须遵守反洗钱规定的金融机构:

- 外汇交易
- 支票兑现
- 签发或出售旅行支票或汇票
- 提供或出售预付存取产品
- 资金转账

资金转账服务或价值转移服务 (Money Transfer Service / Value Transfer Service)

通过通讯、信息、转账或资金 / 价值转移服务所属的清算网络，在一地接收现金、支票或其他可储值的金融票据并在另一地把相应的金额以现金或其他形式向受益人支付的金融服务。这一服务提供的交易可能涉及一个或多个中介以及第三方最终支付。资金或价值转移服务可由个人（自然人或法人）正式通过受监管的金融系统（如银行账户）提供，也可非正式地通过非银行类金融机构和监管系统外的商业实体提供。在有些司法管辖区，非正规体系被称为替代性汇款服务处或地下（或平行）银行业务体系。

评估反洗钱措施特设专家委员会 (MONEYVAL)

即“欧洲委员会评估反洗钱措施特设专家委员会”。前身为 PC-R-EV 的欧洲委员会评估反洗钱措施特设专家委员会于 1997 年由欧洲委员会部长委员会成立，其职能是对欧洲委员会成员国中非 FATF 成员国的反洗钱措施开展自评和互评。欧洲委员会评估反洗钱措施特设专家委员会 (MONEYVAL) 是欧洲委员会欧洲犯罪问题委员会 (CDPC) 的下设机构。

监控 (Monitoring)

机构反洗钱制度的一个部分，用来审查客户活动中的异常或可疑模式、趋势或与正常模式不吻合的交易。机构通常使用软件将活动与客户“正常和预期”活动的阈值进行比较，从而对交易进行监控。

司法互助协定 (Mutual Legal Assistance Treaty; MLAT)

允许各国出于官方调查和指控目的，在各自国家私营和公共部门中的法律诉讼以及文件、证人和其他法律和司法资源的获取方面提供互助的协定。

N

连环代理 (Nesting)

委托银行通过其委托的代理银行为其他金融机构提供下游代理服务的做法。代理银行为金融机构提供此类服务时，未对其进行尽职调查。代理银行在为委托银行的客户提供代理银行服务时须遵守一个常规要求，即对该委托银行的反洗钱制度进行增强尽职调查，以便充分规避其“客户的客户”的交易风险。

非政府组织 (Non-Governmental Organization; NGO)

与特定国家的政府没有直接关联的非营利组织，提供各种类型的服务并拥有多种人道主义职能，其中包括：向政府传达公民诉求、拥护某项事业以及提升人们的政治参与度。有些国家针对非政府组织的反洗钱法规仍然存在漏洞，恐怖分子或恐怖分子的同情者可能利用这些漏洞来秘密转移资金。

非营利组织 (Non-Profit Organizations; NPO)

根据司法管辖区和法律制度的不同，非营利组织拥有多种存在形式，包括协会、基金会、筹资委员会、社区服务组织、公益社团、有限公司和公共慈善机构。金融行动特别工作组已为当局提供了一些建议，这些建议有助于对那些为慈善、宗教、文化、教育、社会或友好目的而筹集或提供资金的组织提供保护，使其不被恐怖融资活动者所利用或滥用。

O

离岸 (Offshore)

从字面上看，即某人的祖国之外。如果某人住在欧洲，美国便是其“离岸”所在地。在洗钱专用词汇中，这一术语特指因低税率甚至零税率或严格的银行保密规定而有利于外国投资的司法管辖区。

离岸银行业务许可证 (Offshore Banking License)

批准离岸银行开展银行业务，但其得到许可证的条件是不得与当地居民进行业务往来或以当地货币开展业务。

离岸金融中心 (Offshore Financial Center; OFC)

迎合或以其他方式鼓励银行、贸易公司和其他公司或法律实体在某一司法管辖区实际存在或仅在法律意义上存在，但将其业务限制在该司法管辖区外的“离岸”地区的各类机构。（*参见“离岸 (Offshore)”*）。历史上的离岸金融中心往往位于与美国和欧洲的主要金融中心较近的加勒比海或地中海诸岛。

综合账户 (Omnibus Account)

参见“清算账户”。

经营风险 (Operational Risk)

因内部流程、人员或系统的不足或失败，或因外部事件而造成的直接或间接的经营损失风险。公众认为如果银行不能有效管理其经营风险可能扰乱或危害银行的日常运转。

经济合作与发展组织 (Organization for Economic Cooperation and Development; OECD)

就全球经济中的经济发展问题为政府提供协助的国际组织。金融行动特别工作组的秘书处设在位于巴黎的经济合作与发展组织内。

美洲药物滥用管制委员会（西班牙语：Comisión Interamericana para el Control del Abuso de Drogas; CICAD）

美洲药物滥用管制委员会发布了多项反洗钱建议，其中包括 1992 年发布的美洲国家组织 (OAS) 示范条例修正案。

汇出方 (Originator)

账户持有人或在没有账户存在的情况下任何指示金融机构进行电汇转账的自然人或法人。

P

通汇账户 (Payable Through Account)

外国金融机构在某一储蓄机构开立的交易账户，该外国金融机构的客户可以直接通过该交易账户或通过其子账户开展银行业务与交易，同时该外国金融机构的客户应享有账户资金的直接控制权。这类账户会给开户储蓄机构带来风险，其原因在于，机构很难对最终使用通汇账户进行交易的外国机构的客户进行尽职调查。

实体经营 (Physical Presence)

在其留存业务记录并接受监管的国家中，机构拥有实体位置以及有实际意义的经营管理。仅有当地代理人或低层次员工不构成实体经营。

处置 (Placement)

洗钱过程的第一个阶段：对非法活动所得进行实际处置。

政治公众人物 (Politically Exposed Person; PEP)

根据金融行动特别工作组于 2012 年修订的 40 项建议，政治敏感人物是指在某个国家被赋予重要公共职能的人物，如国家元首、资深政治家、高级政府官员、司法或军事官员、国有企业高管或重要政党官员以及他们的家属和关系密切人员。政治公众人物不包括上述类别中的中级人员。不同国家的法规对政治公众人物这一术语有着不尽相同的定义，既可能指本国人士，也可能指外籍人士。

庞氏骗局 (Ponzi Scheme)

以查尔斯·庞兹 (Charles Ponzi) 命名的洗钱体系。庞兹是一位意大利移民，他通过自己设计的骗局从 4 万人手中骗得 1,500 万美元，此后在美国被判 10 年监禁。他的名字成为用新投资者的资金来清偿先前投资者这一手段的代名词。庞氏骗局虚构根本不存在的虚假投资计划，并通过异常高额的回报承诺来欺骗投资者进行投资。骗局的操控者使用新投资者的资金来清偿先前投资者，直至项目崩盘且 / 或操控者卷走剩余资金逃得无影无踪。

上游犯罪 (Predicate Crimes)

指“特定非法活动”，涉及此类交易的所得可引发洗钱指控。多数反洗钱法律都对此类潜在的犯罪作出了宽泛的定义或罗列出清单。上游犯罪有时被定义为重罪或“刑法典中规定的所有罪行”。

私人银行业务 (Private Banking)

金融机构中为富有客户提供高端服务的部门。私人银行业务交易的特征有：保密性、实益所有权安排的复杂性、离岸投资工具、税收庇护以及信贷延长服务等。

私人投资公司 (Private Investment Company; PIC)

私人投资公司又称个人投资公司，通常是在具有严格保密法律的离岸司法管辖区建立的旨在保护所有人隐私的一类公司。在部分司法管辖区，国际商业公司或免责公司被称为私人投资公司。

金字塔骗局 (Pyramid scheme)

参见“庞氏骗局 (Ponzi scheme)”。

R

危险信号 (Red Flag)

旨在引起人们对潜在可疑情形、交易或活动注意的警示信号。

监管机构 (Regulatory Agency)

负责监督和监管一类或多类金融机构的政府机关。监管机构通常拥有发布规章、执行检查、实施罚款和处罚以及限制活动的权力，有时还能吊销其司法管辖区内机构的执照。多数金融监管机构在洗钱以及其他金融犯罪的防范和侦测方面起着重要作用。大多数监管机构主要监管国内机构，但有些也能够对机构的海外分支机构和业务进行监管。

汇款服务处 (Remittance Services)

汇款服务处又称为货币所或货币兑换处，其业务是收取现金或其他资金并将其通过银行系统转入另外一个账户。该账户由位于其他司法管辖区的关联公司持有，最终收款人可在该管辖区提取资金。

声誉风险 (Reputational Risk)

针对某金融机构业务商业惯例及相关活动的负面新闻（不管准确与否）导致公众对该机构的诚信失去信心的潜在可能性。银行和其他金融机构可能成为客户从事非法活动的工具或受害者，因此特别容易受到声誉风险的影响。此类机构可通过“了解您的客户”和“了解您的员工”制度来保护自己。

委托银行 (Respondent Bank)

接受另一金融机构建立、维持、经营或管理代理账户服务的银行。

风险为本的方法 (Risk-Based Approach)

为了提高反洗钱制度的有效性，对于不同类型的企业、客户、账户和交易相关的各种风险所进行的评估的方法。

S

安全港 (Safe Harbor)

给金融机构及金融机构的董事、高管和员工提供的法律保护。如果他们出于善意向金融情报机构报告可疑情况，即使他们并不知晓潜在犯罪活动的确切信息，也不管违法活动是否真实存在，安全港都将为他们提供法律保护，使其免于承担因违反合同或任何法律、法规和行政禁令关于限制信息披露的规定而引起的刑事或民事责任。

扣押 (Seize)

由主管当局或法院根据资产冻结机制发起的禁止转移、转换、处置或转移资金或其他资产的行动。然而，与冻结不同的是，扣押允许主管当局控制特定资金和其他资产。尽管主管当局通常会占有、经营或管理被扣押的资产，但被扣押的资产仍属于在扣押时对其享有利益的个人或实体。

高级外国政要 (Senior Foreign Political Figure)

用于形容“政治公众人物”的美国术语。*参见“政治公众人物 (PEP)”*。

信托人 (Settlors)

通过信托契约将资产所有权转移给受托人的个人或公司。虽然受托人在信托资产的投资及分配方面拥有一定的自行决定权，但契约可附带一份不具有法律约束力的信件，明确信托人希望的资产处理方式。

空壳银行 (Shell Bank)

仅在名义上存在的银行，在其成立或经营许可国并无实体经营，且不隶属于任何接受全面有效监管的金融服务集团。

拆分洗钱法 (Smurfing)

一种常用的洗钱方法，该方法利用多人和 / 或多项交易存储现金、购买金融票据或银行汇票，但其额度都不超过需要报告的限额。受雇开展此类交易的个人被称为“拆分洗钱人员”。*参见“拆分交易 (Structuring)”*。

卧底行动 (Sting Operation)

一种调查策略，即便衣人员伪装成罪犯，通过“前台”企业等方式赢得疑似或已知犯罪分子的信任，以便收集信息并获取犯罪行为的证据。在洗钱和其他案件中，此类行动是识别犯罪分子、渗入犯罪集团内部以及识别涉案财产的有效手段。

拆分交易 (Structuring)

将现金存款或取款分成若干较小金额，或购买金额低于报告限额的金融票据的非法活动。该做法可能涉及将大笔现金分拆为小笔现金以及分两次或多次进行存款或取款，其总额与原先数额一致。洗钱犯罪分子运用拆分交易来防止金融机构提交报告。这一手段在规定了强制性现金交易报告要求的司法管辖区相当常见。*参见“拆分洗钱法 (Smurfing)”*。

作证传票 (Subpoena)

由法院实施的强制某证人出席某一司法诉讼，有时要求证人提供特定文件的强制性法律程序。这一术语可指强制证人采取行动的法律程序或实际文件。

可疑活动 (Suspicious Activity)

可能与洗钱、其他犯罪或恐怖融资活动相关的异常或可疑的客户行为或活动。也可指与客户的已知合法业务、个人活动或此类企业或账户的正常活动不匹配的交易。

可疑活动报告 (Suspicious Activity Report; SAR)

参见“可疑交易报告 (Suspicious Transaction Report)”。

可疑交易报告 (Suspicious Transaction Report; STR)

包含金融机构对可疑交易进行的解释且由报送机构要求提交的政府报告。很多司法管辖区要求金融机构通过可疑交易报告向有关政府机构（如金融情报机构）报告可疑交易，这一报告又被称为“可疑活动报告”或 SAR。

T

避税天堂 (Tax Haven)

为外国投资者和存款人提供特殊税收激励或避税机制的国家或地区。

恐怖融资 (Terrorist Financing)

恐怖分子为开展恐怖活动融通资金的过程。恐怖活动融资的资金来源主要有两种：一种是来自国家、组织或个人的资金支持；另一种则涉及多种获利活动，其中包括走私和信用卡诈骗等非法活动。

证词 (Testimony)

证人对所知事实的口头陈述，通常需要经过宣誓。

泄露消息 (Tipping Off)

通知嫌疑人其已被列入可疑交易报告或正被当局调查或追捕的不当或非法行为。

贸易金融 (Trade Finance)

参见“信用证 (Letter of Credit; L/C)”。

透明国际 (Transparency International; TI)

总部设在柏林，致力于增加政府责任感并遏制国际和国内腐败的非政府组织。成立于 1993 年，现已在近 100 个国家积极开展活动。该组织每天在其网站上发布“腐败新闻”并提供与腐败有关的新闻报道和报告。透明国际拥有的“腐败在线研究和信息系统”(CORIS) 可能是全球最为全面的反腐数据库。透明国际发布的年度“清廉指数”(CPI) 享誉全球，该指数根据官员的腐败水平对各国进行排序；“行贿指数”(BPI) 则根据行贿倾向对主要出口国家进行排序。透明国际的年度《全球腐败报告》将清廉指数 (CPI) 和行贿指数 (BPI) 结合起来，根据整体腐败水平对各国进行排序。该排序可以帮助金融机构确定特定司法管辖区的风险情况。

信托 (Trust)

财产所有人（让与人）、受益人和财产管理人（受托人）之间的一种合约安排。基于这一安排，受托人应根据让与人设定的条款出于受益人的利益对资产进行管理。

受托人 (Trustee)

可以指领取薪酬的专业人员或公司，也可以指持有信托基金中其自身资产以外资产的不支薪个人。受托人根据信托人的信托契约对资产进行投资和处置，另外还必须兼顾信托人的意向书。

类型 (Typology)

金融行动特别工作组的术语，指洗钱方法。

U

最终受益所有人 (Ultimate Beneficial Owner; UBO)

参见“受益所有人 (Beneficial Owner)”。

地下钱庄 (Underground Banking)

参见“替代性汇款体系 (Alternative Remittance System)”。

联合国 (United Nations; UN)

成立于 1945 年，由 51 个创始国组成的旨在通过合作和集体安全来维护世界和平的国际组织。如今，全世界几乎所有国家都已成为联合国的成员国。*参见“《维也纳公约》(Vienna Convention)”*。联合国致力于打击有组织犯罪，它倡导的“全球反洗钱计划”(GPML) 是联合国毒品控制与犯罪预防办公室的重要工具。联合国通过全球反洗钱计划帮助成员国出台反洗钱立法，发展各种反洗钱机制以打击洗钱犯罪。该计划鼓励反洗钱政策的制定，对出现的问题及应对方式进行监控和分析，努力提高公众关于洗钱的意识并在联合国与其他国际组织间的联合反洗钱行动中发挥着协调作用

联合国安理会第 1373 号决议 (2001) (UN Security Council Resolution 1373 (2001))

联合国安理会于 2001 年通过的要求成员国通过制定法律法规及建立行政管理机构等一系列行动来打击恐怖主义的决议。决议同时要求各成员国“在与资助或支持恐怖活动相关的刑事调查或刑事诉讼方面，相互提供最大限度的协助”。

异常交易 (Unusual Transaction)

规避报告要求、与账户交易模式不符或偏离该类账户预期活动类型的交易。

美国《爱国者法》(USA PATRIOT Act)

即《2001 年团结和强化美国通过提供适当方法以截断和阻止恐怖主义法》（公法 107-56）。这项具有历史意义的美国法案于 2001 年 10 月 26 日开始实施，给反洗钱领域带来了巨大变化，其中包括对《银行保密法》进行的 50 余项修订。该法案第 3 篇，即 2001 年《国际反洗钱和反恐融资活动法》涵盖了大多数与洗钱相关的条款，但并非全部。

V

价值转移服务 (Value Transfer Service)

参见“资金转账服务 (Money Transfer Service)”。

《维也纳公约》(Vienna Convention)

即 1988 年《禁止非法贩运麻醉药品和精神药物公约》。该公约的签约国致力于对毒品走私以及相关洗钱活动进行定罪并颁布没收走私毒品非法所得的措施。公约第 3 条对洗钱的全面定义已成为后续全国性立法的基础。

虚拟货币 (Virtual Currency)

虚拟货币是数字领域的交换媒介，通常可兑换为法定货币（如政府发行的货币）或用于替代真实货币。

W

有意忽视 (Willful Blindness)

美国在处理洗钱案件时适用的法律原则，法院将其定义为“有意回避明知的事实”或“故意放任”。这些法院认定，有意忽视即等同于切实明知资金的非法来源或洗钱交易中客户的意图。

电汇 (Wire Transfer)

金融机构之间代表己方或其客户进行的资金电子化转移。在反洗钱领域，很多国家或地区都针对电汇这一金融工具制定了监管要求。

沃尔夫斯堡集团 (Wolfsberg Group)

沃尔夫斯堡集团以其在瑞士召开首次工作研讨会时的沃尔夫斯堡城堡命名，是一个全球金融机构协会，成员包括西班牙国际银行、美国银行、东京三菱银行、巴克莱银行、花旗银行、瑞士信贷集团、德意志银行、高盛、汇丰银行、摩根大通、法国兴业银行、渣打银行以及瑞银集团。2000 年，成员机构与透明国际和全球专家共同制定了针对国际私人银行的全球反洗钱指南。此后，该集团还发布了多份与代理银行业务和恐怖融资活动等问题相关的指南。

世界银行 (World Bank)

世界银行是发展中国家获得金融和技术援助的重要来源。世界银行并不是通常意义上的银行，它由 184 个成员国所共同拥有的两大独特开发机构组成，即国际复兴开发银行 (IBRD) 和国际开发协会 (IDA)。这两个组织均向发展中国家提供低息贷款、无息贷款和赠款。2002 年，国际货币基金组织和世界银行发起了一个为期 12 个月的试点项目，对各国反洗钱和反恐融资活动的措施进行评估。世界银行、国际货币基金组织与金融行动特别工作组共同制定了一套基于金融行动特别工作组 40 项建议进行评估的通用方法。

备注：

第 6 章

练习题

本章练习并不反映 CAMS 的真实题量和题型，而是旨在帮助应试人员复习考试手册中的内容。

1. 下列选项中，哪一项是通过合法金融服务企业进行洗钱的最常用方法?

   A. 通过拆分交易购买货币金融工具。

   B. 走私大量现金。

   C. 通过通汇账户 (PTA) 进行转账。

   D. 在黑市兑换哥伦比亚比索。

2. 通常，洗钱分为三个阶段：处置、_____?

   A. 拆分交易和操纵。

   B. 离析和融合。

   C. 离析和拆分洗钱。

   D. 融合和渗透。

3. 下列选项中，哪一项是正确的?

   A. 破产骗局在大额破产欺诈案中很常见，企业不断增加贷款直到贷款总金额超过了其公司或财产的实际价值，然后携款潜逃，使得贷方产生呆账、坏账，从而蒙受巨额损失。

   B. 布谷鸟式拆分洗钱法是反洗钱金融行动特别工作组所确认的一种重要洗钱手段，即通过位于保密庇护所的空壳银行所开立的连环账户进行拆分交易。

   C. 金融行动特别工作组 (FATF) 在其 40 项建议中发布了可指控洗钱犯罪的“特定犯罪类型”清单。

   D. 电子货币对于洗钱者不具备吸引力，是因为它无法完全匿名，并且不允许大额资金“快速且容易地进行转移”。

4. 下列哪三种情形是保险行业可能存在洗钱的行为手法?

A. 通过中介、代理商或经纪商销售保险产品。

B. 折价赎回整付保费的保险债券。

C. 保单持有者不关心因提前撤销保单而造成的损失。

D. 保单持有者在“保单撤销期”内赎回保单。

5. 下列哪两个选项通常与黑市比索交易 (BMPE) 洗钱体系相关?

A. 将毒品交易的非法所得从美元或欧元兑换成哥伦比亚比索。

B. 将毒品交易的非法所得从哥伦比亚比索兑换成美元或欧元。

C. 通过比索经纪人为购买美国或欧洲生产的产品的哥伦比亚进口商提供便利。

D. 通过比索经纪人为购买哥伦比亚生产的产品的欧洲进口商或美国进口商提供便利。

6. 在打击洗钱犯罪的国际合作领域中，“互惠权”是指:

A. 它是一种法律原则，当一家金融机构在向其他金融机构推荐其客户时，允许该家金融机构与其他这些金融机构共享客户信息。

B. 巴塞尔委员会的一条规定，允许该委员会其他成员国中接受妥善监管的金融机构在授予相同权利的另一国开展业务时无需接受额外监管。

C. 金融行动特别工作组 (FATF) 成员国有权将一起洗钱案件转交给已经在调查同一案件的另一成员国调查及起诉。

D. 它是一种法律原则，在双边法律允许的情况下，一国当局可以与另一国当局在适当法律范围内开展合作。

7. 对于赌场来说，最大的洗钱风险在于:

A. 为客户提供各类赌博服务。

B. 在非埃格蒙特集团成员国内进行运营。

C. 允许拥有贷方余额的客户在另一司法管辖区内使用支票提取资金。

D. 只能向其经营地所在国的金融情报机构发送可疑交易报告。

8. 下列关于政治公众人物 (PEP) 的选项中，哪一项是正确的?

A. 政治公众人物可与金融机构尚未开展充分尽职调查的第三方发生联系。

B. 政治公众人物获得政治腐败资金（包括受贿或挪用政府资金）的可能性很大。

C. 当政治公众人物为外国客户时，他们参与的跨境交易将会面临更大的风险。

D. 鉴于政治公众人物的政治地位，他们不会对机构造成更大的风险；相反，他们还会提升机构的声望。

9. 2014 年，沃尔夫斯堡集团发布了《代理行反洗钱原则》。该原则建议在对代理行客户进行尽职调查时，应包含以下哪三项内容?

A. 地理风险。

B. 所有权结构和管理层结构。

C. 合规专员履历。

D. 客户群。

10. 一名到银行开立商业账户的新客户。该客户提供的开户地址与该支行所在地相距甚远。当客户代表问及是否需要其他银行服务时，该客户表示有兴趣开立一个个人投资账户。于是该客户代表将客户推荐给了他们的经纪自营商。该客户向公司代表表明此前自己从未持有经纪账户，然后客户针对投资账户如何进行操作咨询了一些问题。客户提出的问题包括：如何将钱存入她的账户，是否存在任何的交易报告要求，以及如何使用电汇将账户余额转出。但对账户的交易费用问题却置之不问。下列选项中，哪三项属于可疑行为?

A. 客户提出多个关于经纪账户的问题，但都与投资无关。

B. 客户在开立商业账户的同时开立个人投资账户。

C. 账户持有人的地址和客户开立账户的分行相距甚远。

D. 客户似乎不关心费用。

11. 贸易洗钱具备哪些能力：

A. 高开商品发票或低开商品发票。

B. 尽可能少地销售进口货物。

C. 利用无需申报的货物。

D. 避免利用豪华轿车或豪华游艇之类的高价值资产。

12. 下列选项中，哪一项是正确的？在哪种情形下，代理行业务最容易被洗钱分子利用：

A. 为银行类外国金融机构持有代理账户。

B. 不直接向第三方提供代理账户服务。

C. 在任何国家都没有实体经营的外国银行，为其持有代理账户。

D. 为作为中介机构的外国上市私人银行持有代理账户。

13. 下列选项中，哪一项是正确的？律师：

A. 在金融行动特别工作组成员国中，一般不能为那些设立信托的公司、前台公司或空壳公司创建代理。

B. 与类似的专业“守门人”一起被称为金融服务企业。

C. 一般不能担任受益所有人的代名股东。

D. 可以被洗钱分子利用，为他们开立账户来处置与离析资金。

14. 下列关于欧盟第四号反洗钱指令的选项中，哪三项是正确的？

A. 成员国可自行决定是否将其纳入本国法律以及纳入的时间。

B. 该指令替换并废除了欧盟第三号反洗钱指令。

C. 该指令规定受益所有人应直接或间接至少拥有公司 25% 的所有权。

D. 将国内政治公众人物纳入政治公众人物定义的范畴。

15. 根据欧盟指令的规定，在下列哪种情形下，独立的法律专业人员有义务报告委托人关系中存在的可疑洗钱行为：

A. 在法律事务中担任客户的代表。

B. 确认客户的法律地位。

C. 参与金融交易或公司交易。

D. 获取与司法程序相关的信息。

16. 对于与美国存在代理银行业务关系的外国金融机构来说，以下哪一项是最难应对的监管挑战？

A. 美国《爱国者法》。

B. 《巴塞尔委员会银行尽职调查原则》。

C. 《FATF 反恐融资活动指南》。

D. 联合国安理会关于代理银行业务的决议。

17. 巴塞尔委员会在《银行客户尽职调查白皮书》中鼓励建立严格的“了解您的客户”制度，此举的两大主要动机是什么？

A. 反映金融行动特别工作组的了解您的客户建议

B. 满足欧盟指南的要求。

C. 保障银行业的安全和稳健发展。

D. 保护银行系统的整体性。

18. 上游犯罪的定义是什么？

A. 存在“有意忽视”和国际性犯罪因素，可能引发可疑交易报告的合法行为或非法活动。

B. 涉及交易的不法所得，可能导致洗钱犯罪指控的非法活动。

C. 作为可疑交易监测系统的基础部分的一个结合点。

D. 通过集中账户来欺骗与该账户并无直接关联的客户的特定非法活动。

19. 下列哪一项是受益所有人或受益账户？个人或实体：

A. 对账户具有直接签名权限，名字或名称出现在该账户上的个人或实体。

B. 即使其名字可能没有出现在账户上，但最终获得账户资金的个人或实体。

C. 账户内多数（并非全部）交易的汇出方和接受方，但并非是最终控制资金的个人或实体。

D. 对账户拥有合法所有权的守门人，往往将资金转账到信托基金的个人或实体。

20. 美国金融犯罪执法网络于 2014 年发布的“美国金融机构合规文化推动公告”中列出了六大重要事项。下列哪三项属于该六大事项的内容：

A. 领导层应参与其中。

B. 应当在整个机构共享信息。

C. 领导层和员工应明白他们的银行保密法报告该如何使用。

D. 机构必须配备一名有胜任资格的合规专员。

21. 在根据加勒比地区金融行动特别工作组 (CFATF) 19 项建议将洗钱定为犯罪时，国内立法应考虑以下哪三个因素？

A. 不限定特定的洗钱上游犯罪的数量。

B. 将洗钱同谋或参与洗钱的人定为犯罪。

C. 指出如果上游犯罪发生在当地司法管辖区外时，洗钱能否入罪。

D. 判定洗钱犯罪时，应证明犯罪者已了解该资金与犯罪行为的相关性。

22. 下列关于欧盟第四号反洗钱指令的选项中，哪三项是正确的？该指令：

A. 确保欧洲共同体的立法与反洗钱金融行动特别工作组 40 项建议保持一致。

B. 政治公众人物的定义与之前的指令相同。

C. 有关客户尽职调查的要求与之前的指令相同，但增加了更多的细节要求，如：识别该受益所有人这一特定要求，以及持续监控的要求。

D. 在基于风险的基础上，该指令要求公司在适当时机对存量客户进行客户尽职调查。

23. 下列关于金融行动特别工作组 (FATF) 40 项建议对各国要求的选项中正确的是：

A. 不允许不记名股票的发行以及发行不记名股票的法人的存在。

B. 收集有关可疑交易报告的数据；检控和定罪；财产冻结、扣押和没收；以及司法互助的统计数据，但并不一定根据国际合作的请求而收集数据。

C. 针对银行和其他金融机构以及中介机构，考虑在其不设最低固定金额的情况下报告现金交易的体系是否可行。

D. 不批准设立空壳银行或不允许其持续经营。

24. 埃格蒙特集团于 2001 年 6 月 13 日发布的《金融情报机构间洗钱案件信息交换原则》中包含以下哪一项内容?

A. 信息交换协议必须遵照埃格蒙特集团发布的范本。

B. 按照协议要求共享的信息不会受到各国隐私权法律的管辖。

C. 金融情报机构间的信息交换仅用于为寻求或提供该信息为特定目的。

D. 要求获取信息的金融情报机构可在未经提供信息的金融情报机构事先同意的情况下，将信息用于行政目的。

25. 将小额现金存入几个相关账户的行为属于洗钱的哪一阶段?

A. 融合。

B. 拆分交易。

C. 处置。

D. 构建。

26. 使用被清洗的资金购买高价值资产和奢侈品的行为属于洗钱的哪一阶段?

A. 融合。

B. 拆分交易。

C. 处置。

D. 构建。

27. 大部分将洗钱定为犯罪的法律都有如下规定:

A. 除非政府将某一客户列入严格审查名单,否则金融机构无需对该机构账户内的洗钱或可疑交易负责。

B. 告知客户其账户和 / 或交易正在接受反洗钱调查，这样的行为将不会受到惩罚。

C. 由于隐私权法律的存在，参与洗钱的脏钱不得被没收。

D. 机构须识别账户的受益所有人。

28. 个人通过多笔小额存款来逃避侦测的手段被称为:

A. 平行。

B. 融合。

C. 投资。

D. 拆分交易。

29. 以下哪种情形下无需提交可疑交易报告?

A. 客户使用来源可疑的资金进行存款且拒绝回答金融机构工作人员的提问。

B. 客户试图转移疑似来自犯罪活动的资金。

C. 开设大型超市的某客户每天进行几次大额现金存款。

D. 客户账户显示的交易活动与其已知的财务能力不符。

30. 在打击洗钱方面，金融机构应：

A. 指定一名合规专员。

B. 仅仅依靠国家工作人员来打击洗钱。

C. 拒绝接受低于报告限额的小额现金存款。

D. 拒绝为来自高风险司法管辖区的人员开立账户。

31. 一位初级合规分析人员在与一位计算机运营部门的友人共进午餐时了解到，上周，传送至交易监控应用程序的数据出现了问题。友人认为这纯粹是一个电脑系统问题，所以认为自己能在当天早上及时解决此问题，并为此而颇感自豪。该分析人员应采取哪些行动？

A. 祝贺友人及时解决了问题。

B. 祝贺友人，并尽快通知合规专员要注意这种情况。

C. 无需采取任何措施，因为已经有针对此类事件的适当应对措施。

D. 立刻向监管机构汇报。

32. 有意忽视的定义是：

A. 在与来自离岸避税庇护的公司或金融机构进行交易时未能提交可疑交易报告。

B. 未按照机构规定的程序执行客户身份识别程序。

C. 有意回避明知的事实或忽视明显的洗钱危险信号。

D. 鉴于客户行为反映出其可能为洗钱人员或恐怖分子这一推测而有意回避该客户。

33. 在反洗钱术语中，“危险信号”是指：

A. 预示有潜在的可疑交易、风险交易、风险活动的警示信号。

B. 在结余为负或逾期未付款时使用的银行业一般术语。

C. 在打击洗钱和恐怖融资活动领域，不合作国家的标准信号。

D. 显示客户被列入经济制裁名单。

34. 金融机构的反洗钱报告专员应：

A. 将机构人员提交的所有信息进行报告。

B. 将高级管理层和董事会提交的所有信息进行报告。

C. 针对所有异常或潜在可疑的活动，审查所有相关信息，并提交可疑交易报告。

D. 报告专员仅报告上级所同意报告的内容。

35. 下列选项中，哪一项是正确的?

A. 由于现金支付方面的限制，信用卡不太可能用于洗钱的离析阶段。

B. 由于信用卡交易不会留下审计线索，所以信用卡是有效的洗钱工具。

C. 洗钱者可通过以下方法进行洗钱：使用银行的资金预付信用卡，在其账户中创建贷方余额，然后申请信用卡退款。

D. 洗钱者可使用事先投入银行的非法资金来支付因购买商品所产生的信用卡账单，这就是一个处置的示例。

36. 为何通汇账户容易被洗钱者利用?

A. 对最终使用这些账户进行交易的外国机构客户，进行尽职调查的难度很大。

B. 这些账户是外国银行的当地分行所开立的集中账户。

C. 这些账户是客户在外国空壳银行的连环代理账户，国内银行无法对客户进行尽职调查。

D. 国内银行通常无法对这些主要托管账户进行定期核查。

37. 落实“以风险为本的反洗钱方法”其背后的原因是?

A. 该方法协助监管人员关注银行以外行业的反洗钱控制措施。

B. 机构可充分利用有限的资源，关注洗钱风险最高的领域。

C. 定量方法比定性方法更为有效。

D. 该方法允许机构关注那些销售投资回报率更高的产品。

38. 根据金融行动特别工作组 (FATF) 40 项建议的规定，“特定非金融行业”包括：

A. 赌场、房地产经纪商和宝石经销商。

B. 金融服务企业、守门人和电子货币发行商。

C. 贵金属经销商、律师和商品期货交易商。

D. 人寿保险公司、房地产经纪商和公证员。

39. 根据金融行动特别工作组 (FATF) 40 项建议，金融机构应对客户的一次性金融交易识别的限额为：

A. 5,000 欧元 / 美元。

B. 10,000 欧元 / 美元。

C. 15,000 欧元 / 美元。

D. 20,000 欧元 / 美元。

40. Tom 是 ABC 银行的合规专员。他正监控着支票兑现公司所有人 Brown 先生的交易。在过去的六个月中，Brown 先生在支票账户中未提取任何现金。他还存入了两张由赌场签发的支票，金额分别为 2000 美元。Tom 在核查了解您的客户文件时发现，在开立账户时，Brown 先生要求银行提供费用和佣金方面的详细信息。下列哪一情形最应引起 Tom 的怀疑？ Brown 先生：

A. 存入来自赌场的支票。

B. 未在支票账户中提取任何现金。

C. 对所收取的佣金和费用表现出不寻常的好奇心。

D. 没有托管账户。

41. 一家小型经纪自营商制定了处理可疑交易报告提交程序的反洗钱合规制度，其中包括用于客户身份识别、账户监控和识别洗钱危险信号的政策、程序和内部控制措施。该经纪自营商的每位员工分别于 1 月和 7 月通过互联网接受反洗钱方面的培训。董事会成员没有接受互联网培训。合规专员为董事会成员组织了一次午餐会并邀请外部人员对其进行培训。该制度规程对合规专员的任命有所规定，并要求合规专员进行年度审计以测试该制度规程。该制度规程在哪一方面还需改进?

A. 反洗钱制度规程应由独立人士而非合规专员进行测试。

B. 反洗钱制度规程的测试每年至少两次。

C. 董事会成员应接受与员工相同的培训。

D. 员工不应该通过互联网接受培训，因为课堂培训的效果更佳。

42. Susan 是 XYZ 银行的高级反洗钱报告专员。她正密切关注几个客户的活动。下列哪一情形最应引起她的怀疑?

A. 在当地，该客户拥有多家支票兑现的公司，且该客户在不同的支行租用银行的保管箱。

B. 客户拒绝休假。

C. 小型企业提供的财务报表不是由会计师事务所编制。

D. 客户参与的投资管理项目，项目所承诺的投资回报率极高，大大高于其他的竞争对手。

43. 下列关于“替代性汇款体系”的选项，哪一项最为准确?

A. 在合法的银行系统外，进行的跨境价值转移。

B. 非电子数据汇兑系统在其他一些国家和地区被用来报告可疑活动。

C. 通常用于不合作国家和地区的旧式报告要求。

D. 在两个或多个金融机构间使用集中账户进行资金转移。

44. 在审查 XYZ 银行客户的过程中，一名客户（Sam Tropicana 先生）引起了反洗钱合规专员的注意。他在几个月的时间里，他通过其账户完成的现金存取金额在 7500 美元至 17000 美元之间。此外，Sam 还存入了两张由赌场签发的支票，金额分别为 32000 美元。在开立账户时，Sam 声称其经营的是一家进出口公司。下列哪一种情形最应引起反洗钱合规专员的怀疑?

A. Sam 同时拥有个人账户和企业账户。

B. Sam 的家庭电话上个月停用。

C. Sam 申请信用证用来向新供应商支付进口货物的货款。

D. Sam 为其进出口企业进行大额现金交易。

45. 下列选项中，哪三项是正确的?

A. 在线赌博为洗钱提供了绝佳的方法，因为这一交易通常由信用卡或借记卡完成且网站通常为不受监管的离岸企业。

B. 金融机构能够了解信用卡被用于在线赌博交易的情形，因为信用卡凭借代码可以显示交易的类型。

C. 在线赌博为洗钱提供了绝佳的方法，因为其接受任何类型的现金流动且与客户没有面对面的接触。

D. 部分银行不再允许将信用卡用于在线赌博交易。

46. 下列选项中，哪一项是正确的?

A. 埃格蒙特集团由各国国家金融情报单位组成。

B. 沃尔夫斯堡集团由十国集团各国中央银行行长组成。

C. 欧盟建议在成员国间通过立法。

D. 巴塞尔委员会对不遵守反洗钱法规的成员国处以罚金。

47. 下列哪三个选项是《爱国者法》第 313 节关于空壳银行的“实体经营”的定义?

A. 拥有一个固定的经营场所。

B. 至少聘用了一名全职员工。

C. 董事会的多数成员必须为当地居民。

D. 在固定场所保存银行记录。

48. 在年度洗钱类型报告中，金融行动特别工作组 (FATF) 一直关注利用赌场进行洗钱的手法。以下哪一项是涉及赌场洗钱的手段:

A. 要求获得以第三人为收款人或收款人为空白的奖金支票。

B. 通过利用赌场来规避守门人。

C. 使用提前汇入赌场体系的资金预付赌场筹码，创建一个借方余额。

D. 通过赌场内的多种游戏项目进行大量赌博。

49. 反洗钱师应在内部调查日志中包含以下哪项内容?

A. 因客户未能支付子女抚养费而要求扣押其工资的政府命令。

B. 对于拒绝向信用评级不良的客户提供服务的支持文件和材料。

C. 记录异常活动，但反洗钱师未就该活动提交可疑交易报告。

D. 向公司企业管理层提交的与预算和其类似问题相关的谅解备忘录。

50. 在反洗钱风险评级中的三大关键指标是?

A. 客户类型、地理位置、使用的产品和服务。

B. 地理位置、客户类型、就业情况。

C. 使用的产品和服务、客户类型和此前的银行关系。

D. 就业情况、客户类型、使用的产品和服务。

51. 一家金融机构正准备建立在线账户开立服务。该机构计划向该国境内的新客户和现有客户提供此产品。为确保机构能够核查客户身份，下列哪一项是反洗钱师应该建议的最佳行动方案?

A. 不提供该产品，因为无法当面核实客户身份，存在极高的风险。

B. 要求所有客户向机构发送附有照片的有效身份证明副本。

C. 确保机构可以通过可靠的第三方来核查客户身份。

D. 允许客户输入必要的信息，但要求所有客户需亲临机构进行身份核查。

52. 以下哪项控制措施可以最为有效地在客户开立账户流程中收集所需的客户信息?

A. 安排有资质的审查人员核查书面申请，确保所有栏位均填写完整。

B. 建立自动账户开立平台，要求客户在开立账户前录入资料数据。

C. 要求主管审查并批准所有新开账户的申请。

D. 制定一套程序，规定开立账户所需的步骤程序。

53. 在为负责账户开立工作的员工进行反洗钱培训时，下列哪项是培训中需要考虑的最为重要的因素?

A. 员工需要完成的反洗钱程序、反洗钱工作的重要性以及违反法律法规可能导致的处罚。

B. 政府的反洗钱机构、员工需要完成的反洗钱程序以及反洗钱工作的重要性。

C. 违反法律法规可能导致的处罚、政府的反洗钱机构以及员工需要完成的反洗钱程序。

D. 反洗钱工作的重要性、政府的反洗钱机构以及违反法律法规可能导致的处罚。

54. 在起草反洗钱政策时，下列哪一个内部机构在政策的批准过程中显得最为重要?

A. 高级管理层。

B. 审计部门。

C. 销售团队管理层。

D. 运营人员管理层。

55. 机构反洗钱合规专员 Suzy 正考虑为代理银行客户提供资金管理服务（如电汇、支票清算、外币汇票的签发等服务）。在该机构应对此类客户的能力方面，苏茜最应关注下列哪一项?

A. 新的账户系统是否能够处理这些外国客户。

B. 代理账户是否能够获得政府监管方的批准。

C. 代理账户能否在开立时提供与客户身份信息相关的证明。

D. 代理账户是否能够接受银行监控系统的监控。

56. 下列哪三项属于恐怖融资特有的方式?

A. 绑架并勒索赎金

B. 人口贩运

C. 慈善组织捐赠

D. 国际电汇

57. 一名客户希望与金融机构建立紧密且长远的业务关系。反洗钱专员对客户关于资金来源的解释不太满意，但客户经理却愿为该客户提供担保并急于与其建立业务关系。反洗钱专员为了验证客户的资金来源，应该要做哪些工作?

A. 接受客户经理对该客户的审批。

B. 允许开立账户，但应确保对账户活动进行监控。

C. 通过背景调查确定客户的资金来源是否可靠。

D. 拒绝为其开立账户。

58. 一名反洗钱合规专员正在对其发现的客户账户中的异常活动进行调查。该客户拥有退休金账户、以其子为受益人的信托储蓄账户、与其妻联名的支票账户、公司支票账户以及个人经纪账户。合规官员认为该客户可能从企业中挪用公款。下列哪一项是追查其怀疑事项的最佳途径?

A. 关注支票账户，因为支票账户的资金转移速度最快。

B. 对于储蓄和经纪账户置之不理，因为这两种账户通常不用于洗钱的处置阶段。

C. 关注所有账户的资金动向，因为客户可能使用所有的账户进行洗钱。

D. 关注企业账户，因为客户正从公司挪用公款。

59. 个人因违反反洗钱法规需面临的三大风险。

A. 民事处罚

B. 终止雇佣关系

C. 刑事处罚

D. 被剥夺护照

60. 一名客户在经纪公司表示，自己是属于保守型的长期投资者。该客户最近参与了低价股票的日间交易。在这一情形下，反洗钱合规专员应该怎么做?

A. 与客户专员核实，确定该客户是否曾表明要在投资策略上有所改变。

B. 根据投资低价股票的事实将客户作为可疑对象进行报告。

C. 联系客户，询问其为何参与高风险的日间交易活动。

D. 将客户提交给高级管理层进行审批。

61. 一名入职十余年的金融机构支行经理近四年都没有休假。该公司不允许员工逐年累积休假。一名反洗钱合规专员注意到该支行的几个账户都存在异常活动。反洗钱专员应该做些什么?

A. 由于员工不休假是一种危险信号，所以应坚持要求该经理休假。

B. 向当局报告该经理涉嫌参与可疑活动。

C. 确定该经理是否参与了发生异常账户活动的交易。

D. 通过背景调查确定该经理是否参与犯罪活动。

62. 一名反洗钱合规专员希望在其小型机构中建立可疑活动报告流程。以下哪一项是最佳行动方案?

A. 允许员工尽快向政府当局直接报告可疑活动。

B. 要求员工向内部独立的审计部门反映所有异常活动，从而评估该活动是否需要报告。

C. 要求员工向高级管理层反映所有异常活动，从而确保高级管理人员知道机构内的所有异常活动。

D. 要求员工向自己反映所有异常活动，从而确保其就需要向当局进行报告的内容开展调查。

63. 在向有关当局报告可疑活动后，当局要求提供与报告相关的后续资料，反洗钱合规专员应采取以下哪一项措施?

A. 通知客户，说明其活动已被作为可疑活动上报且相关当局正就其进行询问。

B. 告知当局，在将可疑事项上报当局后，您的监管任务已经完成。

C. 提供当局要求提供的一切资料。

D. 在法律允许的范围内与当局进行密切合作。

64. 一名合规专员希望改进一家在多个国家开展业务的金融机构的合规制度。对于超出各国限额的所有客户，该机构制定了统一的客户尽职调查 (CDD) 标准要求。在提交机构客户尽职调查合规工作管理报告时，以下哪一项最合理?

A. 报告每个国家遵守其国内法律要求的情况。

B. 报告遵守并符合公司规定要求的合规情况。

C. 对于接受多个国家分支机构服务的客户，报告其对各国合规要求的遵守情况；对于其余客户，报告其对公司规定要求的合规情况。

D. 报告对于帐户活动进行监控的水平情况。

65. 将合规作为金融机构每位员工的重要责任的最佳途径是什么?

A. 高级管理层要求将合规作为雇用条件。

B. 审计师对员工的合规情况进行测试。

C. 在培训中指出违反法律法规可能造成的监管后果。

D. 反洗钱专员亲自告知员工其责任所在。

66. 巴塞尔委员会 2015 年发布了《账户开立咨询文件通用指南》，该指南列出了确认“法人”时需获得的信息。下列哪三项内容是建议确认的信息?

A. 该法人的名称、法律公司形式、状态及注册证明。

B. 该法人主要活动场所的永久地址。

C. 客户专员对走访主要经营活动场所进行的报告。

D. 确认有权操作账户的自然人身份，即能通过所有权等方式控制该法人的自然人身份。

67. Robert 是一家金融机构的合规专员。他希望评估当前反洗钱制度的有效性。在评估制度有效性的过程中，Robert 应考虑以下哪些因素？

A. 销售人员的反洗钱工作调查、客户尽职调查的错误率、可疑交易报告中的质量保障测试。

B. 客户尽职调查的错误率、销售人员的反洗钱工作调查、能够接受可疑活动监控的产品和服务比例。

C. 可疑交易报告中的质量保障测试、销售人员的反洗钱工作调查、能够接受可疑活动监控的产品和服务比例。

D. 客户尽职调查的错误率、可疑交易报告中的质量保障测试、能够接受可疑活动监控的产品和服务比例。

68. 小型银行的合规专员 Joe 注意到，最新法规规定超过特定限额的跨境交易需要报告。为了帮助该银行应对最新的监管要求，乔需要采取的后续步骤有哪些？

A. 咨询监管人员、向相关合作伙伴提供培训并与技术合作伙伴合作发现所有需要报告的跨境交易。

B. 向相关合作伙伴提供培训、与技术合作伙伴合作发现所有需要报告的跨境交易并实施测试计划以确保发现并报告符合条件的交易。

C. 与技术合作伙伴合作发现所有需要报告的跨境交易、实施测试计划以确保发现并报告符合条件的交易。

D. 实施测试计划以确保发现并报告合适的交易、向相关合作伙伴提供培训并咨询监管人员。

69. 在对培训工作持续记录时，应记录以下哪一项以证明已对相关员工进行了培训。

A. 是否向董事会成员提供培训。

B. 培训讨论的议题。

C. 参与培训的员工姓名和员工所从事工作的领域。

D. 参与培训的员工是否通过培训后的评估。

70. 在评估新产品时，下列哪项应成为反洗钱评估的一部分？

A. 产品的固有风险、降低产品风险的控制环境以及产品在控制措施方面的剩余风险。

B. 降低产品风险的控制环境、产品在控制措施方面的剩余风险以及产品的预期盈利性。

C. 产品的预期盈利性、降低产品风险的控制环境以及产品的固有风险。

D. 产品在控制措施方面的剩余风险、产品的固有风险以及产品的预期盈利性。

71. 金融机构的合规专员 Marie 参加年度反洗钱行业会议并了解到新实施的法规会对其当前的反洗钱流程产生影响。数年来，该行业的监管环境一直相对稳定，但 Marie 很高兴能够在会议上了解到最新要求的相关信息。为了面对并符合将来监管要求的变化，Marie 应该做些什么?

A. 请求在未来获得参加年度反洗钱行业会议的机会。

B. 要求内部审计师提供制度所需变动的通知。

C. 实施流程，确定新法规的发布时间并评估新法规对反洗钱制度的影响。

D. 开展风险评估，根据法规的变动频率确定是否需要实施用于检查法规变动的工作流程。

72. 一名合规专员希望通过某种方式向高级管理层报告反洗钱制度的有效性。以下关于向高级管理层报告反洗钱工作进展的方法中，哪一项最为合适?

A. 撰写报告，其中包含可以反映各类关键制度因素有效性的指标。

B. 依靠内部审计报告和监管检查。

C. 提供所有已上报可疑活动的概要。

D. 针对高级管理层的反洗钱义务为其提供详尽的培训。

73. 金融机构的内部审计部门发现反洗钱流程中的一个问题，即反洗钱专员对机构某些产品未能实施足够的账户监控。反洗钱合规专员应该怎么做?

A. 鉴于独立审计部门发现了问题的存在，就应由该部门进行纠正，问题的处理与合规部门无关。

B. 与审计部门争论，因为合规专员有充分的权力对机构内所有与反洗钱相关的问题作出决策。

C. 制定并遵循用于纠正问题的实施计划，并向审计部门报告在该问题上取得的进展。

D. 将问题提交给账户开立团队并由其作出合适的商业决策。

74. 金融行动特别工作组 (FATF) 40 项建议共分为七大部分。下列选项中，哪三项是这七大部分的标题?

A. 洗钱和没收。

B. 金融机构和非金融机构的防范措施。

C. 主管部门的权力、职责以及其他指令性措施。

D. 各国间的合作。

75. 银行的一位长期客户在几星期内多次进行大额存款，并在次日要求将资金电汇至第三世界国家。该行为与其正常的商业活动不符。合规专员应提出下列哪项建议?

A. 尽快联系董事会并告知此活动。

B. 立即电话联系执法部门，告知其潜在的洗钱活动。

C. 收集相关文件并进行审查，目的是为了提交可疑交易报告。

D. 对该活动进行记录但不提交可疑交易报告，避免失去该位长期客户。

76. 下列哪一选项是司法互助协定的定义?

A. 是一国中央政府为寻求司法管辖区外的证据而向另一国的中央政府发出的法律或司法协助书面请求。

B. 允许各国出于官方调查和指控的目的，在各自国家私营和公共部门中的法律诉讼以及文件、证人和其他法律和司法资源的获取方面提供互助的协定。

C. 双方就制定一系列原则来处理双方在特定事项上的关系而达成的协议。谅解备忘录通常被各国用来管理国际资产没收案件中的资产共享事宜或者确定各自在反洗钱工作中的义务。

77. 收到可疑交易报告后，相关执法部门要求与熟悉相关交易的银行职员进行面谈。合规专员应提出下列哪项建议?

A. 合规专员应与银行法律顾问商议，确定是否要求执法部门出示作证传票。

B. 在大陪审团或正式法庭未就调查下达命令前，合规专员应拒绝所有此类面谈。

C. 合规专员仅应允许愿意与执法部门进行面谈的员工前去面谈。

D. 合规专员仅应在员工获得执法部门的豁免权后允许员工参与面谈。

78. 在决定是否对金融机构提起刑事诉讼时，检察官应该考虑的三大因素是什么？

A. 该机构是否有犯罪历史记录。

B. 该机构是否配合执法调查。

C. 机构是否发现并自行报告了潜在的违法犯罪行为。

D. 该机构是否为大型机构，对其提起诉讼是否会使执法部门成为舆论关注的焦点。

79. 埃格蒙特集团设有五个工作组。下列选项中，有哪三项是该集团的工作组？

A. 运营工作组。

B. 法律工作组。

C. 检查工作组。

D. 外联工作组。

80. 合规专员正在设法制定一套处理潜在可疑交易审查的程序。合规专员应建议在程序中包含以下哪种做法？

A. 机构主要借助后台业务部门来识别账户活动中的可疑趋势。

B. 机构应将识别可疑活动的责任落实到所有员工。

C. 机构主要借助账户的账户关系经理来识别可疑活动。

D. 机构通过在银行各部门宣传各种洗钱危险信号，以此来涵盖所有可能存在的可疑活动。

81. 合规专员正在设法制定一套制度程序，用来决定是否提交可疑交易报告。合规专员应建议在制度程序中包含以下哪种做法？

A. 合规专员应该建议提交可疑交易报告的集中处理，以此来确保统一性。

B. 专员应建议将决策权分散，以加快流程的速度并确保作出决策的机构与活动具有最为紧密的联系。

C. 专员应建议仅在获得银行董事会授权的情况下提交可疑交易报告。

D. 专员应建议仅在接受彻底法律审查的情况下提交可疑交易报告。

82. 以下场景中，哪两个潜在危险信号反映出需要进一步调查的可疑活动?

A. 某大家族拥有多个账户，账户以多位家庭成员的姓名开立。

B. 企业账户的开户行地点与企业所在地相距甚远。

C. 个人拥有多个开在同一名称下的账户。

D. 公司拥有多个账户，其中每个附属企业各自拥有一个账户。

83. 在开展刑事调查时，执法部门的调查人员应完成哪三件事?

A. 刑事调查人员应尽量“以交易中的资金为线索”确定资金的来源和去向。

B. 刑事调查人员应识别潜在的非法活动，在某些国家，这些活动被称为“特定非法活动”。

C. 刑事调查人员应记录该笔交易可能涉及的潜在活动和潜在交易。

D. 刑事调查人员应研究所有近期在相关领域发生的类似案例。

84. 一般来说，金融机构应在何时提交可疑交易报告?

A. 准备销户时。

B. 侦测到异常或可疑交易时。

C. 仅在能够确认犯罪行为确实存在时。

D. 仅在董事会批准提交可疑交易报告时。

85. 当银行收到要求提供指定账户信息的作证传票时，合规专员应采取哪两大步骤?

A. 合规专员应确保工作人员研究并收集可用于回应作证传票的所有文件。

B. 合规专员应坚持要求执法部门解释签发作证传票的原因以及执法部门的调查目标。

C. 合规专员应确保对账户以及账户间的交易进行独立的审查。

D. 合规专员应在收到银行法律顾问的批准后方可遵守作证传票的要求。

86. 执法部门的代表召见合规专员，并紧急要求其提供指定账户的信息，原因是该账户与一项持续的恐怖融资活动调查有关。合规专员应该做些什么?

A. 获得董事会的批准后向执法部门提交材料。

B. 鉴于要求的紧迫性，应立即向执法机关提交材料。

C. 除非银行已就该事项提交可疑交易报告，否则应要求执法机构代表提供法庭命令或大陪审团作证传票。

D. 在向执法机关提交材料前获得银行法律顾问的允许。

87. 在执行刑事调查时，执法部门的调查人员应该完成哪三件事?

A. 借助电脑对涉案个人和实体进行搜索。

B. 审查此前提交的关于涉案个人和实体的可疑交易报告。

C. 分析金融交易和活动，尝试发现其中的高风险因素或异常因素。

D. 对个人或实体的信用记录和借贷记录进行审查。

88. 合规专员在晨报中读到一篇关于大型疑似欺诈案件的报道。到银行后，合规专员发现疑似的欺诈案件涉及到银行的一位重要客户。在进行内部调查后，合规专员发现该客户的账户不存在可疑活动。专员接下来应该做些什么?

A. 专员应将内部调查的性质和结果告知董事会。

B. 专员应记录内部调查的性质和结果并保存在合适的文件夹中。

C. 如客户账户能够为执法部门的正式刑事调查提供帮助，专员应提交可疑交易报告。

D. 专员应提交可疑交易报告来证明内部调查所花费的时间，以免遭受银行检查人员的事后批评。

89. 促使金融机构进行内部调查的三大因素是什么?

A. 金融机构收到大陪审团针对机构部分账户的交易而签发的作证传票。

B. 数名员工将某账户存在可疑交易的信息告知高级管理层或合规专员。

C. 当机构审计师发现机构反洗钱政策和程序存在诸多不足的时候。

D. 当地一家小型企业参与的海外活动涉及多笔原因不明的电汇。

90. 可能引发调查或提交可疑交易报告的三大可疑或异常活动危险信号是什么?

A. 在没有提供当地电话号码或公用事业账单的情况下开立新账户。

B. 月度结余与已知收入来源相比过高。

C. 账户资金的流动速率快，但日初和日终的余额很少。

D. 多次存入低于报告限额门槛的现金。

91. 聘请代表金融机构的外部顾问开展内部调查有何优势?

A. 外部顾问会以公正、合法的法律视角进行审查。

B. 外部顾问可逼迫员工承认与罪犯合谋。

C. 外部顾问不仅可以为银行创设律师 - 委托人特免权，而且还可以与每个雇员建立联系。

D. 外部顾问可说服检察官不对机构提起任何诉讼。

92. 国际合作和信息共享的三大传统途径是什么?

A. 司法互助协定 (MLATs)。

B. 执法部门使用大陪审团作证传票。

C. 金融情报机构间的信息交换 (FIU)。

D. 监管机构间的信息交换。

93. 应对执法质询的三种推荐方式是什么?

A. 尽量配合执法质询。

B. 尽可能迅速且彻底地回应所有正式的信息要求，除非有正当的反对意见可以且应当提出。

C. 确保书面和口头的所有沟通通过一个集中点进行传递。

D. 通过尽可能拒绝所有质询和要求来保护信息不被无故公开。

94. 如存在针对银行本身的刑事调查，应采取哪三大步骤?

A. 应将调查的进展通知并告知高级管理层和董事会。

B. 银行应考虑聘请资深的外部顾问来协助银行应对调查。

C. 银行应立即联系媒体说明自己没有犯错的原因。

D. 银行的相关员工应知晓现有的调查，并就应对方式和应对步骤获得指导。

95. 当金融机构在应对执法部门的正式刑事调查时，要求通过机构内一个核心人员集中处理信息的主要目的是什么?

A. 确保损害金融机构利益的信息不被公布。

B. 确保金融机构的回应及时、内容全面，且涉及保密的材料不会因疏忽而错误提交给无权限人员。

C. 确保机构员工没有泄露可能违反客户隐私权的信息。

D. 确保有人能够充分且彻底地向董事会告知调查的进展。

96. 当金融机构被执法部门出示搜查令后，金融机构的员工需要做哪三件事?

A. 在外部顾问到场前，他们不应该提供任何文件。

B. 他们应与执法部门紧密合作，并保持冷静和礼貌。

C. 他们应获得执法部门从机构所获取的材料清单。

D. 他们应查看搜查令以确定其执法范围。

97. 金融机构何时应考虑聘请资深的外部顾问来提供协助?

A. 当金融机构收到任何一间执法机构的作证传票时。

B. 当金融机构自身成为刑事调查的对象时。

C. 当金融机构关注机构内一位信誉良好的长期客户时。

D. 当银行业监管机构对机构反洗钱监控程序的充分性提出批评时。

98. 合规专员何时应建议金融机构进行内部调查？请从以下四项答案中选出三项。

A. 当怀疑员工与银行的长期客户共谋试图通过银行进行洗钱的时候。

B. 当多名客户使用相同的联系信息在多家分支机构开立独立账户时候。

C. 当银行监管机构对银行的反洗钱合规工作给予较低评分时。

D. 当一名长期雇员决定进行间断性休假，而非按照银行政策连续休假两星期时。

99. 当员工已经证实异常交易或者可疑交易了，那么在与员工面谈时，可以采用哪三种实用技巧?

A. 一旦发生类似情况，应立即与员工进行面谈，确保员工的记忆处于最为清晰的状态。

B. 在面谈中尽量使员工感到放松，从相对轻松且没有争议的问题开始，逐渐深入较为敏感的问题。

C. 向员工提出开放性的问题，确保问题不会反映出意料之中的答案。

D. 尽量掌控面谈进程，以便迅速解决问题并发现犯错的人员。

100. 在各国金融情报机构间的信息交换方面，哪三大原则最为重要?

A. 只有在中央银行也参与信息共享时，金融情报机构间的信息共享方可进行。

B. 应基于互惠原则尽可能自由地共享信息。

C. 应基于对方的请求进行信息共享或主动共享信息。

D. 犯罪定义的差异不应妨碍信息的自由交换。

101. 机构违反反洗钱法律的三大风险。

A. 资产扣押。

B. 民事罚款。

C. 股票价值下跌。

D. 监管力度加大。

102. 选出房地产行业的三种洗钱方式。

A. 斥巨资购买房产。

B. 掩饰受益所有权。

C. “倒卖”房地产。

D. 创造租金收入。

103. 选出利用律师洗钱的三种方式。

A. 为客户建立信托公司。

B. 购买并出售资产。

C. 建立并管理慈善机构。

D. 为客户提起民事诉讼。

104. Roy 在一家大型金融机构担任银行保密法 (BSA) 专员，负责审查有可能涉及反洗钱的案件。他应该关注哪三大危险信号?

A. 短期内进行大量的房产买卖交易。

B. 利用网络或手机的方式进行大额交易。

C. 国外的新客户开立企业账户。

D. 两人或多人使用同一个身份。

105. Jim 在一家赌场担任反洗钱专员，他识别出几个涉及客户的潜在危险信号。下列哪一选项最为棘手?

A. 一位客户购买了一些筹码，只玩了一小段时间后，就想要把筹码的收益汇至国外的另一家赌场。

B. 一位客户在赌博了一段比较长的时间后，想要把手上的筹码兑换为赌场签发的支票。

C. 一位客户在赌博了一段比较长的时间后，想要把手上的筹码兑换为现金。

D. 一位客户要求参与赌场的高额赌注游戏项目，但该客户看起来并不了解他所选赌博项目的游戏规则。

106. 选出美国、联合国和欧盟实施制裁的目的。

A. 为了惩罚参与非法贸易融资的银行。

B. 为了保护金融系统，防止洗钱行为。

C. 为了明确银行保密法专员应遵循的指导方针。

D. 为了协调这些司法管辖区之间的信息共享事宜。

107. 金融机构比较关心的是贩运人口所得的收益可能会流入金融机构，并利用金融机构为其提供金融服务。对此，金融机构应关注和警惕下列哪三项内容?

A. 来自国外的多笔数额低于报告阈值的电汇。

B. 多个互不相关的个人向同一受益人进行电汇。

C. 作为外国劳工的帐户，雇用机构是该帐户的保管人。

D. 四位女士结伴前往金融机构，但分别开立各自单独的账户。

108. 一位新产品经理提议推出一项涉及预付卡的新产品，但是反洗钱专员认为该产品存在一些问题。该反洗钱专员可能提出哪三大风险或问题呢?

A. 客户可以通过该产品在全球范围内快速转移资金。

B. 该产品可续值，且可被匿名使用。

C. 事实上，可能有大量的客户未经审查，便试图使用该产品。

D. 身份欺诈风险会上升。

109. 选出海外资产控制办公室具有域外管辖权的三个关键职能。

A. 限制美国公民出境。

B. 根据美国外交政策实施经济和贸易制裁。

C. 冻结美国司法管辖区内的海外资产。

D. 封锁“特别指定国家和禁止往来人员”。

110. 选出类似承担“金融行动特别工作组”职能的区域性组织所具备的三大职能。

A. 编写 FATF 40 项建议。

B. 定期发布类型报告。

C. 积极在识别反洗钱技术上给予必要的支持。

D. 推动金融行动特别工作组相互评估流程。

111. Jim 在一家大型银行担任反洗钱专家，负责审查客户账户的可疑活动。下列各项情境中，哪三项疑似反洗钱报警信号最强，最值得他的关注?

A. 客户威胁银行员工，极力阻止银行履行交易记录保存义务。

B. 反洗钱专家对客户交易所涉及的国家不太熟悉。

C. 公司账户的经常性活动很少或者几乎没有。

D. 员工抱怨必须向金融犯罪执法网络提交大量报告。

112. 在下列选项中，选出对不同员工和工作岗位开展针对性培训时应注重的三个关键方面。

A. 确定重点分析真实案例或者模拟案例。

B. 确定培训方式。

C. 确定培训重点。

D. 确定培训对象。

113. 执法部门调查人员在调查金融机构提交的可疑活动报告时，应首先考虑下列哪三个方面？

A. 识别非法活动及一切特定非法活动。

B. 追踪所有相关账户非法资金的来源和所有权。

C. 决定是否冻结或扣押存在非法资金流动的账户。

D. 决定是否豁免该调查目标，以迅速获得更多信息。

114. Jack 是一家金融机构的反洗钱专员，现正在处理一件银行职员为洗钱犯罪嫌疑人员提供协助的案件。Jack 在调查此案件时应考虑下列哪三项因素？

A. 确定该员工在银行内部的升迁是否存在异常。

B. 确定该员工是否过着奢侈的生活。

C. 确定该员工是否曾协助客户隐藏其账户的最终受益人。

D. 确定该员工是否频繁涉及一些还未解决的例外情况。

115. Suzy 是一家大型金融机构的反洗钱合规专员，董事会要求她想办法保证机构提交的可疑活动报告及其内容的保密性。她应考虑下列哪三方面内容？

A. 确保员工了解如何通过客户姓名快速、高效地检索获取到可疑活动报告。

B. 培训员工，确保其不会无意中向目标客户泄露提交报告的相关事宜。

C. 制定严格的记录程序，分开保存可疑活动报告信息，确保其保密性。

D. 制定相关程序，以便在收到提供可疑活动报告副本的要求时，能够及时恰当地进行回应。

116. 金融机构发现客户通过账户洗钱的危险信号后，应首先采取下列哪三项措施？

A. 识别并审查该客户参与的内部交易。

B. 针对该客户进行网络调查，包括对法院记录进行审阅。

C. 当面询问该客户账户异常的事宜。

D. 将客户的收入与该地区的同类企业进行比较。

117. 某金融机构的合规专员收到了执法机构的作证传票，因为执法机构认为其反洗钱制度存在潜在缺陷。该合规专员应采取下列哪三项措施？

A. 应告知员工对所有可疑活动报告要保密。

B. 应将收到作证传票一事告知机构董事会和高层管理人员，以及作证传票涉及的重点内容。

C. 应建议机构聘请该领域的资深外部顾问。

D. 应将机构开展的所有内部调查结果提供给执法部门。

118. 在下列选项中，选出三项可使金融机构重新评估其反洗钱制度的因素。

A. 发布新产品。

B. 收购另一家金融机构。

C. 选举新一届董事会。

D. 距上次评估已过去一段时间（如 12-18 个月）。

119. 在决定如何以及何时向金融机构高层管理人员或董事会提交可疑活动报告时，应考虑下列哪三项因素？

A. 所提交的可疑活动报告是否超过上一年提交的可疑活动报告。

B. 可疑活动报告中是否涉及重大问题，特别是与声誉风险相关的问题。

C. 可疑活动报告是否表明存在任何的合规制度缺陷。

D. 可疑活动报告是否显示出任何重大的反洗钱发展趋势。

120. Diane 是一家大型金融机构的反洗钱合规专员，发现了一些相连账户涉嫌严重的洗钱行为。在确定是否对这些账户进行销户时，她应考虑下列哪三项因素？

A. 账户持有者是否与董事会成员有密切关系。

B. 所谓的洗钱活动是否在所有帐户中发生，还是只是发生在部分帐户中。

C. 销户的法律依据。

D. 保留这些账户将为机构带来的声誉风险。

121. Rick 在一家小型银行担任反洗钱合规专员，该银行曾遇到过反洗钱问题，目前与联邦政府达成了暂缓起诉协议。美国联邦调查局要求 Rick 保留其正在检查的一个账户，以便对其后续的交易进行监控。Rick 应采取下列哪两项措施？

A. 请其提交书面申请。

B. 确保该要求由拥有相关权力的人员发出。

C. 在进行内部调查后，请求董事会批准保持该账户的活动状态。

D. 保持该账户的活动状态，避免与联邦政府的意见不一致。

122. Jane 在一家大型金融机构的反洗钱部门担任调查专员，目前正在调查一个涉嫌反洗钱行为的案件，涉及范围极广，包括多个国家及多家机构。她为了进一步调查，可查阅下列哪三项公共资源或公共记录？

A. 国内公司档案。

B. 法院记录。

C. 警察局拘留记录。

D. 信用记录。

123. 在下列选项中，选出执法部门在开展刑事调查中，要求金融机构提交信息时可以使用的三种方式。

A. 获得、签发大陪审团作证传票。

B. 出示搜查令。

C. 要求与所提交可疑报告活动有关的文件记录。

D. 要求反洗钱专员提交该目标嫌疑人的所有账户记录。

答案

1. A	21. A, B, C	41. A	61. C	81. A	101. A, B, C	121. A, B
2. B	22. A, C, D	42. D	62. D	82. B, C	102. A, B, C	122. A, B, D
3. A	23. D	43. A	63. D	83. A, B, C	103. A, B, C	123. A, B, C
4. B, C, D	24. C	44. D	64. B	84. B	104. A, B, D	
5. A, C	25. C	45. A, B, D	65. A	85. A, C	105. A	
6. D	26. A	46. A	66. C	86. C	106. B	
7. C	27. D	47. A, B, D	67. D	87. A, B, C	107. A, B, C	
8. B	28. D	48. A	68. B	88. B	108. A, B, D	
9. A, B, D	29. C	49. C	69. C	89. A, B, D	109. B, C, D	
10. A, C, D	30. A	50. A	70. A	90. B, C, D	110. B, C, D	
11. A	31. B	51. C	71. C	91. A	111. A, B, C	
12. C	32. C	52. B	72. A	92. A, C, D	112. B, C, D	
13. D	33. A	53. A.	73. C	93. A, B, C	113. A, B, C	
14. B, C, D	34. C	54. A	74. A, B, C	94. A, B, D	114. B, C, D	
15. C	35. C	55. D.	75. C	95. B	115. B, C, D	
16. A	36. A	56. A, B, C	76. B	96. B, C, D	116. A, B, D	
17. C, D	37. B	57. C	77. A	97. B	117. B, C, D	
18. B	38. A	58. C	78. A, B, C	98. A, B, D	118. A, B, D	
19. B	39. C	59. A, B, C	79. A, B, D	99. A, B, C	119. B, C, D	
20. A, B, C	40. B	60. A	80. B	100. B, C, D	120. B, C, D	

备注：

第 7 章

指导文件与参考资料

本章列举了 CAMS 认证考试的部分证明文件和参考资料。另外，本章还包含此类补充证明材料的网址和期刊名称。部分致力于反洗钱和反恐融资活动的国际组织发布了一系列有价值的指导文件和参考资料，这些资料对于 CAMS 认证考试的备考具有一定帮助。

从学习的目的来看，参考文件一般由导论和正文组成，有时还会在最后阐述研究方法。例如，在金融行动特别工作组 (FATF) 发布的每份“风险为本的方法指南”文件中，第一章都用于阐述“风险为本的方法”的目的。之后，核心材料会对特定的反洗钱风险（指南的焦点）以及用于降低风险的最佳实践进行描述。CAMS 认证考试考查的正是核心材料。

在所有文件中，有两个文件（即金融行动特别工作组的 40 项建议及其解释）需要引起 CAMS 应试人员的特别关注。我们强烈建议您从金融行动特别工作组（FATF）网站上下载免费的 PDF 版本并结合其他 CAMS 学习资料一同使用。40 项建议是个国家级层面的金融机构反洗钱系统的基本，其他材料多半以此为基础，然后针对某一方面具体展开。

指导文件与参考资料

（PDF 版本：复制链接并粘贴在网页浏览器中，以便查看参考资料。）

I. 金融行动特别工作组 (FATF)： http://www.fatf-gafi.org

- **40 项建议及其解释（2012 年 2 月）**
  http://www.fatf-gafi.org/publications/
  fatfrecommendations/?hf=10&b=0&s=desc(fatf_releasedate)

II. 巴塞尔银行监管委员会： www.bis.org

- **银行客户尽职调查**（2001 年 10 月）
  www.bis.org/publ/bcbs85.htm

- **一体化了解您的客户风险管理**（2004 年 10 月）
  www.bis.org/publ/bcbs110.pdf
- **洗钱和恐怖融资风险健全管理（2014 年 1 月）**
  http://www.bis.org/publ/bcbs275.htm
- **账户开立通用指南**（2016 年 2 月）
  http://www.bis.org/bcbs/publ/d353.htm
- **跨境电汇支付信息的尽职调查和透明化**
  http://www.bis.org/publ/bcbs154.pdf
- **各司法管辖区之间共享与反恐融资活动有关的金融记录（2012 年 4 月）**
  www.bis.org/publ/bcbs89.pdf
- **《账户开立和客户身份识别通用指南》**（2003 年 2 月）
  （巴塞尔委员会出版物《银行客户尽职调查》的附件）
  www.bis.org/publ/bcbs85annex.htm
- **银行合规和合规部门**
  http://www.bis.org/publ/bcbs113.pdf

III. 与金融行动特别工作组类似的区域性组织：

A. 亚太反洗钱工作组

www.apgml.org

- **方式与类型**
  http://www.apgml.org/methods-and-trends/page.
  aspx?p=a4a11dca-75f2-4dae-9c25-6215103e56da

B. 加勒比地区反洗钱金融行动特别工作组

www.cfatf.org

- **洗钱类型研究**
  https://www.cfatf-gafic.org/index.php/documents/typologies

C. 评估反洗钱措施特设专家委员会 (MONEYVAL)

http://www.coe.int/t/dghl/monitoring/moneyval/

D. 东南非反洗钱工作组

www.esaamlg.org/

- 类型——http://www.esaamlg.org/reports/typologies.php

E. 欧亚反洗钱与反恐融资活动工作组

http://www.eurasiangroup.org/

- 类型——http://www.eurasiangroup.org/typology_reports.php

F. 拉美国际金融行动特别工作组 (GAFILAT)

http://www.gafilat.org/?id=inicio&lang=en

G. 非洲政府间反洗钱行动工作组 (GIABA)

http://www.giaba.org/

- 类型——http://www.giaba.org/reports/typologies/reports.html

H. 中东与北非反洗钱金融行动特别工作组 (MENAFATF)

www.menafatf.org/

- 类型——http://www.menafatf.org/TopicList.asp?cType=typ

IV. 联合国 (UN)： http://www.un.org

- **针对洗钱和恐怖主义融资活动的立法范本**

  http://www.unodc.org/unodc/en/money-laundering/Model-Legislation.html?ref=menuside

- **联合国安理会打击恐怖主义的决议**

  http://www.un.org/en/counterterrorism/index.shtml

V. 国际洗钱信息网： www.imolin.org

VI. 欧盟：http://europa.eu/

- 欧盟第四号反洗钱指令（欧洲议会暨欧盟委员会第 (EU) 2015/849 号指令，2015 年 5 月 20 日）
  http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32015L0849
  （注：该指令废除了欧盟第三号反洗钱指令）
- 欧洲议会和欧洲委员会发布的欧盟第三号指令 2005/60/EC（2005 年 10 月）
  http://eur-lex.europa.eu/LexUriServ/LexUriServ. do?uri=CELEX-:32005L0060:EN:NOT
  （注：该指令扩展了欧洲议会和欧洲委员会关于防范将金融系统用于洗钱的欧盟第 2 号指令 2001/97/EC（2001 年 12 月）。）

VII. 金融情报机构埃格蒙特集团：www.egmontgroup.org

- 100 个洗钱案例 http://www.egmontgroup.org/library_sanitized_cases.html

VIII. 沃尔夫斯堡集团：www.wolfsberg-principles.com

- **《沃尔夫斯堡代理银行业务反洗钱原则》**（2002 年发布，2014 年修订）
  http://www.wolfsberg-principles.com/pdf/standards/Wolfsberg-Correspondent-Banking-Principles-2014.pdf
- **《沃尔夫斯堡抑制恐怖融资活动的声明》**（2002 年 1 月）
  http://www.wolfsberg-principles.com/pdf/standards/Wolfsberg_Statement_on_the_Suppression_of_the_Financing_of_Terrorism_(2002).pdf
- **《沃尔夫斯堡私人银行反洗钱原则》**（2002 年发布，2012 年修订）
  http://www.wolfsberg-principles.com/pdf/standards/Wolfsberg-Private-Banking-Prinicples-May-2012.pdf
- **《沃尔夫斯堡关于反洗钱监控、筛查和搜索的声明》（2009 年）**
  http://www.wolfsberg-principles.com/pdf/standards/Wolfsberg_Monitoring_Screening_Searching_Paper_(2009).pdf
- **《沃尔夫斯堡反腐败指南》（2011 年）**
  http://www.wolfsberg-principles.com/pdf/standards/Wolfsberg%20Anti%20Corruption%20Guidance%20Paper%20August%2018-2011%20(Published).pdf

其他网站提供有用的反洗钱资料

获得 CAMS 资格认证的专业人员需要定期访问所在国监管机构的网站。此外，其他网站也提供有用的反洗钱资料。

公认反洗钱师协会

www.ACAMS.org

澳大利亚交易报告和分析中心 (AUSTRAC)

www.austrac.gov.au

加拿大金融交易和报告分析中心 (FINTRAC)

www.fintrac.gc.ca

国际货币基金组织

www.imf.org/external/np/exr/facts/aml.htm

英国金融市场行为监管局

https://www.fca.org.uk/firms/financial-crime/money-laundering-terrorist-financing

美国金融犯罪执法网络主页

www.fincen.gov

联邦金融机构检查委员会 (FFIEC) 的银行保密法 / 反洗钱数据库

http://www.ffiec.gov/bsa_aml_infobase/default.htm

美国海外资产控制办公室 (OFAC)

https://www.treasury.gov/about/organizational-structure/offices/Pages/Office-of-Foreign-Assets-Control.aspx

世界银行

www.worldbank.org

与反洗钱相关的期刊

《今日 ACAMS》

面向 ACAMS 会员发行的季刊，内容包括反洗钱领域的案例以及当今全球反洗钱领域的问题及发展。

http://acamstoday.org/wordpress/

ACAMS MoneyLaundering.com

每月一期的时事通讯，内容包括当前全球、法律、监督与执行问题以及有关洗钱的新闻、分析和指南。

www.moneylaundering.com

洗钱快报

英国的时事通讯，每年 10 期，主要讨论洗钱实践、监管和各行业反洗钱系统的问题。

http://www.moneylaunderingbulletin.com/

美国银行家协会银行合规

美国银行家协会发行的月刊，内容包括法律、监管和合规问题以及相关信息。

http://www.aba.com/Products/bankcompliance/Pages/default.aspx

备注：

美国总部

Brickell City Tower
80 Southwest 8th Street
Suite 2350
Miami, FL 33130
USA
电话：+1-866-459-CAMS
美国以外：+1-305-373 0020
传真：+1-305-373 7788
或 +1-305-373 5229

ACAMS 新加坡

Level 25, North Tower
One Raffles Quay
Singapore 048583
电话：+65-6622 5611
传真：+65-6491 5699

ACAMS 日本

Business Garden Yotsuya Annex
1-6-1-212 Wakaba, Shinjuku-ku
Tokyo, Japan
160-0011
电话：+81-3-5366 4745
传真：+81-3-6730 9541

ACAMS 印度

Tower A, Building No-5, 18th Floor
DLF Cyber City, DLF Phase III
Gurgaon 122002
India
电话：+91-124-663 7637
传真：+91-124-388 2999

亚太区总部

香港鲗鱼涌
华兰路 18 号
港岛东中心 23 楼
电话：+852-3750 7658 / 7694
传真：+852-3010 1240

ACAMS 北京

中国北京市
东城区建国门北大街 8 号
华润大厦 1201-51 室
邮编：100005
电话：+86-10-5811 1930 / 1783 / 1797
传真：+86-10-5804 3600

ACAMS 上海

中国上海市
上海国际金融中心二期 36 楼
邮编：200120
电话：+86-21-6062 7207
传真：+86-21-6192 4307

ACAMS 台湾

台湾台北市
信义路 5 段 7 号
台北 101 大楼 37 楼
邮编：110
电话：+866-2-8729 2988
传真：+886-2-6602 1991