

《今日 ACAMS》—— 事业型反洗钱专家的专业期刊

## 勒索软件： 数字战场

本期相关阅读：

“9·11”：  
20 年的旅程

第 20 卷 第 4 期 | 2021 年 9 月 - 11 月号

公认反洗钱师协会® (ACAMS®) 出版

[acams.org](http://acams.org) | [acamstoday.org](http://acamstoday.org)

# 金融科技反洗钱合规 岗位证书 (CAFCA)

由金融科技企业开发，为金融科技企业服务。由世界反金融犯罪专家们组成的全球最大会员组织为您认证。

了解更多信息，请访问：

[acams.org/cafca](https://acams.org/cafca)





# ACAMS-NIFA 互联网金融反洗钱培训

扫描二维码，  
率先利用优惠登记！



## 即刻报名，享勤学者优惠！

由中国互联网金融协会 (NIFA) 指导发起，公认反洗钱师协会 (ACAMS) 合作开发研发了《ACAMS-NIFA 互联网金融反洗钱培训》课程，为国内互联网金融业发展提供符合国情的反洗钱/反恐怖融资发展的培训内容。

### 课程八大模块

- ✓ 反洗钱 / 反恐融资基础知识
- ✓ 国际反洗钱监管框架
- ✓ 中国监管环境
- ✓ 互联网金融产品和服务
- ✓ 互联网活动的固有风险
- ✓ 互联网金融公司和金融科技公司风险评估
- ✓ 反洗钱 / 反恐融资保护、控制措施和风险缓释
- ✓ 调查和治理流程

### 免费附加学习素材

#### ACAMS WEBINARS 网络研讨会视频 (10个)



#### ACAMS TODAY 《今日 ACAMS》精选文章 (10篇)



#### ACAMS MONEYLAUNDERING.COM MoneyLaundering.com 精选文章 (10篇)



请访问 ACAMS 官网，了解更多详情。

编辑总监  
Kieran Beer, CAMS

总编辑  
Karla Monterrosa-Yancey, CAMS

## 编辑与设计

编辑：  
Stephanie Trejos, CAMS  
国际编辑：  
Monica Mendez, CAMS

创意与设计：  
Victoria Racine  
Joya Jones

## 编辑团队

主席：Elaine Rudolph-Carter, CAMS  
Kevin Anderson, CAMS  
Kevin Antis, CAMS  
Brian Arrington, CAMS  
Edwin (Ed) Beemer, CAMS-FCI  
Robert Goldfinger, CAMS  
Jennifer Hanley-Giersch, CAMS  
Debbie Hitzeroth, CAMS-FCI  
Stacey Ivie  
Sanjeev Menon  
Ari Redbord  
Joe Soniat, CAMS-FCI  
Amy Wotapka, CAMS

## 高层领导团队

主席兼董事总经理：  
Scott Liles

课程开发和营销副总裁：  
Angela Salter

全球人力资源总监：  
Bill Lumani

全球销售副总裁：  
David Karl

集团副总裁与全球协会事业拓展执行长：  
Hue Dang, CAMS-Audit

全球战略沟通副总裁：  
Lash Kaur

融资和全球运营副总裁：  
Mariah Gause

高级全球制裁和风险监控总监：  
Justine Walker

## 中文版审阅

邓芳慧 (Hue Dang), CAMS-Audit  
许朐方 (Joyce Hsu), CAMS-FCI

## 咨询委员会

联席主席：Rick A. Small, CAMS  
联席主席：Markus Schulz  
John J. Byrne, CAMS  
Sharon Campbell  
Jim Candelmo, CAMS  
Vasilios P. Chrisos, CAMS  
David Clark, CAMS, CGSS  
Howard Fields, CAMS  
María de L. Jiménez, CAMS, CGSS  
William D. Langford, CAMS  
Dennis M. Lormel, CAMS  
Rick McDonnell, CAMS  
Karim A. Rajwani, CAMS  
Anthony L. Rodriguez, CAMS, CPA  
John Smith

## 咨询委员会 (继续)

Daniel D. Soto, CAMS  
Dan Stipano  
Philippe Vollot

## 内部撰稿人

欧洲、中东和非洲地区反洗钱合规策略总监：  
Shilpa Arora, CAMS  
美洲反洗钱部门高级总监：  
Lauren Kohr, CAMS-FCI  
亚太地区反洗钱合规策略总监：  
Rosalind Lazar, CAMS  
中国反洗钱合规策略总监：  
李娜 (Lynn Li), CAMS-Audit

## 区域销售代表

业务开发高级副总裁：  
Geoffrey Chunowitz, CAMS

美洲、加拿大和拉丁美洲销售总监：  
Sonia Leon, CAMS-Audit  
Gerald Sandt

战略客户总监：  
Jose Victor Lewis, CAMS

欧洲销售总监：  
Paolo Munari

中东和非洲销售总监：  
Michel Nassif

加勒比地区执行长：  
Denise Perez, CAMS

赞助和广告开发总监：  
Andrea Winter, CAMS

澳大利亚业务拓展区域总监：  
Nick Griffith

南亚 / 东南亚和日本业务拓展区域总监：  
Christine Lim

北亚业务拓展区域总监：  
杨智全 (Yokel Yeung), CAMS

中国区首席代表：  
郭荣军 (Jerry Guo), CAMS

ACAMS 全球总部  
芝加哥 +1-305-373 0020

ACAMS 亚太区总部  
香港 +852-3750 7684 / 7694 / 7658

ACAMS 亚太区  
北京 +86-10-5811 1797 / 1783 / 1775  
上海 +86-21-6062 7207  
成都 +86-28-6511 8323  
广州 +86-20-2881 8569  
台北 +886-2-8729 2988 / 2982  
新加坡 +65-6622 5611  
东京 +81-3-6831 0622  
孟买 +91-22-4905 4372  
悉尼 +61-2-8017 0295

apac@acams.org  
www.ACAMS.org.cn  
www.ACAMSToday.org

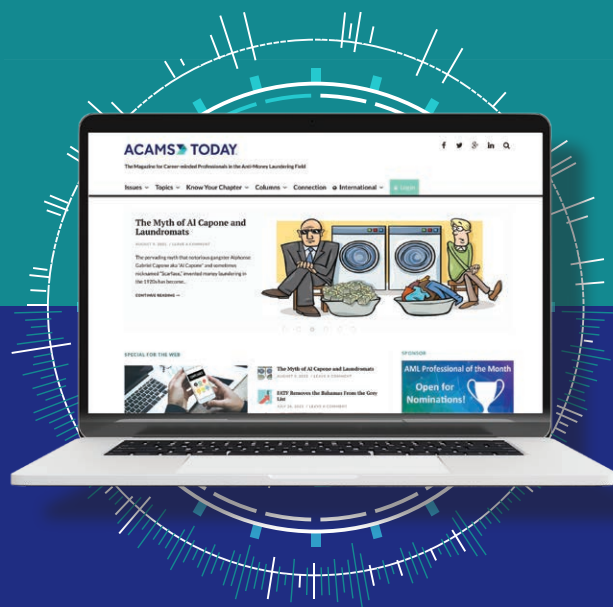
如要刊登广告，请联系：Andrea Winter  
电话：1-305-373-0020 (分机 3030)  
电子邮件：sponsorsandexhibitors@acams.org

《今日 ACAMS》© 2021 版权所有，公认反洗钱师协会 (ACAMS) 保留所有权利。未经 ACAMS 明确书面许可，不得复制本期的任何内容。如中文译本之文义与英文原文有歧异，概以英文原文为准。

《今日 ACAMS》是一本屡获殊荣的杂志，旨在提供正确、具权威的关于国际洗钱控制及其相关主题的信息。发表之文章并不代表作者或本协会参与提供法律或其他专业服务。如需要协助，请寻求专业人士提供服务。《今日 ACAMS》每年为 ACAMS 会员出版四期。

想要阅读更多  
《今日 ACAMS》  
的内容？

欢迎访问  
ACAMSToday.org!



在纸质版刊物以外，ACAMSToday.org 网站还提供许多网络专享内容，包括独家文章、访谈、互动民意调查、“ACAMS 月度反洗钱专业人士”等等！



# 在此投放 广告

登上《今日 ACAMS》，触达由超过  
86,000 名反金融犯罪会员组成的网络。

如欲在《今日 ACAMS》  
投放广告，请联系：

Andrea Winter  
1.786.871.3030  
[awinter@acams.org](mailto:awinter@acams.org)

ACAMS  TODAY™

# 目录



插图：Milos Hall

封面：

56

## 勒索软件： 数字战场

Colonial Pipeline 勒索软件攻击案例分析  
及其对反金融犯罪专业人士的影响。

8

编者按

10

会员聚焦

12

编辑总监寄语

14

非营利机构：  
了解捐赠者的资产来源

捐赠者建议基金的发展可能在非营利  
组织部门滋生洗钱活动。

18

猜谜：出口管制？

细说出口管制的内容、地点、原因和  
对象。

22

加密货币退出骗局——  
骗局解密及防骗攻略

加密货币退出骗局的定义及防范方法。

26

数据对合规和反金融犯罪  
工作的影响

无法正确管理数据会带来什么样的后果？

28

勒索软件、加密货币和洗钱  
之间的关系

随着勒索软件威胁的增长，犯罪分子  
开始用加密货币作为交换媒介洗钱。

32

赌场和洗钱原因

要抓住洗钱者，赌场工作人员必须像  
洗钱者一样思考。







38

38

## 增强 DPMS 监管合规工具包

深入了解珠宝行业的诸多洗钱机会。

42

## 如何通过审计

审计生存核对清单，助您完成审计准备、管理和事后行动。

46

## 数据泄露危机管理 最佳实践（上）

金融机构的数据泄露预防和应对之道。

50

## 了解您的客户制度取得成功 所需要的数据

反洗钱专业人士必须超越个体数据元素的采集和整理。

54

## 20 年来的 20 件大事

ACAMS 咨询委员会联合主席 Rick Small 和前咨询委员会委员 Lauren Kohr 放眼 ACAMS 发展历史，点出反洗钱领域的 20 大变化。

62

## “9·11”：20 年的旅程

“9·11”的历史及其对反金融犯罪工作的持续影响。

66

## 老年人钱财诈骗：巨大危机

从执法角度审视老年人钱财诈骗问题的解决之道。

70

## 反洗钱专业人士需要了解的新举报人制度

详解《反洗钱法》对《银行保密法》举报人制度的拓展。

74

## 欧洲网络安全生态系统： 一场打击网络犯罪的战争

回顾欧洲关于打击网络犯罪的最新提案、指导方针、战略和立法。

82

## 韩国“N 号房”案例分析

透过“N 号房”增进人们对数字性犯罪和现代奴隶制的认识。

92

## 《隔离引起的沉思》第 3 章： 求职者的反击

求职者如何把握疫情所致衰退结束带来的机遇。

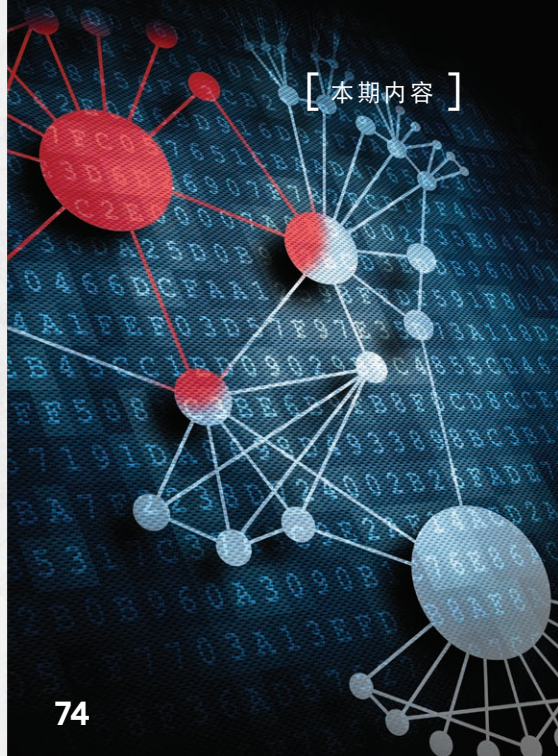
96

## 令事件触发审查切实发挥作用

如何通过事件触发审查机制更有效地管理金融机构的客户风险。



62



[ 本期内容 ]

74

## 亚太专栏

88

## 如何将洗钱风险纳入 风险管理：（上）

如何评估和衡量洗钱风险造成的损失。

## 了解您的分会

100

## 大凤凰城分会： 调整、发展与适应！

回顾大凤凰城分会加密货币时代反恐融资活动。

102

## 会见 ACAMS 员工： Winnie Yuen

104

## 进阶认证毕业生

106

## 公认反洗钱师 (CAMS) 毕业生

117

## 国际制裁合规师 (CGSS) 毕业生

[ 2021 年 9 月 - 11 月号 ]

7



# 对“9.11”的反思

今

年是美国本土最严重恐怖袭击事件 20 周年。我们还记得听到这个消息的时候，我们在哪里。我当时住在落基山脉，刚坐到车里，准备开车去上班。我打开收音机，听说一架飞机撞上了双子塔。起初，我以为听错了。我换了一个电台，但听到了相同的消息，于是震惊地开着车上班去了。一到公司，我就发现同事们也是满脸震惊。我们都挤在电脑屏幕前，像疯了一样，想找到更多的最新消息，了解事态发展。我们看到，第二架飞机撞上双子塔，南塔倒了。我有个同事，家里有个人在一架飞机上，她非常焦急，想知道亲人的飞机发生了什么。全世界都难以置信，我认识的每个人都开始问同样的问题。美国本土怎么可能发生这种事？难道没出现过警示信号？我们怎么毫无准备？

毫无疑问，“9.11”对我们生活的多个方面产生了深远的影响。特别是，它改变了银行业和所有金融机构。“9.11”促使美国颁布了《爱国者法》，当时最具颠覆性的法规。反洗钱 (AML) 和恐怖融资 (TF) 成为每个人的首要任务。现在在公营和私营机构需要合作，才能成功打击洗钱和恐怖融资活动，同时也需要完善记录保存和“了解您的客户”要求。《爱国者法》最重要的成就是推动了美国 and 全球的恐怖融资检测和遏制进程。

当我们反思“9.11”以来过去 20 年里发生的事情时，不仅是合规行业，也包括

整个世界，我们要问的是，在打击金融犯罪方面，我们是否有进步？我相信有进步。我相信，整个行业在不断发展，作为 ACAMS 会员和反金融犯罪专业人士，我们都在贡献自己的力量，不断打击洗钱和恐怖融资活动。虽然新技术使打击犯罪分子的斗争发生了变化，但目标始终未变——即打败“犯罪分子”。标题文章《勒索软件：数字战场》探讨了如今面临的巨大威胁之一——网络犯罪。该文对 Colonial Pipeline 案例进行了分析。在美国司法部将网络入侵提升到反恐调查同一优先级后，文章中有些说法可谓一针见血。作者称：

“执法机构的这种变化可能标志着 20 多年来国家安全政策的首次转向——承认 9.11 已经成为过去，恐怖分子、网络犯罪分子和流氓国家行为体已进入数字战场。”

显然，在这 20 年里，我们做了很多，但远远不够。

无独有偶，ACAMS 也迎来了 20 年华诞。为此，《今日 ACAMS》请到两位顶级领域专家，董事及前董事 Rick Small 和 Lauren Kohr。他们分享了过去 20 年里影响反金融犯罪格局的 20 大颠覆性事件。不出所料，2001 年 9 月 11 日发生的事件被他们列为榜首。阅读相关文章，深入了解他们的想法，以及他们对未来前沿事件的预测。



年会专刊内容丰富，包括新的举报人制度、加密货币退出诈骗、“9.11”的影响、出口管制、捐赠者建议基金、赌场与洗钱、成功过审等。

希望您能加入我们，共迎 ACAMS 20 周年华诞。这些庆祝活动将贯穿整年，持续到 2022 年，还会在 2022 年 3-5 月专辟周年纪念专刊，共贺《今日 ACAMS》成立 20 周年。关注本空间，了解庆祝计划的更多细节。

在“9.11”20 周年之际，让我们花点时间，记住在那个悲惨的日子里失去生命的人们，并向他们致敬。让我们记住在那个可怕的日子里，冒着生命危险，甚至不惜牺牲自己挽救生命的急救人员，也向他们致敬。A

*Karla Monterrosa-Yancey*

Karla Monterrosa-Yancey, CAMS

总编辑

欢迎关注我们的 Twitter 账号：

@acamstoday



# 联合 175 个 国家或地区的 反金融犯罪社群

访问

[acamsconferences.org](https://acamsconferences.org),

参加当地会议

ACAMS  CONFERENCES



**Sandra Edun-Watler, CAMS**  
**开曼群岛**

**S**andra Edun-Watler 是开曼群岛 Mourant Governance Services 的一名律师兼合规与报告部负责人，负责为开曼群岛实体提供反洗钱和自动信息交换报告及合规官服务。

在加入国际律师事务所 Walkers 之前，Edun-Watler 曾在开曼群岛金融管理局担任法律顾问。在 Walkers 工作期间，她先后担任多个职位，包括担任开曼群岛、英属维尔京群岛和百慕大办事处合规事务负责人。此外，她还以监管律师身份为客户提供建议，在反洗钱专员服务业务条线的设立和启动中发挥了重要作用。

Edun-Watler 在反洗钱和合规职能的各个方面均有丰富的知识和实践经验。她目前担任开曼群岛合规协会主席、开曼群岛法律从业者协会反洗钱指导小组副主席，并且是加勒比地区合规协会会员和前任主席。此外，Edun-Watler 还曾担任加勒比地区金融行动特别工作组英属维尔京群岛第三轮互评工作的法律评估员。她目前还在杜鲁门博登法学院任反洗钱客座讲师，代表开曼群岛合规协会在多个工作组任职。



**Muhammad Rizwan Khan, CAMS-FCI、CGSS、CTMA、CKYCA**  
**巴基斯坦**

**M**uhammad Rizwan Khan 因对反金融犯罪领域的杰出贡献而广受认可。Khan 已获得 ACAMS 的多项合规认证，包括公认反洗钱师 (CAMS)、交易监控认证专员 (CTMA)、客户尽职调查认证专员 (CKYCA)、国际制裁合规师 (CGSS) 和高级公认反洗钱金融犯罪调查师 (CAMS-FCI)。他目前就读于牛津大学赛德商学院，攻读组织领导学文凭课程。

Khan 目前在阿联酋 Al Dahab 货币兑换所担任总经理，负责实施侦查和防范金融犯罪的最佳实践。

Khan 在反洗钱和反恐融资领域拥有丰富的经验。作为合规专业人士，他专注于为金融服务行业及银行提供金融犯罪和独立洗钱审查服务。他的专业知识还包括独立审查和调查、威胁 / 风险评估、国内外培训、指导、专家证词和反洗钱制度体系开发等。Khan 在众多国际学术合规刊物上发布过大量文章，被公认为该领域的世界顶级专家之一。






## Howard Spieler, CAMS 美国纽约

Howard Spieler 是 ACAMS 纽约分会联席主席，拥有近 20 年的合规相关工作经验。在整个职业生涯中，他在反金融犯罪和其他合规风险领域适用法律、监管和政策要求方面，为众多企业和其他利益相关的部门或机构提供指导和监督服务。

Spieler 目前任三菱银行金融集团全球制裁合规部副总裁，作为制裁领域专家，为各种程序性倡议提供支持，包括风险评估、国内及全球产品审查等。此前，他曾在花旗银行和美国国际集团担任反金融犯罪职务，为全球利益相关的部门或机构提供专业咨询服务。

在此之前，Spieler 在彭博行政部门工作了 10 年，其中 7 年在纽约市经济发展公司担任合规主管，帮助制定和实施风险为本合规制度。他曾负责持续监测和评估价值 300 亿美元的公私房地产交易组合，包括管理监管报告。

Spieler 撰写了《A Global Review of Sanctioned Countries》(受制裁国全球评论) 和《The Impact of the U.S. President on Economic Sanctions》(美国总统对经济制裁的影响)，两篇文章均发表于《今日 ACAMS》。他是公认反洗钱师 (CAMS) 和公认国际制裁合规官 (ISCO)。Spieler 拥有肯恩大学会计学硕士学位、圣约翰大学工商管理硕士学位和纽约州立大学奥尔巴尼分校政治专业文学学士学位。 

### SARSnSTRIPS™

由于最近发生许多网络攻击事件，这位 CEO 现在开始认真对待网络安全问题。



是的。他邀请了一些退役的军队网络安全专家来训练我们这些真正对生物测定学感兴趣的人。



听好了！您将学会如何打击网络犯罪分子！



这是我的指纹。有很多人的指纹和我的类似，但这是我独一无二的指纹。



SAR 58

# 二十年后： 我们失去了什么，得到了什么？

# 大

多数人都能清楚地想起  
2001年9月11日，20年  
前的那天我们在哪里。

上午8点46分，一架小型飞机撞上了世贸中心北塔，起初，许多人都以为事故是因飞机偏离航线所致。但9点03分，又一架飞机撞上了南塔，人们明显地感觉到，美国受到了攻击。

上午9点59分，在曼哈顿中城的彭博新闻台，满墙屏幕显示南塔倒塌，见此情景，我站立不稳，跪倒在地。一位女迎宾跑过来问我是否还好。“我没事，但成千上万的人被夺去了生命”，我记得当时是这样回答的。

从我们位于布鲁克林的家中可以清楚地看到曼哈顿下城的天际线，但那天，我妻子只能看到双子塔所在地的滚滚浓烟。但她记得，在与佛罗里达的父母通电话，听妈妈说有一座塔倒了的时候，她说“别瞎说！”

北塔于上午10点28分倒塌。

当天死亡的近3,000人来自不同的种族、宗教和社会经济阶层，就像美国本身一样。

一位前同事回忆起与一大群人一起逃离布鲁克林大桥的经历，许多人全身都是建筑物的烟尘和灰尘。飞机在头顶呼啸而过时，每个人都非常害怕，听到有人喊“是我们的飞机，是我们的飞机”时才松了一口气。

上午9点37分，第三架飞机撞上五角大楼，10点03分，飞往国会大厦或白宫的

第四架飞机坠毁在宾夕法尼亚州的一块田地里，因为乘客冲进了被恐怖分子控制的驾驶舱。

这些恐怖袭击改变了世界，我们对这些恐怖袭击的反应也改变了世界。

全美国及世界各地的大小社区和各级政府团结在一起。

在我附近，朋友们尽其所能互相安慰，帮助家人查找失踪的人。每当有人要求医院接线员检查或重新检查入院记录时，他们都非常有礼貌。

我们看到，共和党人和民主党人几乎团结了起来。到10月，成立了一个两党委员会，从袭击中汲取教训，关于财务透明的不同提案以及之前遇到政治障碍的监督条款都签署成法，成为美国《爱国者法》的一部分。

本期，“9.11”之后成立的美国联邦调查局反恐融资行动科(TFOS)第一任科长Dennis Lormel回顾了反恐措施彰显的决心和团结，尤其是公私合作信息共享机制的建立。


这些合作机制恰巧诞生于ACAMS构想成形之时。小型媒体和会议组织Alert Global Media萌生了一个想法，对反洗钱和反恐融资专业人士进行认证，建立一个专业协会，作为信息集散中心和新想法以及最佳实践的分享平台。现在，ACAMS在全球拥有超过83,000名会员，将在2022年3月至5月发布《今日ACAMS》20周年专刊。有关庆祝活动的更多信息，请参阅总编辑的信。

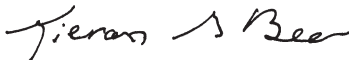


Lormel 恳请我们本着共有的“9.11”经历，保留那份反恐紧迫感、那份勤勉，正如他在整个执法生涯，与随后的顾问经历，及以顾问委员会成员身份参与ACAMS工作的过程中所做的那样。

随着塔利班在阿富汗重新掌权，以及新型恐怖主义威胁的兴起，包括来自国内极端分子，特别是有着种族或民族动机的暴力极端分子(RMVE)的威胁，这一请求使我们倍感辛酸。

今天，美国乃至整个世界都不像“9.11”之后那样对恐怖主义同仇敌忾，尽管当时建立的一些重要联盟仍有强大实力。

然而，只要想一想我们在“9.11”中失去的东西，想一想我们团结一致得到的东西，就会发现，保持勤勉的呼声以及ACAMS的全球使命有多重要。 



Kieran Beer, CAMS

首席分析师，编辑总监

欢迎关注我的 Twitter 账号：

@KieranBeer

“Financial Crime Matters with Kieran Beer” (Kieran Beer 谈金融犯罪问题)

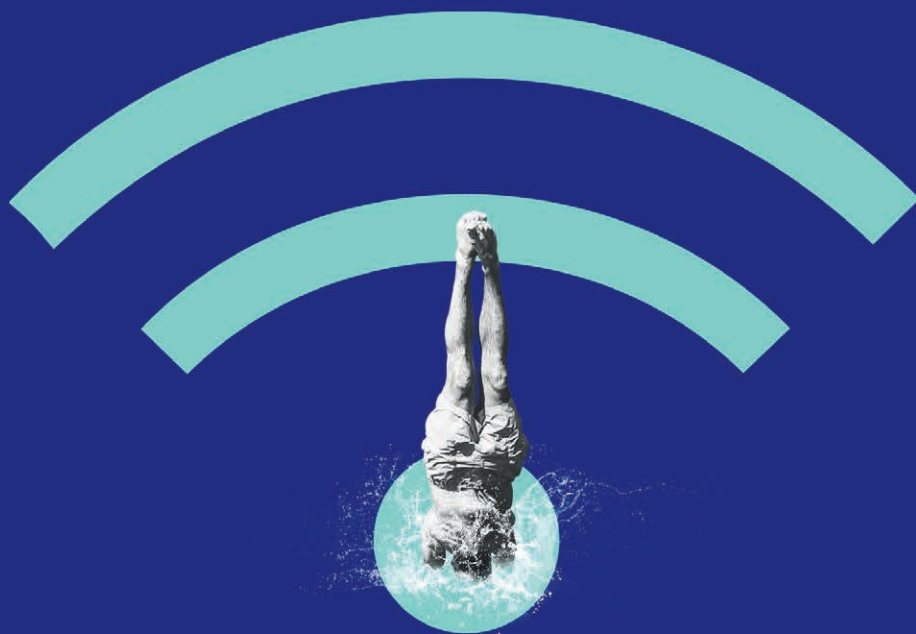


# 开启 在线学习 之旅

ACAMS 专题培训助您打击金融犯罪。

访问 [www.acams.org](http://www.acams.org)，了解 ACAMS 推出的  
多种在线认证、证书课程，以及免费数字学习内容。

#OnlineWithACAMS



# 非营利机构：

## 了解捐赠者的资产来源







插图：Joya Jones



们通过反金融犯罪专家了解洗钱新趋势的时候，一般不会考虑非营利部门和非营利机构(NPO)在促进非法交易方面的风险。

在帮扶社会弱势群体方面，非营利机构发挥着至关重要的作用；然而，由于缺乏“了解您的捐赠者”(KYD)政策，而且捐赠者建议基金(DAF)复合资产赠与行为近期显著增长，非营利机构有可能成为复杂洗钱计划的实施对象。

## 了解捐赠者建议基金

在非营利机构当中，捐赠者建议基金越来越受欢迎，这种捐赠工具通常简称为DAF。根据富达慈善基金会，<sup>1</sup>认为因建立手续简便，而且享有慈善捐赠税收优惠，DAF已成为美国增长最快的慈善捐赠工具。

由于捐赠者可即时享受赠与税收减免优惠，还能保留对捐赠资产的建议权，因此DAF越来越受欢迎。据美国国家慈善信托基金的信息显示，<sup>2</sup>2018年至2019年间，DAF托管资产规模从1,220亿美元跃升至1,420亿美元，增幅达16.2%。《巴伦周刊》(Barrons)近期报道称，2018年至2019年，DAF的数量增长了19.4%，增至873,228家，过去10年的增幅超过300%。<sup>3</sup>

DAF管理资产规模和账户数量快速增长，年增幅达15%-20%，捐赠者通过复合资产进行捐赠的行为也日益复杂。据美国国家慈善信托基金，认为非流动性捐赠越来越受到DAF行业的欢迎。<sup>4</sup>随着越来越多的基金会和赞助组织纷纷建立自己的DAF，不道德的捐赠者越来越有可能利用被忽视的小型基金会，为其他非法非营利机构（未实施“了解您的捐赠者”政策的组织）提供资金支持。



## 复合资产使尽职调查复杂化

加密货币、非流动性私人基金等复杂金融工具纷纷进入非营利机构领域。2017年，美国国家慈善信托基金管理的DAF<sup>5</sup>报告称，非现金捐赠有所增加。在2017年调查的60%的捐赠资产中，有60%为非现金资产。这些资产包括公共和非公共有价证券、房地产，甚至艺术品。

这些复杂的另类资产捐赠带来了更大的风险，有可能被误解、未经审查、通过非营利机构传递。

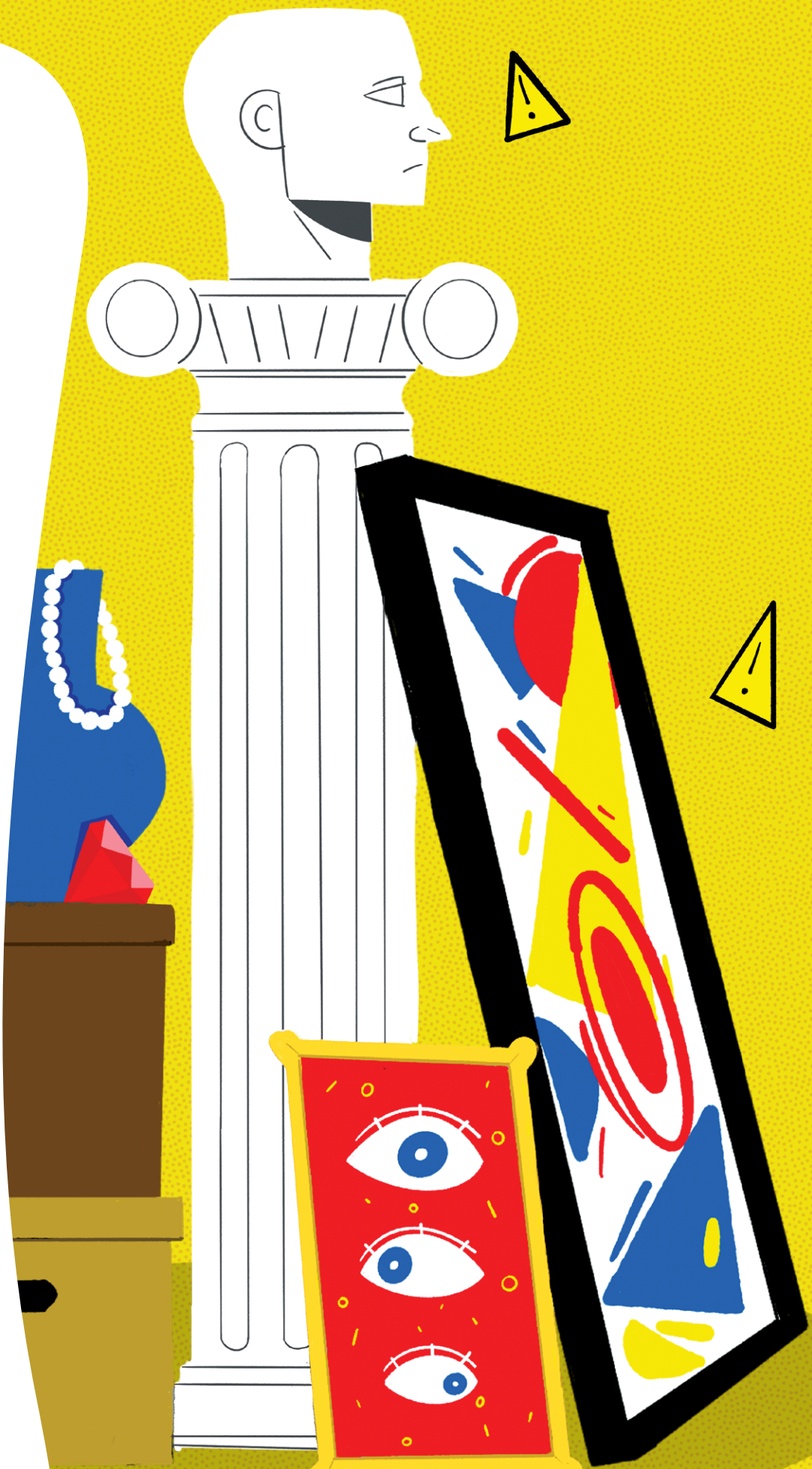
## 案例分析

下面举例说明，对DAF资产进行最低限度的审查就能发现现代版逃税者，更糟糕的是，甚至发现恐怖融资者。

捐赠者是一位非常成功的私营企业家。由于非营利机构依靠资产赠与生存，因此为了推进非营利性使命、造福社会，非营利机构更有可能接受大规模资产类别和资产结构赠与。该捐赠者特别希望向基金会捐赠另类资产，例如通过其私人银行捐赠复杂的离岸和在岸对冲基金，其目的是获得赠与减税优惠，享有就资产的最终赠与方式向DAF提出建议的资格。DAF提供方接受了该项捐赠，仅采取了最低限度的反洗钱和反恐融资措施，由此成为捐赠者潜在非法交易的合法中间人。捐赠者知道，资产接收者是DAF提供方本身，因为现在资产归基金会所有，不在捐赠者的名下。这样，捐赠者就能将复合资产从其名下转入金融系统，造成更多层次，使问题更加复杂，进一步掩饰其潜在非法交易。

## 金融行动特别工作组指南

2002年10月，在发现高风险非营利机构普遍为非法交易提供便利之后，





金融行动特别工作组 (FATF)<sup>6</sup> 针对美国发生的 9·11 恐怖袭击, 采取了有力措施, 大力打击滥用非营利机构的行为。该工作组提出了其 40 项建议中的第 8 条, 以提高人们对非营利机构在全球恐怖融资领域潜在作用的认识。

2014 年, 金融行动特别工作组进行了第三轮评估,<sup>7</sup> 审查各司法管辖区是否符合第 8 条建议的规定。在这次评估中, 该工作组发现这些高风险司法管辖区有 57% 不符合或仅部分符合第 8 条建议的规定。只有 5% 完全符合或基本符合该建议。

## 金融犯罪执法网络近期就非营利机构和慈善机构客户尽职调查工作给出了指导方针

2020 年 11 月, 金融犯罪执法网络与美国联邦银行机构联合发布了一份非常有用的情况说明,<sup>8</sup> 提醒商业银行对慈善机构和其他非营利机构采取风险为本的方法。值得注意的是, 美国并未将整个非营利部门列为“高风险”。但监管机构确实敦促金融机构考虑审查捐赠者。

## 非营利机构可以采取的措施

正如监管机构所指出, 慈善机构和非营利机构应确保“了解您的捐赠者”政策实施到位。当今, 非营利部门不断发展壮大, 非营利机构不应仅仅依靠金融机构“了解您的客户”制度。


在接受复杂捐赠之前, 非营利机构可以成为第一道防线, 投入更多资源实施“了解您的捐赠者”政策和正式尽职调查程序。

在制定“了解您的捐赠者”政策时, 非营利机构可以从下列问题出发:

- 捐赠者的地理位置在哪里?
- 当前的受益所有人是谁?
- 捐赠者目前是否在美国财政部海外资产控制办公室特别指定国民名单上?
- 赠与资产采用什么结构?
- 赠与资产的目的是什么?
- 赠与资产的最终接收人是谁?
- 捐赠者是否打算将资产捐赠给有海外业务的非营利机构?

如果非营利机构发现捐赠者逃避这些简单的“了解您的捐赠者”问题, 则在接受捐赠前应实施增强尽职调查。这种简单的尽职调查可以维护非营利机构的诚信, 提高其声誉。

## 结语

随着犯罪分子对日益流行的 DAF 及其匿名性的了解不断加深, DFA 有可能成为非法交易的目标和掩盖非法所得的工具。非营利机构可以多加询问资产来源, 在发现高风险时开展尽职调查, 从而保护自身和所服务的弱势群体。 

Josh Ortner, CAMS, 美国俄亥俄州

<sup>1</sup> “What is a donor-advised fund?” (何为捐赠者建议基金?), 富达慈善基金会, <https://www.fidelitycharitable.org/guidance/philanthropy/what-is-a-donor-advised-fund.html>

<sup>2</sup> “The 2020 DAF Report” (2020 年度 DAF 报告), 美国国家慈善信托基金, 2020 年, <https://www.nptrust.org/reports/daf-report/>

<sup>3</sup> Abby Schultz, “Donor-Advised Fund Assets Reach \$142B, Grantmaking Hits \$27B” (捐赠者建议基金管理资产达 1,420 亿美元, 捐赠金额达 270 亿美元), 《巴伦周刊》, 2021 年 2 月 2 日, <https://www.barrons.com/articles/donor-advised-fund-assets-reach-142b-grantmaking-hits-27b-01612298241>

<sup>4</sup> “2020 Donor-Advised Fund Report: Grants to Charities Increase 15% to \$27 Billion and Total Charitable Assets Surpass \$141 Billion” (2020 年度捐赠者建议基金报告: 对慈善机构的捐赠增长 15%, 至 270 亿美元, 慈善资产总额超过 1,410 亿美元), Business Wire, 2021 年 2 月 2 日, <https://www.businesswire.com/news/home/20210202005410/en/2020-Donor-Advised-Fund-Report-Grants-to-Charities-Increase-15-to-27-Billion-and-Total-Charitable-Assets-Surpass-141-Billion>

<sup>5</sup> Eileen R. Heisman, “Findings from our 2018 Donor-Advised Fund Report” (2018 年度捐赠者建议基金报告的调查结果), 美国国家慈善信托基金, 2018 年 12 月 3 日, <https://www.nptrust.org/philanthropic-resources/philanthropist/findings-from-our-2018-donor-advised-fund-report/>

<sup>6</sup> “Best Practices on Combating the Abuse of Non-Profit Organisations” (打击非营利机构滥用行为的最佳实践), 金融行动特别工作组, 2015 年 6 月, <https://www.fatf-gafi.org/publications/fatfrecommendations/documents/bpp-combating-abuse-npo.html>

<sup>7</sup> “Risk of Terrorist Abuse in Non-Profit Organisations” (非营利机构被恐怖主义滥用的风险), 金融行动特别工作组, 2014 年 6 月, <https://www.fatf-gafi.org/media/fatf/documents/reports/risk-of-terrorist-abuse-in-non-profit-organisations.pdf>

<sup>8</sup> “Joint Fact Sheet on Bank Secrecy Act Due Diligence Requirements for Charities and Non-Profit Organizations” (关于慈善机构和非营利机构的银行保密法尽职调查要求的联合情况说明), 美联储系统理事会、联邦存款保险公司、金融犯罪执法网络、国家信贷联盟行政署、美国货币监理署, 2020 年 11 月 19 日, [https://www.fincen.gov/sites/default/files/shared/Charities%20Fact%20Sheet%2011\\_19\\_20.pdf](https://www.fincen.gov/sites/default/files/shared/Charities%20Fact%20Sheet%2011_19_20.pdf)



何故？

何事？

何地？

何人？

# 猜谜： 出口 管制？

## 各

国政府纷纷想方设法达成国家安全和外交政策目标，监管重点也日渐转向出口管制合规。长期以来，政府领导人一直把出口货物管制作为工具，防止危险产品（如武器、化学品）进入普通分销渠道，防止战略产品（如超级计算机、先进电子产品）落入对手手中。随着时间的推移，结果形成了高风险的监管“拼图”，既需要破译，也需要遵从，就像猜谜一样。《韦氏词典》把“谜语”一词定义为“作为需要解决的难题提出的，令人迷惑费解且具有误导性的问题。”许多金融合规从业人员可能会用这个定义来描述出口管制；然而，出口管制并非如此令人生畏。无论货物来自何方，去向何处，始终都有四个谜需要解决：产品是什么？去哪里？发给谁？为什么？



## 白话出口管制

若非当然权利，世界上任何国家或地区的公民和企业都无权出口，除非他们获得了政府的许可。另一方面，没有政府愿意花费时间和资源审查所有交易的出口许可申请。为此，政府制定了出口管制规则，正如其名，这些规则旨在对本国/地区的出口货物流动进行控制。出口管制规则和最佳实践建议构成一个整体，表示政府试图在“危险”和“不危险”两类出口货物、产品、技术和服务的控制上取得平衡。凡列入受控清单，均须取得出口许可，但这一要求仅限于某些情况。政府让出口商自己确定在什么情况下不需向政府申请出口许可证，在什么情况下需要考虑全部出口管制规则。

在明确提出许可申请并取得出口许可证之后，出口商在哪些情况下可以继续进行交易，情况千变万化。随着商用和军民两用产品的发展、成熟和上市交易，出口管制也会随之变化。此外，出口管制也会出于犯罪控制、外交政策、国家安全、国内经济的需求，当然还有政治的考量而变化，有时甚至会发生重大变化。出口法规、法令和法律先例多达数万页，内容令人迷惑费解，偶尔还具有误导性，当然在要求细节上也令人难以捉摸。这些因素需要从整体上把控并采取行动，这正是全球贸易合规经理、董事及其员工的职责。



对于偶尔参与出口管制合规工作的其他所有人来说，那些看似令人迷惑费解、偶尔具有误导性的细节可以归为四个简单的谜语。知晓解谜之道是理解出口管制的核心。

### 谜语1：出口的产品是什么？

出口的产品类型对于解答出口管制的第一个谜语至关重要。如果装运的是回形针、尺子或其他办公用品，这类良性商品无需考虑安全或外交政策因素。因此，政府肯定不希望出口商就订书机申请出口许可证。但对于特定产品类别（如导弹、弹药、高端计算机和核原料），政府就需要要求出口商提交冗长而详细的出口许可申请。在两个极端之间还有很多产品，如医药、电子、电池、多类工业品。所有实物商品分为两类：出口管制商品和非出口管制商品。此外，用于支持出口管制商品的多数无形商品亦受管制，如售后服务电话、技术支持、软件、加密技术和其他技术，这类无形商品的作用是使出口管制商品保持正常

运行。如果某个商品、软件或技术受管制，则针对每个出口国家/地区进行分类，分配一个出口分类号（ECN）。分配的这个ECN号决定了出口商的产品是否符合出口许可证的要求。在令人迷惑的大量例外和豁免条件下，产品及其相关技术和服务也可以免除出口许可义务。要知道，出口管制合规领域存在“抓放”原则，并且该框架的实操由全球贸易合规团队负责。产品是什么？本谜语的谜底可以在商品的ECN号中找到。

### 谜语2：去哪里？

要理解出口管制，一个重要方面是了解与出口管制风险管理相关的风险。可以说，出口去向与产品本身同等重要。值得一提的是，某项商品能出口并不表示其到货即可进口。基于地点的出口管制非常复杂，体现为制裁、禁运、条约授权、国家级和多国国别管制以及机构管理此类风险的意愿。有些出口目的地受到严格限制，出口商根本不会去费心申请出口许可证，因为即使是不受管制的办公用品也属禁止范围（比如美国对朝鲜、叙利亚和古巴的出口）。除严格管制商品、酷刑工具和大规模杀伤性武器外，针对其他国家或地区的出口管制屈指可数。在其他国家或地区，只有某些地区（如乌克兰克里米亚共和国）或特定地址（如海外资产控制办公室和类似国际机构公布的制裁清单所列地址）



要求取得出口许可证。但大多数国家或地区处于中间位置，出口许可证的必要性取决于产品（谜语 1）以及机构全球贸易合规团队负责解读的、令人眼花缭乱的量多边和双边规则。如果把商品发往或转往伊朗，大型跨国商业出口商通常会陷入困境，部分原因是《伊朗贸易制裁条例》难以理解，增加了合规管理的难度。最后，许多基于地点的出口管制在实施时不会考虑出口行为的实际发生地点，进一步增加了操作难度。为了应对与这种（有时）难以理解的大量规则相关的风险，机构会颁布自己的国别“禁运”管制措施，其依据不仅仅是政府的强制性规则，也包括公司声誉、绕行、信用和公司愿意承担的其他经营风险。出口商品的去向决定着实施的出口管制措施，也是谜语 2 的谜底。

### 谜语 3：发给谁？

这是出口管制的谜语 3，反金融犯罪人士应该最为熟悉。商业伙伴和交易对手制裁名单筛查、所有权结构分析、国有实体审查和军事隶属关系验证，这些是解答出口管制谜语 3 的重要内容，就如它们在金融犯罪分析中一样重要。如果机构通过尽职调查流程确定，潜在业务伙伴的财务供应链或整体合规状况不符合标准，则不建议与该合作伙伴共同参与实体供应链。政府执法官员

十分有效地明确传递出了这一信息。但解答谜语 3 不能仅停留在表面。


办公用品，没问题。制裁名单筛查，没问题。从美国发往德国，没问题。发给德国军队——有问题！本次出口交易涉及的产品和国家或地区不会触发许可证要求，买方不是被制裁方，但“发给谁”这个谜语的谜底是军事机构，这正是改变交易有效出口管制规则的因素。虽然军事最终用户规则最近才成为头条合规新闻，但最终用户政军关系验证作为出口管制的一个方面已有数十年。尽管评估最终用户相关业务类型费力又费时，却是解答出口管制谜语 3 的必备条件。

### 谜语 4：为什么？

巴西一家孤儿院为什么要买高端超级计算机？问得好，不查就出口，后果要自负。除非在交易过程中出现这种恶意危险信号，否则大多数出口商不需要找出买家订购产品的原因或产品的使用方式。出口商需要进行制裁和受限方筛查，根据产品进行军事最终用途核查，对照国家/地区目的地清单比较产品的指定 ECN 号，视情况取得出口许可证，完成基于国家/地区的风险核查。采取这些步骤即可解答前三个出口管制谜语。第四个谜语过去几乎无需提出，但在当今紧张的合规和风险缓释环境下，要多提。即使出口交易

不涉及两用（商用和潜在军用）商品，也需如此。买家为什么需要这一商品？预期用途是什么？他们买此商品是否合理？购买量是否合理？他们从这家公司买是否合理？最终用途审查在商业上要深入，对经营会造成多大影响，这是个主观问题。虽然军用和军民两用商品出口商对此习以为常，但对大多数其他出口商来说，却是个全新的概念。基础总是很重要，必须解出前三个谜语：产品是什么，去哪里，发给谁，这些至关重要。在确定最终用途验证要求时，这些因素的综合作用是不断变化的。中断出口交易去解答谜语 4 会耗费公司的时间和财力，使得本已十分庞杂的供应链变得更加复杂。

### 这些谜语不难猜，对吧？

虽然非常复杂，合规风险巨大，但出口管制并不像看起来那么令人生畏。跟风险为本合规制度一样，出口管制就是要在保持业务发展及合规之间取得平衡。这就是风险为本出口管制合规制度的首要目标，也是政府要求机构制定合规制度的初衷。 

Anne Marie Lacourse,  
美国道琼斯风险与合规公司顾问,  
[annemarie@lacourse.us](mailto:annemarie@lacourse.us)



## ACAMS 专题证书课程

### 满足不同业务条线的实务工作需求及不同规模合规团队的建立

ACAMS 证书课程以在线学习的模式，针对不同的反洗钱犯罪领域，提供深入的培训。证书课程适合各种规模的合规团队，也不仅限于初级及中级合规专业人员，而且对于资深员工而言也是难得的再培训或深化课程。

提供简体中文的在线证书课程包括：



#### 金融科技企业反洗钱基础课程 AML for FinTechs

提供金融科技业所需的知识和实际步骤，协助金融组织建立及落实稳健可靠的反金融犯罪计划。



#### 金融科技企业客户课程 FinTechs as Your Customers

揭示金融科技机构的运作模式，说明如何针对潜在和现有的金融科技客户，进行开发及制定有效的金融犯罪风险管理策略。



#### 贸易洗钱课程 Trade-Based Money Laundering

协助您的团队了解各种形式的贸易洗钱行为，例如地下金融系统，装载不足、黑市比索交易等。



#### 制裁基本原则课程 Sanctions Foundations

确保员工接受充分培训，以了解并识别具有制裁风险的交易。



#### 交易监控课程 Transaction Monitoring

帮助您的团队确定触发洗钱警报的条件，学习如何正确应用控件进行监控。



#### 了解您的客户 / 客户尽职调查课程 — 进阶 KYC/CDD Intermediate

扩展您的调查技巧，探索第三方的解决方案，识别空壳公司，并了解最终受益人的法规。

ACAMS 亦提供其他英文在线证书课程，请浏览 [acams.org/certificates](https://acams.org/certificates) 了解更多。





# 加密货币 退出骗局——

骗局解密及防骗攻略



多

年以来，加密货币一直是一个富争议的话题，主要原因是有两股力量在彼此博弈。

一方是加密货币技术的信徒、未来主义者和创新者购买比特币，<sup>1</sup> 并把它们安全地存起来。

另一方是有些人瞄准受教育程度较低的人群，试图利用他们知识匮乏的弱点，骗他们放弃加密货币。这种行为以多种不同方式表现，并且难以识别。

随着加密货币的发展，这些骗局采用的手段也在不断演进。退出骗局就是最难发现的一种骗局。那么，退出骗局到底是什么意思，如何避免成为当中受害者？本文将对退出骗局进行定义，并就如何防骗提出建议。

## 什么是加密货币退出骗局？

退出骗局指通过从市场上“撤出”所有资金、从早期投资者身上获利的一种加密货币。换句话说，拥有大量特定新加密货币的人试图通过营销和促销活动人为抬高（哄抬）价格，后来却将他们的个人包袱甩给（甩卖）新的投资者。

## 在哪里可以发现这样的骗局？

2017 年，随着首次募币 (ICO) 快速发展，加密货币退出骗局大肆流行。前景良好的新项目利用其影响力和社群推广即将推出的代币，承诺超高的回报率，后来却跳过交付流程，卷款跑路。

最近，随着加密货币领域的发展，出现了各种不同形式的相关“退出骗局”：

- 在非集中化交易所上市的非集中化金融相关项目存在极大的风险，因为这个领域到处都是“拉地毯”骗局（另一种形式的退出骗局）。这种情况已发生多次，甚至在主流集中化交易所上市的代币也出现过这种骗局。例如，Iron Finance 近期的 TITAN 项目因获得 Mark Cuban 的投资而大受欢迎。<sup>2</sup> 在被“拉地毯”后，Cuban 呼吁加强对加密货币领域的监管，<sup>3</sup> 但由于该领域具有去集中化的性质，因而是无法进行监管的。
- 当今时代，只要粉丝足够多，任何人都可以推出同质化代币 (NFT)，比如名人、油管达人、运动员，不一而足。现在，只要看到这个领域过度饱和的状态，就会感觉 NFT 似乎代表着“无才无能” (No Freaking Talent)。然而，代币售价通常达数十个以太币，最后却丧失流动性，所有人都对二级市场失去兴趣。这方面的一个例子是 Logan Paul 最近推出的同质化代币，其承诺向三名买家赠送价值 40,000 美元的第一版宝可梦卡以及其他奖品。该代币最初估值超过 20,000 美元，但现在有一部分在 OpenSea 上的售价不到 1,000 美元，而且无人问津。<sup>4</sup>
- 最后，近来出现了一个非常有意思的概念，就是卖推特。换言之，人们可以买下名人推特的所有权，把它变成同质化代币。发布几天后，一位用户用 639 美元买了一个推特，但这个推特不久后却被删除了。<sup>5</sup> 这是一个真正的退出骗局。

## 保护自己，远离退出骗局

在这个相对成熟阶段进入该领域的大多数投资者可能想知道，如何才能有效地发现哪些项目合法，哪些不合法。就退出骗局而言，可以记住以下与投资策略有关的贴士：


- 先不要冲动购买喜欢的油管达人推广的代币（其价格通常已经处于高位），要先审查项目的基本面。项目通常只是现有解决方案的廉价“副本”，缺少支撑将来增长的坚实基础。
- 如果遇到回报率高于平均水平的项目，务必要进行调查研究。虽然有些项目可能是合法的，但有些项目却可能非常危险。更具体地说，一定要全面了解加密货币的权益质押、收益率耕作和高收益率储蓄账户等知识。此外，要定期通过 CoinGecko 等价格跟踪平台，获取有关目标代币的最新信息和研究资料。
- 如果有感兴趣的项目并有强烈的买入冲动，不妨等一等。至少等一周的时间，观察价格走势。很多时候，推广者会局部高价推广代币，



这样，有意买入的各方可以先让市场冷静下来，然后在更好的点位买入。

最重要的是，要知道耐心持有加密货币的价值才会增加。虽然最爱的推特账户可能渴望得到100倍杠杆的小盘代币，但如果秉承长期投资理念，实际获利的几率会成倍增加。

因此，尽管加密货币价格经常出现中期波动，但一定要知道赢家通吃的道理。<sup>6</sup> 投资比特币、以太坊以及 UNI、BNB、FTT 等主流交易所的原生代币。虽然价格在短中期内可能有波动，但现在有足够的证据表明，其长期呈现上升趋势。即使情况并非如此，但此类项目大量的流动性使得投资者能够快速买卖持有的头寸。这在 NFT 世界中是不可能的，因为在 NFT 世界里，用户经常在市场下滑期间被昂贵的艺术品套牢，付出高昂代价，后悔不已。

在数字资产投资中，信心、流动性和真实案例仍然是最重要的因素。为免被骗，务必要秉承以下原则：“如果好得令人难以置信，很可能是骗局。” 



Judy Smith, Paybis 营销经理 / 作家, 拉脱维亚,  
smijudy33@gmail.com

<sup>1</sup> “Buy Bitcoin with Credit Card or Debit Card” (用信用卡还是借记卡买比特币), paybis, <https://paybis.com/>

<sup>2</sup> Jeff Benson, “Mark Cuban ‘Hit’ by Apparent DeFi Rug Pull” (Mark Cuban 受到去中心化金融拉地毯骗局打击), Decrypt, <https://decrypt.co/73810/mark-cuban-hit-apparent-defi-rug-pull>

<sup>3</sup> Billy Bambrough, “Billionaire Bitcoin Investor Mark Cuban Calls For Crypto Regulation After Price Of Radical New Token Suddenly Crashes To Zero” (比特币亿万富翁投资者 Mark Cuban 在激进新代币价格突然跌至零之后呼吁对加密货币进行监管), 2021 年 6 月 18 日, <https://www.forbes.com/sites/billybambrough/2021/06/18/billionaire-bitcoin-investor-mark-cuban-calls-for-crypto-regulation-after-price-of-radical-new-token-suddenly-crashes-to-zero/?sh=1361db762607>

<sup>4</sup> Geoff Weiss, “Logan Paul Sells \$5 Million Worth Of NFTs Ahead Of His Pokémon Box Break” (Logan Paul 在宝可梦拼单活动之前卖出了价值 500 万美元的非同质化代币), Tubefilter, 2021 年 2 月 22 日, <https://www.tubefilter.com/2021/02/22/logan-paul-sells-5-million-nfts-pokemon-box-break/>

<sup>5</sup> Jamie Redman, “NFT Immutability Debate Grows as Tokenized Tweets Get Deleted and NFT Images Are Replaced” (代币化推特被删, NFT 图像被换, NFT 不变性引发更多争议), Bitcoin.com, 2021 年 3 月 11 日, <https://news.bitcoin.com/nft-immutability-debate-grows-as-tokenized-tweets-get-deleted-and-nft-images-are-replaced/>

<sup>6</sup> “Prices” (价格), paybis, <https://paybis.com/price/>



# 国际制裁合规师 (CGSS)

考获由公认反洗钱师协会 (ACAMS) 推出的全球认证 – CGSS，彰显机构及其员工对遵守制裁法规，及建立专业制裁合规团队的承诺。

CGSS 简体中文版学习教材以及考试现已正式上线。

下载《考生手册》：[www.acams.org/cgss](http://www.acams.org/cgss)



# 数据对合规和反金融犯罪工作的影响

## 针

对金融机构的威胁持续增多，不仅如此，监管和合规要求亦不断变化，结果形成了一个艰难的环境，使得业务难以开展。最近的一份报告指出，自 2019 年以来，全球罚款和处罚量增加了 141%，仅总部设在美国的金融机构就遭到了 75 亿美元的罚款。<sup>1</sup> 全球疫情只会继续增加这些风险的数量，加快其速度，加剧其复杂性，进而推动对数据和合理洞察的需求，以正确避免和缓释风险。但太多的金融机构并不健全，无法正确管理数据，这可能会造成可怕的后果。

毕竟，数据是反金融犯罪行业的命脉。借助以有效且高效的流程管理的优质数据，使金融机构的领导者在角色中取得成功。随着世界开始从疫情复苏，数据环境发生了明显的变化。促成这些变化的因素主要有两个：

- **监管重点不断演变：**国内和国际监管机构正在重塑和扩大其职责范围。人们期望对新兴技术进行审查、测试和部署。例如，美国《2020 年反洗钱法》(AMLA) 专门解决行业技术能力问题。不出所料，由于公司正忙着努力重组其技术和人力资源去解决这些警报，金融机构在 2020 年和 2021 年的响应有所减弱。
- **数据的量和多样性问题日益复杂：**近年来，银行和其他金融机构积累了大量客户和合作伙伴数据。再加上来自暗网、加密货币和电子通信的数据，新的挑战已经出现；这些数据根本无法分离到并非针对这些数据源和类型设计的先有技术和 workflows 当中。

## 增效方案

业界前所未有地依赖虚拟数据生态系统，但传统数据源和分析这些数据的不同传统技术系统也承受着前所未有的压力。许多金融机构采取了积极的数字化战略，部分是为了提高效率、深化与全球客户的合作。但这些战略显著增加了数据量，然而，已经不堪重负机构缺少对这些信息进行相应协调、解释和行动的能力。特别是对于金融机构而言，在欧盟“支付服务指令 2”等新法规的背景下，这会直接影响金融机构满足日益增长的“了解您的客户”和客户尽职调查要求的能力。因此，金融机构现在必须采取额外措施，了解其客户的客户。此类要求给现有技术和合规工作带来了更大的压力。

传统合规解决方案依赖核心银行系统和来自多个地点的其他运营数据源中提取的批次数据或一天的旧数据。在逐步走向实时交易的当今世界，这会造成显著的延迟；决策时间需要达到微秒级才能打击机构面临的许多威胁，包括监管问题，也涉及到支付欺诈、网络攻击等。



除了数据处理挑战，还有一个更大的问题：这些系统用于回答现有交易监控 (TM) 考试问题的分析策略存在不足。许多规则是基于上世纪 90 年代业界已知和所理解的非法犯罪活动制定的，此后几乎没有更新。它们倾向于一视同仁地对待所有客户，但事实并非如此。它们很少包括或适当地利用来自客户尽职调查系统或其他客户接纳及定期风险评估数据的风险指标。这些规则往往与其他规则相互排斥。因此，它们无法根据实体的整体行为充分识别实体的整体风险。

结果如何？大量的噪音导致误报。误报率最高达 90%，<sup>2</sup> 这意味着调查人员无法高效地工作，运营成本高昂，甚至更糟：调查人员无法专注于识别金融机构面临的真实、复杂的威胁，而这类威胁通常会因违规登上新闻头条。虽然这并非新的问题，但大多数人会说误报水平在不断增高，使调查人员需要处理所积压的工作越来越多。

问题的核心是与银行客户相关的数据，而且需要 360 度全方位、清晰地了解客户身份及其有效预测行为。通过调高或调低灵敏度来更改警报阈值会违背有效识别洗钱、欺诈或制裁违规行为的初衷。准确判断何为合法客户行为——基于可靠和完整的客户相关数据，在风险评级矩阵中准确评分——是实现高效预防和有效合规的唯一途径。然而，找到这种平衡需要新的动态方法，不再依赖于通过不堪重负的不同数据采集和交易监控系统进行过时的静态数据分析。

相反，机构必须摆脱传统的核心银行交易监控范式，利用实时流分析技术弥补缓慢、过时的批处理架构方法的不足。数据量和数据类型的多样性只会促进信息在不同业务条线的共享。捕捉到数据后，需要有效的技术以微秒级的时间精度即时分析信息，并在适当的时候生成警报。


通过在前端部署技术进行分析，金融机构可以按特定路线传输结果，解决正在处理的各种“测试”问题。通常，对于架构相同的许多业务条线来说，这些问题都需要回答。通过部署实时数据分析的结果，现在可以在许多业务条线之间无缝共享报告，这些报告过去一直被“锁在”单一的孤岛式技术分析和报告环境当中。借助这种更高效的数据捕获和存储技术，通过赋能和融合人工智能 (AI)、机器学习或机器人过程自动化 (RPA) 得到的结果具有更大的价值。

## 结语

显然，金融机构现在面临的挑战是评估当前的技术，确定如何以及能否对这些技术进行现代化和调整，以应对海量数据的冲击和不断变化的威胁环境。通过以下步骤可以确定一个基准，提升业务管理水平和风险防范能力：

1. 对现有处理方法和实践进行审计，找出问题的根本原因，包括接收的数据内容和接收方式，以确定数据质量和内容对最终结果的影响。这项审计工作可由第三方咨询机构与技术供应商共同开展。
2. 征询内部团队成员的意见和见解，揭示现有技术的不足，然后启动项目，更新、更换或增强这些技术。
3. 仔细审查侧重于业务条线要求的现有监管要求，确定必须解决的紧迫需求，以避免处罚或强制纠正。考虑采用一种替代技术，通过改进处理方法、帮助人力资产更高效地执行任务来降低这种风险。
4. 购置流分析技术，部署在核心银行系统前部，集成到支付处理渠道，主动应对风险，而非像目前这样，采取一种“事已至此”的被动响应策略。
5. 采用高级分析技术进行异常检测，揭示现有规则无法识别的风险，发现前所未见且可能导致罚款的风险。
6. 增强现有的交易监控系统，在生成警报后，对“实体”进行 360 度全方位行为风险分析，通过在 1 级“分类”和 2 级“处置”步骤的机器人流程自动化，减少噪音、防止误报并提高效率。这样做最终会降低成本、识别真正的风险并使金融机构在监管机构那里保持良好的信誉——最终避免罚款、股东价值损失和声誉受损。

金融机构每天都要打击试图破坏其技术基础设施的企图。勒索软件攻击和需求影响了金融机构、企业和政府实体的运营和响应方法。在美国和其他国家，国内恐怖分子的演变改变了金融机构识别个人及其资产的责任，这些信息可能存在于客户的账户和相关行为当中。

您是否优化了技术和合规方法，做好准备迎接新的现实？ 

John Dalton, KX 高级副总裁兼金融服务产品与解决方案战略部全球主管

Robert Goldfinger, CAMS, 退役上尉, KX 金融犯罪技术销售主管

<sup>1</sup> Jaclyn Jaegar, “Report: Fines against financial institutions hit \$10.4B in 2020” (报告：2020 年对金融机构罚款金额达 104 亿美元), Compliance Week, 2020 年 12 月 22 日, <https://www.complianceweek.com/surveys-and-benchmarking/report-fines-against-financial-institutions-hit-104b-in-2020/29869.article>

<sup>2</sup> Stuart Breslow et. al, “The new frontier in anti-money laundering” (反洗钱的新前沿), 麦肯锡, 2017 年 11 月 7 日, <https://www.mckinsey.com/business-functions/risk-and-resilience/our-insights/the-new-frontier-in-anti-money-laundering>



## 勒索软件、加密货币和洗钱之间的关系





## 2

2021 年 5 月，美国弗吉尼亚州、佐治亚州和北卡罗来纳州的汽车司机惊惶失措，

争先恐后前往加油站加油，原因是 Colonial Pipeline 公司遭受网络攻击，被迫关闭柴油、汽油和航空汽油供应，造成油荒。Darkside 发动的勒索软件攻击导致 Colonial Pipeline 运营中断——该犯罪团伙要求支付 75 个比特币（430 万美元）的赎金。Colonial Pipeline 支付比特币后，收到了解密工具，解开了被黑客入侵的系统。<sup>1</sup>在 7 月 3 日发生的另一个案例中，连锁超市品牌 Coop Sweden 旗下 500 家超市被迫停业，因为其销售点收银台和自助结账通道停止工作。连锁超市本身并非黑客攻击的对象，但一家软件提供商受到勒索软件攻击，因而被附带波及。这家提供商提醒所有客户，立即停止使用其服务并下线。<sup>2</sup>

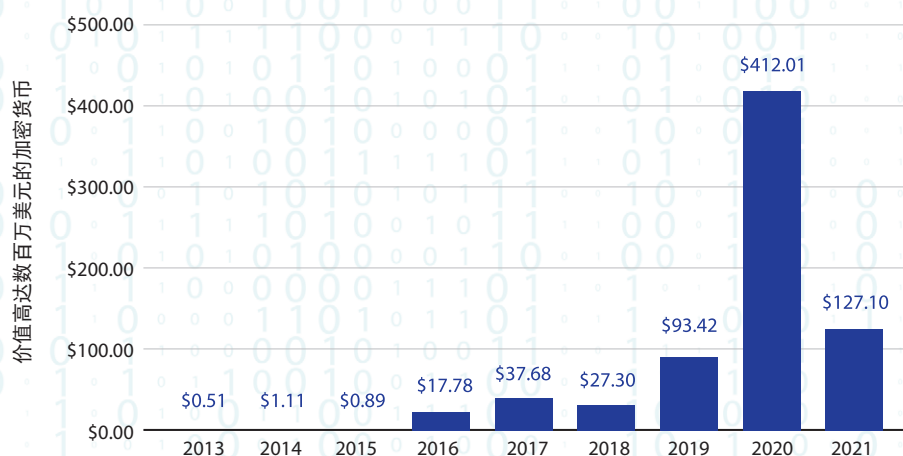
FBI 网络犯罪小组通过赎金追踪到加密货币地址，追回了由 Colonial Pipeline 支付的 63.7 个比特币（230 万美元）。<sup>3</sup>但 Colonial Pipeline 并不是唯一的受害者。被勒索软件犯罪分子如 Ryuk / Conti、Sodin / REvil、ClOp、DoppelPaymer、DarkSide 和 Avaddon 祸害的其他机构还包括加拿大飞机制造商庞巴迪、华盛顿特区警察局、电子公司宏碁、科罗拉多大学、亚特兰大和巴尔的摩、广达计算机公司和 CNA 金融公司。勒索方式大多为加密货币——也称为可兑换虚拟货币（CVC）。这是价值的一种数字表示，是一种交换媒介、一种记账单位和价值储存手段。加密货币不由任何实体发行，亦不受监管。从事 CVC 交易者要自担风险，并接受汇率的大幅波动。

## 加密货币对勒索软件的诱惑力

2020 年，超过 4 亿美元的加密货币被汇入与勒索软件犯罪分子有关的数字地址；执法机构、金融机构、保险公司和其他利益相关的部门或机构要注意这个趋势（见图 1）。

图 1：勒索软件地址收到的加密货币总价值

2016 - 2021（年初至今）



资料来源：“Ransomware 2021: Critical Mid-Year Update”（勒索软件 2021：年中重要更新），Chainalysis，2021 年 5 月，<https://go.chainalysis.com/rs/503-FAP-074/images/Chainalysis-Crypto-Crime-2021.pdf>

犯罪分子对加密货币情有独钟的原因是什么？加密货币为何如此受欢迎？词根“crypto”源自希腊语 kryptós，表“隐藏”之意。根据当今的说法，加密货币指比特币、以太坊、莱特币、Zcash 和鲜为人知的门罗币等另类支付机制；谷歌搜索结果显示，门罗币宣称具有“安全、私密和不可追踪”的特点。黑客喜欢加密技术的匿名性和不透明性，这样可以保护数字地址和掩盖资金目的地。他们通过运行电子邮件网络钓鱼活动、利用远程桌面协议漏洞、识别广泛使用的软件程序中的安全漏洞，用恶意软件感染受害者的计算机。恶意软件对公司计算机上的数据加密，使其无法使用。网络犯罪分子将公司扣为人质，威胁若收不到赎金，会销毁受害者的数据或将其发布在社交媒体上。只有收到赎金才会解密信息并恢复对系统或数据的访问。千万不能低估勒索软件对国家、政府机构、警察和消防部门、医院、航空公司和其他关键基础设施运营的影响。

## 加密货币类洗钱活动的三个阶段

只要将 CVC 用作交换媒介，勒索软件就与洗钱形成了关联关系。图 2 所示为 CVC 洗钱活动的三个阶段。在这一趋势不断深化的背景下，金融犯罪执法网络在 2020 年 10 月发布了一份咨询报告。<sup>4</sup> 据金融犯罪执法网络：“勒索软件付款的处理通常包括多个步骤，涉及至少一个储蓄保管机构和一个或多个货币服务企业 (MSB)。” 由于多数受害者没有加密货币钱包或账户，因此交付赎金需要将资金从他们在受监管金融机构开立的银行账户转移到 CVC 交易所。这属于处置阶段。此外，还出现了这样一些情况，数字取证和事件响应公司或网络保险公司收到受害者的资金，将其兑换为 CVC，然后把 CVC 转移到网络犯罪分子控制的指定数字地址。

在另一种方法中，骗子诱使人们接受将资金“捐赠”到他们自己的银行账户，并会给他们一笔好处费。骗子会告诉他们，将资金转换为 CVC，再汇入到不同的数字地址。“捐款”很可能是赎金或从他人那里偷来的钱。新冠疫情期间，有许多钱骡愿意允许骗子利用他们的银行账户或数字地址进行非法勾当，毫无愧疚之意。

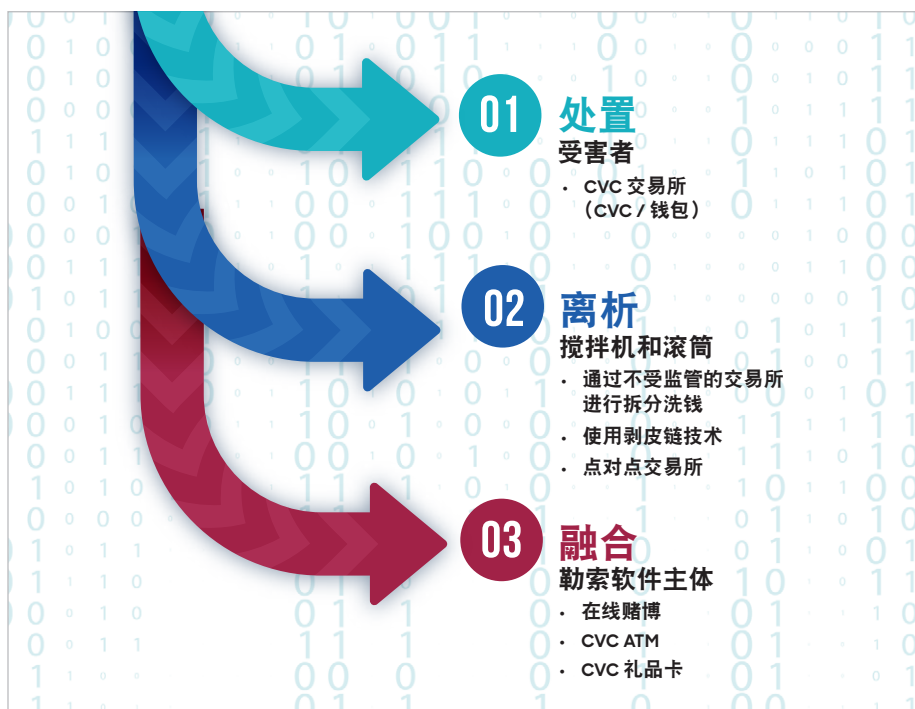
犯罪分子在随机时间段内将来自数字地址链的多笔资金汇集在一起，由此将收到的赎金与其他加密货币资金混在一起，进入离析阶段。这样做是为了掩盖 CVC 踪迹，打破 CVC 发送地址和 CVC 接收地址之间的联系。AlphaBay、Helix、Darklauder、Bitlaunder 和 CoinMixer 等搅拌机和滚筒平台接收加密货币，把不同来源的资金混合起来，然后汇回另一系列目的地地址，支付 1%

到 2% 的手续费。据 Chainalysis 分析，<sup>5</sup> 根据交易的复杂程度，混合所需的时间短至 1 到 6 个小时，长至 7 天。交易通过混合服务后，与代币关联的地址记录会被有效地删除。<sup>6</sup>

其他离析方法涉及通过大量账户和交易所拆分的加密货币交易，或者将 CVC 转移到反洗钱 / 反恐融资 (AML/CTF) 控制薄弱的知名司法管辖区不受监管的交易所或点对点交易所。这种方法要用到剥皮链技术，剥皮链是一种钱包链，资金会通过这些钱包掩盖非法所得 CVC 的踪迹。

加密货币洗钱最后是融合阶段，此时赎金被合法化，证明其合法属于网络犯罪分子所有。帮助洗白数字资产的渠道包括不受监管的加密货币交易所，这些交易所不要求核查用户身份，安全政策宽松。它们可以帮助将 CVC 兑换为法定货币。其他交换媒介包括接受 CVC 付款的在线游戏和赌博网站，CVC 可用于购买积分或虚拟筹码。犯罪分子经常光顾这些网站，并通过一系列小额交易将 CVC 转换成法定货币。另一种交换源是 CVC ATM 和 CVC 礼品卡。据 coinatmradar.com 指出，7 月初全球约有 23,000 台加密货币 ATM。<sup>7</sup> 数量虽然不多，却足以支持洗钱活动。同时也出现了一种趋势，消费者用加密货币购买奢侈品。高档手表制造商 Franck Muller 今年早些时候推出了一款价值 12,000 美元的手表，其具备钟表和数字钱包双重功能。这款手表仅可通过比特币购买，41 毫米表盘上刻有独有的公共地址，私钥保存在密封的 USB 当中。<sup>8</sup>

图 2：CVC 洗钱的三个阶段





## 金融机构、受监管 CVC 交易所、网络保险公司和执法机构迫在眉睫的风险是，对控制 CVC 资金的收款人身份知之甚少

### 结语

对于那些试图规避严格资本管制、洗白非法所得或逃避对国家或地区、公司、个人或恐怖组织的金融制裁的人来说，加密货币是一个理想的选择。金融机构、受监管 CVC 交易所、网络保险公司和执法机构迫在眉睫的风险是，对控制 CVC 资金的收款人身份知之甚少。如果收款地址属于受制裁个人或或者位于受严厉制裁的司法管辖区中与勒索软件有关连的网络犯罪分子，该怎么办？海外资产控制办公室已经将两个数字货币地址与针对公司、医院和大学的 SamSam 勒索软件攻击的受制裁犯罪分子联系起来。这些钱包地址被用来与全球 40 多个不同的数字货币交易所进行交易，成为洗钱离析阶段的一部分。<sup>9</sup>

遗憾的是，数字货币地址列表并不详尽，也不全面。如果有隐形地址则更糟。汇款人每笔交易使用一个一次性地址，就属于这种情况。同一汇款人对同一收款人完成的多笔交易采用不同的地址，掩盖了 CVC 付款细节及其财务明细。因此，如果发现资金流向受制裁的个人或实体，参与或协助对数字货币地址交易的机构将面临罚款和无法使用其美元清算授信的风险。

尽管一些监管机构要求完全透明并披露受益人和汇款人的地址，以及法定货币资金转移的目的，但他们并未限制其管辖范围内虚拟货币的持有和交易。存在不同程度的控制——某些国家或地区已经禁止金融机构和支付公司提供加密货币交易相关服务，但并未禁止其公民持有 CVC。其他国家或地区则让金融机构自行决定——其中许多金融机构向客户明确表示，不能用他们的银行账户进行加密货币交易。

最近的卡比斯湾 G7 峰会公报强调，政府需要“识别、打击境内实施勒索软件攻击、滥用虚拟货币洗钱及实施其他网络犯罪的人并追究他们的责任。”<sup>10</sup> 但是，在加大力度实施跨境协同之前，相关机构必须主动实施网络安全控制，定期进行业务连续性模拟，推动落实网络卫生实践做法，<sup>11</sup> 因为未雨绸缪胜过亡羊补牢。A

Deepa Chandrasekhar, 联合海湾银行高级副总裁、首席合规官、洗钱报告专员

本文仅代表作者的个人观点，并不代表其所在机构观点。

<sup>1</sup> Thomas Brewster, The Ransomware Group Behind The Colonial Pipeline Hack Says It Is Disbanding” (Colonial Pipeline 黑客攻击背后的勒索团体称即将解散), 《福布斯》, 2021 年 5 月 14 日, <https://www.forbes.com/sites/thomasbrewster/2021/05/14/the-ransomware-group-behind-the-colonial-pipeline-hack-says-it-is-disbanding/?sh=14e242eb7775>; Nicole Perloth, “Colonial Pipeline Paid 75 Bitcoin, or roughly \$5 million, to hackers” (Colonial Pipeline 向黑客支付 75 个比特币 (约合 500 万美元)), 《纽约时报》, 2021 年 5 月 13 日, <https://www.nytimes.com/2021/05/13/technology/colonial-pipeline-ransom.html>

<sup>2</sup> Joe Tidy, “Swedish Coop supermarkets shut due to US ransomware cyber-attack” (瑞典 Coop 超市因美国勒索软件网络攻击关闭), BBC, 2021 年 7 月 3 日, <https://www.bbc.com/news/technology-57707530>

<sup>3</sup> Matthew J. Schwartz, “How Did FBI Recover Colonial Pipeline’s DarkSide Bitcoins?” (联邦调查局是如何追回 Colonial Pipeline 支付给 DarkSide 的比特币的?), BankInfoSecurity, 2021 年 6 月 11 日, <https://www.bankinfosecurity.com/how-did-fbi-recover-colonial-pipelines-darkside-bitcoins-a-16863>

<sup>4</sup> “Advisory on Ransomware and the Use of the Financial System to Facilitate Ransom Payments” (关于勒索软件和利用金融系统促成勒索赎金支付的公告), 金融犯罪执法网络, 2020 年 10 月 1 日, <https://www.fincen.gov/sites/default/files/advisory/2020-10-01/Advisory%20Ransomware%20FINAL%20508.pdf>

<sup>5</sup> Thibault de Balthazar 和 Julio Hernandez-Castro, “An Analysis of Bitcoin Laundry Services” (比特币洗钱服务分析), Chinalysis and University of Kent, 2017 年 9 月, [https://www.researchgate.net/publication/319944399\\_An\\_Analysis\\_of\\_Bitcoin\\_Laundry\\_Services](https://www.researchgate.net/publication/319944399_An_Analysis_of_Bitcoin_Laundry_Services) (访问日期: 2021 年 6 月 28 日)。

<sup>6</sup> Faisal Khan, “Twitter hackers employing ‘peel chains’ to launder the Bitcoin bounty” (推特黑客使用“剥皮链”洗白比特币赎金), Technology.org, 2020 年 7 月 23 日, <https://www.technology.org/2020/07/23/twitter-hackers-employing-peel-chains-to-launder-the-bitcoin-bounty/> (访问日期: 2021 年 6 月 28 日)。

<sup>7</sup> Coin ATM Radar, <https://coinatmradar.com/> (访问日期: 2021 年 7 月 8 日)。

<sup>8</sup> Rachel Cormack, “Franck Muller’s Newest Watch Doubles as a Bitcoin Wallet, and You’ll Need Cryptocurrency to Buy It” (Franck Muller 最新款手表兼具比特币钱包功能, 只能用加密货币买), Robb Report, 2021 年 2 月 24 日, <https://robbreport.com/style/watch-collector/franck-muller-new-timepiece-doubles-bitcoin-wallet-1234598536> (访问日期: 2021 年 6 月 30 日)。

<sup>9</sup> “Treasury Identifies Iranian Nationals and Their Digital Currency Addresses Used to Facilitate Ransomware Attacks” (美国财政部发现伊朗国民及其用于促进勒索软件攻击的数字货币地址), JD Supra, 2018 年 12 月 4 日, <https://www.jdsupra.com/legalnews/treasury-identifies-iranian-nationals-29943/>

<sup>10</sup> “Carbis Bay G7 Summit Communiqué” (卡比斯湾 G7 峰会公报), 美国白宫, 2021 年 6 月 13 日, <https://www.whitehouse.gov/briefing-room/statements-releases/2021/06/13/carbis-bay-g7-summit-communicue/>

<sup>11</sup> “Advisory on Ransomware and the Use of the Financial System to Facilitate Ransom Payments” (关于勒索软件和利用金融系统促成勒索赎金支付的公告), 金融犯罪执法网络, 2020 年 10 月 1 日, <https://www.fincen.gov/sites/default/files/advisory/2020-10-01/Advisory%20Ransomware%20FINAL%20508.pdf>



# 赌场和 洗钱原因

## 赌

场工作人员观察是赌场反洗钱 (AML) 制度体系的重要组成部分，因为与银行不同，赌场客户的所有交易发生时客户几乎都是在场的。因此，赌场应重视反洗钱培训，努力提高赌场工作人员的能力，助力他们识别需要提交可疑活动报告的异常行为。

学习专家们形成了一个普遍共识：培训的重点是让学员理解知识，而非死记硬背。针对赌场工作人员的反洗钱培训通常侧重于让赌场工作人员记住可疑交易行为的类型（实施方式），而不解释洗钱犯罪分子为何会参与此类交易。

洗钱并非是只有经验丰富的反洗钱专业人士才能理解的高深话题。《黑钱胜地》(Ozark)、《毒枭》(Narcos)、《绝命毒师》(Breaking Bad) 等热门电视剧发挥了很大的普及知识作用，让公众对洗钱有了一些了解。剧本里充斥着大量对洗钱原因的戏剧化描写——正是这些原因令剧目引人入胜、妙趣横生。

著名组织学专家 Simon Sinek 在一次 TED 演讲中阐述了解释原因的诸多益处，这次演讲成了观看次数最多的 TED 演讲之一（超过 5,500 万次）。在其畅销书《Start with Why: How Great Leaders Inspire Everyone to Take Action》(《从原因开始：伟大领导者如何激励每个人采取行动》) 中，Sinek 断言，成功的组织先讲原因（目的），后讲方式（过程），由此来激励员工。在反洗钱培训和赌场风险评估方面，赌场应效仿 Sinek，从原因开始。<sup>1</sup>



从广义上讲，犯罪分子洗钱的原因是为了躲避执法部门，防止因资金线索获罪。这是洗钱的首要目标，但没有解释他们为什么要从事某些交易（或流程）来达到最终的洗钱目的。医生的最终目的是救死扶伤，但这并不能解释他们为什么会执行某些医疗程序，例如心脏听诊、抽血或拍 X 光片。医生进行的每个程序都是为了实现特定目标。如果病人理解医生进行某些程序的原因，他们就可以更好地理解治疗方案，判断某些程序是否有必要。

如果赌场工作人员理解洗钱犯罪分子参与某些流程的原因，他们就能更有效地判断交易是可疑行为，还是单纯的赌博行为。

洗钱目的培训法

围绕洗钱交易原因这个主题提供培训有一种直观的教学法，即洗钱目的培训法 (MLGM)。该方法侧重交易意图，并使用相关术语对洗钱进行解释。犯罪分子从事特定洗钱交易时，他们至少要实现表 1 中描述的洗钱目的之一。

借助洗钱目的培训法，可以使赌场工作人员了解洗钱交易。为什么犯罪分子会拆分现金存款，使用虚假身份证件，扮演未知角色，交换席位，或者委托代理人代表他们进行交易？因为犯罪分子可能打算向当局隐瞒其活动。为什么犯罪分子会用小额钞票塞满老虎机然后兑现，用大量借记卡取款或定期开兑现支票？因为犯罪分子可能打算转换资金，提高资金的追踪难度或资金的使用便利性。

表 1：赌场洗钱目的和交易意图

赌场洗钱目的	交易意图
掩藏	掩藏交易中的受益所有人身份，或在向政府提交的信息报告中掩藏受益所有人身份
转换	将资金转换为难以追踪和方便使用的形式
转账	将资金从一个人或地方转移到另一个人或地方
洗白	伪造资金来源于赌博所得的不在场证据或混淆资金线索
花费	享用非法资金，通常不考虑实现任何其他洗钱目的
储存	把资金储存在传统银行系统之外





基于洗钱目的培训法开展的培训强调洗钱原因，促使赌场人员站在洗钱犯罪分子的角度进行思考。洗钱目的培训法不但能促使赌场工作人员好好记住反洗钱知识，还能帮助他们更有效地识别疑似洗钱交易行为，降低误判正常交易的风险。如果交易看起来没有达成洗钱目的，则可能表明不存在洗钱行为。

## 明确洗钱目的和过程

务必要将洗钱目的与实现过程区分开来。将大量资金留在休眠的预付款账户中，持有大额赌场支票

而不存入银行，囤积赌场筹码，这些均非洗钱目的，而是实现储存资金目的的过程。获取 W-2G 表，将非法资金与赌博奖金混合起来，或者试图向账房索要现金提取收据，这些也不是洗钱目的，而是实现资金洗白目的的过程。

用于实现洗钱目的的过程是方式而非原因。教授方式（过程）而不解释原因，不利于赌场工作人员记住和理解课程内容。相反，首先教授原因然后举例说明方式，有助于赌场工作人员加深对洗钱的理。他们可以确定特定交易模式是否表明存在洗钱行为，或者只是客户的独特赌博风格。例如，有人可能不会一次兑换超过 10,000 美元的筹码，因为他们想尽快返回赌场。他们的目的是再次赌博而不必买筹码，不是隐瞒洗钱目的。



## 逃税和恐怖融资

一般而言，要提起洗钱指控，交易须涉及非法所得。因此，对资金来源展开尽职调查，对有效实施反洗钱制度体系至关重要，因为大多数时候犯罪分子只是在赌场花脏钱而已。另一方面，大多数时候逃税行为涉及合法资金，但逃税者可能需要达成某些洗钱目的，例如隐藏、转换、转移和储存资金。与其他金融机构相比，他们在赌场实现这些目的的能力相当有限。正如《2018 年美国财政部全国洗钱风险评估》报告所指，赌场并非以协助逃税而闻名，但根据《银行保密法》，赌场必须报告涉及逃税的可疑活动。<sup>2</sup>

恐怖融资活动不一定会涉及非法程序，但恐怖融资者可能会利用赌场实现某些洗钱目的，推动犯罪活动，例如转换、转账、掩藏或储存资金。然而，《2018 年美国财政部全国恐怖融资风险评估》报告并未提及赌场。<sup>3</sup>

表 2：赌场洗钱目的和过程

赌场洗钱目的	过程
掩藏	<ul style="list-style-type: none"> <li>· 拆分交易</li> <li>· 虚假身份证件</li> <li>· 代理人</li> <li>· 筹码失踪</li> <li>· 席位交换</li> <li>· 未分级赌博</li> </ul>
转换	<ul style="list-style-type: none"> <li>· 小额换大额钞票</li> <li>· 借记卡提现</li> <li>· 支票兑现</li> <li>· 现金换赌博工具</li> </ul>
转账	<ul style="list-style-type: none"> <li>· 支付他人的信用金 / 费用</li> <li>· 把筹码作为一种货币</li> <li>· 第三方付款</li> </ul>
洗白	<ul style="list-style-type: none"> <li>· 获取 W-2G 表</li> <li>· 混合 / 离析</li> <li>· 抵消投注</li> <li>· 获取取款收据</li> </ul>
花费	<ul style="list-style-type: none"> <li>· 赌博损失</li> <li>· 零售</li> <li>· 娱乐</li> <li>· 餐饮</li> </ul>
储存	<ul style="list-style-type: none"> <li>· 休眠的预付款账户</li> <li>· 囤积筹码</li> <li>· 赌场支票未存入</li> <li>· 把钱存在赌博钱包中</li> </ul>

确定交易原因的最好办法是观察交易人。特别是，对他们的资金来源和赌博历史了解多少？如果确定其资金来自合法渠道，那么他们为什么要达成洗钱目的？如果试图仅根据交易信息确定原因，结果可能导致将交易活动错误地归类为可疑活动。洗钱目的培训法促使赌场工作人员在确定交易原因时，关注交易者是谁。

负责洗钱案件的刑事调查人员需要证明相关交易的意图。如果证据并未表明存在洗钱意图，则不构成刑事案件。仅仅因为有人把钱放入老虎机，然后不怎么赌就兑现（这种模式称为“最低额度赌博”），这并不意味着他们打算洗钱。接受过洗钱目的培训法培训的合规人员能更熟练地分析最低额度赌博等交易行为，找出是否存在完成洗钱目的的意图，客户只是以某种特定方式进行赌博，还是在给赌博活动充钱而已。这样一来，他们就能更加熟练地撰写可疑活动报告，在其中写入对执法工作有用的信息（谁、方式和原因）。

洗钱目的培训法还能帮助赌场工作人员理解为什么需要某些控制措施来检测、预防和报告洗钱活动。赌场工作人员理解了这些控制措施后，就会更加愿意落实这些措施。

右面的表 2 对洗钱目的和过程进行了细分。

## 体育博彩与提供便利

如果赌场提供体育博彩，则有可能增加另一个洗钱目的——推动。“推动”是指利用赌场持续为犯罪活动提供便利。众所周知，在体育博彩中，非法博彩经纪人会利用体育博彩平账，避免因比赛结果而失衡，这一过程通常被称为“平衡下注”。

## 另一重要原因

赌场工作人员不仅要理解洗钱交易的原因，还要接受培训，了解为什么银行保密法 / 反洗钱工作对于防止犯罪分子利用赌场为犯罪活动提供便利至关重要。如此，他们就会理解，《银行保密法》是执法部门不可或缺的工具，赌场现金交易报告和可疑活动报告发挥了重要作用，成功地将各种重要罪犯绳之以法，包括毒贩、人贩子和重要欺诈者。他们会看到，自己的努力有助于维持社区安全。理解银行保密法 / 反洗钱的原因，有助于激励赌场人员参与反洗钱活动。

## 处置、离析与融合： PLI 模型

传统上，银行保密法 / 反洗钱专业人士会将洗钱过程分解为处置（placement）、离析（layering）与融合（integration）三个阶段（通常称为“PLI 模型”），由此解释洗钱的原因。尽管 PLI 模型可以解释大规模洗钱活动（例如卡特尔）中的复杂洗钱行为，但很难解释赌场洗钱活动。通常，客户将非法资金带到赌场，他们的洗钱活动不会逐一经历 PLI 模型的三个阶段。例如，许多犯罪分子只需要避免有人提交现金交易报告，


表 3：PLI 模型与赌场洗钱

PLI 模型	赌场洗钱目的
处置	掩藏
	转换
	转账
离析	洗白
融合	花费
	储存

就可以避开执法部门的注意。既然许多犯罪分子只想通过单笔交易完成洗钱，为什么还要将洗钱解释为由三个阶段构成的过程？另一个考虑因素是，非法资金进入赌场，更多只是为了享受犯罪活动的果实，根本无意完成整个洗钱周期，过去没有，现在也没有。

洗钱目的培训法强调单笔交易的原因，不考虑将交易强制归入洗钱周期的某个阶段。也就是说，洗钱目的培训法确实与 PLI 模型不兼容，如表 3 所示。

## 结语

要抓住洗钱犯罪分子，必须与洗钱犯罪分子换位思考。如果从原因出发，赌场工作人员就会从竭力避开执法部门审查的犯罪分子的角度思考问题。理解了原因，赌场工作人员就能理解洗钱，同样重要的是，理解为什么交易只是客户赌博风格的体现。理解了原因，反洗钱制度体系就能更突出风险为本的特性，减少向政府报告交易的几率，因为这些交易实际上只是合法客户在享受赌场活动而已。在这方面，反洗钱制度体系对执法部门打击金融犯罪更加有用。 

Paul Camacho, CAMS, 国税局刑事调查科退休负责探员、黑帮博物馆董事

<sup>1</sup> Simon Sinek, “How great leaders inspire action”（伟大领导者如何激励他人采取行动），拍摄时间：2009 年，TED 视频，17:27，[https://www.ted.com/talks/simon\\_sinek\\_how\\_great\\_leaders\\_inspire\\_action?language=en](https://www.ted.com/talks/simon_sinek_how_great_leaders_inspire_action?language=en)

<sup>2</sup> “2018 National Money Laundering Risk Assessment”（2018 年全国洗钱风险评估），美国财政部，[https://home.treasury.gov/system/files/136/2018NMLRA\\_12-18.pdf](https://home.treasury.gov/system/files/136/2018NMLRA_12-18.pdf)

<sup>3</sup> “2018 National Terrorist Financing Risk Assessment”（2018 年美国财政部全国恐怖融资风险评估），美国财政部，[https://home.treasury.gov/system/files/136/2018ntfra\\_12182018.pdf](https://home.treasury.gov/system/files/136/2018ntfra_12182018.pdf)



## 在复杂的世界中 管理风险



获得管理金融犯罪风险的全球资格认证，  
证明您在风险管理领域深厚的专业知识。

访问 [www.acams.org](http://www.acams.org)  
开启您的旅程





# 增强 DPMS 监管合规 工具包



## 对

于贵金属和宝石交易商 (DPMS) 行业，以及该行业交易的商品，金融机构往往知之甚少。该行业与受反洗钱监管的其他报告机构有所不同，因为前者完全建立在向消费者零售的基础上，而且业内跨国交易商品的控制措施千差万别，具体视各国或各地区的法律而定。此外，该行业涉及的商品（钻石、宝石、贵金属等）不仅用于储存和转移财富，还可作为货币替代品，用于产生犯罪收益。珠宝行业本身，对于借助其实现的大部分洗钱活动并不了解。无论是合法还是非法活动带来的收益，许多都流入珠宝行业，又流入为珠宝行业提供服务的银行。这些因素相互叠加，令 DPMS 反洗钱监管愈发困难，最终导致 DPMS 反洗钱风险敞口增大。



## 假借贵金属和宝石洗钱

有一种司空见惯的误解：洗钱就是非法活动所得的现金购买其他商品。这一前提不假，却忽略了一整个存在洗钱可能性的行业——即处置非法所得货物以换取现金或其他（贸易）商品的行业。对于与钻石/宝石/贵金属盗窃，以及其他非法所得相关的珠宝犯罪来说，明晰这一概念尤为重要。珠宝的处置或洗白，指的是以珠宝换取毒品或其他商品，或者将珠宝卖回合法市场的行为。如果珠宝商认为洗钱就是“将珠宝卖给犯罪分子，从而获得现金”，就会忽略“犯罪分子出售非法珠宝”这类洗钱行为。

鉴于大量珠宝因盗窃、抢劫、擅闯等罪行而丢失，澄清上述概念尤为重要。在私闯民宅类案件中，珠宝往往是第二容易被盗的物品；<sup>1</sup> 此类案件的平均损失金额约为 2,566 美元。<sup>2</sup> 美国联邦调查局统计数据显示，每 10 万人口中，就会发生 376 起私闯民宅案件<sup>3</sup>（2018 年，加拿大每 10 万人口中，发生了 431 起此类案件<sup>4</sup>）。据此数据估计，在美国一座 500 万人口的城市中，此类犯罪造成的珠宝损失每年高达两千万美元。以此类非法方式获得的珠宝，经过洗白回流至合法珠宝市场，相关收益最终流入为

该行业提供服务的银行；而这仅仅是通过 DPMS 行业洗钱的其中一种方式。该行业可能采取的另一种洗钱方式是：犯罪分子利用犯罪所得赃款，以实际购买的方式获取新的珠宝（如高端腕表、高成色金、钻石首饰等），或者凭借钻石和宝石进行贸易洗钱（TBML）活动。

深入了解该行业之所以困难重重，部分原因在于：该行业内零售商与批发商之间的商业模式存在显著差异。低端珠宝、高端珠宝、手表、彩色宝石、钻石、高成色金、寄售/二手销售等，均有可能成为采取不同商业模式（如实体店、网店、线上线下混合经营模式等）的零售商的主要关注点。每种商业模式均有各自的目标市场（客户）、供应链、价位及商业周期；此外，由于具体业务不同，每种商业模式供应链的涉及面也大相径庭：区域性、全国性乃至全球性，不一而足。在供应商端，最重要的是了解货物供应的市场、供应商与地理位置。

零售与批发贸易实际发生的各个司法管辖区施行的反洗钱法律不同，这进一步增加了反洗钱工作的复杂性。以发生在加拿大与美国之间的简单贸易为例，两国的反洗钱法律对于“宝石”一词所指的具体对象，规定就大相径庭。两国在贸易合作领域关系虽密切，但各自的反洗钱法律就“宝石”一词的具体规定存在显著差异（见下表 1）。

**表 1：加拿大和美国对“宝石”一词的法律定义对比**

加拿大	美国
钻石、蓝宝石、红宝石、绿宝石、坦桑石和亚历山大变石 <sup>5</sup>	钻石、刚玉（包括红宝石和蓝宝石）、绿柱石（包括绿宝石和海蓝宝石）、金绿宝石、尖晶石、黄玉、锆石、电气石、石榴石、水晶和隐晶质石英、橄榄石、坦桑石、硬玉、软玉、锂辉石、长石、绿松石、青金石和蛋白石 <sup>6</sup>

而这只是反洗钱法律方面难点的沧海一粟。在与 DPMS 相关的反洗钱法律的其他方面，各国法律也存在众多差异。虽然任何宝石均有可能被用作洗钱工具，但由于缺乏国际公认的定价方案，实际情况是：彩色宝石（非钻石）是 TBML 的主要载体。这么一来，问题就愈发错综复杂，专业人员很难厘清不同司法管辖区内与宝石溯源相关的风险，何况还有成百上千种宝石尚未纳入现行反洗钱法律。协调制度（全球广泛认可并使用的一种产品代码体系，涵盖了所有进出口产品，其中包括所有宝石）有可能涵盖了所有宝石，但此种制度尚未用于反洗钱和宝石相关法律。

**有一种司空见惯的误解：**  
**洗钱就是以非法活动所得的**  
**现金购买其他商品**

## 全面了解珠宝行业对于深入剖析 DPMS 业务及其国内国际市场至关重要

### 增强 DPMS 反洗钱合规能力


要想知道犯罪分子可能钻的空子、洗钱发生的具体领域，就需要了解相关商品的业务、市场以及犯罪手法。面对 DPMS 行业如此；面对任何其他报告机构，无论是赌场、房地产商还是货币服务企业，也是如此。银行业者可以通过增强 DPMS 行业知识、业务模型映射和交易分析能力，全面巩固反洗钱合规与风险管理账户。

DPMS 行业相对小众，虽然作为零售业的一部分，它大约已存在千年之久，但除了该行业从业人员（以及相关银行）之外，其他人群对该行业依然知之甚少。针对 DPMS 交易评估需求打出一套组合拳，有助于提升调查、分析和交易监控能力。首先，全面了解珠宝行业对于深入剖析 DPMS 业务及其国内国际市场至关重要。了解犯罪分子利用钻石、宝石、贵金属的方式，以及犯罪企业进入合法珠宝市场的模式，同样分外重要。综合运用上述知识，有助于全面了解 DPMS 行业让犯罪分子有哪些空子可钻，相关犯罪实践涉及哪些商品，以及高风险点在于何处。

其次，充分运用行业与业务基础知识，请 DPMS 账户审查方面的资深调查人员对现有的高风险 DPMS 账户进行审查。理想的审查方式，是根据业务模式、业务规模、地理位置、年度销售周期、市场比较分析等因素开展交易对账。此外，应鼓励开展过 DPMS 行业分析，并具有相应业务知识的调查人员深入钻研，致力于成为 DPMS 行业专家，就像深耕其他报告机构相关领域的专家一样。

第三，坚定落实“了解您的客户”综合流程以及预防措施，在开立相关账户之前，针对 DPMS 的特点认真开展客户接纳筛查。DPMS 行业十分特殊：相关企业应均已投保特定行业保险，进行特定行业登记，隶属于特定行业协会，并且采用特定商业模式。此外，DPMS 零售商应当制定反洗钱合规制度体系。应对相关内容认真审查，办理登记，并确定其满足现行合规要求。开户调查问卷的细节至关重要，因为调查人员需运用收集到的相关数据完整绘制出客户业务模型，才能如前所述，顺利开展交易比较分析。

### 结语

珠宝行业是一个奇妙的行业，作为全球商业的组成部分，拥有源远流长、丰富多彩的历史。然而，该行业性质特殊，商业模式繁多，业内买卖的商品多种多样，为犯罪分子洗白犯罪所得提供了不少机会。珠宝行业存在众多风险点，让犯罪分子能够伺机洗白犯罪所得，相关资金流入珠宝行业，后流入服务于珠宝行业的金融机构。珠宝行业处于一线，却与银行不同：后者拥有达到监管要求的反洗钱知识、能力与资源；此外，银行、反洗钱调查员和分析师对大多数报告机构的相关交易分析高度敏感。如需改善这一状况，培训、调查 / 分析指导、专业化、客户接纳筛查等均是实用工具，可借之增强相关企业的 DPMS 监管合规能力。 

Kelly Ross, 硕士, CAMS, FCGmA,  
Kelly Ross 咨询公司宝石学专家,  
加拿大艾伯塔省, Kross5c@gmail.com

<sup>1</sup> Joseph B. Kuhns et. al, “Understanding Decisions to Burglarize from the Offenders Perspective” (从犯罪分子角度理解行窃决定), 北卡罗来纳大学夏洛特分校刑事司法与犯罪学系, 2012 年 12 月, [https://www.researchgate.net/publication/268444817\\_Understanding\\_Decisions\\_to\\_Burglarize\\_from\\_the\\_Offender's\\_Perspective/link/546b48410cf2f5eb18091770/download](https://www.researchgate.net/publication/268444817_Understanding_Decisions_to_Burglarize_from_the_Offender's_Perspective/link/546b48410cf2f5eb18091770/download)

<sup>2</sup> “2018 Crime in the United States” (2018 年美国犯罪报告), 美国联邦调查局, <https://ucr.fbi.gov/crime-in-the-u.s/2018/crime-in-the-u.s.-2018/topic-pages/tables/table-23>; “Crime in the United States by Volume and Rate per 100,000 Inhabitants, 1999–2018” (1999–2018 年美国每 10 万居民犯罪量与犯罪率调查报告), 美国联邦调查局统一犯罪报告 (UCR) 计划, <https://ucr.fbi.gov/crime-in-the-u.s/2018/crime-in-the-u.s.-2018/topic-pages/tables/table-1>

<sup>3</sup> 同上。

<sup>4</sup> “Table 1: Police-reported crime for selected offences, Canada, 2017 and 2018” (表 1: 2017 年和 2018 年加拿大警方报告的特定犯罪行为), 加拿大统计局, <https://www150.statcan.gc.ca/n1/pub/85-002-x/2019001/article/00013/tbl/tbl01-eng.htm>

<sup>5</sup> “Dealers in precious metals and precious stones” (贵金属和宝石交易商), 加拿大金融交易和报告分析中心, <https://www.fintrac-canafe.gc.ca/re-ed/dpms-eng>

<sup>6</sup> “Financial Crimes Enforcement Network; Anti-Money Laundering Programs for Dealers in Precious Metals, Stones, or Jewels” (金融犯罪执法网络: 贵金属、宝石或珠宝交易商反洗钱制度体系), 金融犯罪执法网络, 2003 年 2 月 21 日, <https://www.fincen.gov/sites/default/files/shared/antimoneylaundering060305.pdf>





# ACAMS 每年在全球 举办 25 场活动

涵盖您最为关切的关键问题，包括机构反洗钱文化的建设、反洗钱领域技术的更新换代，以及对反洗钱从业者不断提高的执业要求。

**一切尽在 ACAMS**

了解您所在地区的最新情况：





# 如何通过审计





没有人喜欢受惊。因此，务必详细了解合规要求、风险因素和风险评估，以及（内部和外部）合规制度的运作细节，这几点至关重要，直接关乎审计工作的成败。审计流程旨在找出现行政策与程序之间的差距，以期完善相关制度。有些审计师对审计工作抱着欢迎态度，因为开展审计工作，有助于避免监管机构的介入。而更常见的是，有些人将审计视为一种对抗，他们认为，审计师的唯一目的似乎是对制度挑刺，无论审计结果究竟如何。审计的目的，是消除或显著减少审计流程中的潜在冲突。要做到这一点的关键，就是如实对制度开展自评，对合规环境具有敏锐的意识，实现完整而全面的备案，并妥善进行数据管理。

显然，组织机构越大，其合规责任就越错综复杂。举例来说，许多监管行动的诱因并非故意渎职，而是缺乏对合规风险的全面指挥和控制。从这个意义上讲，良好的沟通和制度知识不仅能够推动审计流程顺利进行，还有助于消除可能的监管后果，从而改善公司的声誉、传承理念以及利润率（这一点，是高级管理人员最看重的）。

# 俗

话说，生活中唯一可靠的是死亡和税收。对合规专业人士来说，这句话还可稍作补充——生活中唯一可靠的是死亡、税收和审计。

不过，正如死亡和税收一样，审计的具体情况，可能因许多因素大相径庭，这些因素包括而不限于：具体所属行业、审计机构与人员、所在组织的风险、合规制度等等。虽然合规专业人士可能几乎不受外部审计因素影响，但往往可以改进或增强组织内部审计流程，从而减轻审计工作的负担，缓解审计工作带来的损耗。本文将介绍有助于增进审计流程顺畅性的审计战略准备、参与和响应措施。

要想通过审计，就得从审计流程开始之前抓。审计准备是一个持续的过程，需要不断地评估和打磨。因此，客观进行内部审查和 / 或聘请不偏不倚的第三方审计师，这点至关重要。同样重要的是，定期进行自省性评估，因为商业环境、监管要求等并非一成不变。只要外部因素发生了巨大变化，几年前密不透风的制度就可能存在重大问题。必须在审计师发现这些问题之前，主动加以修正。

以下是审计活动的基本清单，或许有助于增强您的审计体验。

## 审计通过必备清单

### 审计准备

- 全面了解组织机构制度，并确保所有同事、员工均精通自身职责范围。发现部分员工不完全了解自身职责，是审计工作完成后的常见结果之一。
- 确保同事接受过全面而充分的培训，并能够提供此类培训的证明。还需证明员工具备执行所分配到的任务的背景与能力。员工和主要承包商的简历，均应保持最新状态且备案可查。
- 确保组织机构之中，所有将与审计师沟通的人，或者将向审计师提供书面信息的人，口径均统一；此外，将相关人员针对审计的响应职责限制在该人员专业领域以内。例如，IT 技术员不应就危险信号提出意见，除非涉及到“如何将危险信号编入合规技术当中”的事宜。提供的回应若存在错误，均有可能给您再次带来麻烦，哪怕时隔多年。
- 告知与审计师打交道的人员，务必直接回答审计师的问题；回答任何

问题时，不要超出该问题的范围。如若不然，有可能造成混乱，导致意想不到的额外调查，从而令审计过程复杂化，导致审计过程延长。总结：仅提供事实，不发表观点。

- 定期进行风险评估和内部审查；或者，在引入全新因素（如推出新产品、新服务，或开拓新销售渠道）之前开展上述活动。如有可能，聘请一位对所在行业了解透彻、不偏不倚的第三方审计师，对组织机构制度加以深入审计。审计师可能要求您提供相关审查报告的副本，以及您为解决调查中发现的问题而采取的行动的说明。做好准备，及时提供这些文件。
- 确保您的政策和程序手册完整，并适时按需更新。最重要的是：做好充分准备，证明您严格执行相关政策并遵守相关程序。如果出现这类司空见惯的缺陷，审计师不会施以同情。您的组织机构制定了政策和程序，如果不按书面规定予以落实，很可能遭到监管处罚。
- 开展全面的差距分析，并重视发现的问题。如果忽视或轻视发现的差距，很容易引起审计师和监管机构的注意。
- 在风险评估的参数范围内，尽可能修正、增补并加强现行政策与程序。编制详尽的文件记录，说明未弥补所发现差距的理由，以及弥补相关差距的计划与时间表。始终努力制定或寻找解决方案。如有可能，制定临时缓解措施，直至能够实施长期解决方案为止。
- 及时了解行业最佳实践；如有可能，将其整合进组织机构制度之中。审计师会审查这一点。
- 必须承认，发现问题是审计师的职责。要接受的是，即使在最理想的合规制度当中，审计师也能找到问题。没有合规程序会是完美的。即使是监管机构，也并不期望完美。而不完美，就意味着总会有政策或程序需要加强、增补或优化。

### 审计管理

- 审计开始前，与审计师就审计范围达成一致，加以备案，并让双方以适当形式签字。这样做有助于防止审计范围扩大，避免与审计师之间存在误解。如果在审计期间，审计范围发生变化，务必让审计师以书面形式记录变更，并完成相应的存档备案。

**审计准备是一个持续的过程，需要不断地评估和打磨**




- 如有必要，对审计师开展适当的培训；如果组织机构制度存在独特性或有特殊要求，就更需要这样做。尤为重要的是，务必全面记录特定法规或最佳实践不适用的原因。若只表示其“不适用”，哪怕您觉得显而易见，却往往无法令审计师信服。
- 各个行业、许多组织机构都有自己的行话，其中有些可能与行业标准术语不符。最好的补救办法是，统一采用行业标准语言。如果难以实现，建议准备一份术语表，列出您所在机构特有的术语及其常见的对应表达。应当于审计工作开始前，就准备好这份术语表，避免审计过程中产生误解。
- 承认有问题，始终比忽视问题或试图掩盖问题要好。对于试图掩盖问题的人，审计师不会手下留情。
- 密切配合审计师的工作，对于任何不符合预期的数据，或出乎意料的文件要求，一一做出澄清。提供数据之前，确保就测试内容和具体参数达成一致。若您提供了不符合审计师预期的信息，审计师可能认为您是在试图拖延或掩盖制度问题。在最坏的情况下，这会导致审计过程延长，直至达到审计师的要求为止。如果无法对审计请求做出回应，就应做好准备，详细解释个中原因。深入研究一下，现成替代方案能否满足审计师的要求。如果审计范围及流程均得当，则流程早期便应能发现难以回应的请求，并加以妥善处理。另外，若审计准备工作扎实，大概率能够满足多数请求，并且能够随时提供相关信息。
- 仅提供审计准备工作中涉及的事实，不发表观点。审计过程中，关于政策或程序是否有效或者政府法规是否合理的意见并不重要，发表此类意见反倒可能导致出现问题。与审计师进行沟通时，应保持专业、冷静且有分寸。审计的对象是制度，不是个人感受。
- 如果审计师在审计期间发现缺陷，应建议制定初步优化方案，并于审计完成之前提供给审计师。

## 审计后行动

- 无论某次审计是例行公事，还是折腾磨人，都应从中汲取经验教训。发现不尽人意的审计因素，并积极改进；否则后续审计中，很可能还会获得同样负面的审计体验。如发生最坏情况，组织机构会遭到罚款和处罚。谨记客观评估团队的表现。若放任审计流程导致的挫败感和负面情绪，让其影响审计过程中的任何响应甚至下一次审计，结果将适得其反。

- 如果审计开始前做足了功课，应该不会有太多意外的发现。这意味着：只要准备充分，审计过程中大多数时候，无需疯狂翻找资料，也能从容给出响应。若调查结果中存在任何误解或错误看法，务必加以纠正。纠正相关误解或错误看法，并不意味着审计师会接受您的答复；但如果不回应问题，有可能被视为承认存在缺陷，从而为未来的审计埋下一枚暗雷。
- 妥善计划并落实必要的纠正措施，不可等到下次审计之前临渴掘井。若只想在下次审计之前临阵磨枪，匆匆回应之前审计中发现的问题，不仅会削弱审计准备工作的作用，还可能导致相关缓解措施效力下降。任何审计师若发现之前审计中给出的建议未得到充分重视，都不会心慈手软——无论是组织机构落实得不够充分，还是苦苦解释未落实建议的原因都不行。
- 若聘用内部审计师或第三方审计师，确保将监管审计结果和纠正措施提供给他们。他们的调查结果有可能帮助您确定您的回应能否令官方审计师满意。
- 规划过程中，应充分考虑审计需求。对于任何合规制度，审计都是不可或缺的一部分，因此应将其纳入年度计划、预算，以及组织合规文化。制定一套准备程序可能颇为实用，但应确保其与合规程序分开，并且独具特色。
- 涉及审计之时，准备、管理、响应与重复，缺一不可。

## 结语

要想成功通过审计，既需要优化管理流程，也需要团队的密切配合。审计，就像是一位要求严格的老师出具的专业成绩单。审计结果不尽相同，可能是工作出色（有效期为下次审计前），也可能是对您所在组织机构合规工作的坦率评估。事实上，通过审计仅仅是可接受的最低结果。以开放的心态自信地接受审计。本文中提出的建议措施，并非审计的金科玉律；这些建议的基础，与商界的许多其他要求一样，均是业界常识，是了解自身职责并尽己所能履行职责的敬业精神。与开展预算流程一样，只需扎实准备、优化管理、专注跟进，就能有效节省精力，从容应对各种挑战。 

Ed Beemer, CAMS-FCI, [efb@compliancecomm.com](mailto:efb@compliancecomm.com)

Lauren Hughes, CAMS-FCI, [laurenhughes81@gmail.com](mailto:laurenhughes81@gmail.com)

# 数据泄露危机管理 最佳实践（上）





近

年来，许多公司的机密信息接连遭受非法访问，令这些公司深陷危机，焦头烂额。除了数据泄露外，各大企业或许还面临其他危机。新冠疫情爆发后，各大企业不得不启动危机管理计划；若此前无相应计划，就只得立即制定。设想一下，如果媒体突然报道，您有一家重要客户与某一恐怖组织或不为人知的组织存在直接联系，试图洗钱。您之前已经采取了所有预防措施，但结果会如何？毫无疑问，您的“了解您的客户”和风险管理流程均将受到严格审查。此外，新闻一旦公之于众，又将带来何种影响？

数据泄露事件代价巨大。Ponemon 研究院的一份报告指出，数据泄露事件的平均总成本高达 386 万美元，其中包括：检测与升级成本 111 万美元、业务损失成本 152 万美元、通知成本 24 万美元、事后响应成本 99 万美元。<sup>1</sup> 当中与“收入损失”相关的成本占比最高，约占总成本的 40%。同一份报告还指出，如果企业设有事件响应团队，并预先开展事件响应预演，则平均成本会降低 200 万美元左右。

本文分为上、下两篇，旨在介绍危机管理的最佳实践，并探讨一些值得钻研的数据。文中提及的最佳实践，或许可以用于多种危机管理，但本文的关注重点是非法访问数据泄露危机。

专家们在某些方面意见一致，在某些方面却争论不休。他们的首要认识是：必须未雨绸缪，做好准备。俗话说得好：防患于未然。重点不是此等数据泄露事件是否会发生，而是何时会发生。

针对数据泄露的风险敞口，必须实施信息安全、计算机安全、控制措施、隐私政策、培训课程等举措。事实上，成功打造出“安全文化”至关重要。<sup>2</sup> 本文对上述维度绝非置之不理，只是希望重点探讨危机管理流程的其他相关方面。

## 预防措施（危机前）

危机预防措施涉及多个方面、众多部门，自然也涉及高级管理层。有些预防措施偏重技术层面（适当的管理控制措施，或者特定的 IT 安全措施），有些偏重财务层面（购买网络保险<sup>3</sup>），有些则偏重战略管理层面（整体风险管理与合规）。

以下是危机预防的最佳实践：

- 建立危机管理团队
- 制定危机管理计划
- 制定公关计划

## 建立危机管理团队

如需进行危机管理，首要的预防举措之一，就是建立一支多领域危机管理团队，并提前考虑到成员出差、度假等因素的影响，确定好后备力量。<sup>4</sup> 要实现此目标，需要明确每位团队成员的职能与责任，并确定好负责人。<sup>5</sup> 这支团队的主要任务是：<sup>6</sup>


- 制定（或更新）危机管理计划
- 针对危机管理计划，为团队成员和所有员工提供培训
- 模拟不同的危机情境

鉴于危机管理具有重要的战略意义，应在团队里安排一名高级管理人员。<sup>7</sup> 此人除了能够从高级管理层的角度给予支持以外，也能成为团队与高管及董事会成员的联系人。Experian 强调：“高管层的参与，很大程度上决定了数据泄露响应计划能否成功地……打造出网络安全文化。”<sup>8</sup>

危机管理团队应由哪些人组成，相关人士的观点不一。不过，由于本文探讨的是数据泄露，因此团队中至少应有：

- 一位高级管理人员
- 一名 IT（或安全）专家
- 一名法律顾问
- 一位公共关系专家
- 一名人力资源负责人

此外，团队应拥有可自由裁量的预算，能够视情况咨询或聘用外部资源。若危机真的发生，绝无时间协调相关资源，苦苦等待批复。



**如需进行危机管理，  
首要的预防举措之一，  
就是建立一支多领域危机  
管理团队，并提前考虑到  
成员出差、度假等因素的  
影响，确定好后备力量**

## 制定危机管理计划

完成职能与责任的分配之后，下一步就是制定危机管理计划。正如 Experian 所述：“危机管理计划是一切企业网络安全战略的重要组成部分。”<sup>9</sup> 危机管理计划不仅能够指引组织内部成员的行动，还有助于减少响应时间，降低财务影响。<sup>10</sup> 由于威胁因素、经济环境等瞬息万变，相关技术日新月异，危机管理计划需要定期更新。<sup>11</sup>

危机管理计划的主要构成如下：<sup>12</sup>

- 危机管理团队成员的姓名与职能，后备人员、负责人的身份信息
- 危机管理团队成员的职能与责任
- 需要遵循的规程
- 外部利益相关者（如：征信机构、执法人员、监管机构、外部法律顾问、专门从事数据泄漏调查的调查公司、可能受影响的业务合作伙伴等）的联系人
- 公关计划（见下文）
- 业务连续性应急方案

鉴于商业勒索有增无减，企业机构应针对此类威胁制定危机管理计划，并对可能面临此类情况的员工开展培训。<sup>13</sup> 此外，建议开设加密货币账户，因为加密货币是此类犯罪的首选支付方式。<sup>14</sup>

上述所有步骤，均有助于组织机构节省宝贵时间，尽快恢复正常运作。最后，还需确定几处战略性位置，并要求危机管理团队在该等位置保存危机管理计划的若干份复印件，因为若网络黑客发起阻断服务攻击，组织机构内部人员有可能长时间无法进入系统。

## 制定公关计划

最重要的预防措施之一，是预先准备好公关演讲文稿，以便组织机构发言人在数据泄漏事件发生后发表。<sup>15</sup> 文稿的措辞、语调，以及组织机构发表响应的速度，均具备重大战略意义。在这些方面做得妥帖，有助于保护组织机构的声誉，而且有可能减少财务影响。

公关计划至少应包含：

- 公关团队成员、后备人员和负责人的姓名与职能
- 组织机构的官方发言人（应为公共关系专家）
- 公关团队成员的任务与职责

公关计划还应包括的要素：<sup>16</sup>

- 设立一个危机网站，并预先获取批准。若发生危机，启用、完善并更新该网站


**最重要的预防措施之一，  
是预先准备好公关演讲  
文稿，以便组织机构  
发言人在数据泄漏事件  
发生后发表**

- 准备好高级管理层新闻稿草案，并预先获取批准。若发生危机，根据具体情况进行相应修订，再行发布
- 准备好符合监管合规要求的（监管）公告，并预先获取批准
- 组织危机应对模拟简报会，帮助组织机构内成员做好应对危机的准备。正如 Communispond 首席执行官 Bill Rosenthal 所言：“做好准备，才能从容回答棘手问题。”<sup>17</sup>

公关计划需要规定，若发生数据泄露危机，应如何通知组织机构员工、可能已遭信息泄露的个人用户、媒体、相关机构和业务合作伙伴，包括主要征信机构（Equifax、Experian、TransUnion 等）：

- 如需联系员工，最好通过内网联系。若发生危机，应尽快通知员工，尤其是客服中心的员工。<sup>18</sup> 根据 Coombs 的说法，“了解情况的员工，就如同一条额外的公关渠道，可以通过这些员工联系其他利益相关者。”<sup>19</sup> 此外，还可以通过内网联系业务合作伙伴。
- 至于（疑似和潜在）受害者，可采取多种途径通知：新启用的网站、其当前账户、电子邮件、个人信件、传统媒体、社交媒体等。建议“采取[所有]必要措施，维护客户的信任度和忠诚度。”<sup>20</sup>

总之，数据泄露代价高昂，其影响难以消弭。本文（上）至此接近尾声。本篇主要阐明，组织机构须为数据泄露事件做好准备。要想实现这一目标，就需建立一支职责明确的危机管理团队，制定健全的危机管理计划（包含公关计划与应急计划，列清程序、外部联系人等）并适时更新。

本文（下）将介绍应对数据泄露危机的最佳实践，探讨跟进措施，并给出几点建议。 



Claude Mathieu, 博士, 教授, 舍布鲁克大学打击金融犯罪研究生课程负责人, 加拿大 ACAMS 蒙特利尔分会联席主席, Claude.Mathieu@USherbrooke.ca

William Poisson, 行政学硕士, CISSP, CISA, CISM, CFE, 加拿大舍布鲁克大学行政学硕士研究生, 攻读打击金融犯罪方向

Yves Trudel, 博士, 教授, 加拿大舍布鲁克大学工商管理硕士及普通硕士课程主任, Yves.Trudel@USherbrooke.ca

- <sup>1</sup> “Cost of a Data Breach Report 2020” (2020 年数据泄露成本报告), IBM, 2020 年 7 月, <https://www.ibm.com/security/data-breach>
- <sup>2</sup> Ramakrishna Ayyagari, “An Exploratory Analysis of Data Breaches from 2005-2011: Trends and Insights” (2005-2011 年数据泄露事件初探: 趋势与洞察), *Journal of Information Privacy and Security*, <https://www.tandfonline.com/doi/abs/10.1080/15536548.2012.10845654>; “Protecting Personal Information: A Guide for Business” (保护个人信息: 企业指南), 美国联邦贸易委员会, 2016 年 10 月, <https://www.ftc.gov/tips-advice/business-center/guidance/protecting-personal-information-guide-business>
- <sup>3</sup> “Cybersecurity Insurance” (网络安全保险), 美国网络安全与基础设施安全局, <https://www.dhs.gov/cisa/cybersecurity-insurance> (访问日期: 2021 年 5 月 5 日); “Fifth Annual Study: Is Your Company Ready for a Big Data Breach?” (第五次年度研究: 应对大数据泄露, 您的公司准备好了吗?), *Experian and Ponemon Institute*, 2018 年 2 月, [https://www.experian.com/data-breach/2018-ponemon-preparedness?ecd\\_dbres\\_blog\\_2018\\_ponemon](https://www.experian.com/data-breach/2018-ponemon-preparedness?ecd_dbres_blog_2018_ponemon)
- <sup>4</sup> 同上; Theodore J. Kobus III, “2019 Data Security Incident Response Report: Managing Enterprise Risks in a Digital World” (2019 年数据安全事件响应报告: 数字世界企业风险的管理), *BakerHostetler*, 2019 年 4 月 3 日, <https://www.bakerdatacounsel.com/data-security-incident-response/fifth-annual-data-security-incident-response-report-released-managing-enterprise-risks-in-a-digital-world/>
- <sup>5</sup> “PwC’s Global Crisis Survey 2019” (普华永道 2019 年全球危机调查), 普华永道, 2019 年, <https://www.pwc.com/ee/et/publications/pub/pwc-global-crisis-survey-2019.pdf>; Jena Valdetero 和 David Zetoon, “Data Security Breach Handbook for Hotels, Venues, & the Hospitality Industry” (酒店、会展和酒店业数据安全漏洞手册), *Bryan Cave*, 2016 年, <https://www.lexology.com/library/detail.aspx?g=d26e57fb-a72e-4d35-a147-1a5bb913b7f0>
- <sup>6</sup> Theodore J. Kobus III, “2019 Data Security Incident Response Report: Managing Enterprise Risks in a Digital World” (2019 年数据安全事件响应报告: 数字世界企业风险的管理), *BakerHostetler*, 2019 年 4 月 3 日, <https://www.bakerdatacounsel.com/data-security-incident-response/fifth-annual-data-security-incident-response-report-released-managing-enterprise-risks-in-a-digital-world/>; “Best Practices for Victim Response and Reporting of Cyber Incidents” (网络安全事件受害者响应与报告的最佳实践), 美国司法部, 2018 年 9 月, <https://www.justice.gov/criminal-ccips/file/1096971/download>; “Data Breach Response Guide” (数据泄露响应指南), *Experian*, 2018-2019 年, <https://www.experian.com/assets/data-breach/white-papers/experian-2018-2019-data-breach-response-guide.pdf>; Katelyn Smith, “Best Practices for Effective Corporate Crisis Management: A Breakdown of Crisis Stages through the Utilization of Case Studies” (企业有效危机管理的最佳实践: 通过案例分析细究危机的各个阶段), 加利福尼亚理工大学, 2012 年 3 月, <https://digitalcommons.calpoly.edu/cgi/viewcontent.cgi?referer=https://www.google.com/&httpsredir=1&article=1045&context=joursp#:text=The%20first%20best%20practice%20for,98>
- <sup>7</sup> “Fifth Annual Study: Is Your Company Ready for a Big Data Breach?” (第五次年度研究: 应对大数据泄露, 您的公司准备好了吗?), *Experian and Ponemon Institute*, 2018 年 2 月, [https://www.experian.com/data-breach/2018-ponemon-preparedness?ecd\\_dbres\\_blog\\_2018\\_ponemon](https://www.experian.com/data-breach/2018-ponemon-preparedness?ecd_dbres_blog_2018_ponemon)
- <sup>8</sup> “Data Breach Response Guide” (数据泄露响应指南), *Experian*, 2018-2019 年, <https://www.experian.com/assets/data-breach/white-papers/experian-2018-2019-data-breach-response-guide.pdf>, 6。
- <sup>9</sup> 同上, 注 4。

- <sup>10</sup> “Best Practices for Victim Response and Reporting of Cyber Incidents” (网络安全事件受害者响应与报告的最佳实践), 美国司法部, 2018 年 9 月, <https://www.justice.gov/criminal-ccips/file/1096971/download>
- <sup>11</sup> 同上; “Data Breach Response Guide” (数据泄露响应指南), *Experian*, 2018-2019 年, <https://www.experian.com/assets/data-breach/white-papers/experian-2018-2019-data-breach-response-guide.pdf>; “Fifth Annual Study: Is Your Company Ready for a Big Data Breach?” (第五次年度研究: 应对大数据泄露, 您的公司准备好了吗?), *Experian and Ponemon Institute*, 2018 年 2 月, [https://www.experian.com/data-breach/2018-ponemon-preparedness?ecd\\_dbres\\_blog\\_2018\\_ponemon](https://www.experian.com/data-breach/2018-ponemon-preparedness?ecd_dbres_blog_2018_ponemon)
- <sup>12</sup> “Crisis Management and Communications” (危机管理与危机公关), 公共关系研究所, 2007 年 10 月 30 日, <https://instituteforpr.org/crisis-management-and-communications>; “Barton (2001), Coombs (2007a) and Fearn-Banks (2001) 发现, 危机发生时, 危机管理计划有助于节省时间: 它能够帮助人们预先分配部分任务、预先收集部分信息, 并将收集到的信息作为参考。”
- <sup>13</sup> Theodore J. Kobus III, “2019 Data Security Incident Response Report: Managing Enterprise Risks in a Digital World” (2019 年数据安全事件响应报告: 数字世界企业风险的管理), *BakerHostetler*, 2019 年 4 月 3 日, <https://www.bakerdatacounsel.com/data-security-incident-response/fifth-annual-data-security-incident-response-report-released-managing-enterprise-risks-in-a-digital-world/>; “Best Practices for Victim Response and Reporting of Cyber Incidents” (网络安全事件受害者响应与报告的最佳实践), 美国司法部, 2018 年 9 月, <https://www.justice.gov/criminal-ccips/file/1096971/download>
- <sup>14</sup> “BakerHostetler 2017 Data Security Incident Response Report Based on 450 Incidents” (BakerHostetler 2017 年数据安全事件响应报告, 基于 450 起事件), *BakerHostetler*, 2017 年, <https://www.databreaches.net/bakerhostetler-2017-data-security-incident-response-report-based-on-450-incidents/>
- <sup>15</sup> Bokyoung Kim, Kristine Johnson 和 Sun-Young Park, “Lessons from the five data breaches: Analyzing framed crisis response strategies and crisis severity” (五次数据泄露事件带来的教训: 结构化危机响应策略和危机严重程度分析), *Cogent Business & Management*, 2017 年 7 月 24 日, <https://www.tandfonline.com/doi/full/10.1080/23311975.2017.1354525>; Katelyn Smith, “Best Practices for Effective Corporate Crisis Management: A Breakdown of Crisis Stages through the Utilization of Case Studies” (企业有效危机管理的最佳实践: 通过案例分析细究危机的各个阶段), 加利福尼亚理工大学, 2012 年 3 月, <https://digitalcommons.calpoly.edu/cgi/viewcontent.cgi?referer=https://www.google.com/&httpsredir=1&article=1045&context=joursp#:text=The%20first%20best%20practice%20for,98>
- <sup>16</sup> “Data Breach Response Guide” (数据泄露响应指南), *Experian*, 2018-2019 年, <https://www.experian.com/assets/data-breach/white-papers/experian-2018-2019-data-breach-response-guide.pdf>; “Fifth Annual Study: Is Your Company Ready for a Big Data Breach?” (第五次年度研究: 应对大数据泄露, 您的公司准备好了吗?), *Experian and Ponemon Institute*, 2018 年 2 月, [https://www.experian.com/data-breach/2018-ponemon-preparedness?ecd\\_dbres\\_blog\\_2018\\_ponemon](https://www.experian.com/data-breach/2018-ponemon-preparedness?ecd_dbres_blog_2018_ponemon)
- <sup>17</sup> Nate Lord, “Data Breach Experts Share the Most Important Next Step You Should Take After a Data Breach in 2019 & Beyond” (数据泄露专家分享重要跟进步骤, 助您从容应对 2019 年及未来的数据泄露危机), *Data Insider*, 2020 年 8 月 11 日, <https://digitalguardian.com/blog/data-breach-experts-share-most-important-next-step-you-should-take-after-data-breach-2014-2015>
- <sup>18</sup> Katelyn Smith, “Best Practices for Effective Corporate Crisis Management: A Breakdown of Crisis Stages through the Utilization of Case Studies” (企业有效危机管理的最佳实践: 通过案例分析细究危机的各个阶段), 加利福尼亚理工大学, 2012 年 3 月, <https://digitalcommons.calpoly.edu/cgi/viewcontent.cgi?referer=https://www.google.com/&httpsredir=1&article=1045&context=joursp#:text=The%20first%20best%20practice%20for,98>
- <sup>19</sup> “Crisis Management and Communications” (危机管理与危机公关), 公共关系研究所, 2007 年 10 月 30 日, <https://instituteforpr.org/crisis-management-and-communications/>
- <sup>20</sup> “Fifth Annual Study: Is Your Company Ready for a Big Data Breach?” (第五次年度研究: 应对大数据泄露, 您的公司准备好了吗?), *Experian and Ponemon Institute*, 2018 年 2 月, [https://www.experian.com/data-breach/2018-ponemon-preparedness?ecd\\_dbres\\_blog\\_2018\\_ponemon](https://www.experian.com/data-breach/2018-ponemon-preparedness?ecd_dbres_blog_2018_ponemon), 2。

# 了解您的客户制度 取得成功 所需要的数据





# 在

当今的金融犯罪合规世界当中，监管机构齐心协力，把了解您的客户 (KYC) 要求不断推向新高——至少在许多 KYC 和反洗钱 (AML) 从业者看来是如此。越来越多人士期望能够运用有关客户的大量可用数据。然而，单纯地增加数据要求并不能保证实现最终目标——建立强大的反洗钱合规制度，对金融机构而言，这一制度应能满足监管要求并且无碍业务增长。

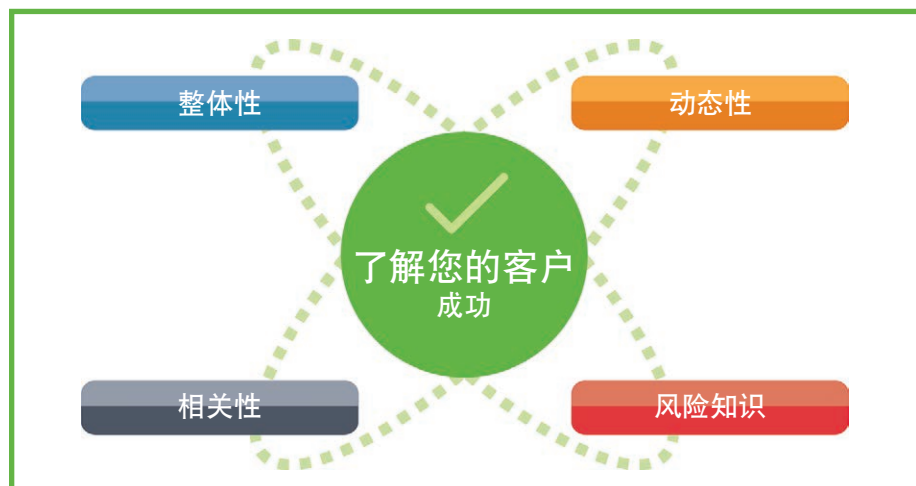
为实现这一最终目标，必须彻底转变 KYC 的实施方式。具体而言，反洗钱专业人士不仅应考虑单个数据元素的收集和整理，还应考虑缺失的数据元素。这些缺失的数据元素，只有通过深入研究围绕每个数据元素的人员决策过程，以及数据元素之间的关系才能识别出。

在讨论何为“了解您的客户制度取得成功所需要的数据”之前，首先需要定义何为“了解您的客户制度取得成功”，包括当前与未来两个维度。

## 当前对“了解您的客户制度取得成功”的定义是什么？

一直以来，“了解您的客户制度取得成功”似乎都是通过收集到的数据量来衡量的。在某些情况下，数据的整理和呈现可能会成为重点关注对象。此外，也有人根据数据收集与整理的速度和效率来定义“了解您的客户制度取得成功”。看起来，古老的“权重测试法”似乎被用到了 KYC 领域——数据越多，越合规。而这正是问题所在：人们关注的历来都是合规与合规成本问题，却未充分关注“如何就正确的客户做出正确的决定，以增加企业收入”。

图 1：了解您的客户制度取得成功的要素



## 未来对“了解您的客户制度取得成功”的定义是什么？

未来对了解您的客户制度取得成功的定义，关注四大制度要素：必须具备整体性、动态性和相关性，必须清晰理解风险以及上述要素之间的相互影响（见图 1）。了解您的客户制度取得成功，有助于更有效地了解潜在客户和现有客户。要想实现这一点，就需要采取整体思路，以动态方式实时汇集收集到的数据。这意味着，我们需要了解当前不同系统和流程之中，数据元素之间存在的运用与流程关系；意味着了解客户带来的风险，以及这些风险在客户生命周期中将产生何种变化。

有人可能会说：这件事已经在做了，但实际上，目前的侧重方向主要是收集供决策参考的完整、准确、及时的数据，而非决策过程。更具体点说，就是尚未有人关注到描述当前所收集数据间关系的数据元素，以及这些数据元素和数据关系对推动客户风险判定的影响。

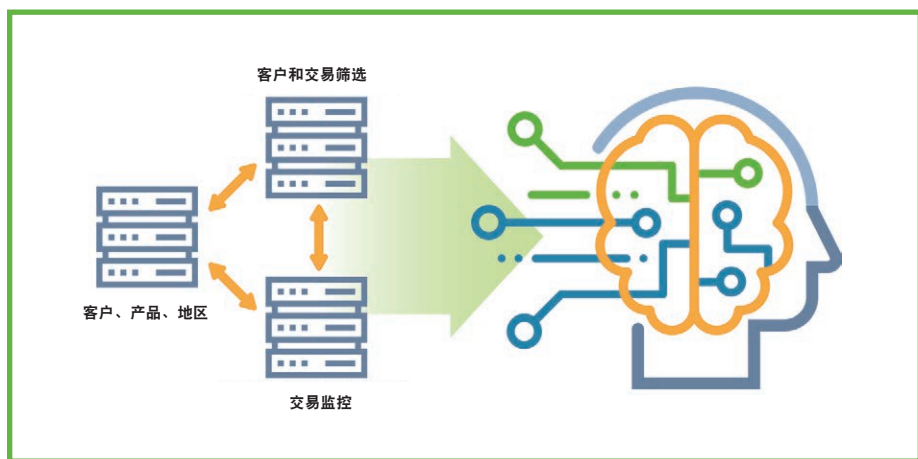
未来了解您的客户制度取得成功的秘诀不再是更多的数据，而是便于理解、可供参考的数据。此种数据具有整体性、动态性和相关性，能帮助您识别您希望接纳的客户，以及/或者您希望与之拓展关系的客户。

## 如何从当前走向未来

当今，反洗钱领域孤岛林立。首先要做的，就是从人员决策的角度，研究、确定并理解三大反洗钱领域（制裁名单筛查、交易监控和 KYC）中的所有数据元素如何共同绘就客户画像（见图 2）。

第一步应当考察在规定的孤岛里单独收集的数据元素，然后研究数据特征或者数据元素之间关系的定义元素——不仅应在孤岛内部进行考察，还应从孤岛相互之间的角度进行考察，这非常重要；实现之后，才有助于形成整体视角。显然，作为此项实践的构成内容，即使无法运用质量上乘的数据，也应当运用质量良好的数据，但其相关性必须从人员决策角度进行定义。

图 2：反洗钱的三大领域



举个基础范例：活动正常且符合预期，活动与多位客户的关系相似，活动与交易的关系相似——无论是与尚需深入研究的客户，还是与普遍情况的客户。当今收集数据的方式，通常是采访客户或潜在客户，询问客户期望实现的目标。此类数据将被忠实记入 KYC 文件，记录人员还将勾选一项复选框，声明已取得该类信息。接下来，则需要由 KYC 分析师（可能是领域专家，也可能不是；但大概率并非客户、行业和交易类型的专家）判定预期的“正常活动”究竟是否确实正常。

在这种情况下，并无机制负责收集和评估其他数据元素，用以证实或以其他方式支持客户提供的信息，而需要依靠 KYC 分析师或案件调查员，基于相关情况查找并评估活动。

但事实是，KYC 文件中可能已经提供了大量数据。例如：对于大型客户，有可能已经取得其年度、季度或其他报告以“证实”公司状况。从这些报告当中，可以收集到哪些数据来证实或预测预期的“正常活动”？其中的挑战在于：

如何读取、识别、提取并分析这些拓展式数据元素，形成更深入、更全面的客户活动图景。

## 未来 KYC 数据思维的范式转变

KYC 不仅应在数据收集与操作方面做出改变，还应就 KYC 数据提出新的问题。新的问题应当比监管要求更深一步，着重关注 KYC 数据的价值——可以是预测性焦点，如信用、营销视点等。

例如，若从贷款（即信用）等角度看待 KYC，就应全面审视客户，评估客户的实力和可靠性，以及其开展业务的可行性。考察客户做过哪些项目，由此预测其将来




可能会开展哪些项目。此外，还应从营销角度看待 KYC，问客户喜欢什么、可能会做些什么，因为客户当前从事的内容，也可能揭示其未来行为。应当将这种思路融入 KYC 反金融犯罪思维之中，因为客户想开展的项目有可能超出规范，需要调查，也可能需要提交报告。

## 新型反洗钱专员

为了实现上述范式转变，反洗钱专员必须转变思维方式。新思维应融合当今所有可用数据，更重要的是，融合与当前数据元素之间关系相关的所有数据；还应当理解当前和未来的决策过程，以及数据与决策过程的关系。只有这样，才能将正确的数据呈现给 KYC 分析师，供他们在决策过程中参考——或者由人工智能技术用于呈现可能决策，供 KYC 分析师确认。

此外，“新型”反洗钱专员还应开拓思路，不单单考虑满足当今的监管要求。获取并运用正确的 KYC 数据，确实需要投入资金。新型反洗钱专员应站在企业角度思考问题，理解正确的 KYC 数据对于企业的促进作用，而非将之仅仅看作另一项要求。

只要新型反洗钱专员拥有正确的思维方式，反洗钱专业人士就有望实现理想图景——“我来自合规部门，我是来帮忙的！”

Steve Marshall, Innovative Systems, Inc.  
总监 / FinScan 咨询服务部总监，  
美国宾夕法尼亚州，  
smarshall@innovativesystems.com



# 让我们 建立联系！



关注我们  
扫一扫 →



# 20 年来的 20 件大事

## 《今

日 ACAMS》将点出 20 年来最具颠覆性的 20 件反金融犯罪 (AFC) 大事, 启动 ACAMS 20 周年庆典活动。

编辑团队向 ACAMS 顾问委员会联席主席 Rick Small (CAMS) 和 ACAMS 前顾问委员会成员 Lauren Kohr (CAMS-FCI) 征求了意见。



Small 是 Truist 反金融犯罪团队负责人, 职责包括管理反洗钱 (AML) 合规事务、控制和调查、欺诈管理以及网络事件所致的金融调查等。他于 2016 年加入 BB&T (现为 Truist), 担任首位金融犯罪制度总监。

Small 在公营和私营机构工作超过 35 年, 经验丰富。加入 BB&T 之前, 他在安永担任反洗钱和反金融犯罪高级顾问; 在美国运通任企业级反洗钱、反腐败和国际监管合规高级副总裁; 在通用电气旗下部门 GE Money 任反洗钱负责人。Small 在私营机构的任职经历始于花旗集团, 担任全球反洗钱董事总经理。

在私营机构任职之前, 他曾在美国政府历任过多个职位, 首先是美国司法部反垄断部门的联邦检察官, 后来供职于打击有组织犯罪工作组, 再后来在美国财政部任执法机构的高级法律顾问。最近的政府职位是在联邦储备系统理事会任监督与监管处副处长。



Kohr 工作经历丰富, 在反金融犯罪部门工作超过 16 年, 在银行保密法 / 反洗钱 (BSA/AML) 和制裁合规、复杂监管问题及补救项目管理以及促进公私合作以制定有效策略打击非法金融活动方面, 拥有丰富的经验。她现任 ACAMS 美洲反洗钱部门高级总监, 专注于建立全球反金融犯罪特别工作组, 专门促进公私合作, 协助执行全球执法策略, 同时担任反洗钱 / 反恐融资 (AML/CTF)、监管政策和反洗钱制度优先事项的领域专家和技术专家。此前, 她曾在弗吉尼亚州泰森斯角的欧道明国民银行 (Old Dominion National Bank, 简称 ODNB) 担任高级副总裁、首席风险官和银行保密法执行官。



任职期间，Kohr 负责该行企业风险管理制度建设工作，包括领导实施该行的银行保密法 / 反洗钱和海外资产控制办公室 (OFAC) 制度。

加入该行之前，Kohr 曾在宾夕法尼亚州哈里斯堡的 Metro 银行担任副总裁 / 总监，负责反洗钱 / 银行保密法 / 海外资产控制办公室工作。在此期间，她负责制定、实施和监督《银行保密法》合规制度各方面的工作，包括美国《爱国者法》、反洗钱和海外资产控制办公室相关法规。2016 年，Kohr 荣获 “ACAMS 年度反洗钱专业人士” 称号和 “《今日 ACAMS》年度文章奖”，2019 年获 “美国首都分会公私合作奖”。她经常在公私营机构举办的国内和国际大会上发言，主题涉及反洗钱、《银行保密法》、海外资产控制办公室和反恐融资等。Kohr 现为 ACAMS 美国首都分会理事和反洗钱合作论坛理事，也是 “共同赋能：反洗钱女性” 倡议发起人之一。她之前还曾在 ACAMS 咨询委员会任职。

作为各自领域的专家和反金融犯罪领域的知名演说家，Small 和 Kohr 向《今日 ACAMS》分享了过去 20 年里他们认为最重要的 20 件反金融犯罪大事。讨论时，Small 和 Kohr 在他们的清单里提到了类似的事件。《今日 ACAMS》采纳了他们的宝贵意见，结合他们的清单，为您带来过去 20 年里最具颠覆性的 20 件大事：

1. “9·11”
2. 美国《爱国者法》
3. 联邦金融机构检查委员会《银行保密法 / 反洗钱检查手册》
4. 公私合作加强
5. 金融机构参与行业活动，共同打击人口贩卖，帮助人口贩卖的幸存者
6. 反洗钱广泛扩容，纳入反恐融资
7. 反洗钱广泛扩容，纳入网络犯罪
8. 反洗钱广泛扩容，纳入欺诈
9. 金融机构参与行业活动，与非营利组织合作，为非政府组织和非营利组织提供指导和银行服务
10. 客户尽职调查的监管
11. 受益所有权要求
12. 《2020 年反洗钱法》
13. 反洗钱国家优先事项首次发布

14. 金融科技公司作为传统银行替代形式兴起，提供银行相关服务
15. 数字货币纳入加密货币、虚拟货币和非正规价值转移体系
16. 反洗钱技术纳入大数据、人工智能、机器学习和自动交易监控系统
17. 识别社会影响问题（如环境犯罪）相关的资金流向
18. 贸易洗钱
19. 制裁规避计划的复杂性
20. 新冠疫情


最后，Small 和 Kohr 就未来 20 年对反金融犯罪行业的影响分享了看法。Small 表示：“在接下来的 20 年里，我预计新兴技术将蓬勃发展，为反洗钱风险管理提供尖端技术解决方案。”

Kohr 补充说：“未来 20 年的重点工作是：

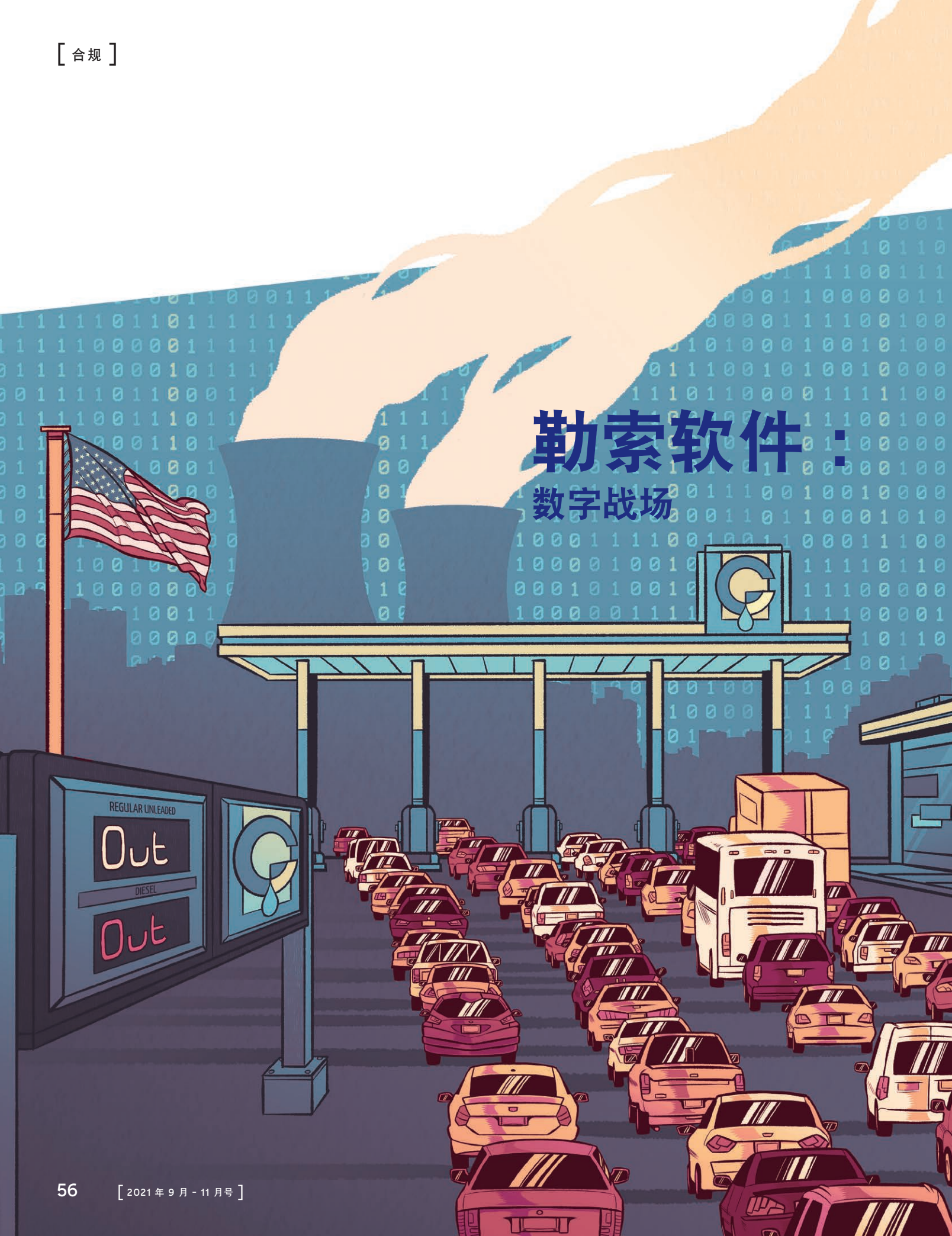
- 继续创新增效，打击洗钱、恐怖融资和扩散融资活动
- 加强公私合作，增加信息共享机会
- 促使反金融犯罪社群积极主动地打击这些令人发指的罪行，提升他们的反应能力
- 超越自我，超越本职工作，拓展思路，打破常规

我们都要发挥自己的作用，想办法推动反金融犯罪社群的发展，推进各项倡议和计划；不找借口，因为我们不能让障碍和挑战阻止了我们尝试的步伐。我们是可以做到的。”

在启动 ACAMS 20 周年庆祝活动之际，我们也希望铭记和缅怀在 “9·11” 那次发生在美国本土最可怕的恐怖袭击中丧生的 2,977 个生命。此外，我们也要铭记并感谢在那个可怕日子不畏危险、拯救同胞的急救人员，向他们的敬业精神致敬。

作为努力结束金融犯罪及相关犯罪活动的社群和行业的一员，《今日 ACAMS》充满感激。希望您能加入我们，从现在开始，继续开展 ACAMS 20 周年庆祝活动，一起走进 2022 年。 

Karla Monterrosa-Yancey, CAMS, ACAMS 《今日 ACAMS》杂志总编辑，美国佛罗里达州，[kmonterrosa@acams.org](mailto:kmonterrosa@acams.org)  
Stephanie Trejos, CAMS, 编辑，ACAMS，美国佛罗里达州，[strejos@acams.org](mailto:strejos@acams.org)



# 勒索软件： 数字战场



# 在

互联网时代，黑客攻击意味着个人身份信息 (PII) 的丢失。在 2018 年黑客对 Facebook 发起的攻击中，5,000 万用户发现，自己的生日、教育背景、位置等个人身份信息轻易成了网络犯罪分子的攻击对象；<sup>1</sup> 连 Facebook 首席执行官 Mark Zuckerberg 的账户也被盗了。他表示，攻击者可以查看被盗账户的私人消息或帖子，但无法访问财务数据。

现在快进到加密货币时代。在货币互联网中，黑客攻击不仅意味着可能丢失个人身份信息，还可能意味着被窃取毕生积蓄——想想以高速互联网实施的盗窃犯罪。同时，这也意味着勒索类软件即服务 (RaaS) 提供商、在线恐怖融资、程序化洗钱行为和民族国家行为体实施的网络安全攻击增长的速度和规模达到前所未有的程度。2021 年 5 月，针对 Colonial Pipeline 的勒索软件攻击不仅导致美国东海岸进出加油站的道路陷于瘫痪，还导致美国国家安全政策发生转变，让执法机构和政策制定者意识到：战斗的硝烟已经转移到网络之上。

## Colonial Pipeline：案例分析

2021 年 5 月 7 日，Colonial Pipeline 惨遭勒索软件攻击，该公司运营着一条 5,500 英里长的管道，向美国东海岸输送 45% 的汽油和航空燃料。为了应对这次袭击，Colonial 主动关闭了业务网点，导致燃油短缺，人们从迈阿密到纽约的加油站排着长队等待加油。为了应对这次袭击，一些学校甚至开始上网课。

5 月 10 日，《纽约时报》报道称，美国联邦调查局证实，DarkSide 勒索软件是导致 Colonial Pipeline 网络瘫痪的罪魁祸首。<sup>2</sup>

DarkSide 是一家勒索类软件即服务提供商，在暗网上销售恶意软件，从买方通过恶意软件获得的利润中分得一杯羹。什么是勒索软件和勒索类软件即服务？勒索软件是一种恶意软件，网络犯罪分子利用此类软件阻止受害者访问自己的数据。此类网络犯罪分子会访问受害者的系统并对文件加密，将数据作为“人质”，收到赎金后再解密。初次感染之后，勒索软件可能试图通过受害者的网络传播到共享驱动器、服务器、接入的计算机和其他可访问的系统上。勒索类软件即服务，让（无编码经验的）不法分子可以发起勒索软件攻击。不妨将其想象成一家网络犯罪麦当劳餐厅，在这里，“特许经营商”可以购买勒索软件服务套件。在暗网上，人们可以通过 Tor 浏览器轻松获得此类软件。勒索软件服务开发人员收取一笔特许经营费，其中包括一定比例的利润（通常为 20%-30%）。作为回报，勒索类软件服务开发人员提供品牌、培训、设备和全天候支持。不法分子无需掌握专业知识，并通常要求受害者用比特币等加密货币支付赎金。

但勒索软件早在加密货币出现之前就已存在。早在 2005 年，不法分子就设立空壳公司接收信用卡、预付现金卡和礼品卡付款。虽然加密货币并非勒索软件形成的原因，但加密货币具有成本低、速度快和匿名的特点，成为网络犯罪分子的首选货币。

在 Colonial Pipeline 遭到攻击后，负责网络与新兴技术的副国家安全顾问 Anne Neuberger 5 月 10 日在白宫举行了简报会。她将此次攻击描述为“勒索类软件即服务的变体”，其中，“犯罪同伙进行攻击，然后与勒索软件开发人员分享犯罪所得，”并证实联邦调查局从 10 月以来一直在调查 DarkSide。<sup>3</sup> 除了锁死 Colonial Pipeline 的计算机系统，还包括公司的计费系统，使公司无法跟踪燃油配送情况、无法计费，DarkSide 还窃取了超过 100 GB 的公司数据。<sup>4</sup>

5 月 13 日星期四，也就是攻击发生近一周后，有报道称 Colonial 支付了 75 个比特币的赎金（价值高达 500 万美元），可以在 5 月 12 日星期三恢复服务。<sup>5</sup> 5 月 8 日，有人从美国的一家交易所提取了 75 个比特币，不久后将其转入 DarkSide 勒索软件支付地址。<sup>6</sup> 这笔资金很快就得以洗白，进了 DarkSide 的比特币钱包。

5 月 14 日星期五这天，对 DarkSide 来说，可谓祸从天降。据 Intel 471 网站消息，Darkside 告诉附属组织，其丧失了对自己的基础设施的访问权限，很快就会关闭服务，因为执法机构进行了干预，美国也施加了很大的压力。DarkSide 补充说，作为“扣押”行动的一部分，他们支付服务器上的资金被转入了一个未知账户。<sup>7</sup> 5 月 13 日，有人从 Darkside 钱包里取走了 113.5 个比特币，存入另一个钱包。

6 月 7 日，Colonial 遭到攻击一个月后，美国司法部宣布成功从存放赎金的加密货币钱包里扣押了 63.7 个比特币（合 230 万美元）。扣押令由加利福尼亚州北区法院出具。<sup>8</sup> “今早，美国司法部已经找到并收回 Colonial 支付给 DarkSide 网络的大部分赎金。勒索软件攻击始终都是不可接受的，如果它们要针对关键基础设施，我们将予以有力回击，”副总检察长 Lisa Monaco 在新闻发布会上这样说道。<sup>9</sup> Monaco 在一份新闻稿中表示：“资金线索追踪能力仍然是我们最基本，也是最强大的工具之一。支付的赎金是驱动数字勒索引擎的燃料，今天的公告表明，美国将使用所有可用工具，使犯罪组织付出更高的代价，使其攻击行为变得无利可图。”<sup>10</sup>

可是，仅靠追踪资金线索，执法行动只能到此为止。区块链分析是非常强大的工具，能使执法机构彻底改变金融犯罪调查格局的方式，追踪开放区块链上的资金流动情况。然而，虽然通过区块链分析能追踪加密货币的动向，但这些工具仍无法查获

非法资金。当美国司法部在新闻稿中宣称，“通过审查的比特币公共台账，执法机构能追踪到以特定地址为目的地……的多笔比特币转账交易，而联邦调查局则有该地址的‘私钥’，”大家不禁想问，“联邦调查局是怎么破解私钥，没收非法所得？”

可能性有多种——从技术的使用到依赖人力情报。正如《纽约时报》报道称，“加密货币专家表示，联邦调查局依靠的似乎不是区块链技术的底层漏洞。可能性更大的是老式的警察调查工作。”《泰晤士报》称，“联邦探员获得 DarkSide 私钥的方式可能是在 DarkSide 网络内部安插卧底，入侵存储 DarkSide 私钥和密码的计算机，或者通过搜查令或其他方式，迫使存有其私人钱包的服务机构交出 DarkSide 的私钥。”<sup>12</sup> 归根结底，这次扣押要归功于出色的侦察工作。无论是高科技还是人，这次成功扣押很可能是几个月来出色调查工作的结果。正如白宫在关于 DarkSide 的首场新闻发布会上提到的那样，联邦调查局自 10 月以来一直在调查 DarkSide。虽然这次迅速地追回比特币，但最可能是多部门全球合作的结果，为了厘清勒索软件提供商和网络犯罪分子网络，他们已经投入了数月或数年的时间。

## Colonial Pipeline 案对美国将来的国家安全政策有何影响？

在 Colonial Pipeline 网络攻击发生后，联邦调查局局长 Christopher Wray 比较了“9·11”和最近发生的网络攻击，如对 Colonial 和全球最大肉食供应商 JBS Foods 的攻击。他告诉《华尔街日报》称，“它们有很多相似之处，我们非常重视打击和预防工作。”<sup>13</sup> 就在前一天，美国司法部将网络入侵提升到反恐调查的级别，指示美国各地的检察官办公室与新成立的勒索软件和数字勒索特别工作组

合作，协同调查涉及勒索软件、网络攻击、病毒预防和清除服务、非法在线论坛或市场、加密货币交易所、防弹托管服务、僵尸网络和在线洗钱服务的案件。<sup>14</sup> 执法机构这种变化可能标志着 20 多年来国家安全政策的首次转向——承认“9·11”已经成为过去，恐怖分子、网络犯罪分子和流氓国家行为体已进入数字战场。

## 合规团队和私营机构可以采取哪些措施防止网络攻击

可以说，最有用的教训来自 1980 年代的好电影，网络防御也不例外。Ronald Reagan 总统看完合规部门必看影片《战争游戏》——上世纪 80 年代的一部经典影片，由 Matthew Broderick 主演，他无意中侵入了一台军用超级计算机并差点引发第三次世界大战——后不久，他做了一件著名的事，就是责成美国国家安全局加强全国政府、企业和个人系统的网络防御能力。<sup>15</sup> 当前，这项工作仍在实施。

若想讨论应该通过何种方式对付参与勒索软件和其他网络攻击的不法分子，就需要探讨全球的公私合作问题。<sup>16</sup> Colonial Pipeline 和 JBS Foods 等关键基础设施是由私营机构实体控制的。2021 年 6 月 2 日，副国家安全顾问 Anne Neuberger 给私营机构写了一封公开信，描述了私营机构加强对勒索软件攻击抵御能力的方式。<sup>17</sup> 具体而言，公开信敦促私营机构立即采取图 1 中描述的行动。

应对勒索软件，无论是主动为之还是被动应对，需要整家企业上下齐心，共同作为。首先要教育员工，让他们不要点击垃圾邮件中的链接或未知网页。勒索软件攻击最常见的来源是钓鱼邮件。<sup>18</sup> 电子邮件通常依靠社会工程攻击——利用人类心理而非技术攻击——来取得计算机系统的访问权限。攻击者依靠社交互动而非高科技黑客技术诱骗员工交出系统访问权限。员工一旦点击链接，恶意软件就会接管系统，传播到接入的系统，搜索有价值的信息。

虽然私营机构大多能积极主动地实施网络卫生举措，强化计算机系统和协议，但随时做好准备、从容应对攻击也很重要。在最近的一次采访中，Hunton Andrews Kurth 网络安全实践部门负责人 Lisa Sotto 这样解释道：

“在发生安全漏洞问题时，公司减轻伤害的一个重要方式是主动作为，防患于未然。至关重要，要制定最新的事件响应计划，通过桌面演练反复操演。公司要组建训练有素的事件响应团队，在发生安全问题时，团队成员知道自己的职能与责任。”

Sotto 继续说道：

“一旦公司意识到网络攻击，就必须迅速召集符合条件的专家协助解决问题，要有经验丰富的法律顾问、司法调查公司、勒索软件谈判专家（如果遭到勒索软件攻击）和外部公关公司（若适用）。强烈建议公司与执法机构合作，及时发现危害迹象或者与威胁行为主体相关的其他信息，加快恢复进度。”<sup>19</sup>

最重要的是，私营机构 IT、合规和金融犯罪专家可以大展才华，主动和被动地应对勒索软件和网络攻击的威胁。有一件事情是清楚的：各国政府、私营机构甚至个人必须在全球范围内密切合作，避开和应对威胁。换句话说，我们可以从《战争游戏》中学到很多东西。



图1：美国政府就防范勒索软件威胁最佳实践提出的建议

**实施拜登总统在“关于改善全国网络安全状况的行政令”中描述的最佳实践：**这些实践做法包括：(a) 使用多因素身份验证而非单独依赖密码；(b) 使用网络检测和响应技术主动检测来搜寻网络上的恶意活动，在恶意活动损坏网络或系统之前予以阻止；(c) 如果勒索软件不仅通过加密将数据作为人质，还泄漏信息，威胁披露敏感信息，甚至在从备份恢复数据时这样做，试图获取更多赎金，则可使用加密技术将损害降至最低；(d) 委托有适当资质的系统安全团队监控可用信息，检测是否存在新的威胁，实时修补和维护企业的IT系统、防范此等威胁。

**将系统镜像、配置和数据备份到离线存储设备上，定期测试这些备份：**勒索软件会定期尝试加密和删除可从业务网络访问的备份。因此，要把备份保存到离线设备上，当受到攻击时，使勒索软件无法访问企业加密了的IT系统。此外，建议企业定期测试备份，确定备份是否足以在发生攻击时恢复系统。

**及时修补和更新系统：**随着新漏洞的发现，打补丁是防止勒索软件攻击的关键举措。组织机构应考虑部署补丁管理系统，采用风险为本的评估策略确定修补操作系统、应用程序和固件的时机。

**测试事件响应计划：**企业应制定事件响应计划，通过桌面仿真定期测试这些计划，及时发现和解决计划存在的任何

缺陷。在审查事件响应计划时，企业应自问几个核心问题，包括(a) 哪些系统对企业持续运营至关重要；(b) 在没有特定系统的情况下，企业可以继续运营多长时间；(c) 如果特定业务系统（例如计费系统）受到勒索软件攻击的影响，企业是否会被迫关停制造业务。在此基础上，企业应酌情调整事件响应计划。

**检查安全团队的工作：**公司应通过渗透测试和其他漏洞测试，测试其系统的安全性。


**网络隔离：**勒索软件攻击可能窃取数据，扰乱公司运营。对于制造和生产运营类企业，如果勒索软件能进入制造和生产控制系统，勒索软件攻击就会产生重大影响。本公开信建议，将制造和生产运营控制类计算机网络与企业业务功能类网络分开，企业要辨别这些网络之间的链接，并仔细过滤和限制这些网络之间的互联网访问。这将可以确保将制造和生产网络隔离开来，在企业网络被隔离时，制造和生产运营能继续进行。企业应定期测试应急计划，例如手动控制，确保在勒索软件攻击期间对安全至关重要的功能可以正常运行。”

资料来源：“What We Urge You To Do To Protect Against The Threat of Ransomware”（关于防范勒索软件威胁的建议），白宫，2021年6月2日，<https://www.iscpo.org/site/wp-content/uploads/2021/06/Memo-What-We-Urge-You-To-Do-To-Protect-Against-The-Threat-of-Ransomware.pdf>

## 超越勒索软件：恐怖融资和程序化洗钱

虽然勒索软件近来最受关注，但其他威胁也转到了网上。2021年7月1日，以色列国家反恐融资局(NBCF)发布行政令，扣押哈马斯代理人控制的比特币、Doge、Tron和其他加密货币地址。<sup>20</sup>不到一年前，美国司法部发布公告称，美国国税局刑事调查处、国土安全调查局和联邦调查局成功扣押150多个加密货币账户，这些账户涉嫌洗钱，且与属于哈马斯军事部门 al-Qassam 旅的账户有资金往来。<sup>21</sup>

2021年2月，美国司法部公布了一份长达33页的联邦起诉书，指控三名朝鲜电脑程序员，称他们参与了大量全球犯罪阴谋，发动了一系列恶意网络攻击，前所未有地从全球金融机构和其他公司盗取了13亿美元的加密货币和法定货币。<sup>22</sup>起诉书反复提到恶意软件、首次募币骗局和针对加密货币企业的网络钓鱼攻击。也许比行为本身更令人担忧的是朝鲜黑客团队 Lazarus Group 的专业性和只有军队才能做到的精准度，为了获得受害电脑系统的后门访问权限，该团队开发了恶意加密货币应用程序。

虽然勒索类软件即服务提供商、恐怖分子资助者和国家支持的网络犯罪分子转向了数字战场，执法机构也是如此。从 Colonial Pipeline 扣押、以色列机构对哈马斯相关加密地址的甄别以及对朝鲜网络犯罪分子的指控来看，执法机构能利用加密货币的力量和前景——依靠开放账本运行——追踪并最终追回被盗资金。就像《悲惨世界》中冉·阿让(Jean Valjean)与沙威(Javert)的精彩对决一样，随着执法人员与不法分子之间猫捉老鼠的游戏转到线上，威胁和应对之道也拥有了互联网的速度。 

Ari Redbord, TRM Labs 法律和政府事务主管, 华盛顿特区, ari@trmlabs.com, Twitter 账号: @ARedbord

<sup>1</sup> Mike Isaac 和 Sheera Frankel, “Facebook Security Breach Exposes Accounts of 50 Million Users” (Facebook 安全漏洞导致 5,000 万用户账户泄漏), 《纽约时报》, 2018 年 9 月 28 日, <https://www.nytimes.com/2018/09/28/technology/facebook-hack-data-breach.html>

<sup>2</sup> David E. Sanger 和 Pranshu Verma, “The F.B.I. confirms that DarkSide, a ransomware group, was behind the hack of a major U.S. pipeline” (美国联邦调查局证实, 勒索软件组织 DarkSide 是美国重大管道黑客攻击的幕后黑手), 《纽约时报》, <https://www.nytimes.com/2021/05/10/us/politics/dark-side-hack.html>

<sup>3</sup> “Press Briefing by Press Secretary Jen Psaki, Homeland Security Advisor and Deputy National Security Advisor Dr. Elizabeth Sherwood-Randall, and Deputy National Security Advisor for Cyber and Emerging Technologies Anne Neuberger, May 10, 2021” (美国白宫新闻秘书 Jen Psaki、国土安全顾问兼副国家安全顾问 Elizabeth Sherwood-Randall 博士以及网络和新兴技术副国家安全顾问 Anne Neuberger 联合新闻发布会, 2021 年 5 月 10 日), 白宫, 2021 年 5 月 10 日, <https://www.whitehouse.gov/briefing-room/press-briefings/2021/05/10/press-briefing-by-press-secretary-jen-psaki-homeland-security-advisor-and-deputy-national-security-advisor-dr-elizabeth-sherwood-randall-and-deputy-national-security-advisor-for-cyber-and-emerging/>

<sup>4</sup> Jordan Robertson 和 William Turton, “Colonial Pipeline hackers stole data on Thursday” (攻击 Colonial Pipeline 的黑客周四窃取了公司数据), 彭博新闻, 2021 年 5 月 8 日, <https://www.bloomberg.com/news/articles/2021-05-09/colonial-hackers-stole-data-thursday-ahead-of-pipeline-shutdown?sref=SCAzRb9t>

<sup>5</sup> William Turton, Michael Riley 和 Jennifer Jacobs, “Colonial Pipeline Paid Hackers Nearly \$5 Million in Ransom” (Colonial Pipeline 向黑客支付近 500 万美元赎金), 彭博社, 2021 年 5 月 13 日, <https://www.bloomberg.com/news/articles/2021-05-13/colonial-pipeline-paid-hackers-nearly-5-million-in-ransom>

<sup>6</sup> “Digging into the Darkside Ransomware Payment” (深挖 Darkside 勒索软件付款), TRM Labs, 2021 年 5 月 14 日, <https://www.trmlabs.com/post/darkside-ransomware-report>

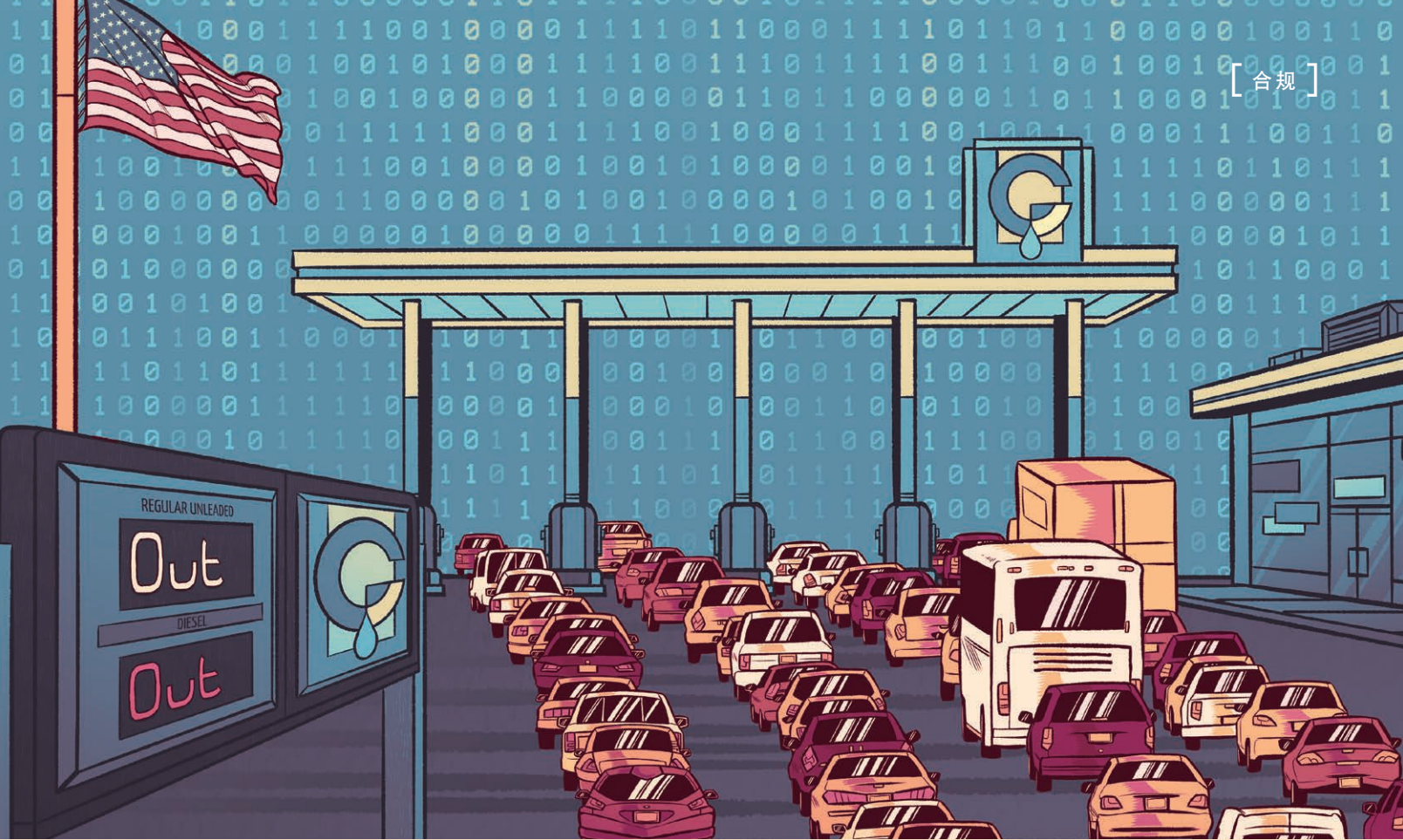
<sup>7</sup> “The moral underground? Ransomware operators retreat after Colonial Pipeline hack” (讲道德的地下组织? 勒索软件运营商在 Colonial Pipeline 黑客攻击事件后开始后撤), Intel 471, 2021 年 5 月 14 日, <https://intel471.com/blog/darkside-ransomware-shut-down-revil-avaddon-cybercrime>

<sup>8</sup> “Darkside Seizure Warrant” (Darkside 扣押令), 美国加利福尼亚北区地方法院, 2021 年 6 月 7 日, <https://www.justice.gov/opa/press-release/file/1402051/download>

<sup>9</sup> “DAG Monaco Delivers Remarks at Press Conference on Darkside Attack on Colonial Pipeline” (副总检察长 Lisa Monaco 在新闻发布会上就 Colonial Pipeline 遭 Darkside 攻击一事发表讲话), 美国司法部, 2021 年 6 月 7 日, <https://www.justice.gov/opa/speech/dag-monaco-delivers-remarks-press-conference-darkside-attack-colonial-pipeline>

最重要的是，私营机构 IT、合规和金融犯罪专家可以大展才华，主动和被动地应对勒索软件和网络攻击的威胁





<sup>10</sup> “Department of Justice Seizes \$2.3 Million in Cryptocurrency Paid to the Ransomware Extortionists Darkside” (美国司法部追回了支付给勒索软件敲诈者 Darkside 的 230 万美元加密货币), 美国司法部, 2021 年 6 月 7 日, <https://www.justice.gov/opa/pr/departments-justice-seizes-23-million-cryptocurrency-paid-ransomware-extortionists-darkside>

<sup>11</sup> 同上。

<sup>12</sup> Nicole Perloth、Erin Griffith 和 Katie Benner, “Pipeline Investigation Upends Idea That Bitcoin Is Untraceable” (对 Pipeline 黑客攻击案的调查颠覆了比特币不可追踪的观念), 《纽约时报》, 2021 年 6 月 9 日, <https://www.nytimes.com/2021/06/09/technology/bitcoin-untraceable-pipeline-ransomware.html>

<sup>13</sup> Aruna Viswanatha 和 Dustin Volz, “FBI Director Compares Ransomware Challenge to 9/11” (联邦调查局局长将勒索软件与“9·11”进行比较), 《华尔街日报》, 2021 年 6 月 4 日, <https://www.wsj.com/articles/fbi-director-compares-ransomware-challenge-to-9-11-11622799003>

<sup>14</sup> “Guidance Regarding Investigations and Cases Related to Ransomware and Digital” (勒索软件和数字相关调查和案件指南), 美国司法部副检察长办公室, 2021 年 6 月 3 日, <https://www.justice.gov/dag/page/file/1401231/download>

<sup>15</sup> Fred Kaplan, “‘WarGames’ and Cybersecurity’s Debt to a Hollywood Hack” (《战争游戏》与好莱坞黑客对网络安全的贡献), 《纽约时报》, 2016 年 2 月 19 日, <https://www.nytimes.com/2016/02/21/movies/wargames-and-cybersecuritys-debt-to-a-hollywood-hack.html>

<sup>16</sup> “The United States, Joined by Allies and Partners, Attributes Malicious Cyber Activity and Irresponsible State Behavior to the People’s Republic of China” (美国联合盟友和伙伴国家, 将恶意网络活动和不负责的国家行为归咎于中华人民共和国), 白宫, 2021 年 7 月 19 日, <https://www.whitehouse.gov/briefing-room/statements-releases/2021/07/19/the-united-states-joined-by-allies-and-partners-attributes->

malicious-cyber-activity-and-irresponsible-state-behavior-to-the-peoples-republic-of-china/

<sup>17</sup> “What We Urge You To Do To Protect Against The Threat of Ransomware” (关于防范勒索软件威胁的建议), 白宫, 2021 年 6 月 2 日, <https://www.iscipo.org/site/wp-content/uploads/2021/06/Memo-What-We-Urge-You-To-Do-To-Protect-Against-The-Threat-of-Ransomware.pdf>

<sup>18</sup> Joseph Johnson, “Most common delivery methods and cybersecurity vulnerabilities causing ransomware infections according to MSPs worldwide as of 2020” (截至 2020 年导致勒索软件感染最常见的攻击方法和网络安全漏洞: 全球管理服务提供商), Statista, 2021 年 2 月 16 日, <https://www.statista.com/statistics/700965/leading-cause-of-ransomware-infection/>

<sup>19</sup> Jason Remillard, “Lisa Sotto of Hunton Andrews Kurth: ‘Relationships are incredibly important’” (Hunton Andrews Kurth 公司 Lisa Sotto: “关系至关重要”), ThriveGlobal, 2021 年 7 月 30 日, <https://thriveglobal.com/stories/lisa-sotto-of-hunton-andrews-kurth-relationships-are-incredibly-important/>

<sup>20</sup> “Seizures of Cryptocurrency” (扣押加密货币), 以色列国家反恐融资局, <https://nbctf.mod.gov.il/en/seizures/Pages/Blockchain1.aspx>

<sup>21</sup> “Global Disruption of Three Terror Finance Cyber-Enabled Campaigns” (全球成功打掉三起恐怖融资网络活动), 美国司法部, 2020 年 8 月 13 日, <https://www.justice.gov/opa/pr/global-disruption-three-terror-finance-cyber-enabled-campaigns>

<sup>22</sup> “Three North Korean Military Hackers Indicted in Wide-Ranging Scheme to Commit Cyberattacks and Financial Crimes Across the Globe: Indictment” (三名朝鲜军队黑客被控参与多起诈骗, 在全球范围内实施网络攻击和金融犯罪: 起诉书), 美国加利福尼亚中区地方法院, <https://www.justice.gov/opa/press-release/file/1367701/download>





# “9·11”： 20 年的旅程

---

有

些事件会永远铭刻在我们的脑海里。对于 2001 年 9 月 11 日在公营或私营机构工作的人来说，基地组织 (al-Qaida) 对美国的袭击显然是其中一个铭刻于我们脑海的历史性时刻。对于在那个可怕日子之后进入职场的人来说，“9·11”事件 20 周年是回顾反思的阴郁时刻。



2001年9月11日，美国东岸一天的开始，平静而美好。美国东部标准时间上午8点，人们正开始一天的忙碌，他们并不知道，不久后一场灾难正在波士顿机场、纽瓦克机场和弗吉尼亚北部机场的四架飞机上徐徐展开。上午8点19分，其中一架飞机上的乘务员通知航空公司航班被劫持，暗示有问题的第一信号出现了。上午8点46分，那架飞机撞向世贸中心北塔。开始时，多数人认为这是一场悲惨的意外事故。后来，上午9点03分，第二架飞机撞向世贸中心南塔。那一刻，人们感到一阵麻木，意识到这并非意外事故。那是一个人们永远无法忘记的时刻。上午9点37分，又发生了一件惊天动地的事，第三架飞机撞向了五角大楼。在接下来的半个小时里，据报道第四架飞机被劫持并飞往华盛顿特区，加剧了人们的恐惧。上午10点03分，由于机上乘客的英勇反抗，这架飞机突然坠毁在宾夕法尼亚州尚克斯维尔的一块田地里。

## 所知与所学

我们知道的是，基地组织是活动在阿富汗且受塔利班保护的一个恐怖组织。其领导人 Osama bin Laden 对美国怀有强烈的仇恨。有大量警告显示，bin Laden 有着在全球范围内攻击美国利益的野心和意图。不幸的是，作为一个国家，美国有一种错误的安全感和无敌感，不担心国际恐怖分子会袭击美国本土。

我们谦卑地学习到，面对恐怖主义，美国这样的开放社会异常脆弱，而基地组织在识别和利用系统性的漏洞方面可谓驾轻就熟。相反，在即时对“9·11”袭击事件展开调查后，美国很快发现，基地组织及恐怖分子主要有两个弱点：通信和金融。袭击发生数周后，美国联邦调查局绘出了此次袭击的通讯和资金信息时间表，以便追根溯源，挖出作为袭击源头的基地组织。

“9·11”袭击发生后，美国国会成立了“9·11”委员会，展开调查。调查结果发布在《“9·11”委员会报告》当中。这份报告是对“9·11”事件最权威、最全面、最客观、最可靠的描述。报告详细地描述了基地组织策划并成功实施此次袭击的过程，美国政府存在且使基地组织得逞的弱点、不足和失败，以及美国对此采取的反制措施。重要的是，报告提出了41条建议，敦促政府制定最佳实践并最大限度减少将来的威胁。

“9·11”委员会发布了一份报告卡，用于监督美国政府反恐措施的实施进度。最高等级为A-，是专门针对反恐融资措施的。评定等级的一项基本依据是通过“反恐融资政策协调委员会”工作组开展的跨部门合作水平，以及与金融界的“卓越合作”（参见“9·11”委员会《恐怖融资专刊》）水平。

## “9·11”事件之前的威胁环境

由于对国家安全存在错误的认识，美国政府没有把反恐工作摆在首位。结果造成政府反恐资源不足、人力情报资源短缺、恐怖融资调查缺乏且不协调、制裁效果不佳。美国执法机构和情报机构之间缺少信息共享，进一步放大了这些不足。从金融情报的角度来看，需要建立更强大的《银行保密法》条例和报告制度。

“9·11”恐怖袭击的第一个警示信号出现在1993年2月，当时有人首次在世贸中心实施炸弹袭击。一枚巨大的卡车炸弹在双子楼下的停车场被引爆。那次事件的目的是



炸塌双子楼。虽然造成了严重破坏和伤亡，但袭击并未达到预期效果。这次袭击的主谋是 Ramzi Yousef，他是 Khalid Sheikh Mohammed (KSM) 的侄子，而后者正是“9·11”事件的主谋。

从1993年到2001年，还出现了许多其他警示信号。1994年，Yousef 和 KSM 在菲律宾策划了“马尼拉航空”袭击计划（又称“波金卡”计划），目的是在从亚洲飞往美国的多个航班上同时引爆炸弹。菲律宾警方成功阻止了这个计划。1996年和1998年，bin Laden 针对美国颁布了两道教令。第一道教令号召穆斯林杀害美国士兵，第二道教令呼吁杀死美国人。基地组织1998年轰炸了美国驻东非的两个大使馆，2000年轰炸了科尔号导弹驱逐舰。除了这些活动，还有大量的碎片情报称可能有人对美国发动恐怖袭击。

在“9·11”事件发生之前，恐怖融资并非情报界的重点工作。同样，执法机构尤其

是联邦调查局，也没有认真对待恐怖融资问题。然而，中央情报局在“9·11”之前提交的情报称，基地组织在此期间的现金流稳定且安全。

## 9.11 恐袭

1996 年，KSM 在托拉博拉会见了 bin Laden，建议在美国劫持 10 架飞机，攻击东岸和西岸的目标。KSM 的计划过于宏大，被 bin Laden 拒绝了。后来，在 1999 年初，bin Laden 在阿富汗坎大哈会见了 KSM。这次会见，bin Laden 同意了 KSM 的计划，劫持大型商用飞机，以飞机为导弹袭击美国境内目标。此后不久，有人组织了一系列的会议，参会人包括 bin Laden、KSM 和基地组织军事领导人兼 bin Laden 高级顾问 Mohammad Atef。这些会议制定了“9·11”恐袭计划，包括初始目标的选择。尽管“9·11”恐袭的种子已在 1993 年播下，但直到 1999 年他们才想出袭击计划。bin Laden 的组织领导，基地组织提供的资金支持和恐怖分子，KSM 的策划和实施领导，这些因素保证了袭击计划的可行性。

“9·11”袭击计划的核心参与者分为三种角色：领导者、协助者和 19 名劫机者，劫机者又分成两组，即 4 名飞行员和 15 名肌肉劫机者。从 1999 年春天开始，bin Laden、Atef 和 KSM 就一直在遴选协助者和劫机者。前两名劫机者于 2000 年 1 月抵达美国。他们最初被选为飞行员，但因无法适应西方文化，于是成了肌肉劫机者。后来，四名比较熟悉西方社会的人被选为飞行员。他们于 2000 年春夏进入美国。这些飞行员在接下来的一年里进行了大量飞行训练，并对飞行中的跨境飞机进行监视，确定最佳劫机时机。剩下的 13 名肌肉劫机者于 2001 年春夏进入美国。在袭击发生前的几天里，19 名劫机者组成了四支飞行队伍。9 月 11 日上午，劫机者成功执行了计划。

对于“9·11”恐袭事件，有一点是无法辩驳的。袭击计划需要资金，成本在 40 万美元到 50 万美元之间，其中大约 32.6 万美元由金融机构经手处理。bin Laden 向 KSM 提供了“9·11”恐袭需要的大部分资金，KSM 则把这些钱直接给劫机者，或者通过三个协助者把钱间接拿给劫机者。19 名劫机者中的每个人都在美国开立了银行账户，用于存取款，推进袭击计划。他们还使用了外国银行账户，以及货币服务企业和外汇。协助者和劫机者之间大约有 20 笔电汇，其中包括未使用的资金，劫机者通过电汇把这部分钱还给了协助者。



恐袭发生后，美国联邦调查局立即展开调查。根据每个被劫持航班发起的手机通话，很快就发现了 19 名劫机者，背后的资金线索开始显现出来。先查明劫机者的购票方式，识别银行账户，追踪电汇，然后确定并构建银行交易活动和通信时间表。金融服务业强大的响应能力对调查工作起到了极大的推动作用。

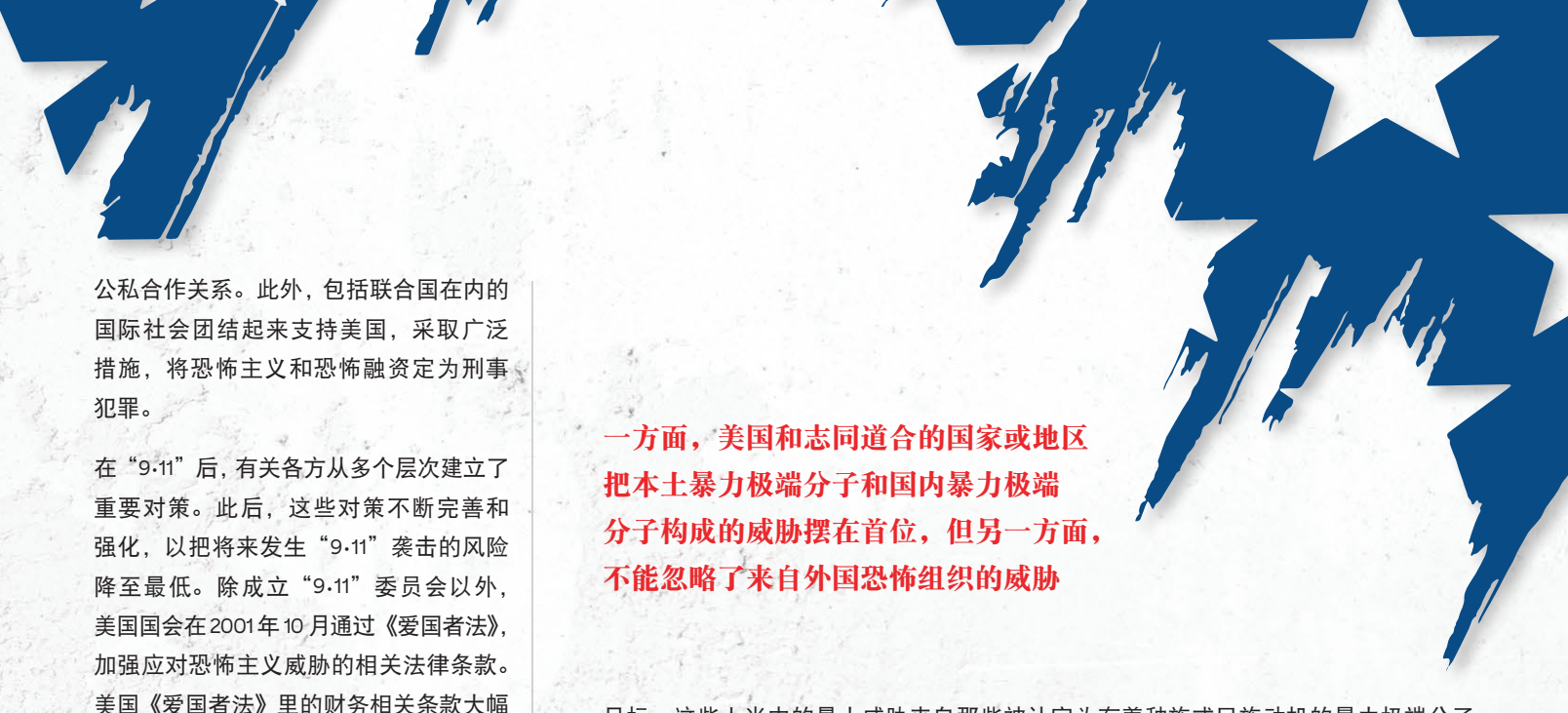
## “9·11”事件后的影响

近 3,000 人在袭击中丧生。在那个悲惨日子之后的几年间，有数百名急救人员因在这四个撞机地点接触到毒素而丧生。次生影响方面，“9·11”事件暴露出多个方面的问题：情报系统存在系统性的问题，过度自满，信息共享缺乏，对恐怖融资重视不足，需要加强《银行保密法》报告要求以及公公和公私合作。所有这些漏洞都成功被基地组织利用。

针对“9·11”事件，美国政府启动了大规模的应急行动，着手解决此次恐袭暴露出来的现有系统性问题。有军事行动，有情报和调查行动，也有监管和制裁行动，还建立了可持续的公公和







公私合作关系。此外，包括联合国在内的国际社会团结起来支持美国，采取广泛措施，将恐怖主义和恐怖融资定为刑事犯罪。

在“9·11”后，有关各方从多个层次建立了重要对策。此后，这些对策不断完善和强化，以把将来发生“9·11”袭击的风险降至最低。除成立“9·11”委员会以外，美国国会在2001年10月通过《爱国者法》，加强应对恐怖主义威胁的相关法律条款。美国《爱国者法》里的财务相关条款大幅提高了《银行保密法》有关要求。2001年10月，金融行动特别工作组就反恐怖融资问题在华盛顿特区举行了一场特别全体会议，会上实施了《反恐融资活动特别建议》。2002年10月，金融行动特别工作组发布了有关恐怖融资活动的分类和指引。此后，工作组继续就反恐怖融资活动定期提供指导意见。

## 当前的威胁环境

“9·11”以来的20年里，恐怖主义威胁环境不断变化。2001年至2019年初，主要威胁都是由组织推动的。组织既有演进，也有退化。“9·11”之前，尤其是在9·11前后，基地组织构成了主要威胁。2013年，随着叙利亚和伊拉克哈里发的发展，伊斯兰国成为最大的恐怖威胁。2019年，哈里发垮台，伊斯兰国变成叛军。

凭借通过互联网招募和培养极端分子的能力，基地组织和伊斯兰国开始假本土暴力极端分子(HVE)，将组织威胁转变成个人威胁。本土暴力极端分子受外国伊斯兰恐怖组织意识形态蛊惑。在本土暴力极端分子形成威胁的同时，从2019年开始，国内暴力极端分子(DVE)的威胁不断增大。国内暴力极端分子是指一些实施暴力行为的人，推动实现源于种族偏见、反政府情绪等国内因素的意识形态


**一方面，美国和志同道合的国家或地区把本土暴力极端分子和国内暴力极端分子构成的威胁摆在首位，但另一方面，不能忽略了来自外国恐怖组织的威胁**

目标。这些人当中的最大威胁来自那些被认定为有着种族或民族动机的暴力极端分子(RMVE)。

2021年，最严重的恐怖主义威胁来自本土暴力极端分子和国内暴力极端分子。2021年1月6日的美国国会大厦骚乱彰显了国内暴力极端分子的重要性，令人震惊不已。一方面，美国和志同道合的国家或地区把本土暴力极端分子和国内暴力极端分子构成的威胁摆在首位，但另一方面，不能忽略了来自外国恐怖组织的威胁。尽管他们目前还没有这个能力，但基地组织和伊斯兰国都渴望对美国发动类似“9·11”的袭击。

从反恐融资的角度来看，威胁环境从以组织为中心到以个人为中心的转变，意味着恐怖融资活动趋向本地化，因为以个人为中心的环境具有去集中化和去领导化的特点。因此，与“9·11”不同，资金不大可能从组织流向恐怖分子，资金更有可能是恐怖分子自己得到的，来自本地资源。无论攻击是本土暴力极端分子发起的，还是国内暴力极端分子发起的，独狼攻击都不需要很多资金。这种攻击需要的资金更少，复杂度较低，规模较小，成功率更高。

## 结语

“9·11”恐袭的策划和实施用了两年多的时间。这两年里，大量的资金被用于准备和执行“9·11”恐怖袭击。在这期间，恐怖分子频繁与银行和货币服务企业接触。即使接触了两年的时间，劫机者的交易活动并不引人注目，也不可疑。然而，在大多数情况下，劫机者及其协助者用的是真实身份，留下了资金线索。利用资金线索，联邦调查局摸清了资金流动轨迹，发现了劫机者与协助者的关系，最终直接追溯到KSM，间接追溯到bin Laden。由于得到了金融部门前所未有的支持，联邦调查局只用了几个星期就确定了“9·11”事件的资金流向。正如国会大厦骚乱证明的那样，威胁形势已经变了。资金需求已从组织转变为独狼或个人群体。要说最佳实践教了我们什么，可以说，自给自足的恐怖分子给我们带来了巨大的挑战，公营和私营机构需要携手共进，展开可持续、有意义的合作。 

Dennis M. Lormel, CAMS, 国际公认反恐融资专家, DML Associates LLC 总裁兼首席执行官, 美国弗吉尼亚州, dlormel@dmlassocllc.com







# 老年人钱财诈骗： 巨大危机

## 老

老年人钱财诈骗这一巨大危机，由众多因素共同促成：新冠疫情爆发，迫使人们在家隔离；人们对电话、电脑等通讯手段的依赖日益增加；成人保护服务机构 (Adult Protective Services) 的工作人员无法家访，致使社会为老年人提供的保护削弱；有些人因疫情失去唯一收入来源，陷入绝望；社会老龄化，每天有1万人年满65岁；犯罪嫌疑人积极寻找易于利用的目标；此外，许多老年受害人因为太要面子，不愿举报，又或者由于认知障碍，不清楚发生了什么事情。对于老年人钱财诈骗而言，这些因素叠加，可谓天时地利与人和。多年以来，诈骗老年人钱财的罪行泛滥全美，如今已恶化成巨大的社会与经济危机，亟需积极有力应对。



1996-2018 这 22 年中，我有幸担任圣地亚哥地区检察官反虐待老人小组的负责人。任职期间，全美各地不断有人打电话来，请求为当地执法机构工作人员、检察官、社会工作者等进行培训。2018 年，经过深思熟虑，我终于下定决心，把接力棒交给更年轻的检察官。如今，我就有了闲暇与机会，向更广泛的受众分享我就虐待老人案件提起公诉的经验。

我提起公诉的虐待老人重罪案件中，有 65% 涉及不同形式的钱财诈骗行为。无论此等诈骗行为属于何种类型（不论涉及现金、不动产、投资还是个人资产），检方面临的困难始终如一，那就是：检方应如何证明，嫌疑人是在未经受害者同意的情况下，剥夺了老年受害人的财产，并意图永久剥夺相关财产？

具体说来，可分为四种情形。其中前两种情形一目了然，而第三、第四种却极难证明。

第一种情形是，受害人有充分能力给出证言，表明被告未经其同意剥夺了其财产。

第二种情形是，受害人因老年痴呆晚期或其他某种极端精神障碍，无法作证；而且诈骗行为发生前，受害人已患上此种疾病。在此情形下，检方可在找到资产转移证据的基础上，采信具有执业资格的医生的证词，证明受害人不具备同意资产转移的能力。

第三种情形是，欺诈罪行揭露时，受害人已去世。按照惯例，在这种情况下，执法机构会立即做出判定，不再调查此事，因为无法证明受害人未同意。但我发现，如果具备第二种情形中所述的医学证据，则仍有可能通过展示受害人有案可查的无行为能力证明，从而辅证诈骗罪行的



发生。如果相关诈骗罪行涉及伪造文件，可考虑通过法医笔迹鉴定来定罪。还有，如果受害人去世前曾经激动“发声”，表明自己未同意转移资产，则检方可能成功说服法庭基于传闻证据规则，破例采信此庭外陈述。

第四种情形是，有证据证明受害人存在记忆损害，受害人只能勉强作证。此种情形下，乍一看来，似乎是受害人自愿将资产转移给被告，而被告通常也会将被转移的资产解释为赠礼或贷款。针对此种情形的案件，执法机构往往拒绝开展调查，理由是不存在明显的犯罪行为。最后的结论往往是：嫌疑人通过巧妙的操纵而非武力或胁迫，以不正当的方式影响了受害人，让受害人放弃了财产。但我们发现，针对此种情形，需围绕以下重点事项开展调查：



- 受害人和嫌疑人是如何会面的？会面地点和时间？
- 受害人在会见嫌疑人之前，消费习惯是什么样的？如果可以确定受害人一向节俭，就可能合理推测出，该资产转移完全不符合受害人的性格特点。
- 嫌疑人影响受害人的具体方法：嫌疑人是否切断受害人与亲朋好友的联系，或者伪造“身份”以吸引受害人？嫌疑人是否做出了某些行为，使受害人越来越依赖与嫌疑人的关系？

若能将老年人钱财诈骗案件归入上述情形之一，肯定有助于对案件进行评估，以便后续提起公诉。不过，将此类案件提交法官或陪审团，需要多领域专业人士通力合作。

## 采取多领域团队协作方法

诈骗老年人钱财的罪行越来越多，甚至有人称之为“21世纪犯罪”。想成功打击这种犯罪行为，需要众多机构共同努力。值得庆幸的是，许多司法管辖区已陆续建立钱财诈骗行为打击专家团队 (FAST)。那么，此种团队需要哪些专业人士？

显然，需要当地执法机构、郡检察官办公室、成人保护服务机构、长期护理监察员、公共监护人等相关岗位的人员，还应邀请州检察长办公室和美国联邦检察官办公室的代表，以及邮政检查局、社会保障管理局、联邦调查局、遗嘱检验法庭调查员、建筑承包商执照委员会等机构的成员。此外，银行、信用合作社、投资经纪人和其他金融机构的反欺诈调查员也很重要。最后别忘了，司法会计师、老年病学专家、当地老年服务提供商的代表，也可以为团队带来宝贵的见解。


诈骗老年人钱财案件的报告，往往递不到法庭之上。有时候，执法机构会称“这只是民事问题”；如果嫌疑人持有授权书，更是如此。有时候，相关机构会告知受害人或受害人亲属“犯罪行为并不在本司法管辖区发生”，或者“嫌疑人可能在海外，我们无法确定其身份。”有些时候，检察官还会暗示称，受害人因年龄或残疾无法给出有效证言，使受害人心生退意，不愿继续推进调查。

犯下此类投机罪行的嫌疑人往往心存侥幸，认为自己的操作经得起执法机构或检察官的任何审查。而疫情的影响，更进一步助长了这些掠夺者的胆量。

## 结语

要迎接这一挑战，务必认清有可能造成阻碍的“年龄歧视”误解，了解团队协作方式的重要性，并洞察综合运用一切资源解决此类阴险犯罪的价值所在。

诈骗老年人钱财，是一种粗暴的罪行：它不仅会影响老年人的财务安全，还会损害老年人的身心健康，更可能导致老年人生活方式的急剧恶化。老年人钱财诈骗案的受害者中，许多人都属于美国“最伟大的一代”。我们不仅应感激他们曾经做出的奉献，还应当为他们争取正义。

如果您还未成为反虐待老人工作组的成员，不妨考虑加入此类工作组；如果您所在地区没有这样的组织，或许可以考虑主动发起一个？ 

Paul Greenwood, 美国圣地亚哥郡退休副地方检察官,  
Greenwood 律师事务所, 顾问兼培训师

诈骗老年人钱财的罪行  
越来越多，甚至有人  
称之为“21 世纪犯罪”。  
想成功打击这种犯罪行为，  
需要众多机构共同努力



# 反洗钱 专业人士 需要了解的新 举报人制度







2020 年《反洗钱法》是美国反洗钱法十多年来最重大的变化，其中有项规定拓展了《银行保密法》举报人制度，金融机构和反洗钱专业人士需要特别予以关注。现在，举报人可以匿名举报《银行保密法》违规行为，最高可获得政府货币制裁 30% 的金钱奖励，而制裁总额有时可达数亿美元。现在实施的高额激励措施有可能导致举报事件急剧增加，就像美国证券交易委员会 (SEC) 在 2010 年建立独立制度后所经历的那样。《银行保密法》要求金融机构实施有效的反洗钱制度体系，检测和报告可疑交易。<sup>1</sup> 如果金融机构违反此要求，则每笔基础交易将面临 25,000 至 100,000 美元的罚款。<sup>2</sup> 虽然《银行保密法》之前有所谓的“线人”奖励制度，但奖励金额上限统一为 150,000 美元。<sup>3</sup> 此外，《银行保密法》没有就匿名披露违规行为作出规定。

《反洗钱法》对《银行保密法》举报人制度进行了几项重要调整，显著提高了对《银行保密法》违规行为披露的奖励金额，增加了报复保护措施，建立了匿名举报程序。现在，对于政府追回的超过 100 万美元的任何货币制裁，针对《银行保密法》违规行为提供“原始信息”的“举报人”，可以获得高达制裁金额 30% 的奖金。<sup>4</sup>

举报人可以是“任何个人”或“联合行动”的群体。<sup>5</sup> 不需要美国公民身份，因为洗钱活动经常跨越国界。举报人提供的“原始信息”可以来自举报人的独立知识或分析，只要政府尚未知晓或公共记录中不存在即可。<sup>6</sup> 举报人也不需要直接向政府报告信息。<sup>7</sup>

相反，举报人可以将其作为工作职责的一部分，向雇主汇报信息。美国财政部长有权决定对举报人的奖励金额，但必须考虑原始信息对后续执法行动的重要性，以及举报人或律师在此类行动中提供的帮助有多少。<sup>8</sup>

新的反洗钱举报人制度可能会带来高额奖励，因为《银行保密法》违规行为经常会导致数亿美元的民事和刑事处罚。例如，2021 年 1 月，金融犯罪执法网络 (FinCEN) 对美国银行协会第一资本银行 (Capital One) 处以 3.9 亿美元的民事罚款，<sup>9</sup> 原因是该银行未能在支票兑现子公司实施有效的反洗钱控制措施。第一资本银行在反洗钱方面的缺陷导致其未能就其支票兑现网点的交易提交可疑活动报告，这些网点后来承认犯有高利贷、非法赌博、逃税、洗钱等罪行。

同样，2018 年，美国银行根据与纽约南区美国检察官办公室达成的暂缓起诉协议，支付了 5.28 亿美元的罚款。<sup>10</sup> 除其他事项外，政府批评称，美国银行雇用反洗钱人员数量不足，使他们“严重超负荷工作”，因而减少了需要审查的潜在可疑交易的数量。根据《反洗钱法》，对第一资本银行和美国银行的处罚可能给提供原始信息的举报人带来超过 1 亿美元的奖励。

《反洗钱法》还制定了针对报复的重要保护措施，<sup>11</sup> 禁止雇主解雇、降级、停职、列入黑名单或以“任何其他方式”歧视披露有合理理由认为违反《反洗钱法》行为的举报人。即使只是将违规行为披露给举报人的上司而非政府，该禁令也适用。受到歧视的

新的反洗钱举报人制度  
可能会带来高额奖励，  
因为《银行保密法》  
违规行为经常会导致  
数亿美元的民事和刑事处罚





## 《反洗钱法》允许 举报人通过律师 “匿名”举报

举报人可以向劳工部长提出申诉。如果劳工部长未在 180 天内发布最终决定，举报人可以向联邦法院提起诉讼。可能的补救措施包括复职、双倍赔偿欠款和其他补偿性损失，包括律师费。

最后，《反洗钱法》允许举报人通过律师“匿名”举报。<sup>12</sup> 在这种方式下，政府只会收到律师的姓名和联系信息，任何后续咨询都通过律师转达举报人。在取得奖励之前，举报人必须披露其身份。这一条必不可少，因为政府雇员等特定群体不能获得举报人奖励。<sup>13</sup> 但在举报人身份信息披露后，《反洗钱法》要求政府对该信息保密，并对披露设有具体的限制，包括《隐私法》规定的限制。

《反洗钱法》可能会使反洗钱执法机构收到举报人报告的数量大幅增加。上述规定与 2010 年《多德 - 弗兰克法案》建立的美国证券交易委员会举报人制度非常相似。该制度颁布以来，美国证券交易委员会收到的举报人报告数量逐年增加，现在总计超过 40,000 条。2012 年至 2020 年，美国证券交易委员会向举报人支付了 5.62 亿美元的奖励。<sup>14</sup>

《反洗钱法》对《银行保密法》举报人制度的拓展，会给反洗钱专业人士和金融机构带来重大影响。了解《银行保密法》违规行为的反洗钱专业人士都有非常

强烈的动机向政府披露他们所知道的信息，现在他们可以匿名举报了。正如美国证券交易委员会举报人制度所证明的那样，这些激励措施可能会促使举报数量大幅增加。

这一全新的现实也会给金融机构带来风险，即使他们完全符合《银行保密法》的规定。举报人提交的报告即使缺乏基础，也有可能引发调查，此类调查针对的金融机构将需要投入大量资源进行回应。金融机构可以采取多种措施，鼓励内部举报，降低意外调查风险。第一步是实施匿名热线等内部举报机制，但光有举报机制是不够的。还需要让员工相信，所在机构会认真对待此类投诉，不会进行报复。金融机构可以通过最高层鼓励举报，制定强有力的反报复保护措施，尽量提高投诉调查透明度，由此培养员工的上述信念。如果员工认为举报制度可信，则机构有机会积极主动地解决问题，而非被动应对调查。《反洗钱法》将内部举报人列入合格奖励对象，起了鼓励内部举报的作用。

反洗钱专业人士和金融机构，若对新的举报人制度有任何疑问或疑虑，最好咨询律师。虽然《反洗钱法》规定了举报人制度的界限，但从多个方面来讲，该制度的未来将取决于执法机构及其

发布的监管规定或其他指导方针。经验丰富的法律顾问可以帮助专业人士和金融机构跟上新的发展，分析其影响，制定有效的行动方案。A

Caleb Hayes-Deats, MoloLamken 律师  
事务所律师法律顾问，美国华盛顿特区，  
chayes-deats@mololamken.com<sup>15</sup>

<sup>1</sup> 31 U.S.C. §5318。

<sup>2</sup> 同上。§5321。

<sup>3</sup> 31 U.S.C. §5323(b) (2020)。

<sup>4</sup> 31 U.S.C. §5323(b)(1)。货币制裁包括“罚款、追缴和利息”，但不包括“没收”、“归还”或其他“受害者赔偿”。同上。§5323(a)(2)。

<sup>5</sup> 同上。§5323(a)(5)。

<sup>6</sup> 同上。§5323(a)(3)。

<sup>7</sup> 同上。§5323(a)(5)。

<sup>8</sup> 同上。§5323(c)(1)。

<sup>9</sup> “Assessment of Civil Monetary Penalty Number 2010-01” (对 2010-01 号案件民事货币罚款的评估)，金融犯罪执法网络，[https://www.fincen.gov/sites/default/files/enforcement\\_action/2021-01-15/Assessment\\_CONA%20508\\_0.pdf](https://www.fincen.gov/sites/default/files/enforcement_action/2021-01-15/Assessment_CONA%20508_0.pdf)

<sup>10</sup> “Manhattan U.S. Attorney Announces Criminal Charges Against U.S. Bancorp For Violations Of The Bank Secrecy Act” (曼哈顿美国检察官宣布对美国银行违反《银行保密法》提起刑事指控)，纽约南区检察官办公室，2018 年 2 月 15 日，<https://www.justice.gov/usao-sdny/pr/manhattan-us-attorney-announces-criminal-charges-against-us-bancorp-violations-bank>

<sup>11</sup> 31 U.S.C. §5323(g)。

<sup>12</sup> 31 U.S.C. §5323(d)。

<sup>13</sup> 31 U.S.C. §5323(c)(2)。

<sup>14</sup> “2020 Annual Report to Congress Whistleblower Program” (国会举报人制度 2020 年度报告)，美国证券交易委员会，[https://www.sec.gov/files/2020%20Annual%20Report\\_0.pdf](https://www.sec.gov/files/2020%20Annual%20Report_0.pdf)

<sup>15</sup> Hayes-Deats 之前曾在纽约南区美国检察官办公室工作，参与了金融犯罪执法网络对美国银行反洗钱处罚的评估工作。本文表达的观点仅代表作者本人观点。







# 欧洲网络安全生态系统： 一场打击网络犯罪的战争

6月23日，欧盟委员会发布消息称，计划成立联合网络部门，以应对网络犯罪相关大规模安全事件。<sup>1</sup>

该提案是欧盟和欧盟委员会为打击网络犯罪而提出的大量提案、指南、战略和立法的一部分。这并非故意为之，只是体现了网络犯罪的性质。物联网<sup>2</sup>现已成为全球互联网基础设施的一部分，形成了没有边界的虚拟空间。在这片空间里，网络犯罪分子可以从全球任何地方攻击任何行业、任何个人。

欧盟目前有27个成员国。因此，若想有效打击和起诉网络犯罪，需要协调欧盟各国法律、文化和宪法规定。

从起诉的角度来看，电子证据的搜查和扣押是打击网络犯罪的核心。国家法律不仅要符合搜查和扣押法，还要符合《欧洲人权公约》(ECHR)规定的公认人权条款。

考虑到这复杂性，促使欧盟开发了一个错综复杂的“生态系统”，供欧盟成员国在其中有效打击网络犯罪（见图1）。

图 1：欧洲网络安全危机管理框架



## 生态系统：欧洲网络安全危机管理框架

### 搜查和扣押立法与《欧洲人权公约》

《欧洲人权公约》是欧盟所有搜查和扣押立法（以及其他人权利益）的监督框架和标准。《欧洲人权公约》的各项原则由欧洲人权法院 (ECtHR) 执行。

《欧洲人权公约》适用于欧洲理事会的 47 个成员国，<sup>3</sup> 于 1950 年 11 月 4 日在罗马签署，1953 年 9 月 3 日在欧洲理事会大会上通过并正式生效。<sup>4</sup>

公约缔约国受欧洲人权法院裁决约束。该法院有权审理国家间和个人的请愿或投诉，而无需地方政府事先批准。<sup>5</sup>

《欧洲人权公约》是欧盟所有搜查和扣押立法（以及其他人权利益）的监督框架和标准



## 欧盟网络与信息安全局

欧盟网络与信息安全局 (ENISA) 成立于 2004 年，宗旨是“在整个欧洲共同实现高水平的网络安全。”<sup>6</sup> ENISA 是欧盟协调应对网络犯罪事件和危机管理的一部分，并在必要时协助欧盟委员会开展工作。<sup>7</sup> 此项工作是在综合政治危机响应 (IPCR) “框架”内完成的。<sup>8</sup> ENISA 与成员国一道制定“欧盟级网络危机管理程序，在发生跨境网络事件时提高态势感知能力，帮助国家和欧盟决策者做出正确的决定。”<sup>9</sup>

## 网络安全法案

ENISA 条例为第 (EU) 2019/881 号条例，<sup>10</sup> 称为《网络安全法案》。《网络安全法案》为产品和服务建立了网络安全认证框架。<sup>11</sup> 该法案加强了对 ENISA 支持成员国应对网络安全威胁和攻击的授权。同时责成 ENISA 支持成员国建立全欧盟网络安全认证框架，ENISA 将在其中发挥关键作用。<sup>12</sup>

## NIS 指令和 NIS2

2016 年发布的 NIS 指令 (EU 2016/1148)<sup>13</sup> 是《欧盟数字十年的网络安全战略》的一部分，也是全欧盟网络安全立法工作的第一项成果。指令描述了成员国应采用的国家网络和信息系統安全框架。<sup>14</sup>

NIS 指令分为以下三个部分：<sup>15</sup>

- “1. 国家能力：欧盟成员国须具备欧盟各国的特定国家网络安全能力，例如：必须设立国家 CSIRT、开展网络演练等。
2. 跨境合作：欧盟国家之间的跨境合作，如欧盟 CSIRT 运营网络、NIS 战略合作小组等。



3. 国家对关键部门的监督：欧盟成员国须监督本国关键市场运营商的网络安全事务：对关键部门（能源、交通、水务、卫生、数字基础设施和金融部门）进行事前监管，对关键数字服务提供商（在线市场、云和在线搜索引擎）进行事后监管”<sup>16</sup>

指令旨在“加强整个欧盟的网络安全水平，”<sup>17</sup> 因该指令为欧盟指令，各成员国均已开始实施。

指令第 23 条要求欧盟委员会定期审查指令的运作情况。审查结束后，NIS2 于 2020 年 12 月 16 日提交欧盟。<sup>18</sup> NIS2 废除了当时实行的 NIS 指令。据称，NIS2 对现行法律框架进行了现代化，“考虑到内部市场数字化程度近年来不断提高，网络安全威胁形势不断变化。”<sup>19</sup>

## 欧盟网络安全战略

欧盟委员会和欧盟外交与安全政策高级代表于 2020 年 12 月 16 日提出了新的欧盟网络安全战略。<sup>20</sup> 欧盟网络安全战略“描述了欧盟应该如何利用和强化所有工具和资源，维护技术主权。”<sup>21</sup> 该战略是一项普遍适用的工具，描述了可以“部署”的“三大工具”，即监管、投资和政策措施。这三大工具旨在解决以下问题：

- “弹性、技术主权与领导力
- 预防、遏制和应对行动的能力
- 合作推进全球开放网络空间”<sup>22</sup>

多项措施（如联合网络部门）共同构成欧盟网络安全战略的一部分。

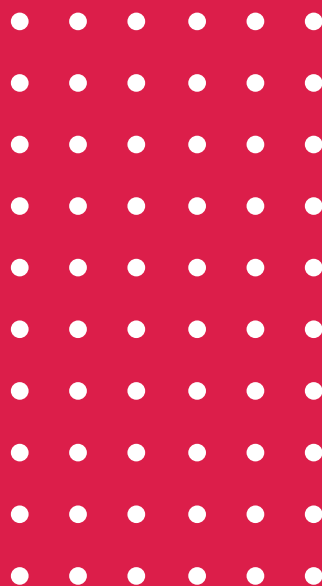
## 欧盟安全联盟战略： “连通新安全生态系统中的各个点”

2020 年 7 月 24 日，欧盟委员会制定了 2020-2025 年的新版欧盟安全联盟战略。与欧盟网络安全战略一样，欧盟安全联盟战略是一项普遍适用的工具，规定了作为其战略的一部分，必须在欧盟层面实施的原则或“四大战略重点”。<sup>23</sup>

四大战略重点如下：<sup>24</sup>

- 面向未来的安全环境
- 应对不断演变的威胁
- 保护欧洲人民免受恐怖主义和有组织犯罪的伤害
- 强大的欧洲安全生态系统

图 2 更详细地描述了这四大战略重点。



联合网络部门的宗旨，  
是汇集欧盟所有的资源  
和专业知识，预防、  
遏制并应对大规模网络  
事件及危机

## 联合网络部门

6 月 23 日，欧盟委员会提出建立一个新的联合网络部门，以“应对不断增加的，影响公共服务以及全欧盟企业和公民生活的严重网络事件。”<sup>25</sup>

联合网络部门的宗旨，是汇集欧盟所有的资源和专业知识，预防、遏制并应对大规模网络事件及危机。该部门也是欧盟网络安全战略和欧盟安全联盟战略的成果。<sup>26</sup>

## 欧盟的资金支持

据称，在未来 7 年，欧盟网络安全战略将获得“前所未有的投资”<sup>27</sup>。此项投资将纳入 2022 年欧盟长期预算。影响欧盟长期预算的机制是数字欧洲计划、<sup>28</sup> 欧洲地平线<sup>29</sup> 和欧洲复苏计划。<sup>30</sup> 除了欧盟长期预算之外，欧盟还制定目标，通过欧盟、成员国和行业的联合投资，投入 45 亿欧元（相当于 53 亿美元）。<sup>31</sup> 欧盟将通过网络安全能力中心和协调中心网络<sup>32</sup> 实现这一目标，确保大部分资金流向中小企业。



图 2：欧盟安全联盟战略



资料来源：“EU Security Union Strategy: connecting the dots in a new security ecosystem”（欧盟安全联盟战略：连通新安全生态系统中的各个点），欧盟委员会，2020 年 7 月 24 日，[https://ec.europa.eu/commission/presscorner/detail/en/ip\\_20\\_1379](https://ec.europa.eu/commission/presscorner/detail/en/ip_20_1379)

## 欧洲网络安全生态系统的影响和现状

目前，生态系统只是一个构想，尚未落实到实际组织构成，因此可将其描述为具有前瞻性的网络安全框架，而不是称其为现行框架。

欧盟将从 2022 年开始对网络安全战略给予资金支持。联合网络部门是欧盟委员会的一项提案，仍然需要实施。因此，该新生态系统对网络犯罪显然尚未产生影响。

欧盟打击网络犯罪的行动，现状如何？自 2004 年以来，ENISA 一直是欧盟打击网络犯罪的重要组成部分，而 NIS 指令发布于 2016 年。

这份具有前瞻性的网络安全框架的影响，还需要几年才会体现出来。资金

支持将从 2022 年开始入场，但其中提案在 2023 年之前是否具有可行性，这点还有待观望。欧盟委员会预计于 2022 年 6 月 30 日展开联合网络部门的运行阶段，并于 2023 年 6 月 30 日全面独立运作。<sup>33</sup>

欧盟委员会网站上发布了如下声明：“欧盟网络安全生态系统广泛而多样。有了联合网络部门，不同群体和领域将享有一片合作共事的空间，届时将可令现有网络充分发挥其潜力。这一生态系统的基础，是从 2017 年开始的各项工作……”<sup>34</sup>

总之，目前看来欧洲网络安全生态系统是一份出色的可行战略，似乎具备所有成功要素，即资金支持、成员国的合作以及必要的技能和专业知识。 **A**

Gideon Bouwer, Cyberlawforensics 信息技术律师，南非，  
[gideon@cyberlawforensics.co.za](mailto:gideon@cyberlawforensics.co.za)

<sup>31</sup> “EU Cybersecurity: Commission proposes a Joint Cyber Unit to step up response to large-scale security incidents”（欧盟网络安全：欧盟委员会提议成立联合网络部门，大力应对大规模安全事件），欧盟委员会，2021 年 6 月 23 日，[https://ec.europa.eu/commission/presscorner/detail/en/ip\\_21\\_3088](https://ec.europa.eu/commission/presscorner/detail/en/ip_21_3088)

<sup>32</sup> “What is IoT?”（什么是物联网？），甲骨文，<https://www.oracle.com/za/internet-of-things/what-is-iot/>。“物联网 (IoT) 描述的是一个嵌入了传感器、软件和其他技术的，由物理对象（‘物’）构成的网络，其目的是通过互联网连接其他设备和系统并与其交换数据。”

- <sup>3</sup> 欧洲理事会成立于1949年，47个欧洲国家为其成员国。
- <sup>4</sup> Dietrich Schindler, “European Convention on Human Rights in Practice” (欧洲人权公约), *Washington University Law Quarterly*, 1962年1月, [https://openscholarship.wustl.edu/law\\_lawreview/vol1962/iss2/2](https://openscholarship.wustl.edu/law_lawreview/vol1962/iss2/2)
- <sup>5</sup> “European Convention on Human Rights: Europe [1950]” (欧洲人权公约：欧洲[1950]), *大英百科全书*, 1950年11月4日, <https://www.britannica.com/event/European-Convention-on-Human-Rights-Europe-1950> (访问日期：2020年9月17日)。
- <sup>6</sup> “About ENISA - The European Union Agency for Cybersecurity” (关于ENISA——欧盟网络安全局), *欧盟网络安全局*, <https://www.enisa.europa.eu/about-enisa>
- <sup>7</sup> “EU-level Cyber Crisis Management” (欧盟级网络危机管理), *欧盟网络安全局*, <https://www.enisa.europa.eu/topics/cyber-crisis-management/eu-cooperation>
- <sup>8</sup> “How does the Integrated Political Crisis Response (IPCR) mechanism work?” (综合政治危机响应(IPCR)机制的运作方式), *欧盟理事会*, 2018年, <https://www.consilium.europa.eu/en/documents-publications/publications/ipcr/>。“IPCR是欧盟理事会的危机应对机制,是握在主席国手中的‘工具’,用于协调政治部门对重大跨部门复杂危机(包括恐怖主义行为)作出反应。”
- <sup>9</sup> “EU-level Cyber Crisis Management” (欧盟级网络危机管理), *欧盟网络安全局*, <https://www.enisa.europa.eu/topics/cyber-crisis-management/eu-cooperation>
- <sup>10</sup> “ENISA Mandate and Regulatory Framework” (ENISA授权和监管框架), *欧盟网络安全局*, <https://www.enisa.europa.eu/about-enisa/regulatory-framework>
- <sup>11</sup> “The EU Cybersecurity Act” (欧盟网络安全法案), *欧盟委员会*, <https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-act>
- <sup>12</sup> “The EU Cybersecurity Act is Now Applicable” (《欧盟网络安全法案》现已实施), *众达律师事务所*, 2019年6月, <https://www.jonesday.com/en/insights/2019/06/the-eu-cybersecurity-act-is-now-applicable>
- <sup>13</sup> “NIS Directive” (NIS指令), *欧盟网络安全局*, <https://www.enisa.europa.eu/topics/nis-directive>
- <sup>14</sup> Dimitra Markopoulou, Vagelis Papakonstantinou 和 Paul de Hert, “The new EU cybersecurity framework: The NIS Directive, ENISA’s role and the General Data Protection Regulation” (欧盟新版网络安全框架：NIS指令、ENISA的作用以及通用数据保护条例), *Computer Law & Security Review*, 35卷,第6期,2019年11月, <https://www.sciencedirect.com/science/article/pii/S0267364919300512> (访问日期：2021年8月11日)。
- <sup>15</sup> “NIS Directive” (NIS指令), *欧盟网络安全局*, <https://www.enisa.europa.eu/topics/nis-directive>
- <sup>16</sup> 同上。
- <sup>17</sup> 同上。
- <sup>18</sup> “NIS Directive” (NIS指令), *欧盟委员会*, <https://digital-strategy.ec.europa.eu/en/policies/nis-directive>
- <sup>19</sup> 同上。
- <sup>20</sup> “The EU’s Cybersecurity Strategy for the Digital Decade,” (欧盟数字十年的网络安全战略), *欧盟委员会*, 2020年12月16日, <https://digital-strategy.ec.europa.eu/en/library/eus-cybersecurity-strategy-digital-decade-0>
- <sup>21</sup> “The Cybersecurity Strategy” (网络安全战略), *欧盟委员会*, <https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-strategy>
- <sup>22</sup> 同上。
- <sup>23</sup> “EU Security Union Strategy: connecting the dots in a new security ecosystem” (欧盟安全联盟战略：连通新安全生态系统中的各个点), *欧盟委员会*, 2020年7月24日, [https://ec.europa.eu/commission/presscorner/detail/en/ip\\_20\\_1379](https://ec.europa.eu/commission/presscorner/detail/en/ip_20_1379)
- <sup>24</sup> 同上。
- <sup>25</sup> “EU Cybersecurity: Commission proposes a Joint Cyber Unit to step up response to large-scale security incidents” (欧盟网络安全：欧盟委员会提议成立联合网络部门,大力应对大规模安全事件), *欧盟委员会*, 2021年6月23日, [https://ec.europa.eu/commission/presscorner/detail/en/ip\\_21\\_3088](https://ec.europa.eu/commission/presscorner/detail/en/ip_21_3088)
- <sup>26</sup> 同上。
- <sup>27</sup> “New EU Cybersecurity Strategy and new rules to make physical and digital critical entities more resilient” (欧盟网络安全新战略,以及关键实体与数字机构弹性提升新规则), *欧盟委员会*, 2020年12月16日, [https://ec.europa.eu/commission/presscorner/detail/en/ip\\_20\\_2391](https://ec.europa.eu/commission/presscorner/detail/en/ip_20_2391)
- <sup>28</sup> “Commission welcomes political agreement on €7.5 billion Digital Europe Programme” (欧盟委员会欢迎就75亿欧元的数字欧洲计划达成政治协议), *欧盟委员会*, 2020年12月14日, [https://ec.europa.eu/commission/presscorner/detail/en/ip\\_20\\_2406](https://ec.europa.eu/commission/presscorner/detail/en/ip_20_2406)
- <sup>29</sup> “Commission welcomes political agreement on Horizon Europe, the next EU research and innovation programme” (欧盟委员会欢迎就下一项欧盟研究与创新计划“欧洲地平线”达成政治协议), *欧盟委员会*, 2020年12月10日, [https://ec.europa.eu/commission/presscorner/detail/en/IP\\_20\\_2345](https://ec.europa.eu/commission/presscorner/detail/en/IP_20_2345)
- <sup>30</sup> “Recovery plan for Europe” (欧洲复苏计划), *欧盟委员会*, [https://ec.europa.eu/info/strategy/recovery-plan-europe\\_en](https://ec.europa.eu/info/strategy/recovery-plan-europe_en)
- <sup>31</sup> “New EU Cybersecurity Strategy and new rules to make physical and digital critical entities more resilient” (欧盟网络安全新战略,以及关键实体与数字机构弹性提升新规则), *欧盟委员会*, 2020年12月16日, [https://ec.europa.eu/commission/presscorner/detail/en/ip\\_20\\_2391](https://ec.europa.eu/commission/presscorner/detail/en/ip_20_2391) (访问日期：2021年8月11日)。
- <sup>32</sup> “Commission welcomes political agreement on the Cybersecurity Competence Centre and Network” (欧盟委员会欢迎就网络安全能力中心与网络达成政治协议), *欧盟委员会*, 2020年12月11日, [https://ec.europa.eu/commission/presscorner/detail/en/IP\\_20\\_2384](https://ec.europa.eu/commission/presscorner/detail/en/IP_20_2384)
- <sup>33</sup> 同上。
- <sup>34</sup> “EU Cybersecurity: Commission proposes a Joint Cyber Unit to step up response to large-scale security incidents” (欧盟网络安全：欧盟委员会提议成立联合网络部门,大力应对大规模安全事件), *欧盟委员会*, 2021年6月23日, [https://ec.europa.eu/commission/presscorner/detail/en/ip\\_21\\_3088](https://ec.europa.eu/commission/presscorner/detail/en/ip_21_3088)





公认反洗钱师协会®

# 成为拥有反洗钱或制裁合规领域 全球资格认证的专业人士



反洗钱认证的  
国际黄金标准



了解并解读不断  
变化的制裁体系

访问 [www.acams.org](http://www.acams.org)  
开启您的旅程





## 韩国“N号房”案例分析

**2**020年，全球封锁导致在线儿童性虐待内容（CSAM）和需求双双增长；希望交换和提供非法内容的用户，通过社交媒体、即时消息工具、聊天室和网络游戏访问这些内容，欧洲刑警组织将这种行为称为“利用隔离”（Exploit Isolation）。

特别令人担忧的是，这些非法内容主要是未成年受害者自己制作的，犯罪分子通过胁迫取得这些内容，试图扩大参与者和幸存者的范围。<sup>1</sup> 儿童和未成年人性剥削的一个新近例子是韩国“N号房”案。

下面我们将通过分析“N号房”一案来提高对这类犯罪的认识，为反金融犯罪专业人士提供必要的知识，使他们能够识别、标记和报告此类犯罪行为；同时为执法机构和检察官提供相关的工具和知识，协助他们逮捕和起诉涉及儿童性虐待内容的犯罪分子。



## 儿童性虐待内容是不断发展的，难以预防、识别、追踪和报告

儿童性虐待内容是不断发展的，难以预防、识别、追踪和报告。儿童性虐待内容交易有着特殊的设计方式，很难确定调查的司法管辖区，难以取得支撑起诉的数据/证据。如果涉及加密货币，也有可能涉及多个司法管辖区。根据所用加密货币的性质，也有可能降低追踪犯罪分子的难度。

### 建立信任

犯罪分子把儿童性虐待内容当作货币使用，为了获得这种内容，他们首先会进行网络诱骗。犯罪分子通过搜索受害者的社交媒体内容或网络游戏玩家，锁定容易上当的攻击目标。确定目标后，他们会通过 Telegram 等即时消息工具结识受害者。

犯罪分子会通过多种方式诱骗儿童性虐待内容目标，包括假冒金主、星探、真爱或好友。诱骗活动往往分步实施，类似于传统的“线下”人口贩卖活动，犯罪分子通过与受害者持续交流或对其做出激励许诺，与之建立信任。他们可能假扮金主或星探，向目标许诺金钱或名声，或向目标承诺真爱。

### 羞耻因素

随着诱骗的发展，如果越来越成功，目标就会陷入骗局、无法脱身，犯罪分子会胁迫他们提供私密信息、照片、视频、财务信息、个人信息等。犯罪分子一旦得到这些私密信息，无论是通过网络欺诈<sup>2</sup>还是无意或被迫披露获得，他们都会利用“羞耻因素”<sup>3</sup>开始勒索，威胁把图片内容放布到网上，让所有人都能看到。

除此之外，在“N号房”一案中，部分儿童性虐待内容是未成年人的家人

提供的，为了获得信任、受邀进入各种聊天室，他们自愿上传照片和视频。<sup>4</sup>这是“N号房”运作方式的一部分——采用会员制服务模式，在不同主题的聊天室里交换性剥削内容。例如，“哥谭室”(Gotham Room)是会员们共享儿童性虐待内容的营销室，“萝莉室”【Loli Room，源自“Lolita complex”（洛丽塔情结）一词】则提供年轻女孩性物化视频。儿童性虐待内容提供者被称为“医生”，通过向“医生室”(Doctor's Room)上传视频获得报酬。<sup>5</sup>为了能获得更多违禁内容，有些人同时扮演两个角色（内容买家和提供者）。

### 残酷的统计数据

“N号房”内容的买家用比特币付款，支付金额从25万韩元（合217.32美元）到155万韩元（合1,347.39美元）不等。<sup>6</sup>

令人作呕的是，“N号房”自2018年开播以来，上传的儿童性虐待内容中除了色情内容外，还包括惨不忍睹的自残内容。



迄今为止，已发现 3,700 多个色情视频短片，<sup>7</sup> 逮捕了 100 多名犯罪嫌疑人。Telegram 上的 56 个受监控聊天群似乎还有超过 26 万用户。令人不安的是，“N 号房”得到很多人的支持，他们打招呼不说“你好”，而是“我们强奸吧。”<sup>8</sup>

## 了解您的客户

幸好“N 号房”被两名韩国女大学生曝光了，她们 2019 年听说有这种剥削现象，<sup>9</sup> 于是着手调查以参加一项新闻调查竞赛。她们在文章《你卖儿童色情内容吗？Telegram 大量滋生犯罪活动》中，描述了二人卧底发现的色情聊天室，最终导致“N 号房”幕后主使被捕。外号“GodGod”的韩国男子被判 34 年监禁。<sup>10</sup> 具有讽刺意味的是，据透露，GodGod 要求潜在会员提供“了解您的客户”文件，筛查并验证他们的身份，通过后才能参与儿童性虐待内容交换。

## 恋童障碍

对儿童性虐待内容的需求推动了此类内容的供应和盈利能力。反金融犯罪和执法专业人士通常认为，儿童性虐待、人口贩卖和现代奴隶制都属于犯罪，必须予以起诉和惩罚。然而，要在全球范围内根除儿童性虐待内容，需要围绕恋童障碍等疾病和可能治疗方案开展宣传教育活动，提高人们的认识。恋童障碍的特点是以未成年人（通常为 13 岁或以下）为对象，反复出现强烈的性幻想、性冲动或性行为。只有年满 16 岁或以上且比性幻想或性行为的对象年长 5 岁或以上的人才可确诊。

针对恋童障碍患者的治疗方案包括心理治疗和药物治疗（如抗雄激素）；然而，这些人可能不会寻求治疗，因为法律要求临床医生和治疗师向有关当局报告疑似儿童性虐待或身体虐待行为。这些要求因国家/地区而异。此外，确诊年龄指南对西方文化适用，但并不适用许多接受未成年人性活动、婚姻和生育的文化。<sup>11</sup> 由于这些原因，许多儿童剥削案件遭到忽视，没人报告，也没有处理。考虑到一些金融机构具有国际影响力，可以利用其平台，宣传恋童障碍知识和相应治疗方案，在全球范围内提高人们的认识，扩大文化影响，防范儿童剥削行为。

在打击儿童剥削犯罪行为方面，必须要  
教育和赋能儿童、帮助他们认识和报告  
剥削行为摆在首位

## 教育的重要性

在打击儿童剥削犯罪行为方面，必须要教育和赋能儿童、帮助他们认识和报告剥削行为摆在首位。棘手的是，在某些文化中，服从父母或长辈比儿童权利重要。因此，人们可能把儿童性剥削行为视为“家庭问题”而非法律问题。在压力较大的家庭环境、自尊心较低且科技设备使用不受限制的情况下，儿童遭受性虐待的可能性更大。<sup>12</sup>

金融机构不仅能发现和报告潜在的儿童剥削行为，还可以利用其平台启动青少年呵护计划，增进他们的心理健康和技术风险意识。金融机构可以结成联盟，支持参与儿童权利和安全事业的地方或国际组织。金融机构和国家或地区可以加入 WeProtect 全球联盟等组织，共同打击全球在线儿童性剥削活动。<sup>13</sup> 还有虚拟全球特别工作组 (VGT)，这是一个旨在解决在线儿童性剥削问题的国际执法联盟。<sup>14</sup> 跨宗教联盟联合世界各地的宗教领袖、执法机构、监管机构和科技行业，共同打击儿童剥削活动，增进儿童尊严。<sup>15</sup>

## 与执法机构合作

传统金融机构和加密货币交易所可以追踪到潜在儿童性虐待内容所得，并向执法机构报告或与其合作。在“N 号房”一案中，一些加密货币交易所为执法机构提供了宝贵的帮助。<sup>16</sup>

儿童性虐待内容提供者和消费者采用不同的交易模式，为了发现交易双方，金融机构需要制定特定的检测规则。消费者交易金额小，利用各种货币服务企业来掩盖资金的目的。提供者可能会使用类似业务账户的账户，但业务性质



## 从诱骗、制作性内容到收款，在整个过程的各个阶段，在线儿童性剥削内容提供者高度依赖互联网

和资金来源可能不明。有时候，可能会使用多个个人账户代表提供者开展活动。

根据加拿大金融交易和报告分析中心对在线儿童性剥削相关披露和可疑交易报告的分析，消费者交易主要是通过货币服务企业对外转账，将资金转移到儿童性剥削高风险司法管辖区，包括菲律宾、泰国、哥伦比亚、美国、加纳、乌克兰、多米尼加共和国、罗马尼亚、牙买加和俄罗斯。<sup>17</sup>

### 可疑活动指标

从诱骗、制作性内容到收款，在整个过程的各个阶段，在线儿童性剥削内容提供者高度依赖互联网。根据具体情况，与潜在犯罪分子相关的可疑活动指标可能包括在线购物、购买应用程序、在线游戏和赌博、使用在线视频和通信技术、使用在线文件存储服务等行为中的一种或多种。这些交易可能涉及支付处理商。<sup>18</sup>

有的提供者可能会用加密货币提供在线儿童剥削内容销售服务，Welcome to Video 即是如此，这是在撰写本文时内容最多的儿童性剥削市场。<sup>19</sup> 该网站使用比特币进行交易，执法机构可以进行追踪。据信，提供者可能会转而使用隐私加密货币以免被追踪，因为这些代币增加了第三方交易处理商，可以隐藏交易记录。在“N 号房”一案中，为方便通过 Telegram 访问，提供者接受比特币付款。<sup>20</sup>

在隐私代币有可能被用来混淆活动来源和目的的情况下，可以把交易模式、交易金额以及有关用户的负面新闻作为指标。例如，在调查 Welcome to Video 时，某些交易金额（如 0.04 个比特币

或 39 美元）出现的频率比其他交易金额高，这些金额可能是某些内容的固定费用。通过以隐私代币计价的这些特定金额的等价值可以洞察交易目的。

尽管可以通过任何类型的加密货币账户购买儿童虐待内容，但这些购买行为更有可能发生在专门为此类交易而开立的账户上，利用这些账户进行其他交易或交易活动的机会很小。韩国非常勇敢，能与全球分享“N 号房”案件及其细节。通过该案，我们可以更清楚了解在线儿童剥削及其可能的检测和防范方法。其他国家或地区需要效仿韩国，披露犯罪分子的身份，保护公众尤其是儿童的安全。

### 社交媒体的作用

全球疫情使得在线儿童虐待内容增多，犯罪分子利用“儿童友好”的应用程序结识和剥削儿童。<sup>21</sup> 儿童剥削问题不是某个平台特有的问题，而是存在于所有社交媒体中。对于社交媒体公司在监管或规定用户发布内容方面需要承担多少责任，人们仍然争论不休。<sup>22</sup> 加拿大等五眼联盟国家（其他四个为美国、英国、澳大利亚和新西兰）发表声明称，将推动全球科技公司采纳一套自愿原则，就在线儿童性剥削内容的识别、披露和删除作出规定。此外，这些国家还努力提高追查和起诉儿童剥削犯罪分子的能力，立法强制社交媒体公司加强对儿童剥削内容的监管。<sup>23</sup>

### 社交媒体的作用与欧盟

为响应上述自愿原则，欧洲议会也通过了一项新的临时立法，允许根据欧盟电子隐私指令的规定，利用扫描技术检测在线

## 儿童剥削问题不是 某个平台特有的问题， 而是存在于所有社交 媒体中

诱骗活动。授权官员对违规实体（此例中为电子服务提供商）进行制裁或约束，强制政府提供保护，这非常重要。<sup>24</sup>

根据 7 月 24 日“欧盟委员会致欧洲议会公函”，<sup>25</sup>“……欧洲刑警组织无法从私营机构直接接收个人数据，妨碍了为成员国提供支持的能力……”这表明，受现行立法所限，欧盟和其他司法管辖区只能被动期望电子服务提供商能自愿披露相关信息。如果不披露，运营儿童性虐待内容服务以及协助传播儿童性虐待内容的特定电子服务提供商将继续开展业务，不会受到阻碍和惩罚。据了解，当今社会需要数据隐私。然而，如果在儿童性虐待内容传播方面依赖自愿披露，结果会造成巨大的真空，保护的只会是犯罪分子。必须在全球范围内建立一种机制，强制、鼓励披露，对不披露行为进行惩罚和追责，使这种自愿披露政策既有益也有意义。

### 结语

人口贩卖（最近被归为现代奴隶制）已经存在很长时间，随着互联网和现代通信的出现，出现了显著增长。




近来，各种形式的网络犯罪已演变为一种有利可图的威胁。加上新冠疫情下，受害者自己发布的内容（欧洲刑警组织将其称为“自我剥削”），网络犯罪变得更加复杂，因为犯罪分子会利用一切机会，获取非法利益，同时最大限度地减少给自己带来风险。

“N 号房”一案和相关参考资料提供了有用的真实案例，使我们从亚洲和欧洲角度了解最新的犯罪方法，深入了解更多可疑活动指标和这些案例的运作方式。

在研究和撰写本文时，笔者不禁自问，ACAMS 会员该如何阻止这类剥削？

ACAMS 专业人士要同心协力，通过提高认识，意识到这些犯罪的存在，了解其运作方式，向执法机构报告可疑活动，继续在打击此类犯罪方面发挥积极作用。

欢迎会员和读者提出宝贵意见。笔者考察过受害链，从网络钓鱼和诱骗预防、犯罪分子识别、付款检测以及服务和操作的角度，明确了可以考虑的潜在解决方案。

金融机构可以参与儿童性虐待内容的预防、检测和报告工作。也可以利用金融机构的平台，提高对 CSAM 主题和预防方法的认识。 



Shann Lu, 法学硕士, CAMS,  
Bitfinex 反洗钱和金融欺诈调查管理

Fara Fallah, CAMS, CGSS, CBP,  
CCI, Bitfinex 合规顾问

编辑和其他内容: Peter Warrack,  
CAMS, CBP, CCI, CFE,  
Bitfinex 首席合规官

- <sup>1</sup> “Exploiting isolation: sexual predators increasingly targeting children during COVID pandemic” (利用隔离: 性掠夺者疫情期间越来越多地转向儿童), 欧洲刑警组织, 2020 年 6 月 19 日, <https://www.europol.europa.eu/newsroom/news/exploiting-isolation-sexual-predators-increasingly-targeting-children-during-covid-pandemic>
- <sup>2</sup> “Internet Fraud” (互联网欺诈), 联邦调查局, <https://www.fbi.gov/scams-and-safety/common-scams-and-crimes/internet-fraud>
- <sup>3</sup> Nicole de Souza, “The Nth Room case and modern slavery in the digital space” (“N 号房” 案件与数字空间里的现代奴隶制), *The Interpreter*, 2020 年 4 月 20 日, <https://www.lowyinstitute.org/the-interpreter/nth-room-case-and-modern-slavery-digital-space>
- <sup>4</sup> Yoon So-Yeon, “The spark that ignited the ‘Nth room’ fire” (点燃 ‘N 号房’ 之火的火花), 韩国《中央日报》, 2020 年 3 月 31 日, <https://koreajoongangdaily.joins.com/2020/03/31/features/The-spark-that-ignited-the-Nth-room-fire/3075527.html>
- <sup>5</sup> Ron Kim, “Victim Of Telegram Nth Room Case Speaks Up About The Horrors She Faced As A Middle School Student” (Telegram “N 号房” 案受害者讲述了她作为一名中学生所遇到的恐怖事件), *Koreaboo*, 2020 年 3 月 24 日, <https://www.koreaboo.com/news/victim-telegram-nth-room-case-speaks-horrors-faced-middle-school-student/>
- <sup>6</sup> 同上。
- <sup>7</sup> Choe Sang-Hun, “South Korean Man Gets 34 Years for Running Sexual Exploitation Chat Room” (韩国男子因经营性剥削聊天室被判 34 年), 《纽约时报》, 2021 年 4 月 8 日, <https://www.nytimes.com/2021/04/08/world/asia/korea-sex-crime-chat-rooms.html>
- <sup>8</sup> Haeryun Kang, “South Korea’s ‘nth rooms’ are toxic mixture of tech, sex and crime” (韩国 “N 号房” 是科技、性和犯罪的有毒混合物), *Nikkei Asia*, 2020 年 4 月 10 日, <https://asia.nikkei.com/Opinion/South-Korea-s-nth-rooms-are-toxic-mixture-of-tech-sex-and-crime>
- <sup>9</sup> Yoon So-Yeon, “The spark that ignited the ‘Nth room’ fire” (点燃 ‘N 号房’ 之火的火花), 韩国《中央日报》, 2020 年 3 月 31 日, <https://koreajoongangdaily.joins.com/2020/03/31/features/The-spark-that-ignited-the-Nth-room-fire/3075527.html>
- <sup>10</sup> Choe Sang-Hun, “South Korean Man Gets 34 Years for Running Sexual Exploitation Chat Room” (韩国男子因经营性剥削聊天室被判 34 年), 《纽约时报》, 2021 年 4 月 8 日, <https://www.nytimes.com/2021/04/08/world/asia/korea-sex-crime-chat-rooms.html>
- <sup>11</sup> 医学博士 George R. Brown, “Pedophilic Disorder” (恋童障碍), *Merck Manuals Professional Edition*, <https://www.merckmanuals.com/en-ca/professional/psychiatric-disorders/paraphilic-disorders/pedophilic-disorder>
- <sup>12</sup> “11 Factors That Increase the Risk of Child Sexual Abuse” (增加儿童性虐待风险的 11 个因素), *Defend Innocence*, <https://defendinnocence.org/child-sexual-abuse-risk-reduction/proactive-parenting/reduce-risk/11-factors-that-increase-the-risk-of-child-sexual-abuse/>
- <sup>13</sup> WeProtect 全球联盟, <https://www.weprotect.org/>
- <sup>14</sup> 虚拟全球特别工作组, <http://virtualglobaltaskforce.com/>
- <sup>15</sup> “Areas of Focus” (重点关注领域), *Interfaith Alliance for Safer Communities*, <https://iafsc.org/areas-of-focus/child-dignity-online>
- <sup>16</sup> Felipe Erazo, “Huobi Korea Delists XMR Amid Nth Room Sexual Exploitation Case Rumors” (“N 号房” 性剥削案谣言四起, 火币韩国交易所下架门罗币), *Cointelegraph*, 2020 年 4 月 12 日, <https://cointelegraph.com/news/huobi-korea-delists-xmr-amid-nth-room-sexual-exploitation-case-rumors>
- <sup>17</sup> “Operational alert: Laundering of proceeds from online child sexual exploitation” (运营警报: 在线儿童性剥削所得洗钱), 加拿大金融交易和报告分析中心, 2020 年 12 月, <https://www.fintrac-canafe.gc.ca/intel/operation/exploitation-eng>
- <sup>18</sup> 同上。
- <sup>19</sup> “South Korean National and Hundreds of Others Charged Worldwide in the Takedown of the Largest Darknet Child Pornography Website, Which was Funded by Bitcoin” (警方打掉使用比特币交易的最大儿童淫秽物品暗网, 对一名韩国人及数百位多国人员提起诉讼), 美国司法部, 2019 年 10 月 16 日, <https://www.justice.gov/opa/pr/south-korean-national-and-hundreds-others-charged-worldwide-takedown-largest-darknet-child>
- <sup>20</sup> Scott Ikeda, “South Korea’s New Crypto AML Law Bans Trading of ‘Privacy Coins’ (Monero, Zcash)” (韩国新加密货币反洗钱法禁止 “隐私代币” (门罗币、Zcash) 交易), *CPO Magazine*, 2020 年 11 月 17 日, <https://www.cpomagazine.com/data-privacy/south-koreas-new-crypto-aml-law-bans-trading-of-privacy-coins-monero-zcash/amp/>
- <sup>21</sup> “Online Child Sexual Exploitation” (在线儿童性剥削), 加拿大政府, <https://www.canada.ca/en/public-safety-canada/campaigns/online-child-sexual-exploitation.html>
- <sup>22</sup> Aaron Barr, “Social Media Regulation: The Line Between Privacy and Protection” (社交媒体监管: 隐私与保护间的界限), *Security Boulevard*, 2021 年 6 月 9 日, <https://securityboulevard.com/2021/06/social-media-regulation-the-line-between-privacy-and-protection/>
- <sup>23</sup> Karen Pauls, “New rules on removal of illegal online content could help in battle against child pornography” (非法在线内容删除新规则有助于打击儿童色情), *CBC*, 2021 年 1 月 4 日, <https://www.cbc.ca/news/canada/manitoba/canada-illegal-online-content-child-porn-1.5847695>
- <sup>24</sup> “Five Country Statement to EU to prevent child abuse online” (五国发表声明, 呼吁欧盟防范在线儿童虐待行为), 澳大利亚内政部部长, 2021 年 1 月 13 日, <https://minister.homeaffairs.gov.au/peterdutton/Pages/five-country-statement-EU-prevent-child-abuse-online.aspx>
- <sup>25</sup> “Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions – EU strategy for a more effective fight against child sexual abuse” (欧盟委员会致欧洲议会、欧盟理事会、欧洲经济和社会委员会及地区委员会的公函——欧盟儿童性虐待有效打击战略), 欧盟委员会, 2020 年 7 月 24 日, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020DC0607>

# 如何将洗钱风险 纳入风险管理： (上)

## 相

关规定将洗钱和恐怖融资风险（以下简称“洗钱风险”）纳入金融机构整体风险管理范畴进行了规范。这些规定包括金融行动特别工作组 2014 年发布的《银行业“风险为本”方法应用指南》、巴塞尔委员会 2017 年发布的《洗钱和恐怖融资风险健全管理》指南、中国银行保险监督管理委员会 2019 年发布的《银行业金融机构反洗钱和反恐怖融资管理办法》等。

中国人民银行印发的《法人金融机构洗钱和恐怖融资风险管理指引》（银反洗钱发〔2018〕19 号）就法人金融机构深化风险为本实践模式作出了详细规定。这些指引还包括贯彻落实《国务院办公厅关于完善反洗钱、反恐怖融资、反逃税监管体制机制的意见》，加强法人金融机构的反洗钱 / 反恐融资工作以及洗钱和相关犯罪活动的有效防范。然而，许多机构对于如何将洗钱风险纳入金融机构整体风险管理工作仍存疑虑，甚至有可能在实践中走弯路。笔者将基于监管实践和金融机构的实际情况，通过系列文章就以下三个方面提出一些指导性建议：洗钱风险的评估与衡量；洗钱风险管理策略的制定；高级管理人员职责的落实。

这是系列文章的第一篇，将讨论洗钱风险的评估和衡量。虽然上述指引和规定将洗钱风险纳入了金融机构的整体风险管理框架，但并未给出评估和衡量风险的方法，也未说明如何衡量该风险给金融机构带来的损失。







## 洗钱风险的评估与衡量

在大多数情况下，洗钱风险本身不会给金融机构带来直接风险或直接经济损失，有时甚至会产生一些收入，却会产生间接风险或损失。正如巴塞尔委员会所说：“如果洗钱/恐怖融资风险管理制度不健全或是缺少该制度，就会使银行面临重大风险，尤其是声誉风险、经营风险、合规风险和集中风险。”<sup>1</sup>值得注意的是，这些风险是相互关联的。然而，对金融机构的任何处罚都有可能同时带来巨大的风险（例如，批量融资和贷款终止成本、对银行的索赔、调查成本、资产冻结和贷款损失）。此外，投入有限且宝贵的管理资源和运营资源以解决洗钱风险带来的问题，这也会产生成本。《法人金融机构洗钱和恐怖融资风险管理指引》（银反洗钱发〔2018〕19号）写道：“任何洗钱风险事件或案件的发生都可能带来严重的声誉风险和法律风险，并导致客户流失、业务损失和财务损失。”

如果金融机构未能认真实施适当的风险管理政策、程序和控制措施，除了“强监管、严问责”带来的反洗钱罚款外，还会增加洗钱风险带来的直接或间接成本。如果金融机构能继续实施有效的风险为本反洗钱/反融资政策和程序，则可以减少或避免此类成本和损失。因此，金融机构需要评估洗钱风险，衡量洗钱风险造成的直接或间接损失，积极反省其洗钱风险状况，使制定的洗钱风险管理策略和洗钱风险状况与机构面临的系统重要性水平相匹配。下面分别介绍用于衡量洗钱风险所致直接或间接损失的具体历史模拟法和情景分析法。

### 衡量合规风险造成的损失

监察部负责监督金融机构代表公众利益履行反洗钱义务、降低洗钱活动对社会危害的情况。如果金融机构未能履行反洗钱义务，监管机构（包括其他司法管辖区）将对金融机构进行处罚。监管部门不仅可以罚款，还可责令金融机构停业整顿，暂停或停止特定业务，不批准新业务，提高各类基金（存款保险基金、投资者保护基金、保险保障基金等）的缴款比重等。

假设合规风险损失表示为  $T_1$ ，罚款损失表示为  $t_{11}$ ，发生概率表示为  $p_{11}$ ；金融机构被责令停业整顿，损失表示为  $t_{12}$ ，发生概率表示为  $p_{12}$ ；暂停或停止业务所致损失表示为  $t_{13}$ ，发生概率表示为  $p_{13}$ ；新业务损失表示为  $t_{14}$ ，发生概率表示为  $p_{14}$ ；增加各类资金的缴款比例，损失表示为  $t_{15}$ ，发生概率表示为  $p_{15}$ ；则有公式： $T_1 = t_{11} \times p_{11} + t_{12} \times p_{12} + t_{13} \times p_{13} + t_{14} \times p_{14} + t_{15} \times p_{15}$ 。各金融机构可根据其注册地、分支机构所在地和境外分支机构所在国家或地区的反洗钱监管力度、频次和实际处罚情况，特别是对同类机构的处罚情况，结合自有洗钱风险自评结果和发现的潜在违规事实，确定  $t_{11}$  和

$p_{11}$  的值；同样，可以结合实际数据或历史数据确定  $t_{12}$ 、 $p_{12}$ 、 $t_{13}$ 、 $p_{13}$ 、 $t_{14}$ 、 $p_{14}$ 、 $t_{15}$ 、 $p_{15}$  的值。

### 衡量声誉风险造成的损失

声誉风险造成的损失很难评估。如果在遭到重大反洗钱行政处罚后，金融机构被曝光卷入洗钱丑闻或出现负面新闻，结果可能导致（新老）客户流失。这不但导致营收减少，甚至可能令银行挤兑。此外，银行会谨慎对待该金融机构带来的业务（代理业务、跨境汇款等），这会加大业务开发的“摩擦系数”，消耗金融机构有限的宝贵管理资源和运营资源，引致潜在损失，甚至与银行的合作关系终止。假设声誉风险造成的损失表示为  $T_2$ ，客户减少造成的损失表示为  $t_{21}$ ，发生概率表示为  $p_{21}$ ；业务损失表示为  $t_{22}$ ，发生概率表示为  $p_{22}$ ；则有公式： $T_2 = t_{21} \times p_{21} + t_{22} \times p_{22}$ 。各金融机构可以根据其现有客户或潜在客户的实际情况设计调查问卷，抽样评估客户获悉金融机构在受到重大反洗钱行政处罚后被曝卷入洗钱丑闻或负面新闻时会采取的措施，然后评估相关损失。这样就可以确定  $t_{21}$  和  $p_{21}$  的值；业务损失—— $t_{22}$  和  $p_{22}$  的值——可以根据各种单据和信息的成本，以及处理各种银行同业业务所需要的各种单据和信息导致的工作效率下降来确定。



## 经营风险和集中风险 有可能直接造成损失； 然而，经营风险和集中 风险有可能放大合规风险、 声誉风险和法律风险

### 衡量法律风险造成的损失

法律风险所致的损失主要指特定客户或受害客户群体在金融机构发生洗钱案件后采取的法律行动，以及金融机构为避免陷入索赔或赔偿过程而承担的损失。例如，一家银行因海外洗钱案而被提起法律诉讼，因此支付了数百万美元的律师费。假设法律风险造成的损失表示为  $T_3$ ，客户赔偿表示为  $t_{31}$ ，发生概率表示为  $p_{31}$ ；律师费表示为  $t_{32}$ ，发生概率表示为  $p_{32}$ ；则有公式  $T_3 = t_{31} \times p_{31} + t_{32} \times p_{32}$ 。

### 衡量经营风险和集中风险造成的损失

经营风险和集中风险有可能直接造成损失；然而，经营风险和集中风险有可能放大合规风险、声誉风险和法律风险。金融机构经营风险和集中风险会增加其他风险的发生概率，很可能导致合规风险、声誉风险、法律风险，进而造成损失。具体而言，如果金融机构存在经营风险，很可能造成内部反洗钱控制制度失效，甚至产生“内外合谋”，使内部反洗钱控制制度形同虚设。

例如，某银行柜员应客户要求办理“假现金”业务，最终导致洗钱案件发生，造成监管部门对该行罚款 500 万元人民币（约合 773,167.95 美元）。如果金融机构存在集中风险，洗钱风险可能有五种表现：一，交易对手集中在洗钱风险高的国家和地区；二，客户集中在洗钱风险高的国家和地区；三，交易量集中于洗钱风险较高的业务或产品；四，交易量集中于洗钱风险高的客户；五，同一受益所有人控制的法律工具或法律安排构成代理规模和资本优势，或者构成大量关联交易。

综上，假设金融机构因洗钱风险承担的总损失表示为  $T$ ，则有  $T = T_1 + T_2 + T_3$ 。在一定时期内，这些损失需要金融机构动用资本金甚至提前动用拨备金来弥补。

为了评估和衡量洗钱风险造成的损失，本文只考虑了实践中的常见风险因素。这些风险因素会相互作用，一个风险要素的发生会影响另一风险要素的发生概率。此外，本文未考虑金融机构的沟通协调能力和舆论的影响，也未考虑其他洗钱风险因素造成的损失。

本文探讨的洗钱风险评估和衡量方法还有待改进，业内人士可以研究探索其他更先进的方法。

下一篇文章将讨论洗钱风险管理策略的制定问题。 

Liu Lihong, 中国人民银行业务办公室

<sup>1</sup> “Guidelines: Sound management of risks related to money laundering and financing of terrorism”（指南：洗钱和恐怖融资风险健全管理），巴塞尔银行监管委员会，2017 年 6 月，<https://www.bis.org/bcbs/publ/d405.pdf>

# 《隔离引起的沉思》 第3章： 求职者的 反击



欲读《隔离引起的深思》第1章和第2章，  
请前往 [ACAMSToday.org](http://ACAMSToday.org) 网站“职业指南”专栏查看。

**13**年来，我一直在反洗钱、合规和监管  
领域从事人才招聘工作，期间经历过  
两次经济衰退。我学到了最宝贵的一课：

与任何其他周期一样，经济衰退可以预测——至少从招聘的角度来看，是可以预测的。我上班的第一天，是2008年7月15日。我之所以记得这么清楚，是因为两个月后，我才刚刚熟悉的一家大银行破产了：2008年9月15日，雷曼兄弟倒闭。自那之后，多米诺骨牌开始坍塌。银行与公司合并，申请破产，向政府求助……坏消息应接不暇，令人备受煎熬。开始时（也是经济





衰退最严重的时候)，首当其冲的便是工作岗位，尤其是低收入岗位。2008 年底，我的电话开始响个不停，直到 2010 年初才算消停。越来越多的电话接踵而至，突然就听到了解聘下岗的故事。2009 年，美国运通一次又一次在礼堂里召集员工开会，然后一下子把员工统统解雇。实际上，这样也无可厚非：5 万人，该怎么一个一个地裁？

经济衰退的影响，往往出人意料地深远。一家又一家公司接着破产。您会意识到，经济只是一座纸牌屋，等待着轻轻的微风将它吹翻。大多数公司首选裁员，通过减少运营成本来节省现金。大规模裁员越来越多，令人们陷入更大的痛苦、更深刻的焦虑，最终逼得政府不得不干预。政府干预后，各种纾困金和现金从四面八方奔涌入场。讽刺的是，即使解雇了一半的员工，

企业也从未停止过招聘。在大衰退，以及新冠疫情所致的衰退期间，市场上均有数百万个空缺岗位。这是因为，在经济衰退期间，买家控制了市场，公司可以挑选最佳求职者。这也有道理，毕竟供大于求嘛。数百万计的人退出了就业市场，因为就业市场处于休眠状态。纾困金帮助失业者度过经济衰退期（希望如此），而从业者则紧紧抓住自己的工作不放，仿佛自己的生活离不开这些工作一样。这样，人们就能够在一段时间内（通常为两三年）保持动态平衡。然后，在这条漫长隧道的尽头出现了光。

人们开始活跃起来，从各个方面慢慢摆脱疫情带来的经济、公共卫生和社会限制。我 2021 年上半年走的路，就已超过了 2020 年全年；2021 年的就业市场，比 7 月份死亡谷的仙人掌还要热。在美国，2021 年 3 月 - 2021 年 7 月期间，市场上增加了超过 329 万个工作岗位，失业率降至 5.4%。<sup>1</sup> 然而，还需要有 760 万员工进入私企工作，就业率才能达到 2020 年 2 月的水平。<sup>2</sup> 人们说，大衰退是大萧条以来最严重的经济危机。但事实上，比起新冠疫情导致的萧条与衰退，大衰退不过是公园漫步。

然而，反弹也更为明显。2021 年 4 月，市场上有 930 万个空缺职位。<sup>3</sup> 2020 年 4 月，有近 500 万个空缺职位。<sup>4</sup> 而大衰退期间的反弹情况是：到 2012 年 1 月，市场上有 350 万个工作岗位。根据美国劳工统计局的数据，2009 年 11 月，市场上有 240 万个空缺职位，降至最低点。<sup>5</sup> 美国的现状（截至 2021 年 6 月），让我想起了大衰退至暗时刻之后的时期。因此，求职者，无论是目前在职还是待业的人员，可以考虑利用经济衰退的有机周期。

大衰退之后，有《多德 - 弗兰克法案》来力挽狂澜；新冠疫情所致衰退之后，有疫苗来扭转乾坤。2010 年，《多德 - 弗兰克法案》出台后，围绕合规和反洗钱工作，大量新的工作岗位在市场上涌现。2021 年，新冠疫苗接种让人们得以走出家门，重启经济。除了创造的数百万个新工作岗位以外，公司企业纷纷宣布，计划当下和未来雇用数十万员工。<sup>6</sup> 与过去一样，这次经济衰退过后的就业市场是卖方市场。这次求职者占上风，因为他们会收到多个工作机会。

还有一些其他因素也加剧了当下的招聘热潮，尤其是在合规、反洗钱和监管领域。第一个因素是金融科技的复兴。去年，银行和金融服务被迫走向数字化。大多数人都在家里办理银行业务和投资。替代性汇款体系、加密货币钱包和交易所以及机器人顾问提升了整个待业的员工需求。反洗钱和合规团队肯定壮大了。第二个因素更多体现为疫情所致衰退的一个细微差别。与大萧条不同，这次衰退不是根本性经济缺陷导致的结果。项目被搁置，因为员工需要迅速适应新的生活方式和工作方式。



这些项目现在开始重启，需要立即招聘额外人员。最后一个因素是政府。美国现任政府是民主派联邦政府，通常意味着更多的监管和执行。所有这些因素相叠加，自然就有了招聘热潮。今后 12 - 18 个月会非常有意思，因为现在有很多的空缺职位，却没有足够的人来填补这些空缺，这种状况将来会持续一段时间。所有行业都是如此，反洗钱和合规领域也不例外。

## 至理名言

许多人在隔离期间可谓收获满满。他们减肥成功，健康水平达到最佳状态，发现了新的爱好，事业蒸蒸日上等等，不一而足。另一些人的景况不太理想。他们失去了工作、家园、健康、家人和亲人。2020 年将因新冠疫情记入史册，新冠疫情也迅速地改变了人们的生活。现在，人们开始逐步恢复疫情前的日子。生活中那些我们认为理所当然却时常错过的小事：随意走亲访友，去快餐店吃饭，在当地酒吧喝啤酒。希望人们不再认为这些都是理所当然。

就业市场正在恢复原状，那就好好利用这个机会吧。作为求职者，如何才能用好经济衰退结束时的机会呢？具体来说，如何才能把握疫情所致衰退结束时的机会？

1. **现在就开始找吧：**反洗钱和合规领域的项目和全职岗位只会有增无减。然而，这并不是说因为您想工作就一定能找到工作。您不知道，在我面试过的人当中，有多少因为得到的面试和工作机会数量不达预期去撞墙的。最终他们失去动力，沮丧地退出了就业市场。那些能坚持下去并摆正位置的人，后来遇到的问题截然不同：收到了多份工作机会，却不知道该选哪一个。




2. **多思考能否提升技能，而非只看有无高薪：**从开始为《今日 ACAMS》撰稿以来，我一直秉持这一理念。掌握更多技能等于更高的薪酬；或者至少可以说，更多技能等于更多的选择。技术和人工智能日益成为传统银行业反洗钱和合规制度的重要组成部分，金融科技和监管科技公司都希望招到精通技术的合规专业人士。把握这个机遇，找一份能开启更多可能性的新工作，学习如何高效地执行合规制度、管理合规职能部门。
3. **善待自己，不要指望所有工作都能 100% 远程办公：**即便没有明说可以 100% 远程办公，也不要马上拒绝潜在工作机会。混合式办公及远程办公已成为人们生活的一部分，但不要以为所有岗位都能选择 100% 远程办公。在一定意义上，人们最终还是会回到办公室。早在 2020 年 3 月，人们突然被迫转向远程办公。这并不是公司企业的选择；高管们还是希望员工回办公室办公。
4. **拓展人际网络：**大衰退期间，人们都有很多机会：午餐、会议、咖啡、鸡尾酒等，能够轻松拓展自己的人际网络。在新冠疫情所致的社交距离限制结束之前，人们则通过 Zoom、Microsoft Teams 和 Google Hangouts 会议的方式互动。您猜怎么着？这两者并无区别。联系以往的同事和老板，联络领英上新的和潜在的联系人，参加网络会议。最后，一切回归正轨时，不妨考虑参加当地分会主办的 ACAMS 会议和活动。
5. **职业道路并非一成不变：**经济衰退之后的时期，是考虑换工作、改行、换居住地的最佳时机之一。在卖方市场下，求职者不仅可以控制常规求职过程，还能够兼顾自己的目标与价值。如果合规和反洗钱工作让您感觉不错，但直觉（甚至可能是内心）告诉您，人生已到了分岔路口，该怎么办？在炙手可热的就业市场，公司迫切需要人才。好好利用公司求贤若渴的心理吧！公司乐于以创造性的方式招人。2021 年和 2022 年，空缺职位数量会多于符合条件的求职者数量，是人们走出舒适区的绝佳时期。
6. **好好利用（免费的）招聘专家：**我不是在给自己打广告。机构招聘人员是免费的信息来源，不妨通过他们了解就业市场状况、共同行业、用人趋势、热门技能组合需求，当然还有工作岗位需求。无论您是主动寻求建议，还是被动了解情况，这些值得信赖的专业顾问都可为您提供参考信息。不妨将机构招聘人员视为自己不断壮大的工作人际网络中的一员。

到 2021 年底，可能会有数十万人重新进入就业市场。找工作的人群中，有很大一部分是之前因需照顾在家上学的孩子而退出了劳动力市场，或是因为之前从州和联邦政府获得的补贴比工资高。

疫情将告结束，孩子们将重返学校，联邦和州政府也会停发补贴。于是，经济将重新变得炙手可热，失业率将降至疫情前的水平。讽刺的是，由于劳动力短缺，很多全职永久岗位暂停招人。与此同时，公司开始聘请承包商和顾问启动项目，等待新的求职者涌入。在已开放的数百万个工作岗位以外，还会新增成千上万个岗位。卖方市场短期内不会结束。

## 结语

当下正是求职者找工作的最佳时机。建议保持灵活的心态，持续充电学习，扩大人际网络，利用卖方市场形势，掌控自己的未来，做到这些，就能够找到最佳工作机会，满足自己的需求。谁知道呢？您完全有可能找到疫情前想都不敢想的理想工作。 

Sanjeev Menon, 《ACAMS 职业指南》专栏作家,  
Infinity Consulting Solutions, Inc. 合规、法律和隐私事务高级经理,  
美国纽约州, smenon@infinity-cs.com

撰稿及编辑意见: Karla Monterrosa-Yancey, CAMS,  
ACAMS《今日 ACAMS》杂志总编辑, 美国佛罗里达州,  
editor@acams.org

- <sup>1</sup> “Civilian unemployment rate” (美国平民失业率), 美国劳工统计局, 2021 年 8 月 6 日, <https://www.bls.gov/news.release/empstat.nr0.htm>
- <sup>2</sup> Scott Horsley 和 Andrea Hsu, “Hiring Picked Up Last Month, But The Economy Still Needs More Workers” (上月用工形势回升, 但经济仍需要更多劳动力), NPR, 2021 年 6 月 4 日, <https://www.npr.org/2021/06/04/1003035263/hiring-picked-up-last-month-a-relief-for-an-economy-desperate-for-workers>
- <sup>3</sup> Jeff Cox, “Job openings set record of 9.3 million as labor market booms” (随着劳动力市场的繁荣, 职位空缺创下纪录, 达 930 万个), CNBC, 2021 年 6 月 8 日, <https://www.cnbc.com/2021/06/08/job-openings-set-new-record-of-9point3-million-amid-economic-reopening.html>
- <sup>4</sup> “Job openings, hires, and separations levels, seasonally adjusted” (职位空缺、聘用人数和离职水平 (经季节性调整)), 美国劳工统计局, <https://www.bls.gov/charts/job-openings-and-labor-turnover/opening-hire-seps-level.htm>
- <sup>5</sup> “Job Openings and Labor Turnover Survey News Release” (职位空缺和劳动力流动调查新闻稿), 美国劳工统计局, 2012 年 3 月 13 日, [https://www.bls.gov/news.release/archives/jolts\\_03132012.htm](https://www.bls.gov/news.release/archives/jolts_03132012.htm)
- <sup>6</sup> “Amazon to hire 100,000 more workers in its latest job spree this year” (亚马逊今年将再招 10 万名员工), CNBC, 2020 年 9 月 14 日, <https://www.cnbc.com/2020/09/14/amazon-to-hire-100000-more-workers-in-its-latest-job-sprees-this-year.html>; Jessica DiNapoli, “PwC to Create 100,000 New Jobs to Help Clients Grappling with ESG Reporting” (普华永道将创造 10 万个新工作岗位, 帮助客户应对 ESG 报告需求), Insurance Journal, 2021 年 6 月 16 日, <https://www.insurancejournal.com/news/international/2021/06/16/618744.htm>

# 令事件触发审查切实发挥作用





# 事

事件触发审查 (ETR) 或事件驱动审查，是持续监控或持续审查反金融犯罪 (AFC) 控制措施的一部分。与周期性的定期审查不同，事件触发审查具有临时性的特点。此外，事件触发审查与反洗钱 (AML) 调查不同，前者通常由业务部门而非合规部门实施。

本文将探讨如何通过事件触发审查，加强金融机构 (FI) 客户风险管理的效果。

## 监管预期

监管机构有着明确的预期。在事件触发审查期间，金融机构需要更新客户信息，核查是否需要审查客户的风险状况。例如：

“建立业务关系后，金融机构需要通过定期审查和 / 或事件触发审查，及时获取对客户的确切认知。如果评估认为存在较大风险，则会视情况提高与客户沟通的频率和强度。”<sup>1</sup>

事件触发审查是定期审查的补充，能够起到更新客户资料的作用。然而，一些金融机构完全依赖事件触发审查，将其作为“风险为本方法”的一部分，用于更新客户尽职调查和风险状况。然而，在这些方面，事件触发审查的效果似乎并不明显。例如，在荷兰银行近期刑事调查的事实纪要中，荷兰检察官<sup>2</sup>提到银行在以下方面未取得成效：

- 在私人银行领域，事件触发审查活动非常有限，缺乏对私人银行业务关系的持续监控。
- 如下例所示，银行系统本应生成触发信息以启动事件触发审查，实际却并未发挥正常作用：
  - 在 2018 年 9 月之前，银行针对负面媒体报道的筛查流程未自动化，而是采用手动模式实施。此外，在筛查匹配项的处理以及后续对受影响客户资料的重新评估方面存在积压问题。2019 年，审计师发现客户筛查流程“差强人意，需要改进”。
  - 受所用风险分类和系统设置方式的影响，交易监控 (TM) 系统错过了若干信号。另外，至少在 2019 年之前，所生成交易监控警报的处理方面存在积压问题。因此，可能导致事件触发审查的警报未能及时处理。

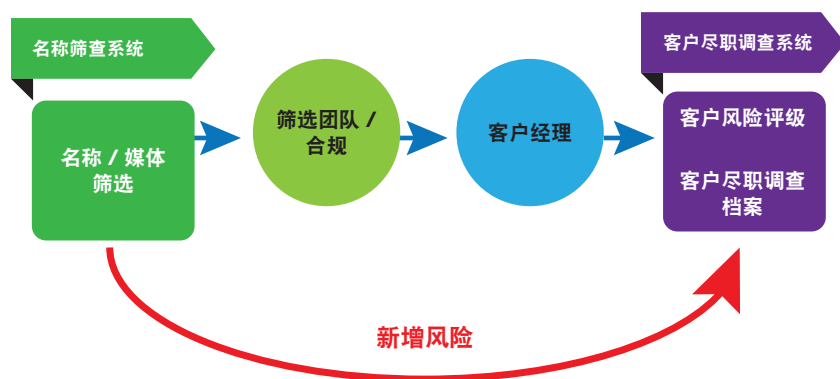
## 新风险和增量风险的评估

客户开户后，后端名称或媒体报道筛查系统会定期根据供应商数据库和内部黑名单筛查金融机构的客户数据库，发现新风险或增量风险。此类风险包括新的政治公众人物(PEP)、重大负面新闻，或者针对客户或其关联方的潜在制裁关系。对大多数组织机构而言，这些风险的识别与升级，似乎是事件触发审查工作的标配（参见图 1）。

但是，必须明确定义升级协议和客户风险评估准则。识别出新风险或增量风险时，必须在金融机构的客户尽职调查系统中迅速标记新风险，同时进行评估并获得特批以留住目标客户。

除了筛选匹配项（或命中项）审查方面存在积压问题之外，真正的风险在于：业务部门及合规部门探讨新风险或增量风险时，可能不会将客户标记为高风险。例如，客户是政治公众人物吗？负面新闻严重吗？制裁关系是否颇为遥远？另一种风险是，尚未将客户标记为高风险，因为仍在征求高级管理层的批准，以期保留客户关系。然而，只要未在金融机构客户尽职调查系统中标记客户，客户就不会受到增强监控。由于金融机构客户尽职调查系统中的风险指标会根据基于风险的阈值馈入交易监控系统以便监控，因此规则应该是先标记、后决定。

图 1：新风险和增量风险的评估



## 交易监控环回

交易监控期间，为回应来自交易监控团队的信息请求(RFI)，客户可能会提供信息以消除对警示交易的疑虑。例如，客户的交易对手可能是其新雇主或供应商，也可能是客户的其他私人投资公司或亲属。客户解释警示交易目的时，也可能披露新的财富或资金来源。客户在金融机构的客户尽职调查档案中找不到此新信息，因而提出信息请求。然而，该信息在金融机构交易监控案例管理系统已关闭警报的审计日志中出现的频率是怎样的？

有效的环回机制，能够触发从交易监控到客户关系经理的事件触发审查。收到事件触发审查要求后，客户关系经理应进行审查，并将附加信息录入客户的客户尽职调查档案中。客户关系经理还应评估是否需要重新分析客户风险等级，是否需要修正客户尽职调查

档案中声明的账户预期用途和预期账户活动，这些均为事件触发审查的一部分。借助金融机构尽职调查系统中修正后的客户尽职调查档案，交易监控团队能够快速评估针对同一客户的下一份交易监控警报的风险关联性（参见图 2）。

由于客户可能在回应信息请求时披露新信息，以解释潜在的交易筛查匹配项（或命中项），因此还应部署环回机制，将信息从筛查团队传达给客户关系经理，启动事件触发审查程序。由于交易筛查匹配项通常涉及客户或其交易对手的潜在制裁关系，因此需将客户对信息请求的回应纳入客户的客户尽职调查档案。新信息也应构成客户制裁尽职调查的一部分，尤其是当新信息与客户或交易对手的潜在匹配被视为虚假匹配时。

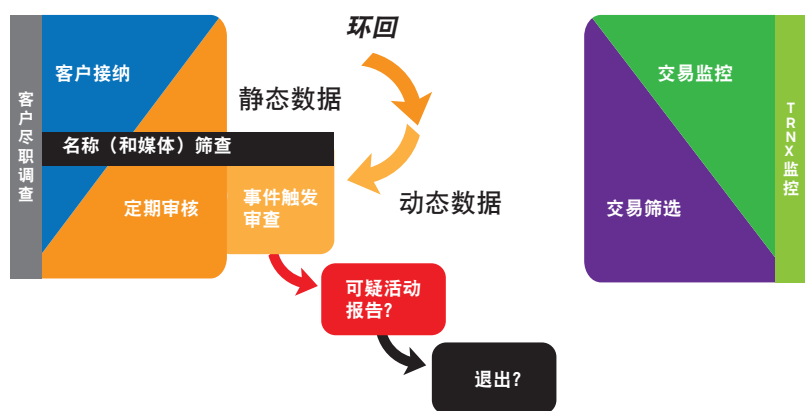
## 触发财富来源和资金来源复审程序

对于私人银行客户和较高等级的零售客户，财富来源(SOW)和初始资金来源需要在客户接纳过程中得到证实或验证。这是要求银行评估客户总财富（即净值）和资金来源(SOF)的合法性。完成客户接纳和定期审查后，客户关系经理通常会要求对客户声明的财富来源或资金来源进行更改（如有）。但若传入交易的规模（单独或合计）超过客户声明的净值，银行是否有机制来启动事件触发审查？或者，若管理资产规模(AUM)超过客户净值，是否有机制启动事件触发审查？交易规模和资产管理规模增加，表明银行可能不清楚客户的财富总额或资金来源。

银行应设立季度或半年仪表盘，若汇入大额款项或客户管理资产规模大幅增加，该仪表盘能够自动提醒客户关系经理。



图 2：环回机制



当客户成为大客户或重要关系（即资产管理规模等于或超过给定阈值）时，仪表板也应能予以提示。仪表板是交易监控及其检测场景事件的附加控件。

作为事件触发审查的一部分，客户关系经理应审查客户声明的净值是否超出；若超出，应向客户询问其新的财富来源和资金来源。此外，当客户成为“大客户”或“重要关系”时，事件触发审查的本质便是对客户财富来源和资金来源进行重新审查，以及对新的或增加的客户风险（如有）进行评估。新的财富来源和资金来源需要记录并验证。若客户风险有所提高，反金融犯罪政策需要有相应的机制，做出特殊审批安排以保留客户关系。仪表板如图 3 所示。

图 3：净值审查触发器仪表板

客户名称				
账号				
声明的净值（截至年 / 月 / 日）		\$X		
	YYYY 年 一季度	YYYY 年 二季度	YYYY 年 三季度	YYYY 年 四季度
交易规模 (\$,000)	500	50	2,000	
资产管理规模（增量百分比）	3	无变化	5	
资产管理规模（大客户）				是
注：反金融犯罪政策基于声明的净值，对大额交易规模和管理资产规模的显著增加作出了规定。该政策还基于资产管理规模对组织机构的大客户进行了规定。				

## 融合最佳实践，提升事件触发审查效果

- 金融机构的反金融犯罪政策应明晰事件触发审查是什么，审查客户尽职调查档案的触发事件或动因，以及重新评估客户风险的时机。

- 阐明事件触发审查的职责与责任，包括升级协议。
- 设计系统流程，将触发事件（和信息）自动传至客户关系经理，以实施事件触发审查工作。
- 确保具备足够的资源，以便及时审查并处置警报和匹配项，从而及时实施事件触发审查。
- 跟踪事件触发审查工作，直至完成为止，其中包括：核查是否已修正客户风险评级，是否更新了金融机构尽职调查系统中的客户尽职调查档案（如适用）。

## 结语

有效的事件触发审查程序，是行之有效的“风险为本反金融犯罪制度”中不可分割的组成部分。有鉴于此，金融机构应设计好事件触发审查流程并严格执行。完成事件触发审查后，及时更新客户的客户尽职调查档案和风险档案，有助于加强反金融犯罪风险管理工作。

Rosalind Lazar, CAMS,  
ACAMS 亚太地区反洗钱合规总监,  
rlazar@acams.org

<sup>1</sup> “Guidance For Effective AML/CFT Transaction Monitoring Controls”（有效反洗钱 / 反恐融资交易监控控制指南），新加坡金融管理局，2018 年 9 月，<https://www.mas.gov.sg/-/media/MAS/Regulations-and-Financial-Stability/Regulatory-and-Supervisory-Framework/Anti-Money-Laundering-Countering-the-Financing-of-Terrorism/Guidance-for-Effective-AML-CFT-Transaction-Monitoring-Controls.pdf>

<sup>2</sup> “Statement of Facts and Conclusions of the Netherlands Public Prosecution Service”（荷兰公共检控服务部事实纪要与结论），国家严重欺诈、环境犯罪与资产没收办公室（Functioneel Parket）和国家办公室（Landelijk Parket），[https://assets.ctfassets.net/1u811bvgvthc/4e UXF7eCnLthKp95RNnmnz/645730a7cd044da33ef4 ad1545470f12/Statement\\_of\\_Facts\\_-\\_ABN\\_AMRO\\_Guardian.pdf](https://assets.ctfassets.net/1u811bvgvthc/4e UXF7eCnLthKp95RNnmnz/645730a7cd044da33ef4 ad1545470f12/Statement_of_Facts_-_ABN_AMRO_Guardian.pdf)



# 大凤凰城分会： 调整、发展与适应！




今年6月，ACAMS大凤凰城分会以“加密货币时代的恐怖融资：监管与执法框架”为题举办了一场网络研讨会。此次研讨会大获成功，超过500名注册会员参加。研讨会伊始，美国国税局网络犯罪小组探员 Chris Janczewski 以三个真实的犯罪案例开场，展示了恐怖组织“调整、发展与适应”融资的方法，尤其是在加密货币方面。Janczewski 探员展示了美国执法机构如何成功查获与哈马斯、基地组织、伊斯兰国有关的组织的网站和货币资产！

一个组织利用网站开展比特币筹款活动，为“巴勒斯坦抵抗运动”寻求捐款；另一组织则利用其 Telegram 渠道寻求捐款以资助恐怖袭击，支持“叙利亚圣战者”。一名服务于伊斯兰国的人员创建了一个网站，声称有 N95 和其他个人防护用品出售，可帮助人们应对新冠疫情。受害者以信用卡支付，购买不存在的商品，结果导致信用卡遭盗用。总计10万美元的犯罪所得随后通过比特币洗白，此人最终被抓！值得庆幸的是，美国政府通过相关行动查获的加密货币随着时间的推移升值了——这当然是锦上添花。

接着发言的是来自 TRM Labs 的 Ari Redbord。Redbord 介绍了 TRM Labs 的使命，即“防范加密货币欺诈与金融犯罪，为数十亿人建立更安全的金融体系。”他强调，加密货币有望出现爆炸性增长，犯罪分子很可能利用新技术来规避检测——如链跳 (chain-hopping)、隐私技术、程序化洗钱等技术。他的演讲重点探讨了加密货币的当前监管环境：即使只有不到2%的比特币链上交易涉及非法实体，但监管重点仍放在加密货币的非法利用，极少关注加密货币的合法使用。

Redbord 指出，美国财政部（包括金融犯罪执法网络）依然重点关注加密货币的非法使用，目前对虚拟资产服务提供商的监管要求，便可证明这一点——许可证、“了解您的客户”、增强尽职调查、交易监控、信息传送规则合规等。他指出，这些要求与金融机构的要求非常相似，带来了挑战。金融机构充当中介机构，负责收集金融情报，

并通过组织架构将其推送至执法机构。然而，加密货币具有去中心化的特点，其结构与典型组织机构不同。犯罪分子利用链跳技巧、隐私技术等给情报收集工作制造障碍。监管行业如何调整、发展与适应，还有待观察。

与会员互动更成为整个研讨会的亮点！问答环节持续了近一个小时，仍有许多问题来不及回答。在后续讨论中，与会者就广泛议题展开了探讨，如利用古董资助恐怖主义、美国国内恐怖主义案件的细微差别、利用更短的交易时间抢占加密货币新市场等，还组织了线上头脑风暴会，讨论了如何降低整个行业的风险。笔者印象最深刻的是，Janczewski 探员提出了完全瓦解恐怖组织与破坏恐怖组织融资/运营之间的区别。参加这场网络研讨会，实在受益匪浅！

Caryn Langolf, 注册监管合规经理、  
CAMS、ACAMS 大凤凰城分会联合通讯  
主管, carynlangolf@gmail.com





公认反洗钱师协会。

# Certifications

通过 ACAMS 认证课程，提升  
员工在防范金融犯罪方面的  
专业知识和技能。

[www.acams.org](http://www.acams.org)

高级专家级别  
认证课程



专家级别认证课程

黄金标准



专员级别认证课程



# Winnie Yuen :

## 以有效协作 为目标的传播

# 本

期《今日 ACAMS》中，  
我们采访了全球营销  
运营经理 Winnie Yuen，

了解她多年以来积累的营销经验以及营销活动成功的关键。Yuen 从事营销传播工作已有 10 多年。加入 ACAMS 前，她在游戏和生活时尚行业工作多年，拥有精湛专业的营销技能。本月，Yuen 将迎来在 ACAMS 工作的五周年。她是 ACAMS 亚太区市场部聘请的第一位员工，见证了 ACAMS 香港办事处的发展壮大，迎来越来越多充满活力的同事。

过去五年，从产品发布到现场会议，促销邮件到活动赠品，Yuen 监督了亚太地区的所有营销推广活动。2019 年，她荣获 Adepta Global Education 颁发的 TEACH 大奖，肯定她在 ACAMS 会员和业务合作伙伴服务工作的杰出贡献。最近，Yuen 晋升全球营销运营经理，负责在营销团队不同部门之间架起沟通的桥梁，并参与多项跨部门项目。

**《今日 ACAMS》：**今年，您在 ACAMS 任职已满五年，祝贺您！想请教一下，您是如何将在游戏和生活时尚行业获得的营销经验，融入 ACAMS 的营销工作？

**Winnie Yuen：**非常感谢！真难以相信，我在 ACAMS 已经工作五年了。游戏、生活时尚与金融合规行业看起来

截然不同，但基本营销原则并无二致。我通过之前公司的任职经历，获得了丰富的营销经验，因此能满怀自信地应对各种营销挑战。分享一个有趣的故事，我在美国办公室见到 ACAMS 全球营销总监 Fernando Beozzo Salomao 本人。交谈中，我们发现，他认识我以前的一个老板，因为他们曾在同一家公司、同一部门工作。世界真小啊！

**《今日 ACAMS》：**您是亚太区营销部门的第一位员工，也是当时的唯一一位员工。从那时至今，该部门有何发展？

**Winnie Yuen：**我 2016 年加入 ACAMS 时，是亚太地区唯一的营销人员，负责亚太地区所有的营销推广工作。当时，我们一年内举办了 10 场现场研讨会和 1 场现场国际会议；在亚太地区推出了四门语言的公认反洗钱师认证课程，同时还开展其他营销项目——可以想象，对于只有一个人的团队来说，这意味着有多少工作要做。幸运的是，我的辛勤工作（和繁重的工作量）得到了管理层的肯定，ACAMS 开始大力建设亚太地区营销部门，2018 年，部门员工人数增加到 4 名。现在，我们有三名同事常驻香港，一名同事常驻北京。我们拥有多样化的背景与经历，我觉得这样的搭配非常好。

**《今日 ACAMS》：**营销活动取得成功的关键是什么？

**Winnie Yuen：**在我看来，营销的核心就是在消费者与产品/服务之间搭建桥梁。要想让营销活动取得成功，就应了解潜在消费者需要什么，他们的痛点是什么。这非常重要。ACAMS 不是零售公司，因此非常依赖数据分析、调查反馈，也非常倚重与销售代表的沟通，因为他们直接与客户接触。此外还应当及时了解行业/市场新闻和动向。


**《今日 ACAMS》：**作为全球营销运营经理，您对跨部门、跨地区的合作有什么建议？

**Winnie Yuen：**重视沟通！无沟通，不成事。这一点放之四海而皆准，对 ACAMS 尤为重要，因为 ACAMS 是一支庞大的全球性团队。每个人都有自己的优势、经验和立场，因此，沟通对于实现共同目标至关重要。

**《今日 ACAMS》：**迄今为止，您印象最深刻的 ACAMS 营销项目是什么？

**Winnie Yuen：**我印象最深刻的有两个项目，一个是我负责的第一场国际会议，另一个是 ACAMS 微信与 LINE 社交媒体渠道的推出。2017 年，我是亚太地区唯一的营销人员，有海量的会前准备工作要做；而微信和 LINE 是华语用户用得最多的社交媒体渠道。那是我首次处理 app 发布活动、发布规划工作，因此整个流程中有大量的知识要学习。

**《今日 ACAMS》：**您闲暇时间喜欢做什么？

**Winnie Yuen：**闲暇的时候，我喜欢远足、跑步、看电视。最近在学习家居维修和泰语。我始终孜孜不倦，不断探索新的爱好——没有什么固定的标准，只要有趣、实用就行！

采访者：Stephanie Trejos，ACAMS，CAMS、编辑，美国佛罗里达州，  
strejos@acams.org







## 进阶认证 毕业生

### 亚美尼亚

Emil Abrahamyan, CAMS-RM

### 巴哈马

Sinead Bethel, CAMS-RM

### 开曼群岛

Christopher Green, CAMS-RM

### 德国

Manuela Drachenberg, CAMS-RM

### 香港特区

Kit Wah Flora Liu, CAMS-RM

Siu Long Wong, CAMS-RM

### 日本

Yasutomo Haruki, CAMS-RM

### 拉脱维亚

Khaled Almustafa, CAMS-RM

Kalvis Bambals, CAMS-RM

### 黎巴嫩

Katia Marrouche, CAMS-RM

### 澳门特区

Ching Chi Percy Wong, CAMS-RM

### 荷兰

Henri Korkalainen, CAMS-RM

Luciano Riccioli, CAMS-RM

Marcin Wasilewski, CAMS-RM

### 挪威

Adis Crnalic, CAMS-RM

### 卡塔尔

Faheem Razzaq, CAMS-RM

### 沙特阿拉伯

Malcolm Sandesh Lewis, CAMS-RM

### 韩国

Yoon Sang Seong, CAMS-RM

### 阿联酋

Kartik Sharma, CAMS-RM

### 英国

Yoe Strous, CAMS-RM

### 美国

Mark Creizman, CAMS-RM

Christopher A. Freiermuth, CAMS-RM

Carlos Ludert, CAMS-RM

Christine Marie Mayer, CAMS-RM

Xiao Chin Mu, CAMS-RM

Brian Pfeiffer, CAMS-RM

Ronnie Augusto Salvador, CAMS-RM

Umamani Selvam Sukumar, CAMS-RM



# ACAMS 网络研讨会 高级订阅账号

## 您的网络研讨会“全通票”

新版 ACAMS 网络研讨会高级订阅账号设有年度访问权。订阅者可以无限制访问 ACAMS 的网络研讨会直播、点播资料库。



**9 场 +**

**全新直播网络研讨会**  
平均每月发布



**40 个 +**

**反金融犯罪 (AFC) 话题**  
每年讨论



**800 小时 +**

**反金融犯罪 (AFC) 培训课程**  
收录在 ACAMS 资料库

如需了解更多信息或订阅相关内容，请访问

[acams.org/en/premium-webinar-subscription](https://acams.org/en/premium-webinar-subscription)

ACAMS 网络研讨会包含在此订阅之中，企业会员也可使用





# 公认反洗钱师 (CAMS) 毕业生： 5月-7月

## 阿富汗

Atal Bahand  
Izatullah Hafizi  
Aimal Mangal

## 亚美尼亚

Gevorg Khachatryan

## 阿鲁巴岛

Kelvin Osmond Halley  
André Carmelo Kelly  
Sandy Odor  
Albertico Gregorio Willems

## 澳大利亚

Kwame Kyei A. Agyapong  
Yuko Asakawa  
Cihan Bahcesaray  
Andrew Barnes  
Christine Chandran  
Yao Chen  
Zhoufu Chi  
Xue Ding  
Shon Edward Fernandes  
Cameron Gale  
Salini Ganesan  
Kevin Horan  
Xiaonong Hu  
Xingying Jiang  
Mingying Jiao  
Yang Ann Joo  
Crisberne Agnello Joseph  
Anusha Kathula  
Ryan John Lawson  
Shana Lay  
Soo Min Lee  
Lingxiao Li  
Mengyu Li

Yilin Li  
Cuixia Lu  
Jodie Mahoney  
Athithya Mayuran  
Connor Oliver Murphy  
Gregory T. T. Nasu  
Jonathan Nathar  
Venkatesh Nathilvar  
Shabnam R. Koshkaki  
Luke Matthew Raven  
Emma Sacre  
Vineet Satish Shetye  
Barun Lal Shrestha  
Harry Solanakis  
Chi-Ping Sun  
Kimberley Tarling  
Arunthethy Thevaraja  
Yudhistira Tiono

Qian Wang  
Charlotte Peiwen White  
Anthony Michael Youssef  
Jiahua Yu  
Bingxin Zhang

## 奥地利

Amaury Crucy

## 阿塞拜疆

Tural Imamaliyev

## 巴哈马

Crystal D. Bleasdel  
Terrel Lawrence Butler  
Makeba Darville Sands  
Tyra K. Duncombe  
Hubert Edwards  
Anastacia Philippa Hepburn  
Patrice Lamm

Kristin Leah Sands  
Nekeisha T. Smith

## 巴林

Stuti Agarwal  
Alla Alnahisi  
Ali Alsawad  
Rahul Appukuttan Mukundan  
Bowen Cai  
Waqas Iftikhar  
Feroze Isaac  
Jiss Maria Jose  
Sujith Surendra Nath  
Muhammad Tariq  
Ravi Kumar Uppu

## 孟加拉国

Shafayet Hussain Ahmed  
Tahmina Akhter  
Kazi Wares Ul Ambia  
Kazi Hossain Ansary  
MST Zannat Ara  
Mohammad N. Chowdhury  
Anup Das  
Rajib Dey  
Bishwarup Dhar  
Nasimul Gani  
Ranjit Gogoi  
Md Monir Hossain  
Md. Zakir Hossain  
Md. Saiful Islam  
Madhab Chandra Karmaker  
Mohammad Golam Kibria  
Shah Selim Hamid Ovi  
Mohammad Saiful Islam  
Md Nazmus Sakib  
Md Salauddin  
Aloka Sarah

Shatabdee Sen Sarma  
Kazi Mazbah Uddin  
Syed Mohammad Walid

## 巴巴多斯

Dennice L. Bend  
Tracia N. Forde  
Kerryanne Gilkes  
Anne-Marie Goddard  
Rosson Howard  
Shauna Kissoon  
Kisha Simpson  
Rasheda Melissa S. Walker

## 比利时

Eduard Hovsepyan  
Roger Kaiser  
Anne-Dorine Ligthart  
Thomas Mareel

## 伯利兹

Salvador M. Awe  
Lissa A. Lord

## 百慕大群岛

Claire Loxley  
Pui Shan Ma

## 博茨瓦纳

Malebogo Hirschfeld  
Masego Matjola  
Gorata Moipolai

## 巴西

Renato Conde Canado  
Rafael Batista Ocanhas  
Hyde de Melo Silva  
Paula Vergamini

## 文莱

Mary Chiew Horng Ong

## 保加利亚

Georgi Denkov  
Aleksandar Tsvetkov  
Pavel Zhelyazkov

## 加拿大

Robert Adah  
Opeoluwa O. Adenaike  
Emmanuella Okoi Adole  
Yara Ahmed  
Akinyinka Akinoso  
Shalina Angelo  
John Athanasiades  
Alex Chiedu Azubike  
Shitang Bakifon  
Yvita Shane Laurent Baldoz  
Azadeh Bell-Irving  
Lynda Boisvert  
Rebecca Marie Bukovcan  
Luiza Carvalho  
Colin Chin  
Juan F. Contreras  
Darryl Andrew Cox  
Katarzyna Czekanska  
Dennis Dai  
Vishal De Silva  
Annie Desautels  
Rohit Dhumal  
Susan L. Dicks  
Nicole Danielle Ferenc  
Yasmine Garreau  
Ami Ghadawala  
Kashif Ghani  
Jonathan Mark Giffin  
Wojciech Gorski



Lancelot Graham  
 Keisha Grosvenor  
 Derek Hall  
 Mitchell Hamlyn  
 Margaret Oluwasayo Hamzat  
 Dan Heinemann  
 Chuan Yu Hung  
 Manisha Jammihal  
 Xiaoqi Jin  
 Muhammad Nour Karmeh  
 Seo Hee Kim  
 Roma Koopla  
 Darshan Kumar  
 Regis Kumar  
 Nibedita Kundu  
 Ashwathi Lakshminarayanan  
 Sin Ying Michele Lam  
 Brenda Lampman  
 Catherine Leger  
 Janet Li  
 Wanwan Li  
 Marie Kimberly Lim  
 Chun Wa Barry Lo  
 Shane Luchun  
 Josna Raju Manjrekar  
 Hayatte Mechmour  
 Mohsin S. Mukaddam  
 Aarti Naidu  
 Karin Lourdina Nanayakkara  
 Khurram Nawaz  
 Morounfoluwa Oduwale  
 Ademola Ogungbemi  
 Florence Ogunsanwo  
 Karen Okura  
 Oluwasegun Oladiran  
 Oluwabukunola O. Omolaja  
 Solomon O. Oyeniran  
 Catherine Paquin-Veillette  
 Verushka Patana  
 Shailee Patel  
 Nataliya Pejko  
 Eldho P. Peter  
 Mark Ross  
 Neil Scott  
 Amala Selvaraj  
 Ndeye Arame Seye  
 Kalpit Jagadishbhai Shah  
 Shabbir M. Shabbir Shah  
 Shivi Sharma  
 Kirill Smirnov  
 Crystal Stuart  
 Alex-Anne St-Vincent  
 Arpan Sur Chowdhury  
 Brian Swallow  
 Mashiyat Tabassum  
 Anne Okimasi Takim-Ndifon  
 Amélie Théberge  
 Mac Thiele  
 Jade Tordecilla  
 Pui Ki Tsui  
 Shane Viragh

Ana Vozian  
 Junlin Wu  
 Mark Wynter  
 Jingwei You  
 Samir Zariwala  
 Ping Zhang  
 Ge (Gary) Zhu

## 开曼群岛

Edgar Ogville Bennett  
 Deepal Bhandarkar  
 Ashley Borde  
 Kayla Bush  
 Elizabeth Byrne  
 Melissa Nastasia Durrant  
 Hilda Farinas  
 Kimberley R. W. Griffith  
 Cassie Camille Knowles  
 Nykemah Kuylen-Perera  
 Nancy Manyange  
 Robyn Elizabeth McCoy  
 Christine C. Olukoya  
 Lashonda Madiera P. Powell  
 Sarai Soto  
 Leonie Taber  
 Sharon Taiy  
 S. van Batenburg-Stafford

## 智利

Valerie Nicole Mori Fernández

## 中国大陆

Yichao An 安艺超  
 Zejin Ban 班泽晋  
 Jian Bao 包剑  
 Haoyu Bi 毕昊宇  
 Shushu Bie 别姝姝  
 Xianqun Bing 邴先群  
 Junrong Cai 蔡均蓉  
 Lingchun Cai 蔡凌春  
 Ming Cai 蔡明  
 Wentao Cai 蔡文涛  
 Yiping Cai 蔡乙萍  
 Weihang Cao 曹玮航  
 Xiaodong Cao 曹晓东  
 Zhiyu Cao 曹芷玉  
 Xuenan Chai 柴雪楠  
 Yubin Chai 柴玉斌  
 Yi Chan 产奕  
 Xiaoxuan Che 车孝轩  
 Dan Chen 陈丹  
 Danni Chen 陈丹妮  
 Fang Chen 陈芳  
 Fei Chen 陈霏  
 Guojun Chen 陈国军  
 Jiadao Chen 陈家道  
 Jian Chen 陈建  
 Jing Chen 陈静  
 Kaiyi Chen 陈恺伊  
 Lei Chen 陈雷

Li Chen 陈莉  
 Liqin Chen 陈丽琴  
 Man Chen 陈曼  
 Meng Chen 陈萌  
 Peilan Chen 陈佩兰  
 Qingyang Chen 陈青杨  
 Wenlin Chen 陈文林  
 Xiaoman Chen 陈小蔓  
 Xiaoxia Chen 陈小霞  
 Xiaoyuan Chen 陈晓远  
 Xinan Chen 陈锡楠  
 Xu Chen 陈旭  
 Yanan Chen 陈雅楠  
 Yang Chen 陈洋  
 Yangting Chen 陈杨婷  
 Yanjun Chen 陈艳君  
 Yi Chen 陈忆  
 Yifei Chen 陈奕飞  
 Yuan Chen 陈媛  
 Yunyu Chen 陈韵羽  
 Yunchun Chen 陈芸芸  
 Ze Chen 陈泽  
 Zhaojing Chen 陈兆晶  
 Zhaorong Chen 陈朝荣  
 Zhihui Chen 陈智辉  
 Ziqian Chen 陈子骞  
 Fang Cheng 程方  
 Haiying Cheng 承海英  
 Jin Cheng 程锦  
 Kai Cheng 程凯  
 Kailin Cheng 成凯琳  
 Lili Cheng 程莉莉  
 Shuxian Cheng 程淑贤  
 Xinyue Cheng 程新月  
 Yi Cheng 程怡  
 Fangfang Chu 储芳芳  
 Jishen Chu 储继深  
 Ning Chu 楚宁  
 Wenyuan Cui 崔文媛  
 Yingjie Cui 崔颖婕  
 Bifeng Dai 戴碧峰  
 Minglu Dai 戴明陆  
 Wenqian Dai 戴文倩  
 Xiaofeng Dai 戴晓峰  
 Xiaoling Dai 戴小玲  
 Yinfang Dai 戴银芳  
 Yue Dai 戴玥  
 Mengzhe Deng 邓梦喆  
 Xinhui Deng 邓新慧  
 Yating Deng 邓雅婷  
 Yunhong Deng 邓蕴弘  
 Hao Ding 丁浩  
 Jian Ding 丁剑  
 Wen Jing Ding 丁文婧  
 Xueliang Ding 丁学良  
 Ya Ding 丁娅  
 Yongxin Ding 丁永昕  
 Jie Dong 董洁  
 JingYi Dong 董静怡  
 Qinyuan Dong 董沁元  
 Rui Dong 董睿

Xin Dong 董欣  
 Zihe Dong 董子禾  
 Chunyu Du 杜春雨  
 Jiaxuan Du 杜嘉璇  
 Tianhao Du 杜天昊  
 Tingting Du 杜婷婷  
 Wan Du 杜婉  
 Xian Du 杜宪  
 Xiaowei Du 杜晓伟  
 Yingying Du 杜莹影  
 Jicheng Duan 段霁晟  
 Yunliu Duan 段韵柳  
 Beibin Fan 范倍彬  
 Guojun Fan 范国举  
 Juan Fan 范娟  
 Meng Fan 樊萌  
 Xin Fan 樊昕  
 Yangyang Fan 范洋洋  
 Hui Fang 方辉  
 Yi Fang 方艺  
 Chunpeng Feng 冯春鹏  
 Fan Feng 冯帆  
 Haitang Feng 冯海棠  
 Jianao Feng 冯嘉饶  
 Kalin Feng 冯卡琳  
 Xuejing Feng 冯雪静  
 Yuan Feng 冯园  
 Yuling Feng 冯育菱  
 Jinbo Fu 傅金波  
 Jingou Fu 付靖鸥  
 Weinan Fu 付伟男  
 Bowen Gao 高博文  
 Guangjian Gao 高光健  
 Hairui Gao 高海瑞  
 Jie Gao 高杰  
 Jingwen Gao 高婧雯  
 Lan Gao 高兰  
 Ling Gao 高凌  
 Shenghan Gao 高圣寒  
 Tong Gao 高彤  
 Wei Gao 高巍  
 Xueyan Gao 高学燕  
 Yongfei Gao 高永飞  
 Zhoulou Ge 葛舟路  
 Ping Geng 耿萍  
 Zhigang Geng 耿志刚  
 Zihao Gong 龚子豪  
 Liming Gu 古立明  
 Xiaowei Gu 顾晓伟  
 Yajun Gu 顾雅君  
 Yijing Gu 古沂静  
 Yu Guan 关愈  
 Yue Guan 管乐  
 Dandan Guo 郭丹丹  
 Hao Guo 郭浩  
 Jingyu Guo 郭婧瑜  
 Lei Guo 郭蕾  
 Ling Guo 郭玲  
 Mingyu Guo 郭明瑜  
 Shihua Guo 郭士华  
 Xiuqing Guo 郭绣晶

Yuli Guo 郭宇力  
 Yuzhen Guo 郭宇豪  
 Jinru Han 韩金儒  
 Lijun Han 韩立军  
 Miao Han 韩淼  
 Tong Han 韩通  
 Xiaomei Han 韩小梅  
 Xiwei Han 韩希伟  
 Yutong Han 韩雨桐  
 Pengyu Hang 杭鹏宇  
 Guoshu Hao 郝国枢  
 Jingying Hao 郝晶颖  
 Liu Hao 刘昊  
 Chunxiao He 何春晓  
 Li He 贺立  
 Lijuan He 贺丽娟  
 Qian He 何倩  
 Xuejiao He 贺雪娇  
 Yixiong He 何意雄  
 Zhidong He 贺志东  
 Shanshan Hong 洪姗姗  
 Yan Hong 洪岩  
 Kaixuan Hou 侯凯轩  
 Zilong Hou 侯子龙  
 Daohai Hu 胡道海  
 Guobin Hu 胡国彬  
 Juan Hu 胡娟  
 Kuili Hu 胡魁丽  
 Tenggui Hu 胡腾贵  
 Tingyu Hu 胡廷宇  
 Xiaoyan Hu 胡晓燕  
 Zhongzhou Hu 胡中洲  
 Fan Huang 黄凡  
 Heng Huang 黄亨  
 Hongmiao Huang 黄泓淼  
 Huang Huang 黄煌  
 Jiheng Huang 黄纪恒  
 Jing Huang 黄婧  
 Jinxu Huang 黄进旭  
 Kaiyu Huang 黄开宇  
 Ling Huang 黄玲  
 Minghui Huang 黄洺慧  
 Rui Huang 黄锐  
 Sheng'an Huang 黄盛安  
 Tongxin Huang 黄童心  
 Weijie Huang 黄伟杰  
 Weizhong Huang 黄维中  
 Xiaohong Huang 黄晓红  
 Xiaojuan Huang 黄笑娟  
 Xiaoping Huang 黄晓萍  
 Xiaoyuan Huang 黄小媛  
 Xin Huang 黄鑫  
 Yanghua Huang 黄扬华  
 Yingxue Huang 黄映雪  
 Zhenzhen Huang 黄真真  
 Tongtong Huo 霍彤彤  
 Xiaoli Ji 季晓莉  
 Yue Ji 季玥  
 Funing Jia 贾馥宁  
 Liangqin Jia 贾亮琴  
 Qifan Jia 贾奇凡

Xiaoni Jia 贾晓妮  
Yinan Jia 贾懿楠  
Peng Jian 简鹏  
Yi Min Jian 简逸旻  
Aijun Jiang 蒋艾君  
Bing Jiang 江兵  
Bo Jiang 姜波  
Fang Jiang 蒋芳  
Kangding Jiang 蒋康定  
Kun Jiang 姜昆  
Nan Jiang 江南  
Qun Jiang 姜群  
Siyi Jiang 蒋思怡  
Wei Jiang 姜薇  
Yun Jiang 蒋芸  
Xuejing Jiao 焦雪静  
Yuehong Jiao 焦岳红  
Rongzhou Jin 金容舟  
Shaoxiao Jin 金绍啸  
Tian Jin 靳田  
Dan Jing 敬丹  
Jiemin Jing 景捷敏  
Bo Ju 巨博  
Wenhua Kang 康文华  
Baoqi Kuang 邝葆琪  
Jiangnan Lai 赖江南  
Xiuli Lai 赖秀丽  
ZhenAn Lai 赖振安  
Chubin Lan 兰楚滨  
Li Lan 蓝莉  
Xiaolin Lan 兰小林  
Shuhua Lao 劳淑华  
Aijie Li 李爱杰  
Bailou Li 李柏楼  
Bin Li 李彬  
Bo Li 李博  
Chao Li 李超  
Chen Li 李晨  
Chenyu Li 李晨瑜  
Congrong Li 李从璐  
Fang Li 李方  
Guangzhong Li 李冠中  
Guowei Li 李国伟  
Haocheng Li 李昊承  
Hong Li 李弘  
Hui Li 李慧  
Huimin Li 黎慧敏  
Jiahui Li 李佳慧  
Jian Li 李剑  
Jie Li 李洁  
Jieqiong Li 李洁琼  
Jing Li 李婧  
Kan Li 李侃  
Li Li 李礼  
Lin Li 李琳  
Lu Li 李璐  
Meiyi Li 李美谊  
Menglin Li 李梦琳  
Minli Li 李敏莉  
Qian Li 李倩  
Qing Li 李青

Qinghua Li 李清华  
Qiuyan Li 李秋妍  
Ran Li 李然  
Ruiping Li 李锐萍  
Sha Li 李莎  
Shan Li 李珊  
Shu Li 李姝  
Sizhen Li 李锡臻  
Subei Li 李苏蓓  
Suyang Li 李苏阳  
Tian Li 李天  
Tingting Li 李婷婷  
Weina Li 李蔚娜  
Xia Li 李霞  
Xiafen Li 李霞芬  
Xingpu Li 李幸璞  
Xiyun Li 李喜燕  
Xue Li 李雪  
Xueyi Li 李雪仪  
Yan Li 李艳  
Yang Li 李洋  
Yanrong Li 李艳蓉  
Yaoren Li 李曜任  
Youyuan Li 李尤媛  
Yuan Li 李鹂  
Yuanbin Li 李苑缤  
Yun Li 黎耘  
Zhenyan Li 李真燕  
Zhenzhu Li 李珍珠  
Zhuoqian Li 李卓倩  
Furong Liang 梁芙蓉  
Jianbin Liang 梁健斌  
Qianyi Liang 梁倩怡  
Zhouyu Liao 廖宙昱  
Chuancheng Lin 林川成  
Fei Lin 林飞  
Honghuan Lin 林洪欢  
Jie Lin 林婕  
Jing Lin 林菁  
Miao Lin 林淼  
Qi Lin 林祺  
Renyi Lin 林任宜  
Xian Lin 林娴  
Xiaofeng Lin 林小凤  
Yishu Lin 林忆舒  
Yuejian Lin 林悦坚  
Zhuoxi Lin 林卓熹  
Yan Ling 凌燕  
Aiping Liu 刘爱萍  
Chuanqi Liu 刘川琦  
Cong Liu 刘聪  
Dandan Liu 刘丹丹  
Gexu Liu 刘格序  
Haiwei Liu 刘海伟  
Jian Liu 刘健  
Jie Liu 刘洁  
Jing Liu 刘静  
Jingya Liu 刘静雅  
Jun Liu 刘俊  
Jun Liu 柳骏  
Junhui Liu 刘军晖

Junyan Liu 刘俊彦  
Liquan Liu 刘力铨  
Mengxi Liu 刘梦茜  
Naiwen Liu 刘乃闻  
Ni Liu 刘旒  
Qian Liu 刘倩  
Qiang Liu 刘强  
Shang Liu 刘尚  
Tingting Liu 刘亭亭  
Weixu Liu 刘维旭  
Xiangchen Liu 刘相辰  
Xiaomeng Liu 刘晓萌  
Xuhong Liu 刘旭红  
Xun Liu 刘勋  
Xuyang Liu 刘旭洋  
Yating Liu 刘雅婷  
Yexuan Liu 刘焯暄  
Yijie Liu 刘奕颀  
Ying Liu 刘莹  
Yushan Liu 刘昱杉  
Zhuoqun Liu 刘卓群  
Xiaoyu Lou 娄小宇  
Jingli Lu 陆静丽  
Xiaoyan Lu 陆晓妍  
Xiuting Lu 卢秀婷  
Ye Lu 卢野  
Yinian Lu 卢奕年  
Bin Luan 栾滨  
Luan Luan 栾鸾  
Hao Luo 罗浩  
Kaifang Luo 罗开放  
Shihui Luo 罗时辉  
Wei Luo 罗威  
Yang Luo 罗阳  
Jiabin Lv 吕嘉宾  
Jianxun Lv 吕建勋  
Jing Lv 吕婧  
Pengfei Lv 吕朋飞  
Yang Lyu 吕洋  
Chunmin Ma 马春敏  
Fengming Ma 马凤鸣  
Jianlin Ma 麻建林  
Junhui Ma 马俊辉  
Li Ma 马丽  
Ruili Ma 马瑞林  
Xiao Ma 马潇  
Xiaojuan Ma 马晓娟  
Xiaoming Ma 马晓鸣  
Xiaoyang Ma 马晓阳  
Xingwu Ma 马星午  
Yuan Ma 马媛  
Yunheng Ma 马云珩  
Jiayin Mao 毛佳音  
Yujia Mao 茅雨嘉  
Zhimeng Mao 茅志萌  
Rui Mei 梅锐  
Juan Meng 孟娟  
Lijun Meng 孟丽君  
Lin Meng 孟琳  
YanJun Meng 蒙延军  
Ying Miao 缪颖

Chuanqi Mo 莫传琦  
Kaina Niu 牛凯娜  
Wenchi Ou 欧文驰  
Jing Pan 潘静  
Tianyu Pan 潘天雨  
Yiting Pan 潘益婷  
Cuiping Peng 彭翠萍  
Huize Peng 彭惠泽  
Gong Qi 齐功  
Qingfeng Qi 祁清峰  
Cheng Qian 钱程  
Guangkun Qian 钱光琨  
Wei Qian 钱蔚  
Lingling Qiao 乔玲玲  
Xi Qiao 乔茜  
Yi Qiao 乔艺  
Haoran Qin 秦浩然  
Li Qin 秦丽  
Liang Qin 覃亮  
Yongtao Qin 秦永涛  
Zhou Qin 秦舟  
Lin Qing 卿琳  
Qihui Qiu 邱琦荟  
Zhimin Qiu 丘志敏  
Shousheng Qu 曲首晟  
Bing Rao 饶冰  
Guangbin Ren 任广斌  
Guocan Ren 任国璨  
Lina Ren 任丽娜  
Shuyu Ren 任姝宇  
Suyi Ren 任素仪  
Tingting Ren 任婷婷  
Xiaozhen Ren 任小真  
Jing Ruan 阮静  
Na Shan 山娜  
Shan Shan 单珊  
Tingting Shan 单婷婷  
Lin Shang 尚林  
Yi Shang 商奕  
Zeyu Shang 尚泽宇  
Jian Shao 邵健  
Jie Shao 邵杰  
MinShen Shao 邵敏慎  
Yuying She 余宇英  
Lei Shen 沈雷  
Tao Shen 沈滔  
Xiaoxu Shen 沈筱栩  
Yan Shen 沈燕  
Yang Shen 沈阳  
Yuting Shen 沈宇婷  
Chengcheng Sheng 盛成成  
Hao Shi 师浩  
Jian Shi 石剑  
Jingjing Shi 施晶晶  
Kegong Shi 石可攻  
Minli Shi 时敏莉  
Pengxiang Shi 石鹏翔  
Tong Shi 施桐  
Xiaojin Shi 施晓瑾  
Miao Shui 水淼  
Zhengfu Shui 税正富

Kunlin Si 司坤林  
Jiahuan Song 宋佳欢  
Jingyue Song 宋景跃  
Liwon Song 宋丽雯  
Mingming Song 宋明明  
Naishan Song 宋乃珊  
Shu Song 宋姝  
Yang Song 宋扬  
Meng Su 苏猛  
Shuang Su 苏爽  
Xiaorui Su 苏小蕊  
Yifei Su 苏亦菲  
Xiaowen Sui 隋晓文  
Congcong Sun 孙淙淙  
Guihua Sun 孙桂华  
Jian Sun 孙健  
Jin Sun 孙瑾  
Li Sun 孙莉  
Lingke Sun 孙冷珂  
Man Sun 孙漫  
Qianyun Sun 孙倩云  
Xinyue Sun 孙新月  
Xu Sun 孙旭  
Yalin Sun 孙雅琳  
Yan Sun 孙妍  
Yanqiu Sun 孙艳秋  
Yizhou Sun 孙亦舟  
Yue Sun 孙玥  
Yuewei Sun 孙玥玮  
Mengying Tan 谭梦莹  
Shishu Tan 谭世殊  
Jie Tang 唐洁  
Rui Tang 唐瑞  
Zhe Tang 唐喆  
Chengcheng Tao 陶成成  
Juan Tao 陶娟  
Yuanyuan Tao 陶媛媛  
Guoying Tian 田国英  
Xin Tian 田欣  
Yuan Tian 田媛  
Yue Tian 田玥  
Yuxin Tian 田雨露  
Zeng Tian 田增  
Shengzhong Tu 涂胜忠  
Ben Wang 王犇  
Chao Wang 王超  
Chen Wang 王琛  
Dan Wang 王丹  
Dongyu Wang 王冬玉  
Feifei Wang 王菲菲  
Gang Wang 王刚  
Haitao Wang 王海涛  
Hongxuan Wang 王鸿轩  
Huihui Wang 王卉卉  
Huiye Wang 王慧晔  
Jiaming Wang 王笏铭  
Jian Wang 王健  
Jing Wang 王晶  
Jing Wang 王静  
Keming Wang 王可铭  
Kun Wang 王琨



Lei Wang 王磊  
Lijie Wang 王丽捷  
Limin Wang 王丽敏  
Limin Wang 王黎敏  
Lin Wang 王琳  
Lu Wang 王璐  
Lujiao Wang 王璐皎  
Manxia Wang 王曼霞  
Meng Wang 王萌  
Qi Wang 王琦  
Qing Wang 王青  
Qiong Wang 王琼  
Run Wang 王润  
Runxiao Wang 王润霄  
Shengxia Wang 王升霞  
Shuangliang Wang 王双亮  
Shuangshang Wang 王双双  
Shukai Wang 王书凯  
Shuo Wang 王硕  
Siyuan Wang 王思远  
Songli Wang 王松立  
Sulan Wang 王素兰  
Tao Wang 王涛  
Tianfei Wang 王甜飞  
Ting Wang 汪婷  
Wei Wang 王薇  
Weitao Wang 王维涛  
Wen Wang 王稳  
Xiaohong Wang 王晓虹  
Xiaolu Wang 王晓璐  
Xinyu Wang 王鑫宇  
Xu Wang 王旭  
Xueying Wang 汪雪莹  
Yanan Wang 王亚楠  
Yanzhu Wang 王延竹  
Yating Wang 王雅婷  
Yicheng Wang 王义成  
Yidan Wang 王一丹  
Ying Wang 王莹  
Yiwen Wang 王怡雯  
Yongjin Wang 王永进  
Yue Wang 王月  
Yuou Wang 王雨鸥  
Yupei Wang 王雨佩  
Yuqi Wang 王育奇  
Zhen Wang 王桢  
Zhen Wang 王镇  
Zhuqing Wang 王竹青  
Ziwen Wang 王子文  
Jingwei Wei 魏鹤巍  
Sunyuan Wei 魏孙媛  
Wei Wei 韦薇  
Yujiao Wei 魏玉娇  
Changkuan Wen 温长宽  
Jiu Wen 温玖  
So Man Wong 王苏曼  
Binzhou Wu 吴彬筠  
Geng Wu 吴庚  
Gengsheng Wu 吴更生  
Hangdan Wu 吴杭丹  
Hao Wu 吴昊

Hongkun Wu 吴洪坤  
Jincai Wu 吴锦才  
Jingwen Wu 吴静文  
Lei Wu 吴蕾  
Ming Wu 吴铭  
Qian Wu 吴倩  
Weiping Wu 吴维萍  
Wenjie Wu 武雯洁  
Xiao Wu 吴晓  
Xintong Wu 吴鑫彤  
Xuefei Wu 吴雪菲  
Xuefeng Wu 吴雪枫  
Yali Wu 吴娅丽  
Yanxuan Wu 吴妍萱  
Yingqi Wu 武颖琪  
Yuchen Wu 吴雨晨  
Yue Wu 吴越  
Yuhan Wu 吴宇涵  
Zhiheng Wu 吴志恒  
Xiaofei Xi 息霄飞  
Lifang Xia 夏理芳  
Yue Xia 夏悦  
Jie Xiao 肖杰  
Lili Xiao 肖黎黎  
Tianyi Xiao 肖天翊  
Tingting Xiao 肖婷婷  
Yao Xiao 肖瑶  
Yuqiu Xiao 肖雨秋  
Zhiying Xiao 肖志颖  
Haihan Xie 谢海涵  
Hengyu Xie 谢恒堉  
Mingxi Xie 谢明希  
Shenwei Xie 谢审为  
Shuting Xie 谢淑婷  
Tuoli Xie 谢托丽  
Yiling Xie 谢易伶  
Guangyan Xing 邢广彦  
Jing Xing 邢晶  
Cong Xu 许聪  
Di Xu 许迪  
Fei Xu 许飞  
Huimin Xu 徐慧敏  
Humei Xu 许胡梅  
Jiayi Xu 徐嘉艺  
Jie Xu 徐杰  
Jingcai Xu 徐静才  
Linxia Xu 徐林霞  
Qi Xu 许琦  
Ruixin Xu 徐睿鑫  
Wei Xu 徐薇  
Xin Xu 许馨  
Jiacheng Xuan 宣佳成  
Quan Xue 薛泉  
Xinlei Xue 薛馨蕾  
Xiongting Xue 薛雄庭  
Shujun Xun 荀淑君  
Chengfang Yan 闫成芳  
Li Yan 严莉  
Meng Yan 闫勐  
Xiangyu Yan 闫翔宇  
Xiaomin Yan 闫晓敏

Xing Yan 颜兴  
Yizhu Yan 闫奕竹  
Bei Yang 杨蓓  
Bo Yang 杨博  
Congyu Yang 杨丛羽  
Danli Yang 杨丹丽  
Dian Yang 杨典  
Fan Yang 杨帆  
Haiwen Yang 杨海雯  
Haiyan Yang 杨海燕  
Jin Yang 杨谨  
Jing Yang 杨静  
Lan Yang 杨兰  
Lei Yang 杨磊  
Li Yuan Shako Yang 杨丽元  
Ming Yang 杨明  
Na Yang 杨娜  
Rui Yang 杨瑞  
Shuhui Yang 杨舒惠  
Weihua Yang 杨炜华  
Xiaou Yang 杨小鸥  
Xiaoting Yang 杨晓婷  
Xiaoying Yang 杨小莹  
Ximin Yang 杨玺珉  
Xuejiao Yang 杨雪娇  
Yan Yang 杨艳  
Yangyang Yang 杨洋洋  
Yi Yang 杨毅  
Ying Yang 杨颖  
Yunying Yang 杨贇颖  
Zhaoyu Yang 杨兆宇  
Dan Yao 姚丹  
Qingyuan Yao 姚清源  
Huanhuan Ye 叶焕焕  
Jingjing Ye 叶晶晶  
Xinru Ye 叶昕茹  
Ying Ye 叶颖  
Chenxing Yi 益晨星  
Fei Yin 殷飞  
Xin Yin 尹忻  
Yan Yin 尹桢  
Zhen Yin 尹桢  
Zhidi You 尤智迪  
Changrong Yu 余光蓉  
Dongli Yu 于冬丽  
Hang Yu 于航  
Hong Yu 于虹  
Jinlong Yu 于金龙  
Lijuan Yu 于立娟  
Miao Yu 俞淼  
Min Yu 于敏  
Shuyao Yu 余姝瑶  
Zhengshu Yu 俞正澍  
Chao Yuan 袁潮  
Ding Yuan 袁丁  
Jiakuan Yuan 袁佳宽  
Juan Yuan 袁娟  
Sailei Yuan 袁赛磊  
Shangcao Yuan 袁上草  
Wei Yuan 原玮  
Junlong Yue 岳俊龙

Yao Yue 岳焱  
Yiyi Yue 岳艺艺  
Jianchao Zang 臧建超  
Chubin Zeng 曾楚滨  
Hui Zeng 曾慧  
Shengnan Zeng 曾晟南  
Xinliang Zeng 曾新亮  
Ying Zeng 曾荧  
Yueqing Zeng 曾玥青  
Jingmei Zha 查靖梅  
Weiyang Zha 查清阳  
Fangyuan Zhai 翟方源  
Xu Zhai 翟翔  
Boyan Zhang 张渤岩  
Chunyu Zhang 张春雨  
Di Zhang 张迪  
Feifei Zhang 张菲菲  
Haobo Zhang 张皓波  
Huihui Zhang 张辉辉  
Jun Zhang 张军  
Kun Zhang 张坤  
Kun Zhang 张堃  
Lei Zhang 张蕾  
Li Zhang 张莉  
Lin Zhang 张麟  
Ludan Zhang 张露丹  
Luxi Zhang 张露曦  
Meng Zhang 张萌  
Mengfei Zhang 张梦飞  
Mengmeng Zhang 张萌萌  
Min Zhang 张敏  
Muqiao Zhang 张木乔  
Ning Zhang 张宁  
Ning Zhang 张凝  
Pinghua Zhang 张坪花  
Qian Zhang 张茜  
Qiang Zhang 张强  
Qing Zhang 张卿  
Qiuling Zhang 张秋玲  
Renchi Zhang 张任驰  
Rui Zhang 张蕊  
Ruiping Zhang 张锐屏  
Sheyu Zhang 张社宇  
Tingting Zhang 张婷婷  
Weiqi Zhang 张伟奇  
Weiyi Zhang 张炜翌  
Xiaobin Zhang 张晓斌  
Xiaomeng Zhang 张晓蒙  
Xin Zhang 张鑫  
Xinyi Zhang 张欣怡  
Xuan Zhang 张璇  
Yansizhuo Zhang 张燕思卓  
Yaoqing Zhang 张耀青  
Yaosheng Zhang 张耀升  
Yatian Zhang 张雅甜  
Yichang Zhang 张义昌  
Yifang Zhang 张一方  
Yihong Zhang 张轶弘  
Ying Zhang 张莹  
Yipeng Zhang 张义朋  
Yiwen Zhang 张译文

Yongxu Zhang 张咏絮  
Yu Zhang 张羽  
Yue Zhang 张悦  
Yunyun Zhang 张云云  
Zhen Zhang 张臻  
Zheng Zhang 张铮  
Zhuo Zhang 张卓  
Zida Zhang 张子达  
Chen Zhao 赵晨  
Cheng Zhao 赵成  
Jun Zhao 赵俊  
Lubin Zhao 赵璐斌  
Min Zhao 赵敏  
Ruoqu Zhao 赵若蕖  
Shaobo Zhao 赵少博  
Shiqin Zhao 赵识琴  
Tong Zhao 赵彤  
Xiaomin Zhao 赵晓敏  
Ying Zhao 赵莹  
Yining Zhao 赵一宁  
Yu Zhao 赵玉  
Yue Zhao 赵越  
Yuezhong Zhao 赵裕中  
Zhenguo Zhao 赵振国  
Zhifang Zhao 赵志方  
Qijun Zheng 郑琪君  
Ru Zheng 郑茹  
Xiyu Zheng 郑希誉  
Yadong Zheng 郑亚冬  
Yanbin Zheng 郑燕彬  
Yanhua Zheng 郑焱花  
Yashan Zheng 郑雅杉  
Yinglan Zheng 郑颖岚  
Yuzhen Zheng 郑钰涓  
Ziyin Zheng 郑子寅  
Sheng Zhong 钟声  
Xiaofen Zhong 钟小芬  
Ying Zhong 钟莹  
Donghui Zhou 周东辉  
Fang Zhou 周芳  
Han Zhou 周涵  
Huiqin Zhou 周慧勤  
Jianhua Zhou 周剑华  
Jie Zhou 周洁  
Lijuan Zhou 周丽娟  
Mengyan Zhou 周梦艳  
Ming Zhou 周铭  
Na Zhou 周娜  
Rui Zhou 周睿  
Xin Zhou 周昕  
Xinyun Zhou 周信云  
Xizhi Zhou 周熙智  
Yan Zhou 周妍  
Yaxin Zhou 周亚新  
Ying Zhou 周颖  
Yingzhe Zhou 周英哲  
Yingzi Zhou 周盈孜  
Yongsheng Zhou 周咏升  
Yu Zhou 周瑜  
Yujiao Zhou 周玉娇  
Chonghe Zhu 朱翀鹤

Hui Zhu 朱辉  
 Jiangning Zhu 朱江宁  
 Jingyi Zhu 朱静怡  
 Li Zhu 朱励  
 Lingling Zhu 朱玲玲  
 Mengjing Zhu 朱梦晶  
 Shengnan Zhu 朱胜男  
 Wanlong Zhu 朱万龙  
 Yadi Zhu 朱雅迪  
 Yining Zhu 朱伊宁  
 Yongbo Zhu 朱泳波  
 Zhengpeng Zhu 朱正鹏  
 Yufei Zong 宗宇飞

## 哥伦比亚

Jose Eduardo Rojas  
 Kimberly Suarez-Contreras

## 科特迪瓦

Cyriaque Towanoun Hounsa

## 克罗地亚

Anton Kohut  
 Maja Kovač

## 塞浦路斯

Marina Agathangelou  
 Kalia Charalampous  
 Theodoros Stavrou

## 捷克共和国

Marek Bocanek  
 Petra Capkova  
 Gabriela Kindlova

## 丹麦

Charlotte Rose Lowry

## 埃及

Yousri Mounir L. Showeitar

## 爱沙尼亚

Evelin Ruus

## 芬兰

Lisa-Maria Altenberger  
 Karola Koivula  
 Wilhelm Lindstrom

## 法国

Natacha Cheron  
 Caroline Lisiecki  
 Geraldine Martinez  
 Florent Paris  
 Guillaume Riès  
 Hind Riouch  
 Julien Winterheimer  
 Yahui Xie  
 Pierre Zennadi

## 德国

Mahshan Ashouri  
 Jens Berke  
 Greta Bortkeviciene  
 Patrizia Zoi Dafulis  
 Sylvia Gisa  
 Ted Hadjisky  
 Sarah Heller  
 Marion Hientz  
 Sheng Jin  
 Charles Steven Lamb  
 Eunyoung Lee  
 Wieland Markert  
 Marcel Pohl  
 Norman Todd  
 Hans-Georg Philipp Treuner

## 加纳

Lilian Danso Affum  
 Langtertaa Karbo  
 Enoch Kofi Koranteng  
 Samuel Osei Kofi Kyeremeh

## 希腊

Zinon Chatziantonoglou

## 圭亚那

Chandan Kumar  
 Melissa Tashana Smith  
 Faith June Taylor

## 洪都拉斯

Gerardo I. Midence Zúniga

## 香港特区

Asif Ahmad  
 Mak Chun Wai Billy  
 Siying Cai  
 Chi Tsun Chan  
 Ching Yin Chan  
 Choi Yee Chan  
 Ka Man Chan  
 Sai Po Chan  
 Ting Yiu Chan  
 Wing On Chan  
 Yin Cheuk Chan  
 Yuen Ying Chan  
 King Shan Chau  
 Siu Tin Chau  
 Wai Ning Winnie Chee  
 Lai Sum Cheng  
 Zehui Cheng  
 Ka Yee Cheung  
 Lok Yee Cheung  
 Sze Sze Tess Cheung  
 Wai Ling Winnie Cheung  
 Wing Tung Sydnee Cheung  
 Wai Yin Chick  
 Wing Chi Remy Ching

Yun Tai Chiu  
 Tak Ki Derek Choi  
 Chi Kwan Johnny Chow  
 Ho Ming Chow  
 Wing Hei Chow  
 Amanda Chu  
 Chung Ting Chu  
 Ho Yi Chu  
 Man Wui Chum  
 Yuen Ying Chung  
 Xinxin Cui  
 Jiaying Dong  
 Jonathan Vincent Galaviz  
 Celeste Goosen  
 Richard David Grasby  
 Dandan Guo  
 Farihah Hassan  
 Qing He  
 Suet Ling Heung  
 Chi Him Sonny Ho  
 Chun Fai Ho  
 Chun Wa Ho  
 Ka Wai Ho  
 Wai Leung Ho  
 Wing Fung Ho  
 Yan Ting Ho  
 Kho Cindy Honggo  
 Madhu S. Hosmane  
 Wei Ling Huang  
 Pik Chi Hung  
 Tsz Chung Hung  
 Wing Ki Hung  
 Vaibhav Surendra Jain  
 Sasha Kalb  
 Ka Yan Kam  
 Kam Chiu Ko  
 Ting Fung Kong  
 Lam Lam Kwan  
 Pui-Hin Basil Kwan  
 Tak Ching Kwan  
 Wing Ni Kwan  
 Chun Hin Kwok  
 Hoo Yee Kwong  
 Man Kei Lai  
 Cheong Lam  
 Ephraim Lam  
 Hiu Yeung Lam  
 Sai Ho Lam  
 Tsun Fai Lam  
 Wai Ip Lam  
 Wai Sum Lam  
 Ying Chun Lam  
 Po Shan Geraldine Lau  
 Ting Ting Lau  
 Tsz Kwan Lau  
 Tze Yue Lau  
 Hoi Yee Law  
 Yat Kan Law  
 Chun Yin Lee  
 Lok Yin Rosalind Lee  
 Nam Ying Lee

Po Yu Lee  
 Wing Kiu Rowena Lee  
 Au Sei Leung  
 Hing-Wa Leung  
 Ka Lee Kany Leung  
 Kevin Leung  
 Yan Chi Ellen Leung  
 Ho Yin Li  
 Jizhao Li  
 Kin Fung Li  
 Kin Kei Li  
 Suet Yee Li  
 Yi Hong Li  
 Jun Liang  
 Shaoling Liang  
 Jiabo Liu  
 Wang Ho Lui  
 Kei Fung Luk  
 Pui Ling Man  
 Aurore Marie  
 Sreya Narayanan  
 Chun Yiu Jason Ng  
 Ka Kin Ng  
 King Hei Ng  
 Yan Wa Ng  
 Yuen Chuen Ng  
 Wun Sze Ceci Ngai  
 Hyun-seok Oh  
 Si Wan Poon  
 Jingjing Qiang  
 John Rinold  
 Yiu Yeung Ser  
 Kin Lok Danny Shiu  
 Hiu Ting Sin  
 Wing Yin Sin  
 Chi Ho Siu  
 Sze Kit Alan Siu  
 Paul So  
 Wai Mi So  
 Amit Soni  
 Andrew Sprake  
 Tsz Yan Tam  
 Carmina Wing Man Tang  
 Tsz Chun Tang  
 Wing Hung Tang  
 Kin Hang Tsang  
 Kin Ming Tsang  
 Ka Lai Wan  
 Tsz Hin Wan  
 Tiancheng Wang  
 Chee Weng Wong  
 Cheuk Gi Churchill Wong  
 Fung Yee Wong  
 Hei Ning Wong  
 Hoi Shing Wong  
 Ka Yu Rico Wong  
 Miu Sheng Wong  
 Pik Ki Wong  
 She Wah Wong  
 Shuk On Wong  
 Tik Man Wong

Tsz Wing Wong  
 Yan Ho Wong  
 Yiu Kai Wong  
 Yuk Lam Navy Wong  
 Chi Kwong Woo  
 Hiu Wing Woo  
 Hei Man Wu  
 Odelia Hew Tung Wu  
 King Leung Andy Yau  
 Chun Hoi Yip  
 Samuel Wai Keung Yip  
 Wai Tai William Yip  
 Cheuk Yin Yiu  
 Wai Shan Yiu  
 Ka Man Yu  
 Pik Tsz Yu  
 Chuen Ho Yuen  
 Kin Ming Yuen  
 Kwun Lok Yuen  
 Yi Lam Yuen  
 Jingxuan Zhang  
 Lulu Zhang  
 Qi Zhang  
 Yanka Zhang  
 Haomiao Zheng

## 匈牙利

Renata Fejes Ujváriné  
 Richárd Katona  
 Zsolt Korosi  
 Tamas Levai  
 Tibor Racz

## 印度

Mrutyunjaya Acharya  
 Hussein Attari  
 Mahalakshmi Ayyasamy  
 Archana B V  
 Harshita Bajaj  
 Paresh Chandra Barik  
 Manoj Kumar Batra  
 Usha Amarnath Bhardwaj  
 Ratna Borse  
 Navaneeth Chanolian Poyil  
 Mobin Cherian  
 Venkata P. R. R. Chintalapati  
 Venkata Aditya R. Choppa  
 Kangkan Das  
 Roopal Dev  
 Deepthi Dominic  
 Nitin Mahendra Ganatra  
 Fezan Gauri  
 Priyanka Giri  
 Premdeep Godara  
 Abhinandan Goswami  
 Nitin Kumar Gupta  
 Poorani Ilango  
 Anurag Jain  
 Smriti Jajodia  
 Jiten Shivrani Joshi





公认反洗钱师协会®

# 走好第一步

ACAMS 最新社群，汇聚大量通过认证的专业人士，面向初入了解您的客户/客户尽职调查、交易监控以及金融科技企业反洗钱合规领域的人员，热烈欢迎您的加入！



访问 [www.acams.org](http://www.acams.org)  
开启您的旅程



Pranav K

Vinod Karade

Rinku H Katharia

Mehnaz Khushtar

Suresh Kothandan

Arun Kumar

Premraj Meena

Madhumita Nag

Jebi Numbipunnilath

Susmita Parankush

Divya K Raj

Rajkrishnan Rajan

Jagdeep Singh Randhawa

Kavya Rastogi

Puja Roy

Sandeep Dilip Ruparelia

Akshara Sunil Sawant

Nikita Shah

Mohd Shareef

Ramanuj Sharma

Rinos Banu Sheik Alavudeen

Ramesh Singh

Krishna Solapnor

Mithunkumar M. Surpur

Karan Tambe

Bhumi Nitin Trivedi

Leonidas Tsismetzoglou

Neethu Vattolli Kumaran

Ravin Vyas

Vishwanath Yelkal

Prakriti

## 印度尼西亚

Febrina Aruan

Anthoneus Ismoyo Djati

Candra Putra

## 爱尔兰

Eleanor Aspell

Daniel Jose Diaz Rey

Emma Gorman

Shane P. Quinn

Tatiana Aparecida Silva

Orla Stockdale

Katie Walsh

## 以色列

Nevo Lapidot

## 意大利

Nicoletta Grilli

Alessandro Andrea Miragoli

Alessandra Vitale

## 牙买加

Leshana Campbell

Natalie Lotoya Forrester

Carlene Johnson-Saunders

Monique Lawrence

## 日本

Meitetsu Emori

Satoshi Hamamura

Masaaki Hara

Rui Hirose

Koji Hisanabe

Toshiaki Hoshi

Aya Igarashi

Yoshitaka Ikeda

Yuko Imada

Yasuko Imura

Hiroyuki Inakazu

Kensuke Kasugai

Chihiro Kawakami

Fumi Kawakami

Tomohiko Kimura

Makoto Koga

Kimihito Kojima

Masashi Konno

Mitsuhiro Kurosaki

Taro Matsuoka

Natalie Mayumi

Sadahiro Miki

Takashi Miyamatsu

Go Mochimatsu

Tomoko Mogi

Takashi Mori

Masato Morisaki

Tomoka Nakamura

Ippei Nakane

Kazuki Niimura

Yoko Nitta

Jiabao Ren

Yoshikazu Saito

Kenjiro Shima

Ryotaro Shimizu

Misato Susaki

Keiji Suto

Maiko Takeuchi

Tomoki Tamura

Nobuhiko Tanaka

Saiko Terada

Mitsuko Yamamoto

Meiko Yamauchi

Atsushi Yasuda

Makoto Yoshida

## 哈萨克斯坦

Gaukhar Akina

## 肯尼亚

Nicholas Kiptoo Bett

Naomi C. Kipsang

Domitilla Wanjiku Kiragu

Enock Olando Mukabi

Zachariah Magoka Oburi

Bernard Ogake Ogendo

## 科威特

Jenan Alabdulrazzaq

Abdulaziz Ali Almondi

Ahmed Yasin Mohamed

Udit Wadhwa

## 拉脱维亚

Olga Barča

Janis Mellups

Natali Sorokina

Olga Tumule

## 黎巴嫩

Vanessa Chamoun

Antoine Salame

Farid Zebib

## 立陶宛

Alina Cibulskė

Kristina Gudaite

Vytautas Mockus

Deivydas Razminas

Diana Urbonienė

## 卢森堡

Laurent Dao

Giedrius Drulia

Feng Du

Luis Esparza

Cristina García Berenguer

Sybilie Giriens Rakintsev

Galit Goldman-Malka

Yadie Li

Andrés Santamaría Alvarez

Maria Isabel Carolina Vago

Siwei Xiong

Xin Zhao

## 澳门特区

Carmen Ao

Yong Chen

Ngan Hou Cheong

Ut Sin Chong

Huimin Huang

Iat Kuai Cecilia Lam

Cheng Lam Lei

Nga Weng Lei

Sok Cheng Lei

Man I Leong

Madalena Lo Pino

Raquel Mak

Chi Chong Abilio Pun

Ut Hong Pun

Yun Qian Su

Sut Nga Tang

Kin Keong Tong

## 马拉维

Tisunge Tiwonge Phiri

## 马来西亚

Mogan Chanderan

Guan Yu Ng

Nurhidayah Binti Abdul Razak

Poh Cheong Seow

Chin Leong Tsai

## 马耳他

Margherita Alessandri

## 毛里求斯

Gowree Roopnah-Dusoruth

## 墨西哥

Federico Cano Robert

Manuel Arturo Vazquez Torres

## 纳米比亚

Menfret Melk

## 荷兰

Tolga Aksoy

Kay Al

Roy William Bottenberg

Aimee Brouwers

Suruchi Gawde

Haci Izci

Hüseyin Keyik

Lonneke Kuilboer

Anran Li

Feng Li

Moniva Martina

M. J. Mertens

Kosara Petrova Mihaylova

Gabriela Muñoz Arenas

Riza Can Ozturk

Amelie Schuler

Runbo Si

Ailin Song

Dolly Sabrina Tolesano

Kasim Emre Türk

W. R. S. van de Steeg

Piet-Hein van Zijl

Liudmila Vegter-Boroshko

Emily Verwaal

Marcin Wasilewski

Daehan Wi

## 新西兰

Kit Chiu

Louise Coad

Charis Danieli

Md Shafiul Azim Faruqui

Kannitha Kaing

Christelle Launay

Lucas Joseph Mansell

Warden Tamuka Nyawo

Owen Bruce Turner

## 尼日利亚

Taiwo Adeniyi

Olufunke Ajani

Bright Chinweotuto Anyanwu

Ajibola Sunday Fakorede

Abisola Gbadebo

Adefunke Ibronke

Unoma Ebelechukwu Ndulue

Uchechukwu A. Nwosu

Adeyinka Adeola Oladepo

Olohitare Omomofe

Egundoyin Ajini Oni

Titilope Oluwakorede Rotimi

Clara Idaoerefama Umanah

## 挪威

Asia Chernova

Runar Nilsen

## 阿曼

Hawraa Al Harthi

## 巴基斯坦

Eitzaz Ali

Shehzad Firdous Ali

Prem Kumar

Asif Naeem

Kamran Shahzad

Priya

## 巴拿马

Helene Tison

## 巴拉圭

María Teresa González Fretes

Oscar Ramon R. Melgarejo

## 秘鲁

Ingrid Del Solar

Armando Martin G. Vasquez

## 菲律宾

Kristine Dela Rosa Candelaria

Mary Grace Jativa

Jerry Labaguis Leal

Blesilda Anne B. Lubag

William Russel Surla Malang

Imelda A. Mifa

Maria Cecilia G. Natividad

Jayvee Roca

Ian Kimmy Tin

Ramon C. Lazp Viado

## 波兰

Radoslaw Jastrzab

Piotr Tadeusz Landowski

Andrzej Lenartowicz

Jan Lutze



Panagiotis Mallios  
Anastasiia Matros  
Tetiana Vorobiova

## 葡萄牙

Flavio R. Erreria

## 波多黎各

Gloriel Mercedes A. Colon  
Ivonne Avilés Domenech  
Jorge M. Rivera González  
Evan Turner

## 卡塔尔

Ali Warsam Abdalla  
Arwa AbuHamdieh  
Abdulla Mohammed Al Saadi  
Moza Alkuwari  
Abdelkebir Azzi  
Irene Kay A. Branzuela  
Modhureema Chatterjee  
Carlos Jorge Coelho Ferreira  
Arun Kumar Soman Pillai

## 俄罗斯

Vladislav Anadikt

## 卢旺达

Ubaldo Sesonga

## 沙特阿拉伯

Essam Abdullah M Al Nasayn  
Abdulrahman K. Alruwaished  
Ibrahim A. Bin Rasheed  
Mohammad Fareed Fatani  
Emtenan Hajar  
Ammar A. Jeddawi  
Zohaib Ali Zahid

## 新加坡

Jing Hao Ang  
Qi Hui Ang  
Bee Huay Joelle Aw  
A Abdul Basith  
Tajudeen Benazir  
Souvik Bera  
Edwina Ai Leng Chai  
Qing Yuan Chan  
How Cher Kayden Chang  
Sai Chuen Chee  
Marcus Qiliang Chen  
Vincent WenDa Chen  
Xinyi Charmaine Chen  
Yongquan Chen  
Jie Yi Cheng  
Wei Jian Clement Cheng  
Hwee San Jessica Cher  
Wei Ling Nicole Chern  
Steven Cheung

Shi Jie Chew  
Wei Bin Stephen Chew  
Yi Ling Vanessa Chew  
Jia Cheng Chia  
Sin Hung Chia  
Satish Kumar Chilamkurthy  
Han Yi Chim  
Shi Min Charmaine Chong  
Shong Kai Mason Chou  
Hui Hong Daphne Chua  
Mei Na Chua  
Ka Tsun Joshua Chung  
Ong Guo Wei Desmond  
Chinmoy Dey  
Si-Qiang Ronald Ding  
Seah Eng Chye  
Jing Jing Joy Gan  
Wai Yee Sarah Gan  
Kiang Kiat Goh  
Mun Lin Doreen Goh  
Zhi Wei Leonard Goh  
Jie Ying Han  
Qiaolin Han  
Wenting He  
Xinni Daphne Heng  
Chu Hong Ho  
Hwee Cheng Christine Ho  
Wei Lik Ho  
Xin Yi Jaslyn Ho  
Audrey Hoa Zimmer  
Chen Hong  
Yin Lin Jacqueline Houg  
Guan Jie James Huang  
Lina Huang  
Peisi Chloe Huang  
Wen Feng Aaron Huang  
Igor Ivanov  
Darren Jolly  
Xiao Pei Kan  
Zhong Ting Zac Kee  
Akshay Avinash Kher  
Onyou Kim  
Kai Shi Kasey Koh  
Lo Min Cheryl Koh  
Xiangrong Kathleen Lai  
Ming Chuan Daniel Lam  
Weijie Jake Lam  
Ze Wei Kenji Lam  
Asyraf Latiff  
Yan Hong Lau  
Chew Yeng Hannah Lee  
Weixiong Lee  
Xuan De Lee  
Wan Li Winnie Leong  
Jing Li  
Lei Li  
Mengran Li  
Yongjing Michelle Li  
Hwee Leng Janice Lim  
Jun Wei Gerald Lim  
Nu Yi Rachel Lim

Weijun Lim  
Yu Feng Lim  
Yuze Lim  
Zi Yun Lim  
Chiao Hsuan Lin  
Daohan Lin  
Siew Fong (Felicia) Loh  
Wei Hao Loh  
Yen Har Josephine Loh  
Yi Sheng Loh  
Zhen Wen Shawn Loh  
Jianhui Low  
Yi Han Elle Low  
Aidalyn De Claro Lualhati  
Whye Mun Jonathan Lum  
Vidhya Madhavan  
Vina Misra  
Tanmoy Mitra  
Khay Mar Myo Aung  
Thulaja Naidu Ratnala  
Cui Shan Rachel Neo  
Boon Tiong Ng  
Han Liong Ng  
Jiehao Ng  
Ng Zi Bryan Ng  
Scott Gabriel Ng  
Su Khay Ng  
Tse Ching Tracy Ng  
Ying Hui Ng  
Wei Chang Ngauw  
Jing Wen Juliene Ong  
Sze Yun Ong  
Xiu Hui Ong  
Rashmi Pabla  
Siak Evelyn Peiyun  
Wen Hui Phua  
Wei Ling Rebecca Poe  
Bowen Qian  
Ying Fang Quek  
Girish Raghavendra Rao  
Ashish Rawat  
Shiew Yi Shi  
Wei Ming Sieng  
Yun Ling Eileen Siew  
Paul H. S. Singh  
Wan Hua Siow  
Xin Yi Sitoh  
Jiayin Song  
Seow Ying Soon  
Yu Fang Soon  
Shuang Su  
Thenmozhi Sundaramurthy  
Ah Heng Tan  
Ailing Tan  
Candace Tan  
Fu Ling Casey Tan  
Hong Jun Rachel Tan  
Joslynn Li Chuin Tan  
Kang Yong Alfred Tan  
Kim Hong Alvin Tan  
Mei Yan Tan

Si Rui Tan  
Tang Lim Heather Tan  
Tze Kye Kenny Tan  
Wee Kiat Joel Tan  
Xiangyun Tan  
Yen Ming Tan  
Yong Da Jason Tan  
Zhi Ming Melissa Tan  
Vishal Taneja  
Zhi Xiang Zax Tang  
Xiangyou Ezra Tay  
Yang Zhi Nicholas Tay  
Xue Bin Teoh  
Arun Thanawala  
Jie Ling Jacqueline The  
Yihua Terence Thien  
Kum Yen Tong  
Vrishali Abhijit Vekhande  
Shi Bin Charlton Wan  
Jingjie Wang  
Shi Yi Wee  
Jing Yu Wong  
Soo Wei Wong  
Wei Xuan Wong  
Chee Wai Samuel Wu  
Jenallynn Jianing Yang  
Chun Woei Yap  
Yeow Boon Danny Yap  
Li Han Jasmin Yeo  
Shang Kun Yeo  
Zhen Hao Yeo  
Thiam Ming Desmond Yong  
Xiaoxin Zhu

## 斯洛伐克

Richard Cukovic  
Ing. Petr Hajda

## 斯洛文尼亚

Sebastijan Peterka  
Masa Zalar

## 南非

Jorge Azevedo  
Sharmilla Gajan  
Meganathan Govender  
Shenghua Jiang  
Lawrence Luke A. Kayamba  
Nolene Singh  
Ofentse Alec Theledi

## 韩国

Jee Woon Bahng  
Ahn Cheol Hong  
Byeongjun Choe  
Su Jeong Choi  
Yangwun Choi  
Seungjoo Han  
Seungmok Han  
Sung Keun Hong  
Kyung Ok Hwang

Seokbong Jang  
Da Eun Jeong  
Eun Hee Jeong  
Hee Yoon Jeong  
Dan Kim  
Dong Hyun Kim  
Dongmin Kim  
Geunwoo Kim  
Hoisuk Kim  
Hyo Won Kim  
Jeongin Kim  
Ji Hyang Kim  
Ji Hyun Kim  
Jooeun Kim  
Myoungshin Kim  
So Eon Kim  
Sung Yeon Kim  
Woo Jeong Kim  
Young Bae Kim  
Young Sic Kim  
Hyun Ji Lee  
Myungah Lee  
Seonghye Lee  
Hyun Sil Lim  
Ki Hoon Nam  
Jiyeon Park  
Moon Sook Park  
Yoon Young Roh  
Woo Seung Sohn  
Pengyang Wang  
Young Chan Yang  
Seomin Yoon

## 西班牙

Ángela Colás González  
María Freire Pequeño  
Fernando Martín Garmendia  
Viktoria Kolesnikova  
Maria Mateos Junquera

## 斯里兰卡

Ramith Bandara Ranathunga  
Janani Srisikandarajah

## 圣基茨和尼维斯

Keishara C. Liburd  
Mark Mangan

## 瑞典

Emil Bexenius  
Carl-David Sukrit Lundström  
Hanna Lüttschwager  
Emil Richlow  
Georgette Shinoda

## 瑞士

V R Phani Kishore Basavaraju  
Leila Boulkerara  
Gonçalo Cardoso  
Anna Cecere

Giulio Filippi  
Myriam Fleurdépine  
Maria Carolina Marcondes  
Christian Peiffer  
Paulius Stulpinas  
Roshnee Kiran Thakore

## 台湾地区

Kuo Chieh Chao 趙國婕  
Hsinyi Chen 陳心儀  
Li-Tang Chen 陳立唐  
Ying Chien Chen 陳穎蓓  
Ying Mei Chen 陳英美  
Chun Yu Carey Chien 簡均書  
Chun-Hui Cho 卓春慧  
Chun-Yao Chuang 莊竣堯  
Hsiao Fei Ho 何小妃  
Huei Shin Hou 侯惠馨  
Chia Chen Hsieh 謝佳臻  
Ning Yu Hsieh 謝甯仔  
Yu-Sheng Hsin  
Yeh-Yi Hsu 徐燁儀  
Fong Jia Hu 胡峯嘉  
Pei Hsuan Huang  
Hsiang-Ting Lee 李翔婷  
Yi Hsing Liang 梁義興  
I Hsia Lin 林依霞  
Fang-Chun Liu 劉芳君  
Shu Lin Liu 劉淑琳  
Yushan Lo 羅于珊  
Chia-ling Ree 呂佳陵  
Shu Chen Shih  
Yen Ping Sun 孫艷萍  
Yu Chi Ta 達宇淇  
Chia-Lung Tang 家隆湯  
Yu-Hsuan Teng 鄧宇玔  
Pei-Chen Tsai 蔡音真  
Hsin Ping Wang 王馨平  
Yi-Hua Wang 王藝樺  
Tsai-Yu Wu 吳彩鈺  
Mei Hsien Yang 楊美賢

## 多哥

Abdoulaye Ibrahim Beidou

## 特立尼达和多巴哥

Kern DeBique  
Anna-Lisa Dialdas  
Stacey L. O. Honore  
Natalie Noel  
Kimberleigh Peterson  
D. J.-M. Selman-Carrington  
Antonio Villaverde Areces

## 土耳其

Ahmet Can Demir  
Caner Kaya  
Engin Simsek

## 特克斯和凯科斯群岛

Soreka Sharonda Brown

## 乌干达

Mugisha Habib  
Kenneth Natukunda

## 乌克兰

Marta Babyak  
Ivan Paramonov

## 阿联酋

Sameer Ahmad  
Mamta Ajmera  
Aisha Essa A. Khalfan Al Ali  
Omar Ibrahim Alhasnawi  
Akhtar Ali  
Reem Abdulrazzaq Anwahi  
Hisham Ayamu  
Stebin Chungath Baby  
Ammar Ali Baig  
Ayesha Butt  
Deepti C. Pillai  
Hanee Ali Chanwan  
Sriram Chokkalingam  
Emma Louise Cowan  
Benjamin Crossland  
Nachiketh Deshpande  
Mugdha Mahesh Dhomkar  
Diana Dsouza  
Roma Dsouza  
Sharon D'souza  
Prince Ebbin  
Arish Ehsan  
Lily Eid  
Diala El Zouineh  
Hanna Joseph Francis  
Melodie Haddad  
Irfan Ullah Ihsan Ullah  
Anubha Jain  
Dilip Jain  
Leroy Mathew Jones  
Sushanth K  
Ibrahim Khaleel P. Mohiddeen  
Divya Khiara  
Bharat Khurana  
Vinodh Kooriyattil  
Girish Krishna Shetty  
Mohamed Lafir  
Kumaravelan Loganathan  
Soumya Mathew  
Lloyd Meadows  
Jayesh Meethale Veettil  
Shamim Meraz  
Anila Mohamed Rafeek  
Nazer Hamzath Mohideen  
Ria Nangia  
Noman Nazim

Ali Hussain Noorjahan  
Sheetal Noronha  
Ammar H. Aldeen Eid Obeidat  
Chandraprabash P C  
Ajith Chandran Pallath  
Yogita Ajay Panandikar  
Vijish Vijayan Panicker  
Vivek Gokuldas Panicker  
Shakkeel Naduvile Purayil  
Saumya Rajan  
Dala Ram Ram  
Sanjay Ramchandani  
Alok Ranjit  
Rakhisha Rasheed  
Mohammad Rayess  
Syed Asif Raza  
Shuja Ur Rehman  
Vishal Relhan  
Smitha Sadasivan  
Ginu K. Samuel  
Sonali Vijay Sathe  
Pinky Nikesah Sawant  
Trisha Sen  
Sherif Shaaban  
Muhammed Shabinudheen  
Soumya Sharanagowda  
Balwant Kumar Singh  
Srithar Srinivasan  
Savitha Subramanian  
Divya Thanvi  
Abdul Azeez Thayyil Kokkatt  
Keo Akemi Yap Tiong  
Aiden Varghese  
Anu Varghese

## 英国

Alimat Oluwatobi Adedayo  
Aramide Akisanya  
Tasmia Akter  
Rimjhim Bijay Kumar  
Sinead Julia Carcavella  
Thomas Davy  
Arianna De Luca  
James Deaville  
Nikolaos Drosos  
Sarah Edney  
Aziz El Kaissouni  
Izabella Eninn  
Idriss Imorou  
Rebekah Jones  
Tejasvi Deepak Karnik  
Agnieszka Kerby  
Siar Khoreishi  
Tomas Yago Lafon Ameijeiras  
Nikhil Lavanian  
Luke Louca  
Philip Michel  
Nicola Morgan  
Oluwatoyin Olanpejo  
Femi Mark Olufeyisann

Charles Edward O'Neill  
Damian Parminter  
Sonia Pereira  
Karol Poplawski  
Jake Nicholas Rawinsky  
Nahilla Razaq  
Elizabeth Reid  
Shruti Revankar  
Najee Riaz  
Vishal Sampat  
Shamaila Shahjahan  
Khalid Sheikh Mohamed  
Loic Sylvain Sienche  
Stuart Philippe Sims  
Ritu Singh  
Rajesh Ramesh Talpade  
Trevor Tanchel  
Carole Turner  
Rita Francesca Valentini  
Monika Visy  
Frances Eve Whittaker  
Yang Yu

## 美国

Monica Abad  
Ramon Abascal  
Alessandro Abate  
Charles Abuah  
Benicia Acevedo  
Itzel R. Aguirre  
Rahat Ahmad  
Vivien Ai  
Korede Michael Ajileye  
Adenike Olajumoke Akinwusi  
Monica Yalul Alarcon Martinez  
Ashley D. Alimbuyao  
Zack Allison  
Max A. Alves  
Abigail Yeboah Ampratwum  
Bruce Anderson Jr.  
Brian Andres  
Oladayo Anipole  
Feyisayo Aregbesola  
Madilynn Ashworth  
Laura Audette  
Ryan Bacher  
Cesar Baez  
Omotola Adesile Bakare  
Jesse Baker  
Nakesha Tania Ball  
Lindsey Barnett  
Jessica Barton  
Kimberly Beckstrom  
Ellie R. Bedford Nowland  
Elena Begunova  
John Kofi Bempoh  
Iana Berger  
Justus Rolf Bieber  
Linus Billings  
Lynda Jean Bird

Joshua Black  
Chad G. Blanchard  
Jeffery Blossom  
Mitchell Bono  
Camille Bossut  
Graeme Bourne  
Caitlyn Briann Brown  
Mason T. Bruner  
Masayo Bruno  
Ethel C. Buangan-Gee  
Joseph R. Burwell  
Hameed Butu Onakoya  
Courtney Hugh Byles  
Erin Callahan  
Ana P. A. Lopes Campanini  
Carlos Meneses Canales  
Julia Elba Cancino  
Gregory Lloyd Carr  
Huei Chacon  
Iram Chapa  
Saramma Cherian  
Sin Yi (Kaitlin) Cheung  
Linnette V. Chew  
Stephen Chicoine  
Erik Chou  
Imtiaz R. Chowdhury  
Veronica Christy  
Joon Woo Chung  
Benjamin Clinard  
Adam Clough  
Connor Lamar Coleman  
Mary Wallace Coleman  
Matthew Collins  
Nicholas Colón  
Normaliz Colon Ascanio  
Donna A. Colwell  
Shawn Connelly  
Natalie Connolly  
Cesar A. Cortez  
Joseph Cosmides  
Katrina Crider  
Rachel Krenzer Crittenden  
Carlos Cuadra  
Jennifer Lynn Cunningham  
Karl Curry  
Anna Cvitkovic  
Janelle Daniel  
Hollie R. Daniels  
Humberto D'ascoli  
Adam John Daufen  
Shivam Rakesh Dave  
Dave Dawson  
Coretta Jordan De Leon  
Hashani Denawakage Dona  
Heather Deyarmin  
Tracey Diggs  
Courtney Dinardo  
Andrew DiOrio  
Richard Doebele  
Jeffrey Doran  
Krystal X. Dou



# 制裁领域

为组织提供全面的解决方案，  
促使其员工遵守复杂的制裁法规。



国际制裁合规师  
(CGSS) 认证



线上培训



大师班系列



制裁月度报告



思维领导力



人际网络

Ciaran Cormac Egan  
 Puthenpurakkal S. Elizabeth  
 Julianna Elyse Ennamorati  
 Lorena Esparza  
 Steve Estevez  
 Yan Fang  
 Christian Fernandez  
 Zachary Fontes  
 Kaitlin Fox  
 Yana Galitsyna  
 William Galton  
 Fabiola Garduño Velázquez  
 Jason Garverick  
 Clark Sherman Gascoigne  
 Brian Gelbert  
 Imisi George  
 Katherine Gillett  
 Nicole Givens  
 Miron Goldgeil  
 Jose Gomez  
 Sandra Gomez  
 Manuel Gonzalez  
 Hubert Grabowski  
 Sheila Lynn Gray  
 William C. Gray  
 Crystal Green  
 Jeff Grimes  
 Erik Grossman  
 Lauren Elizabeth Grzybowski  
 Jose Luis Guerra  
 Jenna Guerriero  
 Jared E. Guthrie  
 Andrew J. Gutshall  
 Glenna Hagopian  
 Syed Aftab Haider  
 Meagan Hailey  
 Ericka Hallgren  
 Siobhan Delaney Hanlon  
 G M Nurul Haque  
 Nicole Harlan  
 Andy Harley  
 Mayra Harmon  
 Cheryl Harris  
 Preston Haxo  
 Evan Warner Henderson  
 Lisa Heuring  
 Jennifer Hicks  
 Alison Hinds-Pearl  
 Preston Holyfield  
 Elise Diamond Howard  
 Anthony S. Hrestak  
 Kai-Ju Hu  
 San Huang  
 Jordan Hudspeth  
 David Hunn  
 Takahiro Ito

Lyndsey Camille Jackson  
 Valerie Jackson  
 Robert Jahanfar  
 Anisha Jain  
 Jennifer James  
 Neal Johanson  
 Carlos M. Johnson  
 Gianna Johnson  
 Thomas Scott Johnson, Jr.  
 Brandon William Jones  
 Cylenithia Drinkard Jones  
 Amrita Vijay Joshi  
 Namita Karunakaran  
 Anna Elizabeth Kasperek  
 Asher Kearn  
 Valeria Brukhis Kennedy  
 Sumer S. Khadra  
 Sameer Khale  
 Sajjad Kamal Khan  
 Sang Yup Kim  
 Hilary Klein  
 Dorota Kobik  
 Jonathan R. Koffmann  
 Oleg Korets  
 Jayson Kowiak  
 Dilyana A. Krasteva  
 Aaron Kruger  
 Erik Krusch  
 Kendra Kubin  
 Felix Y. Kwan  
 Iryna Kyryliuk  
 Wendy Lynn Lambach  
 Ryan Mitchell Landin  
 Luis Lara  
 Christa Lasher  
 Joseph LaSpina  
 Jeffrey Lauer  
 Alina Laumann  
 Patricia Leary  
 Hye Jin Lee  
 John Y. Lee  
 Mariya Leonova-Jones  
 Nancy Halpern Lesser  
 Ka Man Li  
 Eui Kyung Lim  
 Maria Lindstrom  
 Sarah Lohschelder  
 Diana V. Londono  
 Mark Alfred Loucas  
 Joseph Lounds  
 Angus P. Lowe  
 Chun Lu  
 Timothy L. Lukavsky  
 Brandon Luth  
 Norman Ly  
 Kathryn Lynn

Louisiane Maciel  
 Yonique Malbranche  
 Austin Maney  
 Gohar Manukyan  
 Justin Margolis  
 Keith Martell  
 Elias L. Martinez  
 Makayla Martinez  
 Pedro A. Martins Coias  
 Alex Masbruch  
 Perry D. Mastrocola  
 Siewhiang McCreight  
 Ronak McFadden  
 DeAngelina McGee  
 Lola McKindles  
 Stephanie McNeely  
 Valeria B. Melincu  
 Hannah Elizabeth Melot  
 Carlos Mendez  
 Ptoshia K. Merrills  
 Elise Messerli  
 Ibrar A. Mian  
 Leyla Milman  
 Laura Minnick  
 Anna Rose Mobilia  
 Craig Thomas Momborg, Jr.  
 Keion Morgan  
 Kristen Kyle Morgan  
 Anne Moscato  
 Kelly Margaret Moyes  
 Shreya Mozumder  
 Vance Murphy  
 Michael C. Nelson  
 Terehas Nelson  
 Samuel John Njoku  
 Gaddiel E. Nkrumah  
 Pamela A. Nkwocha  
 Lucy Nzei  
 Ndid C. Obicheta  
 Lauren O'Brien  
 Henry Ododah  
 Sakine Oezcan  
 Jacqueline Ogden  
 Julien Ogden  
 Muiyiwa Ogunjobi  
 Olumide John Ogunjobi  
 Scott OKeefe  
 Nancy Olguin  
 Brady Olson  
 Catherine Orfanos  
 Suzi Isedua Oriaifo  
 Michelle Osofsky  
 Simon Alexander Ospenson  
 Julie Paben  
 Suzanne B. Panagopoulos  
 Cueme Parker

Gregory D. Pashayan  
 Hiral Patel  
 Herbert Pau  
 Andre Payan  
 Rui Pereira  
 Kelbi Perkins  
 Jamie Pfanstiehl  
 Cesar Pineda Contreras  
 Michele L. Pitta  
 Lilliana Posada  
 Christian Presto  
 Scott Preston  
 Suman Priya  
 Mingming Pu  
 Gina Pye  
 Jennifer Ragsdale  
 Kennedy Reed-Hoster  
 Amie Reilly  
 Leah Reitmeier  
 Maria Belen Revel  
 Hector M. Reyes  
 Mochamad Reza  
 Chanay Richardson  
 Shimon Richmond  
 Heather N. Riley  
 Ariel Rivero  
 Sharmaine D. Robergeau  
 Jarrett Miles Cash Robinson  
 Sandra Roever  
 Veronica Roman  
 Caesar Romero  
 Steven A. Rosen  
 Alex Ross  
 Danielle Rowekamp  
 Amanda Marie Salasek  
 Luke Salyer  
 Adriana Sanchez  
 Sylvia Sanchez  
 Hari S. S. Venkatachalam  
 Ean Schmitt  
 Ryan Michael Schobert  
 Jesse David Scoular  
 Nathan Segal  
 Dea Semini  
 LeShell Session  
 Vijay Shanker  
 Andy Shanks  
 Ashutosh Sharma  
 Yehia Shalbaya  
 James Sheridan  
 Christopher Sidler  
 Tara Skinner  
 Jennifer Smith  
 Chad Paul Snyder  
 Juliana Ugaya Soileau  
 Krystal M. Somers

Jason Soto  
 Tristan Souness-Wilson  
 Anna O. Stallings  
 Mikel Stevens  
 Sean Stevens  
 William Stewart  
 Michele Struckman  
 Premkumar Subramanian  
 Sunita N. Sugrim  
 Joann Tang  
 Alyssa Tascione  
 Theodore Taylor  
 Brittany Teefey  
 Zach Tekely  
 John Charles Thomas  
 Stefan Ozziel Trevino  
 Fei Ching Tseng  
 Khurath Ul Ain  
 Reecha Upadhyaya  
 Roy Varghese Varghese  
 Cynthia Vasquez  
 Susana Vasquez Franco  
 Raymond Villanueva  
 Bradley Voight  
 Robert Voorhis  
 Robert C. Vreeland  
 Greg Wagner  
 Carrie M. Walchko  
 Reyn Watanabe  
 Jennifer Weinberg  
 Claudia Weinstein  
 Jonathan Glen Wells  
 Hana Wharton  
 Christopher James Wheatley  
 Antoinette Woolner  
 Jason Worley  
 Carrie L. Worthington  
 Tiantian Xiao  
 Jung Eun Yoo  
 Justin M. Zavis  
 Yihan Zhang  
 Crystal Zimmerman  
 Renata M. Zloza

## 越南

Thu Tra Nguyen  
 Thao Minh Tran

## 也门

Osama Omer Ali Mohammed  
 Hussein A. AlMehdhar

## 赞比亚

Sibeso Mutumweno





# 国际制裁合规师 (CGSS) 毕业生： 5月-7月

## 亚美尼亚

Zaruhi Badalyan

## 澳大利亚

Say Pheng (Sophia) Foo

Jun Li

Venkatesh Nathilvar

Qiang Sun

## 巴林

Imtiaz Ahmad

Rajnish Ranjan

Muhamad Nizam Bin Shaidon

## 孟加拉国

Mohammad A. Al Mamun

## 比利时

Frederic Jadot

Geoffrey Max Lepage

## 加拿大

Jinhe Li

## 中国大陆

Yu Bai 柏玉

Ning Bu 卜宁

Lijuan Cai 蔡丽娟

Yinzhu Cai 蔡银珠

Rui Cao 睿曹

Yue Cao 曹玥

Jinxi Chang 常晋曦

Hongwei Chen 陈宏微

Ting Chen 陈婷

Xue Chen 陈雪

Anqi Chou 俞安琪

Ruoyan Fan 范若言

Huaqiang Fang 方华强

Xiangli Ge 葛向丽

Jiayan Guo 郭佳焱

Qian Guo 郭倩

Wenli Guo 郭文莉

Fang Hao 郝放

Peng Hao 郝澎

Keqing He 贺克青

Yuanwei He 何苑维

Qi Huang 黄琪

Wei Huang 黄玮

Wenjing Huang 黄文景

Yanbing Huang 黄燕冰

Ying Huang 黄莹

Zhuojun Ji 计卓君

Ling Jiang 江玲

Xia Kang 康霞

Beidi Li 李贝迪

Carter Li 李承雨

Jing Li 李晶

Na Li 李娜

Pan Li 李盼

Rong Li 李荣

Wei Li 李蔚

Yue Li 李月

He Lian 廉何

Jing Liang 梁静

Juan Lin 林娟

Yun Lin 林云

Min Ling 凌敏

Guanhao Liu 刘冠豪

Haonan Liu 刘浩楠

Juan Liu 刘娟

Xiangning Liu 刘湘宁

Yanbin Liu 刘彦斌

Yitian Liu 刘依恬

Dan Lu 卢丹

Mei Luo 罗梅

Difang Lv 吕迪芳

Xiao Ma 马潇

Ying Ma 马莹

Yiwei Miao 缪一薇

Xingkang Ni 倪邢康

Zhiwei Niu 牛志伟

Rui Pan 潘蕊

Yanmei Pei 裴艳梅

Feifei Qiao 乔斐斐

Wenjiao Qin 秦雯娇

Yifeng Qiu 邱一峰

Yan Ren 任燕

Jian Shuai 帅剑

Bo Song 宋博

Kaijun Su 苏凯军

Liting Sun 孙莉婷

Jing Tan 谭晶

Xinwei Tan 谭新惟

Lian Tang 唐炼

Qi Tang 汤奇

Zhen Kun Tu 涂振堃

Chen Wang 王辰

Hongtao Wang 王红涛

Wei Wang 王唯

Xueping Wang 王雪平

Yanhong Wang 王妍弘

Yuan Wang 王园

Jun Xia 夏俊

Jieyan Xiang 向杰燕

Bingchao Xu 徐秉超

Guangda Xu 许广达

Yuxue Xu 许玉雪

Xiaoting Yang 杨晓婷

Qing Ye 叶青

Chuan Yin 殷川

Xuan Yin 尹璇

Min Yu 于敏

Yueqing Zeng 曾玥青

Naihong Zhang 张奶红

Qiongyue Zhang 张琼月

Yilu Zhang 张艺露

Nan Zhao 赵楠

Yingjiao Zhen 甄莹姣

Shiting Zhong 钟诗婷

Qianyu Zhou 周倩宇

Xiaoying Zhu 朱筱鹰

## 丹麦

Jeffrey Nielsen

## 埃及

Noha Ashraf M. A. Megid

## 芬兰

Mark Bossmann

## 法国

Alberic Botella

Julien Gallo

## 德国

Ruiya Fu

Antonio Stoyanov

## 希腊

Anna Damaskou

## 香港特区

Hau Ying Hollister Chan

Ying Kit Chan

Man Kit Cheung

Wai Lung Chung

Zhenwei Dai

Ting Wai Ho

Bing Hu

Ming Wai Lee

Yuen Shan So

Shing-Yan Tse

Alexey Tyurin

Chi Yin Yau

Aizhen Yu

## 印度

Ravi Chandel

Naveender Singh S

Rohan S Srihari

## 意大利

Marcella Binda

## 日本

Yasuhisa Furuta

Kasahara Kenichiro

Noriko Nakane

Saori Ohira

Muramatsu Osamu

Makoto Sato

## 科威特

John Simon

## 拉脱维亚

Laura Kalnina

## 黎巴嫩

Rita Fares

Khaled Haidar

Myriam Khairallah

## 墨西哥

Tania Balanzario Meraz

Miriam Guillermo Blancas

Benjamin Serra Cruz

## 荷兰

Inbal Djalovski

Ruofei Shen

Erdem Tascilar

Annemarie Verkerk

## 新西兰

Jatin Kumar Mistry

Rani Pillay

Minyu Zheng

## 尼日利亚

Babatunde Olaoluwa Macaulay

## 挪威

Eva Helena Deinoff

Eivind Parr Ohme

## 巴基斯坦

Nasir Mehmood

## 菲律宾

Frances Lynette Sayson

## 波兰

Wenbin He

## 波多黎各

Luis Miguel G. Hernández

Natalia Rodriguez

## 卡塔尔

Muhammad Shahid Farid

Neil Scully

## 俄罗斯

Aleksei Andreevich Pana

## 新加坡

Alkhaff Akthar

Ming Quan Wesley Ang

Qiyang Kenneth Boey

Sau Young Chung

Vijay Gopaladesikan

Weiliang Hu

Janet Gek Lang Low

Soon Hwee Tee

Sok Mun Wan

Raymond Wong

Siew Peng Woo

Xiaoqian Zhao

## 韩国

Dongyeop Hyun

Ping Ji

Jaekyung Kim

Jeongeun Park

Zongrui Yin

## 瑞士

Xavier Charles Didier Béard

Aliaksandra Hurynovich

## 台湾地区

Chih-Feng Chung 鍾至豐

## 土耳其

Melik Bagis Bilici

Bilal Ertogrul

## 阿联酋

Monqez Alrass

Jamie Belino

Jyoti Das

Asmaa Youssef Ali Elalawy

Gurminder Harinder Singh

Amritha John

Amit Kumar

Suranga Buddhike Marcus

Rasha Mortada

Rima Mourad

Sudhakar Sanjeevi

Michael Wong

## 英国

Jane Alimonda

Julie Choudhury

Clare Anne Davies

Monica Handoo

Kevin Penter

Mark Sallis

## 美国

Julio Gabriel Borrás

S. A. L. Broekaart-Hjalber

David Cellante

Alexander Chan

Bin Chi

Harry Paul Cupp

Michelle Alexandra Dominguez

Terence Egan

Sam Adam Elnagdy

Eva Errico

Jiang Q. Huang

Clara Kim

Elizabeth A. Larson

Laura Larson

Jianyu Li

Lin Li

John Victor Medina

Dimitri Michaloutsos

Aya Muto

Sissy Maite Oliver

Yiqiong Pan

Francisca E. Peralta

Steffy Shaji

Eugenia Shraga

Diana Sirila

Michael A. Tooshi

Bieu Bu Tran

Yu Xu





公认反洗钱师协会®

# CAMS 进阶资格认证



公认反洗钱审计师 (CAMS-AUDIT) 进阶资格认证  
是一项高级专业认证，专门面向开展反洗钱  
审计工作以及独立检测反金融犯罪控制措施的  
专业人士。

了解更多

[www.acams.org/cams-audit](http://www.acams.org/cams-audit)



# ACAMS WEBINARS

公认反洗钱师协会。

完全在线的会议，满足您即时的培训要求。  
听业内专家讲述大多数复杂金融犯罪问题，  
了解金融犯罪趋势、全球制裁最新情况以及  
监管变化。

了解详情，请访问 ACAMS 官网或通过电邮  
联系我们： [apac@acams.org](mailto:apac@acams.org)

参加我们的下一次网络研讨会：  
[www.acams.org/webinars](http://www.acams.org/webinars)

