ACAMS TODAY

年 會 專 刊

《今日 ACAMS》—— 事業型防制洗錢專家的專業期刊

勒索軟體：
數位戰場

本期相關文章：

911：
20 年的旅程

第 20 卷 第 4 期 | 2021 年 9 月 - 11 月號
公認反洗錢師協會® (ACAMS®) 出版
acams.org | acamstoday.org

ACAMS
公認反洗錢師協會

金融科技法遵職能證書 (CAFCA)

由金融科技企業，針對金融科技企業所開發。由防範金融犯罪專員組成的全球最大會員組織提供認證。

瞭解更多資訊，請到訪：
acams.org/cafca

CERTIFIED
CAFCA
AML FINTECH COMPLIANCE ASSOCIATE

ACAMS WEBINARS

公認反洗錢師協會

採用線上形式，滿足您的培訓要求。聽取業界專家講述複雜金融犯罪問題，掌握金融犯罪趨勢、全球制裁最新情況，以及監管變化等。

參加我們下一場網絡研討會：
www.acams.org/webinars

ACAMS
公認反洗錢師協會

ACAMS TODAY

《今日 ACAMS》—— 事業型防制洗錢專家的專業期刊

編輯總監
Kieran Beer, CAMS

總編輯
Karla Monterrosa-Yancey, CAMS

編輯與設計

編輯：
Stephanie Trejos, CAMS

國際編輯：
Monica Mendez, CAMS

創意與設計：
Victoria Racine
Joya Jones

編輯團隊

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

高階管理團隊

主席兼董事總經理：
Scott Liles

課程開發和行銷副總裁：
Angela Salter

全球人力資源總監：
Bill Lumani

全球銷售副總裁：
David Karl

集團副總裁與全球協會事業拓展執行長：
Hue Dang, CAMS-Audit

全球戰略溝通副總裁：
Lash Kaur

融資和全球營運副總裁：
Mariah Gause

資深全球制裁與風險主管：
Justine Walker

中文版審閱

鄧芳慧 (Hue Dang), CAMS-Audit
許朧方 (Joyce Hsu), CAMS-FCI

諮詢委員會

委員會聯合主席：Rick A. Small, CAMS
委員會聯合主席：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 McDonell, CAMS
Karim A. Rajwani, CAMS
Anthony L. Rodriguez, CAMS, CPA
John Smith

諮詢委員會（繼續）

Daniel D. Soto, CAMS
Dan Stipano
Philippe Vollot

內部撰稿人

歐洲、中東和非洲地區防制洗錢法遵策略總監：
Shilpa Arora, CAMS

美洲防制洗錢部門高級總監：
Lauren Kohr, CAMS-FCI

亞太地區防制洗錢法遵策略總監：
Rosalind Lazar, CAMS

中國防制洗錢法遵策略總監：
李娜 (Lynn Li), CAMS-Audit

區域銷售代表

業務開發高級副總裁：
Geoffrey Chunowitz, CAMS

美洲、加拿大和拉丁美洲銷售總監：
Sonia Leon, CAMS-Audit
Gerald Sandt

策略性客戶總監：
Jose Victor Lewis, CAMS

歐洲銷售總監：
Paolo Munari

中東和非洲銷售總監：
Michel Nassif

加勒比地區執行長：
Denise Perez, CAMS

贊助和廣告開發總監：
Andrea Winter, CAMS

澳大利亞業務開發區域總監：
Nick Griffith

南亞 / 東南亞和日本業務開發區域總監：
Christine Lim

北亞業務開發區域總監：
楊智全 (Yokel Yeung), CAMS

中國區首席代表：
郭榮軍 (Jerry Guo), CAMS

ACAMS 全球總部
芝加哥 +1-305-373 0020

ACAMS 亞太區總部
香港 +852-3750 7684 / 7694 / 7658

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

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

如要刊登廣告，請聯繫：Andrea Winter
電話：1-305-373-0020（分機 3030）
電子郵件：sponsorsandexhibitors@acams.org

*《今日 ACAMS》*是一本屢獲殊榮的雜誌，旨在提供正確、具權威的關於國際洗錢控制及其相關主題的信息。發表之文章並不代表作者或本協會參與提供法律或其他專業服務。如需要協助，請尋求專業人士提供服務。*《今日 ACAMS》*每年為 ACAMS 會員出版四期。

ACAMS

將廣告放在這裡

登上《今日 ACAMS》，並且接觸超過 86,000 名防範金融犯罪成員網絡。

如需在《今日 ACAMS》刊登廣告，請聯絡：

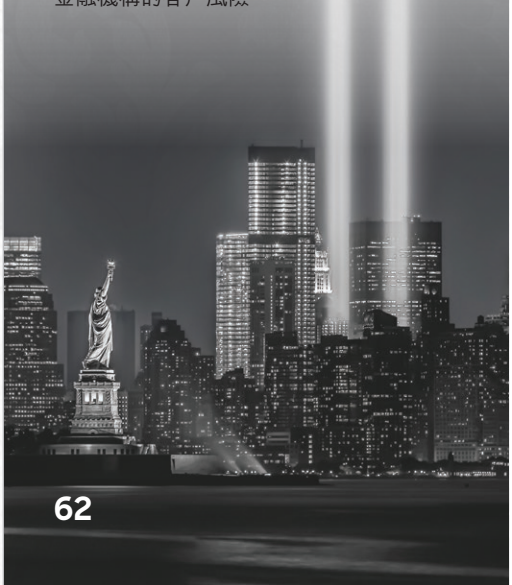
Andrea Winter
1.786.871.3030
awinter@acams.org

ACAMS TODAY

目錄

插圖作者：Milos Hall

封面：



911 的反思

今年是美國本土最嚴重恐怖攻擊事件 20 周年。我們還記得聽到這個消息的時候，我們在哪裡。我當時住在落磯山脈，正跨進車裡準備開車去上班。我打開收音機，聽說一架飛機撞上了雙子星大樓。起初，我以為聽錯了。我換了一個電臺，但聽到相同的消息，開車上班時仍震驚不已。一到公司，我就發現同事們也是滿臉震驚。我們都擠在電腦屏幕前，像瘋了一樣，想找到更多的最新消息，瞭解事態發展。我們看到，第二架飛機撞上雙子星大樓，南塔倒了。我有個同事的家人正好在飛機上，她非常焦急，想知道親人的飛機發生了什麼事。全世界都難以置信，我認識的每個人都開始問同樣的問題。美國本土怎麼可能發生這種事？難道沒出現過警示信號？我們怎麼毫無準備？

毫無疑問，911 事件對我們生活的許多方面產生了深遠的影響。尤其是改變了銀行業和所有金融機構。911 事件促使美國頒佈了美國《愛國者法案》，當時最具顛覆性的法規。防制洗錢 (AML) 和打擊資恐 (TF) 成為每個人的首要任務。公營和私營機構需要合作，同時必須改善有關記錄保存和「了解您的客戶」的規定，才能成功打擊洗錢和資恐活動。《愛國者法案》最重要的成就是推動了美國和全球偵查和遏止資助恐怖活動的進程。

當我們反思 911 事件發生以來，過去 20 年間發生的事情，不僅是法規遵循行業，甚至對全世界，我們要問的是，在打擊金融犯罪方面，我們是否有進步？我相信有長足進步。我認為整個行業在不斷發展，作為 ACAMS 會員和防範金融犯罪專業人士，我們都在貢獻自己的力量，不斷打擊洗錢和資恐活動。雖然新技術使打擊犯罪分子的戰爭發生了變化，但目標始終未變——即戰勝「壞人」。標題文章《勒索軟體：數位戰場》探討了我們如今面臨的最大威脅之一——網路犯罪。該文對 Colonial Pipeline 案例進行了分析。在美國司法部將網路入侵視為與反恐調查同等重要後，文章中有些說法可謂一針見血。作者稱：

> 「執法機關的轉變可能標誌著 20 多年來國家安全政策的首次轉向——承認「911」已經成為過去，恐怖分子、網路犯罪者和流氓國家行為者已進入數位戰場。」

顯然，在這 20 年裡，我們大有進步，但還有許多未盡之事。

無獨有偶，ACAMS 也迎來了 20 年華誕。為此，《*今日 ACAMS*》請到兩位頂級領域專家，董事及前董事 Rick Small 和 Lauren Kohr。他們分享了過去 20 年裡影響防範金融犯罪行業的 20 大顛覆性事件。不出所料，2001 年 9 月 11 日發生的事件被他們列為榜首。閱讀相關文章，深入瞭解他們的想法，以及他們對未來重要事件的預測。

年會專刊內容豐富，包括新的舉報人制度、加密貨幣退場騙局、911 的影響、出口管制、捐贈者建議基金、賭場與洗錢、成功通過稽核等。

希望您能加入我們，共迎 ACAMS 20 周年華誕。這些慶祝活動將貫穿整年，持續到 2022 年，還會在 2022 年 3 - 5 月專闢周年紀念專刊，共賀《*今日 ACAMS*》成立 20 周年。請繼續關注，瞭解更多有關慶祝計劃的細節。

在 911 事件 20 週年之際，讓我們花點時間，記住在那個悲慘的日子裡失去生命的人們，並向他們致敬。讓我們記住在那個可怕的日子裡，冒著生命危險，甚至不惜犧牲自己挽救生命的救難人員，也向他們致敬。

Karla Monterrosa-Yancey，CAMS
總編輯
歡迎追蹤我們的 Twitter 帳號：
@acamstoday

聯合 175 個國家或地區的防範金融犯罪社群

訪問
acamsconferences.org，
參加當地會議

ACAMS CONFERENCES

Sandra Edun-Watler，CAMS
開曼群島

Sandra Edun-Watler 是開曼群島 Mourant Governance Services 的一名律師兼法規遵循與報告部主管，負責為開曼群島實體提供防制洗錢和自動資訊交換報告及法規遵循專員服務。

在加入國際律師事務所 Walkers 之前，Edun-Watler 曾在開曼群島金融管理局擔任法律顧問。在 Walkers 工作期間，她先後擔任多個職位，包括擔任開曼群島、英屬維京群島和百慕達辦事處法規遵循事務主管。此外，她還以法規律師身分為客戶提供建議，在設立和發起防制洗錢專員服務方面發揮了重要作用。

Edun-Watler 在防制洗錢和法規遵循職能的各個方面均有豐富的知識和實踐經驗。她目前擔任開曼群島法規遵循協會主席、開曼群島法律從業者協會防制洗錢指導小組副主席，並且是加勒比地區法規遵循協會會員和前任主席。此外，Edun-Watler 還曾擔任加勒比海防制洗錢工作組織英屬維京群島第三輪互評工作的法律評估員。她目前還在杜魯門博登法學院任防制洗錢客座講師，代表開曼群島法規遵循協會在多個工作小組任職。

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

Muhammad Rizwan Khan 因對防範金融犯罪領域的傑出貢獻而廣受認可。Khan 已獲得 ACAMS 的多項法規遵循認證，包括公認反洗錢師 (CAMS)、交易監控認證專員 (CTMA)、客戶盡職調查認證專員 (CKYCA)、國際制裁合規師 (CGSS) 和高級公認反洗錢金融犯罪調查師 (CAMS-FCI)。他目前就讀牛津大學賽德商學院，攻讀組織領導文憑課程。

Khan 目前在阿拉伯聯合大公國 Al Dhahery 貨幣兌換所擔任總經理，負責執行偵查和防範金融犯罪的最佳作法。

Khan 在防制洗錢和打擊資助恐怖活動領域擁有豐富的經驗。作為法規遵循專業人士，他專注為貨幣服務業和銀行提供金融犯罪和洗錢的獨立審查服務。他的專業知識還包括獨立審查和調查、威脅 / 風險評估、國內外培訓、指導、專家證詞及制定防制洗錢制度體系等。Khan 在眾多國際學術法規遵循論壇上發佈過大量文章，被公認為該領域的世界頂級專家之一。

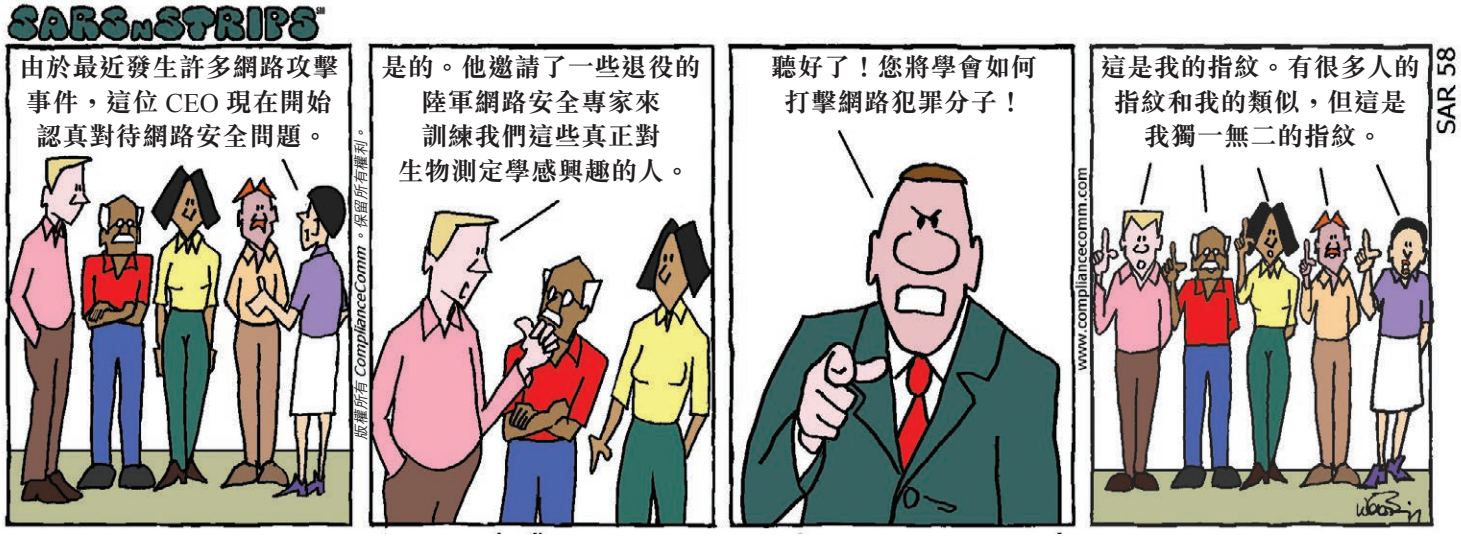
Howard Spieler，CAMS
美國紐約

Howard Spieler 是 ACAMS 紐約分會聯合主席，擁有近 20 年的法規遵循相關工作經驗。在整個職業生涯中，他針對防範金融犯罪和其他法規遵循風險領域的適用法律、監管和政策要求，為眾多企業和其他利益相關部門或機構提供指導和監督服務。

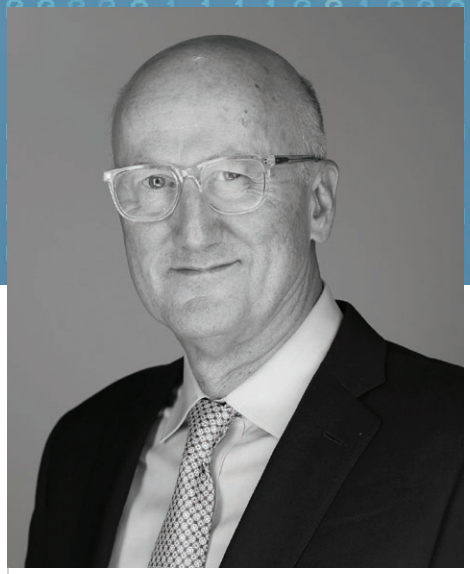
Spieler 目前任三菱日聯金融集團全球制裁法規遵循副總裁，作為制裁領域專家，為各種程序性倡議提供支援，包括風險評估、國內及全球產品審查等。此前，他曾在花旗銀行和美國國際集團擔任防範金融犯罪職務，為全球利益相關的部門或機構提供專業諮詢服務。

在此之前，Spieler 在彭博行政部門工作了 10 年，其中 7 年在紐約市經濟發展公司擔任法規遵循主管，協助制定和實施風險為本的法規遵循制度體系。他曾負責持續監督和評估價值 300 億美元的公私房地產交易組合，包括管理監管報告。

Spieler 撰寫了《A Global Review of Sanctioned Countries》（受制裁國全球評論）和《The Impact of the U.S. President on Economic Sanctions》（美國總統對經濟制裁的影響），兩篇文章均發表於《*今日 ACAMS*》。他是公認反洗錢師 (CAMS) 和公認國際制裁法規遵循專員 (ISCO)。Spieler 擁有肯恩大學會計學碩士學位、聖約翰大學工商管理碩士學位和紐約州立大學奧爾巴尼分校政治學學士學位。



二十年後：我們失去了什麼，得到了什麼？



大多數人都能清楚地回憶起2001年9月11日，20年前的那天我們在哪裡。

上午8點46分，一架小型飛機撞上了世貿中心北塔，起初，許多人都以為事故是因飛機偏離航線所致。但9點03分，又一架飛機撞上了南塔，很明顯是美國受到了攻擊。

上午9點59分，在曼哈頓中城的*彭博新聞台*，滿牆屏幕顯示南塔倒塌，見此情景，我站立不穩，跪倒在地。一位負責迎賓的女士跑過來問我是否還好。「我沒事，但成千上萬的人剛剛失去了性命」，我記得當時是這樣回答的。

從我們位於布魯克林的家中可以清楚地看到曼哈頓下城的天際線，而那天，我妻子只能看到雙子塔所在地的滾滾濃煙。但她記得，在與佛羅里達的父母通電話時，聽媽媽說有一座塔倒了的時候，她說「別瞎說」。

北塔於上午10點28分倒塌。

當天死亡的近3,000人來自不同的種族、宗教和社會經濟階層，就像美國本身一樣。

一位前同事回憶起與一大群人一起逃離布魯克林大橋的經歷，許多人全身都是建築物的煤灰和塵土。飛機在頭頂呼嘯而過時，每個人都非常害怕，聽到有人喊「是我們的飛機，是我們的飛機」時才鬆一口氣。

上午9點37分，第三架飛機撞上五角大樓，10點03分，飛往國會大廈或白宮的第四架飛機墜毀在賓夕法尼亞州的一塊田地裡，因為乘客衝進了被恐怖分子控制的駕駛艙。

這些恐怖攻擊改變了全世界，但世界也因我們對恐攻的回應而改變。

全美國及世界各地的大小社區和各級政府開始並肩團結。

我附近的鄰居、朋友們盡其所能互相安慰，幫助家人尋找失蹤者。醫院的櫃台人員屢屢被要求檢查或再次檢查入院記錄時，他們從未不耐。

我們看到，共和黨人和民主黨人在大多數情況下都站在同一陣線。到10月，成立了一個兩黨委員會，希望從恐攻中汲取教訓，有關財務透明的各種不同提案，以及先前遇到政治障礙的監督條款都一併簽署立法，成為美國《愛國者法案》的一部分。

在本期雜誌中，911之後成立的美國聯邦調查局打擊資恐行動小組(TFOS)第一任科長Dennis Lormel回顧了反恐措施彰顯的決心和團結，尤其是建立起公私合作的資訊共享機制。

這些合作機制恰巧誕生於ACAMS構想成形之時。一個小型的媒體和會議組織Alert Global Media萌生了想法，對防制洗錢和打擊資恐專業人士進行認證，建立一個專業協會，作為資訊集散中心和分享新想法以及最佳實踐的平臺。現在，ACAMS在全球擁有超過83,000名會員，《*今日ACAMS*》的2022年3月至5月號季刊將慶祝20週年慶。有關慶祝活動的更多資訊，請參閱總編輯的信。

除了完整的執法機關職涯歷練，Lormel後續亦曾擔任顧問並在ACAMS出任顧問委員會成員，並且呼籲我們在911恐攻的共同經歷基礎之上，努力延續並保有當時的反恐緊張感和勵精圖治。

隨著塔利班在阿富汗重新掌權，以及新型恐怖主義威脅的興起，包括來自國內極端分子，特別是抱持種族或民族動機的暴力極端分子(RMVE)的威脅，這一請求使我們倍感辛酸。

儘管當時建立的一些重要聯盟仍有強大實力，時至今日，美國乃至整個世界都不像911事件後那樣對恐怖主義同仇敵愾。

然而，只要回想起我們在911中失去的東西，以及我們團結一致可以獲得什麼，就會發現，下定決心勵精圖治以及ACAMS的全球使命有多重要。

Kieran S Beer

Kieran Beer，CAMS
首席分析師，編輯總監
歡迎關注我的Twitter帳號：
@KieranBeer
"Financial Crime Matters with Kieran Beer"（Kieran Beer談金融犯罪問題）

開啟線上學習之旅

ACAMS 專題培訓助您打擊金融犯罪。

瀏覽 **www.acams.org**，瞭解 ACAMS 推出的

多種線上認證、證書課程，以及免費數位學習內容。

#OnlineWithACAMS

ACAMS
公認反洗錢師協會

非營利組織：

瞭解捐贈人的資產來源

插圖作者：Joya Jones

人們透過防範金融犯罪專家瞭解洗錢新趨勢的時候，通常不會考慮非營利部門和非營利組織 (NPO) 在促進非法交易方面的風險。

在為社會弱勢族群提供財務支援方面，非營利組織發揮著至關重要的作用；然而，由於缺乏「了解您的捐贈人」(KYD) 政策，而且捐贈人建議基金 (DAF) 的複合資產贈與行為近期顯著增長，非營利組織有可能成為複雜洗錢計劃的實施對象。

瞭解捐贈人建議基金

在非營利組織當中，捐贈人建議基金越來越受歡迎，這種捐贈工具通常簡稱為 DAF。據富達慈善基金會表示，[1] DAF 因建立手續簡便，且享有慈善捐贈稅收優惠，在美國已經成為增長最快的慈善捐贈工具。

由於捐贈人可即時享受贈與稅收減免優惠，還能保留對捐贈資產的建議權，因此 DAF 越來越受歡迎。據美國國家慈善信託基金的資料顯示，[2] 2018 年至 2019 年間，管理資產規模從 1,220 億美元躍升至 1,420 億美元，增幅達 16.2%。《巴倫週刊》(Barrons) 近期報導稱，2018 年至 2019 年，DAF 的數量增長了 19.4%，增至 873,228 家，過去 10 年的增幅超過 300%。[3]

DAF 管理資產規模和帳戶數量快速增長，年增幅達 15%–20%，捐贈人透過複合資產進行捐贈的行為也日益複雜。據美國國家慈善信託基金，認為非流動性捐贈越來越受到 DAF 行業的歡迎。[4] 隨著越來越多的基金會和贊助組織紛紛建立自己的 DAF，不道德的捐贈人越來越有可能利用被忽視的小型基金會，贊助其他非法非營利組織（未實施「了解您的捐贈人」政策的組織）。

複合資產加深了盡職調查的複雜性

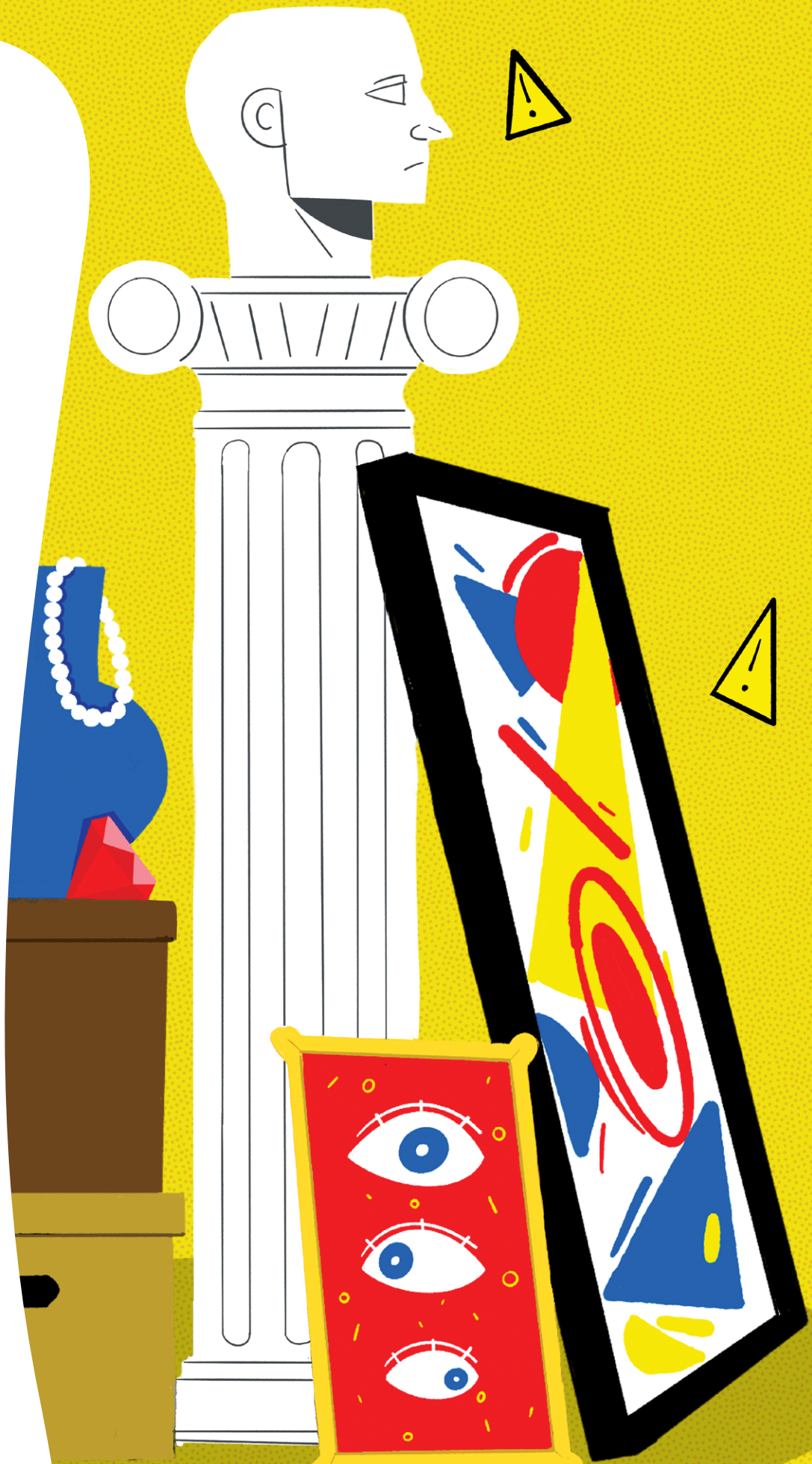
加密貨幣、非流動性私人基金等複雜金融工具紛紛進入非營利組織領域。2017 年，美國國家慈善信託基金管理的 DAF[5] 報告稱，非現金捐贈有所增加。在 2017 年調查的 60% 的捐贈資產中，有 60% 為非現金資產。這些資產包括公共和非公共有價證券、房地產，甚至藝術品。

這些複雜的另類資產捐贈帶來了更高的風險，有可能被誤解、未經審查及通過非營利機構傳遞出去。

案例分析

下面舉例說明，對 DAF 資產進行最低限度的審查就能找出跟上潮流的逃稅者，或者更糟的是，甚至發現恐怖主義的資助者。

捐贈人是一位非常成功的私營企業家。由於非營利組織依靠資產贈與生存，非營利組織更可能接受廣泛的資產類別和資產結構贈與，藉此推進其造福社會的非營利使命。該捐贈人特別希望向基金會捐贈另類資產，例如透過其私人銀行捐贈複雜的境外與境內對沖基金，其目的在於獲取贈與減稅優惠，享有向 DAF 建議資產最終贈與對象的資格。DAF 提供方接受該項捐贈，僅採取了最低限度的防制洗錢與打擊資助恐怖活動措施，由此成為捐贈人潛在非法交易的合法中間人。捐贈人知道，資產接收者是 DAF 提供方本身，因為現在資產歸基金會所有，不在捐贈人的名下。這樣一來，捐贈人就能將複合資產從其名下轉入金融系統，製造出更多複雜層次，進一步掩飾其潛在非法交易。



防制洗錢金融行動工作組織指導方針

2002 年 10 月，在發現高風險非營利組織普遍為非法交易提供便利之後，防制洗錢金融行動工作組織 (FATF)[6] 針對美國發生的 911 恐怖襲擊，採取了有力措施，大力打擊濫用非營利組織的行為。該工作組織提出了其 40 項建議中的第 8 條，讓人們加強認知非營利組織在全球打擊資助恐怖活動領域的潛在功能。

2014 年，防制洗錢金融行動工作組織進行了第三輪評估，[7] 審查各司法管轄區是否針對第 8 條建議落實法規遵循。在這次評估中，該工作組織發現這些高風險司法管轄區有 57% 不符合或僅部分符合第 8 條建議的規定。只有 5% 完全符合或基本符合該建議。

美國金融犯罪稽查局近期就非營利組織和慈善機構客戶盡職調查工作提供了指導方針

2020 年 11 月，美國金融犯罪稽查局與美國聯邦銀行機構聯合發佈了一份非常有用的情況說明，[8] 提醒商業銀行對慈善機構和其他非營利組織採取風險為本的方法。值得注意的是，美國並未將整個非營利部門列為「高風險」。但監管機構確實敦促金融機構考慮審查捐贈人。

非營利組織可以採取的措施

正如監管機構所指出，慈善機構和非營利組織應確保「了解您的捐贈人」政策實施到位。當今，非營利部門不斷發展壯大，非營利組織不應僅僅依靠金融機構「了解您的客戶」制度。

在接受複雜捐贈之前，非營利組織可以成為第一道防線，投入更多資源實施「了解您的捐贈人」政策和正式盡職調查程序。

在制定「了解您的捐贈人」政策時，非營利組織可以從下列問題出發：

- 捐贈人的地理位置在哪裡？
- 當前的受益所有人是誰？
- 捐贈人目前是否在美國財政部海外資產控制辦公室特別指定國民名單上？
- 贈與資產採用什麼結構？
- 贈與資產的目的是什麼？
- 贈與資產的最終接收人是誰？
- 捐贈人是否打算將資產捐贈給有海外業務的非營利組織？

如果非營利組織發現捐贈人逃避這些簡單的「了解您的捐贈人」問題，則在接受捐贈前應實施增強盡職調查。這種簡單的盡職調查可以維護非營利組織的誠信，提高其聲譽。

結語

隨著犯罪分子越來越瞭解日益流行的 DAF 及其匿名性，DAF 有可能成為非法交易的目標和掩蓋非法所得的工具。非營利組織可以多加詢問資產來源，在發現高風險時開展盡職調查，從而保護自身和所服務的弱勢群體。

Josh Ortner，CAMS，美國俄亥俄州

1 “What is a donor-advised fund?”（何為捐贈人建議基金？），*富達慈善基金會*，https://www.fidelitycharitable.org/guidance/philanthropy/what-is-a-donor-advised-fund.html

2 “The 2020 DAF Report”（2020 年度 DAF 報告），*美國國家慈善信託基金*，2020 年，https://www.nptrust.org/reports/daf-report/

3 Abby Schultz，“Donor-Advised Fund Assets Reach $142B, Grantmaking Hits $27B”（捐贈人建議基金管理資產達 1,420 億美元，捐贈金額達 270 億美元），*《巴倫週刊》*，2021 年 2 月 2 日，https://www.barrons.com/articles/donor-advised-fund-assets-reach-142b-grantmaking-hits-27b-01612298241

4 “2020 Donor-Advised Fund Report: Grants to Charities Increase 15% to $27 Billion and Total Charitable Assets Surpass $141 Billion”（2020 年度捐贈人建議基金報告：對慈善機構的捐贈增長 15%，至 270 億美元，慈善資產總額超過 1,410 億美元），*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

5 Eileen R. Heisman，“Findings from our 2018 Donor-Advised Fund Report”（2018 年度捐贈人建議基金報告的調查結果），*美國國家慈善信託基金*，2018 年 12 月 3 日，https://www.nptrust.org/philanthropic-resources/philanthropist/findings-from-our-2018-donor-advised-fund-report/

6 “Best Practices on Combating the Abuse of Non-Profit Organisations”（打擊非營利組織濫用行為的最佳實踐），*防制洗錢金融行動工作組織*，2015 年 6 月，https://www.fatf-gafi.org/publications/fatfrecommendations/documents/bpp-combating-abuse-npo.html

7 “Risk of Terrorist Abuse in Non-Profit Organisations”（非營利組織被恐怖主義濫用的風險），*防制洗錢金融行動工作組織*，2014 年 6 月，https://www.fatf-gafi.org/media/fatf/documents/reports/risk-of-terrorist-abuse-in-non-profit-organisations.pdf

8 “Joint Fact Sheet on Bank Secrecy Act Due Diligence Requirements for Charities and Non-Profit Organizations”（關於慈善機構和非營利組織的銀行保密法盡職調查要求的聯合情況說明），*美國聯邦儲備理事會*、*聯邦存款保險公司*、*金融犯罪稽查局*、*信用合作社管理局*、*美國貨幣監理署*，2020 年 11 月 19 日，https://www.fincen.gov/sites/default/files/shared/Charities%20Fact%20Sheet%2011_19_20.pdf

解謎：出口管制？

各國政府紛紛想方設法達成國家安全和外交政策目標，而監管重點也日漸轉向出口管制的法規遵循。長期以來，政府領導人一直把出口貨物管制作為工具，防止危險產品（如武器、化學品）進入普通銷售管道，防止戰略產品（如超級電腦、先進電子產品）落入敵方手中。隨著時間推移，出口管制形成了高風險的法規「拼圖」，一面要破解、一面要遵循，就像解謎一樣。《韋氏詞典》將謎語定義為「一種令人迷惑費解且具有誤導性的問題，提出來供人猜測解決。」許多金融法規遵循人員也許會用這個定義來描述出口管制；但其實無須對出口管制如此畏懼。無論貨物來自何方，去何處，出口管制只要解決四個謎題：產品是什麼？目的地在哪裡？收貨人是誰？出口原因為何？

淺顯說明出口管制

世界上任何國家的公民和企業都無權出口貨物，也沒有任何推定出口權，而是必須取得政府的出口許可。另一方面，沒有政府願意花時間和資源審查所有出口許可申請。為此，政府制定了出口管制規則，正如其名，這些規則旨在對本國 / 地區的出口貨物流動進行控制。出口管制規則和最佳實踐建議構成一個整體，表示政府試圖在「危險」和「不危險」兩類出口貨物、產品、技術和服務的控制上取得平衡。凡列入受控清單，均須取得出口許可，但這一要求僅限於某些情況。政府讓出口商自己確定在什麼情況下不需向政府申請出口許可證，在什麼情況下需要遵循全部出口管制規則。

在明確提出許可申請並取得出口許可證之後，出口商進行交易的情況仍持續變動且千變萬化。隨著商用和軍民兩用產品的發展、成熟和上市交易，出口管制也會隨之變化。此外，出口管制也會出於犯罪控制、外交政策、國家安全、國內經濟的需求，當然還有政治的考量而變化，有時甚至產生巨幅變化。出口法規、法令和法律判例多達數萬頁，內容令人迷惑費解，偶爾還有誤導的內容，當然在要求細節上也令人難以捉摸。這正是全球貿易法規遵循經理、董事及其員工必須通盤瞭解和採取行動的職責。對於偶爾參與出口管制

法規遵循工作的其他所有人來說，那些看似令人迷惑費解、偶爾具有誤導性的細節可以歸為四個簡單的謎題。知曉解謎之道是理解出口管制的關鍵。

謎題 1：出口的產品是什麼？

出口的產品類型對於解答出口管制的第一個謎題至關重要。如果裝運的是迴紋針、量尺或其他辦公用品，這類無害商品無需考慮安全或外交政策因素。因此，政府肯定不希望出口商就訂書機申請出口許可證。但對於特定產品類別（如導彈、彈藥、高端電腦和核原料），政府則要求出口商提交冗長而詳細的出口許可申請。在兩個極端類別之間還有很多產品，如醫藥、電子、電池、各種工業物品。所有實物商品分為兩類：出口管制商品和非出口管制商品。此外，支援出口管制商品的多數無形商品亦受管制，如售後服務電話、技術支援、軟體、加密技術和其他技術，這類無形商品的作用是使出口管制商品保持正常運行。如果某個商品、軟體或技術受管制，則針對每個出口國家 / 地區進行分類，分配一個出口管制號碼 (ECN)。這個指定的 ECN 決定了出口商的產品是否必須申請出口許可證。但在大量錯綜複雜的例外和豁免條件下，產品及其相關技術和服務也可能免除出口許可義務。要知道，出口管制法規遵循領域存在「抓放」原則，且仰賴全球貿易法規遵循團隊負責實際運作該框架。產品是什麼？本謎題的解答在商品的 ECN 中可找到。

謎題 2：目的地在哪裡？

瞭解與出口管制風險管理相關的風險是理解出口管制的一個重要方向。可以說，出口目的地與產品本身同等重要。值得一提的是，某項商品能出口並不表示其抵達目的地後可進口。基於地點的出口管制非常複雜，體現為制裁、禁運、條約授權、全國和多國的國別管制，以及機構一開始管理此類風險的意願。有些出口目的地受到嚴格限制，出口商根本不會去費心申請出口許可證，因為即使是不受管制的辦公用品也屬禁止範圍（比如美國對北韓、敘利亞和古巴的出口）。除嚴格管制商品、酷刑工具和大規模殺傷性武器外，針對其他國家或地區的出口管制屈指可數。在其他國家或地區，只有某些地區（如烏克蘭境內的克里米亞共和國）或特定地址（如海外資產控制辦公室和類似國際機構公佈的制裁清單所列地址）要求取得出口

許可證。但大多數國家或地區處於中間位置，出口許可證的必要性取決於產品（謎題 1），以及一大堆令人眼花繚亂多邊和雙邊規則，這些都由機構的全球貿易法規遵循團隊負責解讀。如果商品是要運往或轉運至伊朗，大型跨國商業出口商通常會陷入困境，部分原因是《伊朗貿易制裁條例》難以理解，增加了法規遵循管理難度。最後，許多以地點為基礎的出口管制在實施時不會考慮出口行為的實際發生地點，使得實務操作更加困難。為了應對這種（有時）伴隨難以理解的紛亂規則的風險，機構通常不僅依據政府的強制性規則，而且根據公司聲譽、改變目的地或用途、信用和不願意承擔的其他經營風險，制定各自的國別「禁運」管制措施。出口商品的目的地決定出口管制措施的實施，也是謎題 2 的謎底。

謎題 3：收貨人是誰？

這應該是防制金融犯罪人士最為熟悉的出口管制謎題。商業夥伴和交易對手制裁名單篩查、所有權結構分析、國有實體審查和軍事隸屬關係驗證，這些都是破解出口管制謎題的關鍵元素，就如金融犯罪分析的情況。如果機構透過盡職調查流程確定，潛在業務夥伴的財務供應鏈或整體法規遵循情況不符合標準，則不建議與該合作夥伴共同參與實體供應鏈。政府執法官員十分明確有力地傳遞此訊息。但解答謎題 3 不能僅停留在表面。

辦公用品，沒問題。制裁名單篩查，沒問題。從美國運往德國，沒問題。運給德國軍隊——有問題！本次出口交易涉及的產品和國家或地區不會觸發許可證要求，買方不是被制裁方，但軍事機構是「收貨人」的謎底，正是改變這筆交易有效出口管制規則的因素。雖然軍事最終用戶的條規最近才成為法規遵循新聞的頭條，但數十年來驗證最終用戶的政軍關係一直是出口管制的重點。儘管評估最終用戶相關業務類型費力又費時，卻是解答出口管制謎題的必備線索。

謎題 4：出口原因為何？

巴西一家孤兒院為什麼要買高端超級電腦？好問題，不查清楚就出口，後果要自負。除非在交易過程中出現這種紅旗警訊，否則大多數出口商不需要找出買家訂購產品的原因或產品的使用方式。出口商需要進行制裁和受限方篩查，根據產品進行軍事最終用途核查，對照國家 / 地區目的地清單比較產品的指定 ECN，視情況取得出口許可證，完成以國家 / 地區為基礎的風險核查。採取這些步驟可解答前三個出口管制的謎題。第四個謎題過去幾乎無需提出，但在當今緊張的法規遵循和風險緩釋環境下，則需要多提出。即使出口交易不涉及兩用（商用和潛在軍用）商品，也需如此。買家為什麼需要這一商品？預期用途是什麼？他們買此商品是否合理？購買量是否合理？他們從這家公司買是否合理？最終用途審查會造成多少商業干擾，帶來多少經營影響，這是個主觀問題。雖然軍用和軍民兩用商品出口商對此習以為常，但對大多數其他出口商來說，卻是個全新的概念。基礎總是很重要的，必須先解出前三個謎題：產品是什麼、目的地在哪裡、收貨人是誰，這些至關重要。決定是否進行最終用途驗證，端看這些因素不斷變化的結合和相互權衡作用。中斷出口交易以解答謎題 4 會耗費公司的時間和財力，使得本已十分龐雜的供應鏈變得更加複雜。

這些謎題不難解答，對吧？

雖然出口管制非常複雜，充滿法規遵循風險，但並不像看起來那麼令人生畏。如同任何風險為本的法規遵循制度體系一樣，出口管制就是要在保持業務發展及法規遵循之間取得平衡。這是風險為本出口管制法規遵循制度的首要目標，也是政府要求機構制定法規遵循制度體系的初衷。

Anne Marie Lacourse，
美國道瓊風險與法規遵循公司顧問，
annemarie@lacourse.us

ACAMS CERTIFICATES

公認反洗錢師協會

ACAMS 專題證書課程

滿足不同業務實際工作需求及不同規模法遵團隊所建立

ACAMS 證書課程以線上學習的模式，針對不同的防制洗錢犯罪專題，提供深入的培訓。證書課程適合各種規模的法遵團隊，也不僅限於初級及中級法遵專業人員，而且對於資深員工而言也是難得的再培訓或深化課程。


金融科技企業反洗錢基礎


反賄賂和貪污


反恐融資


網絡犯罪


道德操守


金融科技企業客戶


詐欺


《通用數據保護條例》和
《第四號反洗錢指令》


金融犯罪的調查


了解您的客戶 /
客戶盡職調查


了解您的客戶 /
客戶盡職調查 - 進階


風險評估


制裁基本原則課程


可疑活動報告寫作


貿易洗錢


交易監控

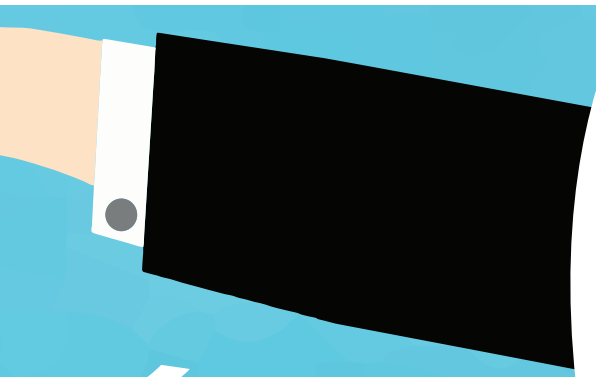

交易監控 — 進階


虛擬貨幣和區塊鏈

到 acams.org/certificates 了解更多 ACAMS 證書課程內容及最新上課日程

加密貨幣的退場騙局 (exit scam)

騙局解密及防騙攻略



多年來，加密貨幣一直是一個富爭議的話題，主要原因是有兩股力量在彼此博弈。一方是加密貨幣技術的信徒、未來主義者和創新者購買比特幣，[1] 並想方設法安全儲存比特幣。

另一方則是有些人瞄準受教育程度較低的人群，試圖利用他們知識匱乏的弱點，騙他們放棄加密貨幣。詐騙行為各式各樣，難以發現。

隨著加密貨幣的發展，這些騙局採用的手段也在不斷演進。退場騙局就是最難發現的一種騙局。那麼，退場騙局到底是什麼意思，如何避免成為當中受害者？本文將對退場騙局進行定義，並就如何防騙提出建議。

什麼是加密貨幣的退場騙局？

退場騙局指從市場上「撤出」所有資金，在加密貨幣早期投資者身上獲利的一種方式。換句話說，擁有特定新加密貨幣最大錢包者，試圖透過行銷和促銷活動人為抬高（哄抬）價格，最後將他們的個人包袱甩（傾銷）給新的投資者。

哪裡可以發現這樣的騙局？

2017 年，隨著首次募幣 (ICO) 快速發展，加密貨幣退場騙局大肆流行。前景良好的新專案利用其影響力和社群推廣即將推出的貨幣，承諾超高的回報率，後來卻逃避交付流程，卷款跑路。

最近，隨著加密貨幣領域的發展，出現了各種不同形式的「退場騙局」：

- 在去中心化交易所上市的去中心化金融相關專案存在極大的風險，因為這個領域到處都是「抽地毯」(rug pull) 騙局（另一種形式的退出騙局）。這種情況已發生多次，甚至在主流中心化交易所上市的貨幣也出現過這種騙局。例如，Iron Finance 近期的 TITAN 專案因獲得 Mark Cuban 的投資而大受歡迎。[2] 在被「抽地毯」後，Cuban 呼籲加強對加密貨幣領域的監管，[3] 但由於該領域具有去中心化特質，因而無法進行監管。
- 如今，只要粉絲足夠多，任何人都可以推出非同質化代幣 (NFT)，比如名人、YouTuber、運動員，數之不盡。現在，只要看到這個領域過度飽和的狀態，就會感覺 NFT 似乎代表著「無才無能」(No Freaking Talent)。然而，代幣售價通常達數十個以太幣，但大家對二級市場不感興趣時，最後卻喪失流動性。近期銷售的 Logan Paul 非同質化代幣就是其中一個例子，銷售時承諾向三名買家贈送價值 40,000 美元的第一版寶可夢卡以及其他獎品。該非同質化代幣最初估值超過 20,000 美元，但現在有一部分在 OpenSea 上的售價不到 1,000 美元，而且無人問津。[4]
- 最後，近來出現了一個非常有意思的概念，就是賣推特。換言之，人們可以買下名人推特的所有權，把它變成非同質化代幣。發佈幾天後，一位用戶用 639 美元買了一個推特，但這個推特帳號不久後卻被刪除了。[5] 這是一個真正的退場騙局。

保護自己，遠離退場騙局

在這個相對成熟階段進入該領域的大多數投資者可能想知道，如何才能有效地發現哪些專案合法，哪些不合法。就退場騙局而言，可以記住以下與投資策略有關的訣竅：

- 碰到喜歡的 YouTuber 推廣代幣（其價格通常已經處於高位），不要衝動購買，要先審查專案的基本面。專案通常只是現有解決方案的廉價「複製本」，欠缺支撐未來成長的堅實基礎。
- 當專案報酬率高於平均時，務必要進行調查研究。雖然有些專案可能合法，但仍有專案可能非常危險。更具體地說，一定要全面瞭解加密貨幣的權益質押、流動性挖礦 (yield farming) 和高收益儲蓄帳戶等知識。此外，要定期透過 CoinGecko 等價格追蹤平臺，獲取感興趣代幣的最新相關資訊和研究資料。
- 如果有感興趣的專案並有強烈的買入衝動，不妨等一等。至少等一周的時間，觀察價格走勢。很多時候，推廣者會使用局部高價

> 推廣代幣，有意買入的各方可以先讓市場冷靜下來，然後在更好的點位買入。

最重要的是，要知道當耐心持有加密貨幣時，其價值才會增加。雖然最愛的推特帳戶可能正憧憬著有 100 倍槓桿效應的小型貨幣，但如果秉承長期投資理念，實際獲利的機率則翻倍增加。

因此，儘管加密貨幣價格經常出現中期波動，但一定要明白贏家通吃的道理。[6] 投資比特幣、以太坊以及 UNI、BNB、FTT 等主流交易所的原生代幣。雖然價格在短中期內可能有波動，但現在有足夠的證據顯示，其長期呈現上升趨勢。即使情況不如預期，但此類專案的大量流動性使投資者能夠快速買賣持有的部份。這在 NFT 世界中是不可能的，因為在 NFT 世界中，用戶經常在市場下滑期間被昂貴的藝術品套牢，付出高昂代價，後悔不已。

在數位資產投資中，信心、流動性和現實情況仍然是最重要的因素。為免被騙，務必要秉承以下原則：「如果好得令人難以置信，很可能是騙局。」

Judy Smith，Paybis 行銷經理 / 作家，拉脫維亞，
smijudy33@gmail.com

1 “Buy Bitcoin with Credit Card or Debit Card”（用信用卡還是簽帳卡買比特幣），*paybis*，https://paybis.com/

2 Jeff Benson，“Mark Cuban ‘Hit’ by Apparent DeFi Rug Pull”（Mark Cuban 受到去中心化金融抽地毯騙局打擊），*Decrypt*，https://decrypt.co/73810/mark-cuban-hit-apparent-defi-rug-pull

3 Billy Bambrough，“Billionaire Bitcoin Investor Mark Cuban Calls For Crypto Regulation After Price Of Radical New Token Suddenly Crashes To Zero”（比特幣億萬富翁投資者 Mark Cuban 在激進新貨幣價格突然跌至零之後呼籲對加密貨幣進行監管），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

4 Geoff Weiss，“Logan Paul Sells $5 Million Worth Of NFTs Ahead Of His Pokémon Box Break”（Logan Paul 在寶可夢開箱活動前賣出了價值 500 萬美元的非同質化代幣），*Tubefilter*，2021 年 2 月 22 日，https://www.tubefilter.com/2021/02/22/logan-paul-sells-5-million-nfts-pokemon-box-break/

5 Jamie Redman，“NFT Immutability Debate Grows as Tokenized Tweets Get Deleted and NFT Images Are Replaced”（代幣化推特被刪，NFT 圖像被換，NFT 不變性引發更多爭議），*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/

6 “Prices”（價格），*paybis*，https://paybis.com/price/

ACAMS
公認反洗錢師協會

CGSS
CERTIFIED
GLOBAL SANCTIONS
SPECIALIST

國際制裁合規師 (CGSS)

考獲由公認反洗錢師協會 (ACAMS) 推出的全球認證 – CGSS，彰顯機構及其員工對遵守制裁法規，及建立專業制裁法規遵循團隊的決心。

下載考生手冊：**www.acams.org/cgss**

ACAMS
公認反洗錢師協會

資料對法規遵循和防範金融犯罪工作的影響

金融機構面臨的威脅持續增多，不僅如此，監管和法規遵循要求亦不斷變化，使業務環境越來越艱難。最近的一份報告指出，自 2019 年以來，全球罰款和處罰量增加了 141%，光是總部設在美國的金融機構就要支付 75 億美元的罰款。[1] 全球疫情只會繼續增加這些風險的數量，加快其速度，加劇其複雜性，因而對資料和真知灼見的需求急遽增加，以適當避免和緩釋風險。但太多的金融機構並不健全，無法正確管理資料，可能會帶來可怕的後果。

畢竟，資料是防範金融犯罪行業的命脈。若能以有效且高效的流程管理優質資料，金融機構的領導者就可成功履行職責。隨著世界開始從疫情中復甦，資料環境發生了明顯變化。促成這些變化的主因有兩個：

- **監管重點不斷演變：**國內和國際監管機構正在重塑和擴大其職權範圍。人們期望對新興技術進行審查、測試和部署。例如，美國 2020 年《防制洗錢法》(AMLA) 專門處理行業的技術能力問題。不出所料，隨著公司努力重組其技術和人力資源，以解決這些警報信號，金融機構在 2020 年和 2021 年的應變力有所減弱。
- **數量龐大且多樣化的資料是日益複雜的問題：**近年來，銀行和其他金融機構累積大量客戶和合作夥伴的資料。再加上來自暗網、加密貨幣和電子通信的資料，已形成新挑戰；既存的技術和工作流程原先就不是為這類資料來源和類型所設計，因此根本無法處理這類資料。

低效率的替代方案

業界對虛擬資料生態系統的依賴程度更勝以往，但傳統的資料來源及各自為政的資料分析老舊技術系統也承受著前所未有的壓力。許多金融機構採取了積極的數位化策略，部分是為了提高效率、加深與全球客戶的合作。但這些策略明顯增加了資料量，而已經不堪負荷的機構顯然缺乏能力去適當協調、解釋和採用這些資料。特別是對於金融機構而言，在各種新法規（例如，歐洲聯盟的《支付服務指令 2》）陸續出爐下，「了解您的客戶」和客戶盡職調查的要求越來越多，而金融機構遵循要求的能力亦受到直接影響。因此，金融機構現在必須採取額外措施去瞭解客戶的客戶。此類要求為現有技術和法規遵循工作帶來更大的壓力。

傳統的法規遵循解決方案依賴核心銀行系統及各地資料作業中心提供的批次資料或每日資料。在全世界已逐步邁向即時交易之際，這顯然會造成延遲；微秒內做出決策才能打擊機構面臨的許多威脅，不僅監管問題，也包含支付詐騙、網路攻擊等。

除了資料處理挑戰外，還有一個更大的問題：這些系統用於回答現有交易監控 (TM) 查核問題的分析策略存在不足。許多規則起源於上世紀 90 年代已知、所理解的非法犯罪活動，此後幾乎沒有更新。它們往往對所有客戶一視同仁，但客戶明明大有不同。況且，它們幾乎沒有納入或適當利用來自客戶盡職調查系統或其他開戶的風險指標，以及定期風險評估資料。這些規則易於與其他規則相互排斥。因此，它們無法根據完整的實體行為充分識別實體的總體風險。

結果如何？大量的雜訊產生誤報。誤報率最高達 90%，[2] 這顯示調查人員徒勞無功，運營成本高昂，甚至更糟：調查人員無法專注於識別金融機構面臨的真實複雜威脅，而這類威脅通常會因違規登上新聞頭條。雖然這不算是新問題，但大多數人還是認為誤報率不斷升高，導致調查人員需要處理的積壓工作越來越多。

問題的核心在於銀行客戶的相關資料，而且需要 360 度全方位瞭解客戶身分及其有效預測行為。以調高或調低靈敏度的方式變更警報門檻，將違背有效識別洗錢、詐欺或制裁違規行為的初衷。準確判斷何為合法客戶行為——基於可靠和完整的客戶相關資料，在風險評等矩陣中準確評分——是實現優質預防和有效法規遵循的唯一途徑。然而，找到這種平衡需要新的動態方法，而不是依賴負擔過重且各自為政的資料收集和交易監控系統提供過時的靜態資料分析。

相反，機構必須擺脫傳統的核心銀行交易監控模式，利用即時串流分析技術補強緩慢、過時的批次處理架構法。資料量與多樣的資料類型才能促進跨部門的資訊共享。擷取到資料後，需要有效的技術在微秒內分析資訊，並在適當的時機產生警報。

金融機構在一開始就部署有效的分析技術，就可以傳送分析結果去解決正在處理的各種「測試」問題。通常，許多架構相同的業務單位都必須回答這些問題。過往報告一直被「鎖在」單一的孤島式技術分析和報告環境中，現在許多業務單位之間可透過有效運用即時資料分析的結果，無縫地共享報告。使用更高效的資料擷取和儲存技術，來自於賦能和融合人工智慧 (AI)、機器學習或機器人流程自動化 (RPA) 得到的結果具有更大的價值。

結語

顯然，金融機構現在面臨的挑戰是評估當前的技術，確定這些技術能否或如何進行現代化和調整，以應對巨量資料的衝擊和不斷變化的威脅環境。以下步驟有助於為提升業務管理和風險防範能力設定基準：

1. 稽核現有的處理方法和實踐，找出問題的根本原因，包括接收的資料內容和接收方式，以確定資料品質與內容對最終結果的影響。這項稽核工作可由第三方諮詢機構與技術供應商共同執行。
2. 向內部團隊成員徵詢意見和見解，揭露現有技術的不足，然後啟動更新、更換或增強技術的專案工作。
3. 仔細審查關注業務單位要求的現有監管規定，確定必須立即解決的迫切需求，以避免處罰或強制糾正。考慮採用替代技術，改善處理方法、協助寶貴的人力資產更高效地執行任務來降低這種風險。
4. 投資串流分析技術，不僅可部署在核心銀行系統前端，亦可在支付處理管道主動應對風險，而非像目前採取「事已至此」的被動回應策略。
5. 採用進階分析技術進行異常偵測，找出現有規則無法識別的風險，發現先前未察覺且可能導致罰款的風險。
6. 增強現有的交易監控系統，在產生警報後，對「實體」進行 360 度全方位的行為風險分析，使用機器人流程自動化的第 1 級「分類」和第 2 級「處置」步驟，以減少雜訊、防止誤報並提高效率。最終會降低成本、識別真正的風險並使金融機構在監管機構面前維持良好信譽——最終避免受罰、股東價值損失和聲譽受損。

金融機構每天都要對抗破壞其技術基礎設施的企圖。勒索軟體攻擊和要求影響了金融機構、企業和政府實體的營運和應對方式。在美國和其他國家，國內恐怖分子的演變改變了金融機構識別個人及其資產的責任，這些資訊可能存在於客戶帳戶及其相關行為當中。

您是否已優化技術與法規遵循方法，做好準備迎接新的現實？

John Dalton，KX 資深副總裁兼金融服務產品與解決方案戰略部全球主管

Robert Goldfinger，CAMS，退役上尉，KX 金融犯罪技術銷售主管

[1] Jaclyn Jaegar，“Report: Fines against financial institutions hit $10.4B in 2020”（報告：2020 年對金融機構罰款金額達 104 億美元），*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

[2] Stuart Breslow 等，“The new frontier in anti-money laundering”（防制洗錢的新領域），*麥肯錫*，2017 年 11 月 7 日，https://www.mckinsey.com/business-functions/risk-and-resilience/our-insights/the-new-frontier-in-anti-money-laundering

勒索軟體、加密貨幣和洗錢之間的關係

2021 年 5 月，美國維吉尼亞州、喬治亞州和北卡羅來納州的汽車司機驚惶失措，爭先恐後地前往加油站加油，原因是 Colonial Pipeline 公司遭受網路攻擊，被迫關閉汽柴油和航空燃油供應，造成油荒。犯罪集團 Darkside 發動勒索軟體攻擊導致 Colonial Pipeline 營運中斷，要求支付 75 個比特幣（430 萬美元）的贖金。Colonial Pipeline 支付比特幣後，收到解密工具，解開被駭客入侵的系統。[1] 在 7 月 3 日發生的另一個案例中，連鎖超市品牌 Coop Sweden 旗下 500 家超市被迫停業，因為其銷售點收銀台和自助結帳櫃台停止工作。連鎖超市本身並非駭客攻擊的對象，但一家軟體供應商受到勒索軟體攻擊，因而被牽連波及。這家供應商警告所有客戶立即停止使用其服務並離線。[2]

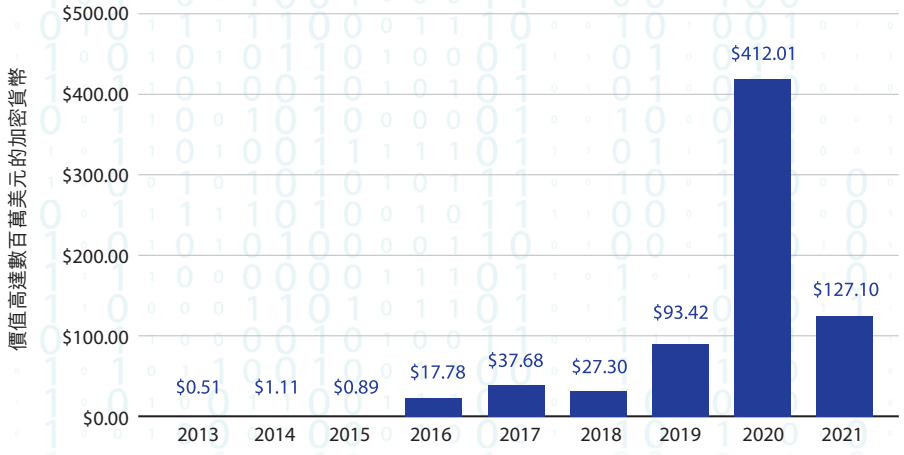
FBI 網路犯罪小組透過贖金追蹤到加密貨幣地址，追回了由 Colonial Pipeline 支付的 63.7 個比特幣（230 萬美元）。[3] 但 Colonial Pipeline 並不是唯一的受害者。被勒索軟體犯罪分子如 Ryuk / Conti、Sodin / REvil、Cl0p、DoppelPaymer、DarkSide 和 Avaddon 禍害的其他機構包括加拿大飛機製造商龐巴迪、華盛頓特區警察局、電子公司宏碁、科羅拉多大學、亞特蘭大市和巴爾的摩市、廣達電腦公司和 CNA 金融公司。勒索方式大多要求支付加密貨幣——亦稱為可兌換虛擬貨幣 (CVC)。加密貨幣是一種價值的數位表示方法、具備交換媒介、記帳單位和價值儲存功能。加密貨幣不由任何實體發行，亦不受監管。從事 CVC 交易者要自擔風險，並接受匯率的大幅波動。

加密貨幣對勒索軟體的誘惑

2020 年，超過 4 億美元的加密貨幣被匯入與勒索軟體犯罪分子有關的數位地址；執法機關、金融機構、保險公司和其他利益相關的部門或機構要注意這個趨勢（見圖 1）。

圖 1：勒索軟體地址收到的加密貨幣總價值

2016 - 2021（年初至今）



資料來源：“Ransomware 2021: Critical Mid-Year Update”（勒索軟體 2021：年中重要更新），Chainanalysis，2021 年 5 月，https://go.chainalysis.com/rs/503-FAP-074/images/Chainalysis-Crypto-Crime-2021.pdf

犯罪分子對加密貨幣情有獨鍾的原因是什麼？加密貨幣為何如此受歡迎？詞根“crypto”源自希臘語 kryptós，表「隱藏」之意。根據當今的說法，加密貨幣指比特幣、以太坊、萊特幣、Zcash 和鮮為人知的門羅幣等另類支付機制；谷歌搜尋結果顯示，門羅幣宣稱具有「安全、私密和不可追蹤」的特點。駭客喜歡加密技術的匿名性和不透明性，這樣可以保護數位地址並掩蓋資金目的地。他們透過電子郵件網路釣魚活動、利用遠端桌面通訊協定漏洞，以及在廣泛使用的軟體程式中找出安全漏洞，用惡意軟體感染受害者的電腦。惡意軟體將公司電腦內的數據加密，使其無法使用。網路犯罪分子將公司作為人質，威脅若收不到贖金，會銷毀受害者的數據或將其發佈在社交媒體上。只有收到贖金才會解密資訊並恢復對系統或數據的存取權。千萬不能低估勒索軟體對國家、政府機構、警察和消防部門、醫院、航空公司和其他重要基礎設施營運的影響。

加密貨幣洗錢活動的三個階段

只要將 CVC 當成交換媒介，勒索軟體就與洗錢有了關聯。圖 2 說明 CVC 洗錢活動的三個階段。由於此趨勢不斷增長，美國金融犯罪稽查局在 2020 年 10 月發佈了一份諮詢意見書。[4] 據金融犯罪稽查局：「勒索軟體付款的處理通常包括多個步驟，涉及至少一個存款機構及一個或數個貨幣服務業 (MSB)。」由於多數受害者沒有加密貨幣錢包或帳戶，因此交付贖金需要將資金從他們在受監管金融機構開立的銀行帳戶移轉到 CVC 交易所。這屬於處置階段。此外，還出現了這樣一些情況，數位鑑識和事故應變公司或網路保險公司收到受害者的資金，將其兌換為 CVC，然後把 CVC 轉移至網路犯罪分子控制的特定數位地址。

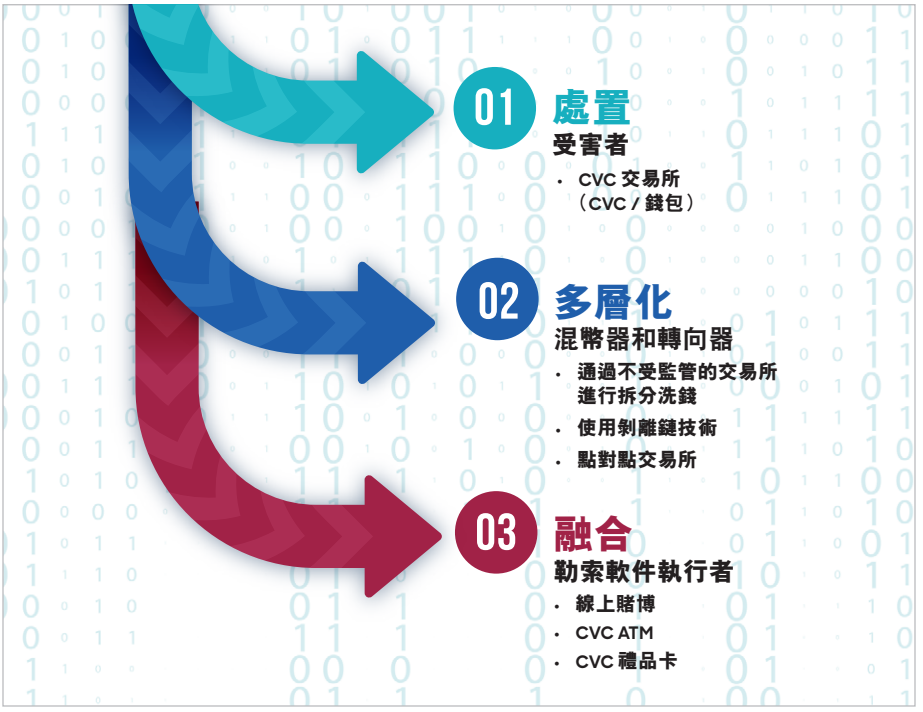
另一種手法則是騙子誘使人們同意將「捐款」資金匯入自己的帳戶，由此換取一筆好處費。騙子會告訴他們將資金轉換為 CVC，再匯入到不同的數位地址。而「捐款」很可能是贖金或從他人那裡偷來的錢。新冠疫情期間，有許多錢騾願意讓騙子利用他們的銀行帳戶或數位地址進行非法勾當，毫無愧疚之意。

犯罪分子在一段隨機期間內將來自一連串數位地址的多筆資金彙集在一起，混合收到的贖金和其他加密貨幣資金，進入多層化階段。這樣做是為了掩蓋 CVC 蹤跡，打破 CVC 發送地址和 CVC 接收地址之間的聯繫。使用 AlphaBay、Helix、Darklaunder、Bitlaunder 和 CoinMixer 等混幣器和轉向器接收加密貨幣，混合不同來源的資金，然後匯回另一系列目的地地址，支付 1% 到 2% 的手續費。據 Chainanalysis 分析，[5] 根據交易的複雜程度，混合所需的時間短至 1 到 6 個小時，長至 7 天。交易經過混合服務後，與貨幣關聯的先前地址會被有效刪除。[6]

其他多層化方法則涉及透過大量帳戶和交易所拆分加密貨幣交易，或者將 CVC 轉移到防制洗錢 / 打擊資恐 (AML/CTF) 控制薄弱的司法管轄區內不受監管的交易所或點對點交易所。這種方法要用到剝離鏈技術，剝離鏈是一種錢包鏈，資金會流經這些錢包掩蓋非法所得 CVC 的蹤跡。

加密貨幣洗錢最後是整合階段，此時贖金被合法化，證明其合法屬於網路犯罪分子所有。幫助洗白數位資產的管道包括不受監管的加密貨幣交易所，這些交易所不要求核查用戶身分，安全政策寬鬆。它們可以幫助將 CVC 兌換為法定貨幣。其他交換媒介包括接受 CVC 付款的線上遊戲和賭博網站，CVC 可用於購買積分或虛擬籌碼。犯罪分子經常光顧這些網站，並透過一系列小額交易將 CVC 轉換成法定貨幣。另一種交換源是 CVC ATM 和 CVC 禮品卡。據 coinatmradar.com 表示，7 月初全球約有 23,000 台加密貨幣 ATM。[7] 數量雖然不多，卻足以支持洗錢活動。同時也出現了一種趨勢，消費者用加密貨幣購買奢侈品。高檔手錶製造商 Franck Muller 今年早些時候推出了一款價值 12,000 美元的手錶，其具備鐘錶和數位錢包雙重功能。這款手錶僅可使用比特幣購買，41 毫米錶盤上刻有獨有的公共位址，私鑰保存在加密的 USB 當中。[8]

圖 2：CVC 洗錢的三個階段



金融機構、受監管 CVC 交易所、網路保險公司和執法機構迫在眉睫的風險是，對控制 CVC 資金的收款人身分知之甚少

結語

對於那些試圖規避嚴格資本管制、洗白非法所得或逃避對國家或地區、公司、個人或恐怖組織的金融制裁的人來說，加密貨幣是一個理想的選擇。金融機構、受監管 CVC 交易所、網路保險公司和執法機構迫在眉睫的風險是，對控制 CVC 資金的收款人身分知之甚少。如果收款地址屬受制裁個人，或者牽涉位於受嚴厲制裁司法管轄區網路犯罪分子相關的勒索軟體病毒株，該怎麼辦？海外資產控制辦公室已經將兩個數位貨幣地址與針對公司、醫院和大學的 SamSam 勒索軟體攻擊的受制裁犯罪分子聯繫起來。這些錢包地址被用來與全球 40 多個不同的數位貨幣交易所進行交易，成為洗錢多層化階段的一部分。[9]

遺憾的是，數位貨幣地址清單並不詳盡，也不全面。如果使用隱形地址則更糟。匯款人每筆交易使用一個一次性地址，就屬於這種情況。同一匯款人對同一收款人完成的多筆交易採用不同的地址，掩蓋了 CVC 付款細節及其財務明細。因此，如果發現資金流向受制裁的個人或實體，參與或協助數位地址交易的機構將面臨罰款和無法使用其美元清算授信的風險。

儘管一些監管機構要求完全透明地揭露受益人和匯款人地址，以及法定貨幣資金轉帳的目的，但他們並未限制其管轄範圍內虛擬貨幣的持有和交易。目前，各地的控制程度亦不盡相同——某些國家或地區已經禁止金融機構和支付公司提供加密貨幣交易相關服務，但並未禁止其公民持有 CVC。其他國家或地區則讓金融機構自行決定——其中許多金融機構向客戶明確表示，不能用他們的銀行帳戶進行加密貨幣交易。

最近的卡比斯灣 G7 高峰會公報強調，政府需要「識別、打擊境內實施勒索軟體攻擊、濫用虛擬貨幣洗錢及實施其他網路犯罪者，並追究其責任。」[10] 但是，在加大力度實施跨境合作之前，相關機構必須主動實施網路安全控制，定期進行業務持續運作模擬，推動落實網路衛生實務，[11] 因為未雨綢繆勝過亡羊補牢。

Deepa Chandrasekhar，聯合海灣銀行高階副總裁、首席法規遵循專員、洗錢防制專責主管

本文僅代表作者的個人觀點，並不代表其機構觀點。

1 Thomas Brewster, The Ransomware Group Behind The Colonial Pipeline Hack Says It Is Disbanding"（Colonial Pipeline 駭客攻擊背後的勒索集團宣稱即將解散），*《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 Perlroth,"Colonial Pipeline Paid 75 Bitcoin, or roughly $5 million, to hackers"（Colonial Pipeline 向駭客支付 75 個比特幣（約合 500 萬美元）），*《紐約時報》*，2021 年 5 月 13 日，https://www.nytimes.com/2021/05/13/technology/colonial-pipeline-ransom.html

2 Joe Tidy，"Swedish Coop supermarkets shut due to US ransomware cyber-attack"（瑞典 Coop 超市因美國勒索軟體網路攻擊而關閉），*BBC*，2021 年 7 月 3 日，https://www.bbc.com/news/technology-57707530

3 Matthew J. Schwartz，"How Did FBI Recover Colonial Pipeline's DarkSide Bitcoins?"（聯邦調查局是如何追回 Colonial Pipeline 支付給 DarkSide 的比特幣？），*BankInfoSecurity*，2021 年 6 月 11 日，https://www.bankinfosecurity.com/how-did-fbi-recover-colonial-pipelines-darkside-bitcoins-a-16863

4 "Advisory on Ransomware and the Use of the Financial System to Facilitate Ransom Payments"（關於勒索軟體和利用金融系統促成勒索贖金支付的意見書），*金融犯罪稽查局*，2020 年 10 月 1 日，https://www.fincen.gov/sites/default/files/advisory/2020-10-01/Advisory%20Ransomware%20FINAL%20508.pdf

5 Thibault de Balthasar 和 Julio Hernandez-Castro，"An Analysis of Bitcoin Laundry Services"（比特幣洗錢服務分析），*Chainalysis and University of Kent*，2017 年 9 月，https://www.researchgate.net/publication/319944399_An_Analysis_of_Bitcoin_Laundry_Services（訪問日期：2021 年 6 月 28 日）。

6 Faisal Khan，"Twitter hackers employing 'peel chains' to launder the Bitcoin bounty"（推特駭客使用「剝離鏈」洗白比特幣贖金），*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/（訪問日期：2021 年 6 月 28 日）。

7 *Coin ATM Radar*，https://coinatmradar.com/（訪問日期：2021 年 7 月 8 日）。

8 Rachel Cormack，"Franck Muller's Newest Watch Doubles as a Bitcoin Wallet, and You'll Need Cryptocurrency to Buy It"（Franck Muller 最新款手錶兼具比特幣錢包功能，只能用加密貨幣購買），*Robb Report*，2021 年 2 月 24 日，https://robbreport.com/style/watch-collector/franck-muller-new-timepiece-doubles-bitcoin-wallet-1234598536（訪問日期：2021 年 6 月 30 日）。

9 "Treasury Identifies Iranian Nationals and Their Digital Currency Addresses Used to Facilitate Ransomware Attacks"（美國財政部發現伊朗國民及其用於促進勒索軟體攻擊的數位貨幣地址），*JD Supra*，2018 年 12 月 4 日，https://www.jdsupra.com/legalnews/treasury-identifies-iranian-nationals-29943/

10 "Carbis Bay G7 Summit Communiqué"（卡比斯灣 G7 高峰會公報），*美國白宮*，2021 年 6 月 13 日，https://www.whitehouse.gov/briefing-room/statements-releases/2021/06/13/carbis-bay-g7-summit-communique/

11 "Advisory on Ransomware and the Use of the Financial System to Facilitate Ransom Payments"（關於勒索軟體和利用金融系統促成勒索贖金支付的意見書），*金融犯罪稽查局*，2020 年 10 月 1 日，https://www.fincen.gov/sites/default/files/advisory/2020-10-01/Advisory%20Ransomware%20FINAL%20508.pdf

賭場和洗錢原因

賭場員工觀察是賭場防制洗錢制度的重要部分，與銀行不同，賭場的所有交易發生時客戶幾乎都在現場。因此，賭場應重視防制洗錢的培訓，努力提高賭場員工的能力，幫助他們識別需要提交可疑活動報告的異常行為。

學習專家們都有普遍共識：培訓的重點是讓學員理解知識，而非死記硬背。對賭場員工的防制洗錢培訓往往只強調賭場員工要記住可疑交易行為的類型（實施方式），而不解釋洗錢犯罪分子為何會從事此類交易。

洗錢並非是只有經驗豐富的防制洗錢專業人士才能理解的高深話題。*《黑錢勝地》*、*《毒梟》*、*《絕命毒師》*等熱門影集發揮了極大的功能，讓普羅大眾對洗錢有一定的瞭解。劇本裡充斥著各種戲劇化的洗錢緣由——這也是影集引人入勝、妙趣橫生的原因。

著名組織學專家 Simon Sinek 在一次 TED 演講中闡述了解釋原因的諸多益處，這次演講是觀看次數最多的 TED 演講之一（超過 5,500 萬次）。在其暢銷書*《先問，為什麼？啟動你的感召領導力》*中，Sinek 斷言，成功的組織在激勵員工時，會先闡述原因（目的），然後才談論方法（過程）。運用在防制洗錢培訓和賭場風險評估時，賭場應效仿 Sinek，從原因開始。[1]

從廣義上講，犯罪分子洗錢的原因是為了躲避執法機關的偵查，以免因資金而洩漏犯罪蹤跡。這是洗錢的首要目標，但沒有解釋他們為什麼要從事某些交易（或流程）來達到最終的洗錢目的。醫生的最終目的是救死扶傷，但這並不能解釋他們為什麼要執行某些醫療程序，例如心臟聽診、抽血或拍 X 光片。醫生進行的每個程序都是為了實現特定目標。如果病人理解醫生進行某些程序的原因，他們就可以更能理解治療方向，判斷某些程序是否有必要。

如果賭場員工理解洗錢犯罪分子參與某些流程的原因，他們就能更有效地判斷交易屬於可疑行為還是單純的賭博行為。

洗錢目的培訓法

洗錢目的培訓法 (MLGM) 是一種教導洗錢交易背後主因的直觀教學法。該方法強調交易意圖，並使用相關術語解釋洗錢方式。犯罪分子從事特定洗錢交易時，他們即準備要實現表 1 所列的洗錢目的之一。

借助洗錢目的培訓法，使賭場員工瞭解洗錢交易。為什麼犯罪分子會拆分現金存款、使用虛假身分證件、假扮身分不明者、交換座位，或者委託代理人代表他們進行交易？因為犯罪分子可能不想讓當局知道他們的活動。為什麼犯罪分子會用小額鈔票塞滿吃角子老虎然後兌現，用大量簽帳卡取款或定期兌現支票？因為犯罪分子可能打算轉換資金，增加資金的追蹤難度或資金的使用便利性。

表 1：賭場洗錢目的和交易意圖

賭場洗錢目的	交易意圖
掩藏	掩藏交易中的受益所有人身分，或在向政府提交的資訊報告中掩藏受益所有人身分
轉換	將資金轉換為難以追蹤和方便使用的形式
轉帳	將資金從某人或某地移轉給另一人或其他地方
洗白	偽造資金來自於賭博所得的託辭或混淆資金軌跡
花費	享用非法資金，通常不考慮實現任何其他洗錢目的
儲存	把資金儲存在傳統銀行系統之外

採用洗錢目的培訓法強調洗錢原因，促使賭場人員站在洗錢犯罪分子的角度思考。洗錢目的培訓法不但能促使賭場員工更妥善記住防制洗錢知識，還能幫助他們區隔疑似洗錢的交易行為，降低誤判正常交易的風險。如果交易看起來未達成洗錢目的，則可能不是洗錢行為。

識別洗錢目的和過程

務必要區分洗錢目的與實現過程。將大量資金留在靜止的預付款帳戶中，持有大額賭場支票而不存入銀行，囤積賭場籌碼，這些均非洗錢目的，而是實現儲存資金目的的過程。索取 W-2G 表，混合非法資金與賭博獎金，或試著向出納櫃台索取現金提領收據，這些也不是洗錢目的，而是實現資金洗白目的的過程。

實現洗錢目的的過程是方式而非原因。僅告知方式（過程）而不解釋原因，將不利於賭場員工記住和理解課程內容。相反，先教授原因然後舉例說明洗錢方式，有助於賭場員工加深對洗錢的理解。他們可以確定特定交易模式是否顯示出洗錢行為，或者只是客戶的獨特賭博風格。例如，有人可能不會將超過 10,000 美元的籌碼一次兌換，因為他們想儘快回到賭場。他們的目的是再次賭博時無須購買籌碼，而不是隱瞞洗錢目的。

確定交易原因的最好辦法是觀察交易者。特別是，對他們的資金來源和賭博歷史瞭解多少？如果確定顧客的資金來自合法管道，那麼他們為什麼要達成洗錢目的？如果試圖僅根據交易資訊確定原因，則很可能導致將交易活動錯誤地歸類為可疑活動。洗錢目的培訓法促使賭場員工在確定交易原因時，關注誰是交易者。

負責洗錢案件的刑事調查人員需要證明有問題交易的意圖。如果證據並未顯示存在洗錢意圖，則不構成刑事案件。僅僅因為有人把錢放入吃角子老虎，然後沒玩幾次就兌現（這種模式稱為「最低額度賭博」），並不意味著他們打算洗錢。接受過洗錢目的培訓法的法規遵循人員能更熟練地分析最低額度賭博等交易行為，找出是否存在實現洗錢目的的意圖，顧客到底是有特定的賭博風格，還是在為自己的賭博遊戲投入資金而已。這樣一來，他們就能更加熟練地撰寫可疑活動報告，納入對執法工作有用的資訊（行為人、方式和原因）。

洗錢目的培訓法還能幫助法規遵循人員理解為什麼需要某些控制措施來檢測、預防和報告洗錢活動。一旦賭場員工理解了這些控制措施後，就會更加願意落實這些措施。

右邊表 2 是洗錢目的與已知洗錢過程的分類。

逃稅和資助恐怖活動

一般而言，若要起訴洗錢罪行，該交易必須涉及非法所得。因此，對資金來源展開盡職調查，對有效實施防制洗錢制度體系至關重要，因為大多數時候犯罪分子只是在賭場花掉髒錢而已。另一方面，大多數時候逃稅行為涉及合法資金，但逃稅者可能需要達成某些洗錢目的，例如隱藏、轉換、轉移和儲存資金。與其他金融機構相比，他們在賭場較難實現這些目的。正如《2018 年美國財政部全國洗錢風險評估》報告所指，賭場並非以協助逃稅而聞名，但根據《銀行保密法》，賭場必須報告涉及逃稅的可疑活動。[2]

資助恐怖活動則不一定會涉及非法程序，但資恐者可能會利用賭場實現某些洗錢目的，推動犯罪活動，例如轉換、轉帳、掩藏或儲存資金。然而，《2018 年美國財政部全國資助恐怖活動風險評估》報告並未提及賭場 。[3]

表 2：賭場洗錢目的和過程

賭場洗錢目的	過程
掩藏	· 分散交易 · 虛假身分證件 · 代理人 · 籌碼失蹤 · 交換座位 · 未分級賭博
轉換	· 小額換大額鈔票 · 簽帳卡提現 · 支票兌現 · 現金換賭博工具
轉帳	· 支付他人的信用借貸金 / 費用 · 把籌碼當成一種貨幣 · 第三方付款
洗白	· 索取 W-2G 表 · 混合 / 分層 · 抵消投注 · 取得取款收據
花費	· 賭博損失 · 零售品 · 娛樂 · 餐飲
儲存	· 靜止的預付款帳戶 · 囤積籌碼 · 未存入賭場支票 · 把錢存在賭博錢包中

體育博彩與提供便利

如果賭場提供體育博彩，則可能增加另一個洗錢目的——推動。「推動」是指利用賭場持續為犯罪活動提供便利。眾所周知，在體育博彩中，非法博彩業者會利用體育博彩平帳，避免因任何比賽結果而一面倒，這一過程通常被稱為「平衡下注」。

另一重要原因

賭場人員不僅要理解洗錢交易的原因，還要接受培訓，以瞭解銀行保密法 / 防制洗錢工作在防止犯罪分子利用賭場為犯罪活動提供便利方面，扮演至關重要的角色。如此一來，他們將理解《銀行保密法》是執法機關不可或缺的工具，賭場現金交易報告和可疑活動報告發揮了重要作用，成功地將毒販、人口販子和主要詐欺犯等各種重要罪犯繩之以法。他們會看到自己的努力有助於維持社區安全。理解銀行保密法 / 防制洗錢的原因，有助於激勵賭場人員參與防制洗錢活動。

處置、多層化與整合：PLI 模型

傳統上，銀行保密法 / 防制洗錢專業人士會將洗錢過程分解為處置 (placement)、多層化 (layering) 與整合 (integration) 三個階段（通常稱為「PLI 模型」），藉此解釋洗錢的原因。儘管 PLI 模型可以解釋大規模洗錢活動（例如卡特爾）中的複雜洗錢行為，但很難解釋賭場洗錢活動。通常，客戶將非法資金帶到賭場，他們的洗錢活動不會逐一經歷 PLI 模型的三個階段。例如，許多犯罪分子只需要

表 3：PLI 模型與賭場洗錢目的

PLI 模型	賭場洗錢目的
處置	掩藏
	轉換
	轉帳
多層化	洗白
整合	花費
	儲存

避免有人提交現金交易報告，就可以避開執法機關的注意。既然許多犯罪分子只想透過單筆交易完成洗錢，為什麼還要將洗錢行為解釋為由三個階段構成的過程？另一個考慮點，當非法資金進入賭場，通常多是為了享受犯罪活動的果實，無論過去或現在根本無意去完成整個洗錢週期。

洗錢目的培訓法著重於單筆交易的原因，不考慮將交易強制歸入洗錢週期的某個階段。也就是說，洗錢目的培訓法並未與 PLI 模型完全一致，如表 3 所示。

結語

要抓住洗錢犯罪分子，必須與洗錢犯罪分子換位思考。如果從原因出發，賭場工作人員就會從竭力避開執法機關審查的犯罪分子的角度思考問題。理解了原因，賭場工作人員就能明白何者正進行洗錢行為，更重要的是能理解為什麼交易只是展現顧客的一種賭博風格。理解了原因，防制洗錢制度體系就能更突出風險為本的特性，降低向政府報告交易的機率，因為往往有些交易實際上只是合法顧客享受賭場活動而已。就這方面而言，防制洗錢制度體系將對執法機關打擊金融犯罪更加有用。

Paul Camacho，CAMS，國稅局刑事調查科退休探員、黑幫博物館董事

[1] Simon Sinek，“How great leaders inspire action”（偉大領導者如何激勵他人採取行動），拍攝時間：2009 年，TED 影片，17:27，https://www.ted.com/talks/simon_sinek_how_great_leaders_inspire_action?language=en

[2] “2018 National Money Laundering Risk Assessment”（2018 年全國洗錢風險評估），*美國財政部*，https://home.treasury.gov/system/files/136/2018NMLRA_12-18.pdf

[3] “2018 National Terrorist Financing Risk Assessment”（2018 年美國財政部全國資助恐怖活動風險評估），*美國財政部*，https://home.treasury.gov/system/files/136/2018ntfra_12182018.pdf

ACAMS™
公認反洗錢師協會

在複雜的世界中管理風險

ADVANCED CAMS™ RISK MANAGEMENT

獲得管理金融犯罪風險的全球資格認證，
證明您在風險管理領域深厚的專業知識。

到訪 **www.acams.org**
開啟您的旅程

增強 DPMS 監管法規遵循工具

對於貴金屬和寶石交易商 (DPMS) 行業，以及該行業交易的商品，金融機構通常不甚瞭解。該行業與受防制洗錢監管的其他報告機構有所不同，因為前者完全以消費者零售為基礎，而各國或地區對於該行業跨國交易商品的控管亦隨各國法律而有所差距。此外，該行業涉及的商品（鑽石、寶石、貴金屬等）不僅用於儲存和轉移財富，還可用來作為貨幣替代品和產生犯罪收益。但其間發生的大部分洗錢活動，珠寶業本身卻不清楚。無論是合法還是非法活動帶來的收益，許多都流入珠寶業，然後流入為珠寶業提供服務的銀行。總而言之，這些因素相互疊加，令 DPMS 防制洗錢監管愈發困難，最終導致了更顯著的 DPMS 防制洗錢風險敞口。

藉貴金屬和寶石洗錢

司空見慣的誤解之一：洗錢就是以非法活動所得的現金購買其他商品。此一前提不假，卻忽略洗錢的一大環節——即出售非法取得的物品以換取現金或其他物品（貿易）。對於珠寶竊盜相關犯罪及非法取得鑽石 / 寶石 / 貴金屬等其他犯罪而言，澄清此概念尤為重要。珠寶的處置或洗白，指的是以珠寶換取毒品或其他商品，或者將珠寶賣回合法市場的行為。如果珠寶商認為洗錢就是「將珠寶出售給犯罪分子換取現金」的行為，就會忽略「犯罪分子出售非法珠寶」這類洗錢行為。

由於珠寶遺失通常涉及盜竊、搶劫、非法入侵等罪行，瞭解此類洗錢行為尤為重要。在非法入侵的案件中，珠寶往往是第二容易遭竊的物品；[1] 此類案件的平均損失金額約為 2,566 美元。[2] 美國聯邦調查局統計數據顯示，每 10 萬人口中會發生 376 起擅闖民宅案件 [3]（2018 年，加拿大每 10 萬人口中，發生了 431 起此類案件 [4]）。據此數據估計，在美國一座 500 萬人口的城市中，此類犯罪造成的珠寶損失每年高達兩千萬美元。以此類非法方式獲得的珠寶，經過洗白回流至合法珠寶市場，相關收益最終流入為該行業提供服務的銀行；這僅是透過 DPMS 行業洗錢的其中一種方式。其他手法包括犯罪分子利用犯罪所得贓款，實際購買新的珠寶（如高價手錶、高成色金、鑽石首飾等），或使用鑽石和寶石進行貿易洗錢 (TBML) 活動。

深入瞭解該行業之所以困難重重，部分原因在於：該行業內零售商與批發商之間的商業模式存在顯著差異。低端珠寶、高端珠寶、手錶、彩色寶石、鑽石、高成色金、寄售 / 二手銷售等，均有可能成為不同商業模式（如實體店、網路店、線上線下混合經營模式等）零售商的主要關注點。每種商業模式均有各自的目標市場（客戶）、供應鏈、價位及商業週期；此外，由於具體業務不同，每種商業模式供應鏈的涉及面也大相徑庭：區域性、全國性乃至全球性，不一而足。在供應商端，最重要的是瞭解貨物供應的市場、供應商與地理位置。

零售與批發貿易發生地的各司法管轄區防制洗錢法律不同，進一步增加防制洗錢工作的複雜性。以發生在加拿大與美國之間的簡單貿易為例，兩國的防制洗錢法律對於「寶石」一詞包含的具體對象，規定就大相徑庭。兩國在貿易合作領域關係雖密切，但各自防制洗錢法律在「寶石」的具體定義上就存在顯著差異（見下表 1）。

表 1：加拿大和美國對「寶石」的法律定義

加拿大	美國
鑽石、藍寶石、紅寶石、綠寶石、坦桑石和亞歷山大變石 [5]	鑽石、剛玉（包括紅寶石和藍寶石）、綠柱石（包括綠寶石和海藍寶石）、金綠寶石、尖晶石、黃玉、鋯石、電氣石、石榴石、水晶和隱晶質石英、橄欖石、坦桑石、硬玉、軟玉、鋰輝石、長石、綠松石、青金石和蛋白石 [6]

而這只是防制洗錢法律的其中一個面向。在 DPMS 相關的其他防制洗錢法律方面，各國法律也存在眾多差異。雖然任何寶石均有可能被當成洗錢工具，但由於缺乏國際公認的定價，彩色寶石（非鑽石）仍然是貿易洗錢 (TBML) 的主要工具。這麼一來，問題就愈發錯綜複雜，專業人員很難厘清不同司法管轄區內與寶石來源相關的風險，何況還有成百上千種寶石尚未納入現行防制洗錢法律。國際商品統一分類協調制度（全球廣泛認可並使用的一種產品代碼制度，用於所有進出口產品，包括所有寶石）或可涵蓋所有寶石，但此種制度尚未用於防制洗錢和寶石相關法律。

司空見慣的誤解之一：洗錢就是以非法活動所得的現金購買其他商品

全面瞭解珠寶行業對於深入剖析 DPMS 業務及其國內、國際市場至關重要

Kelly Ross，碩士，CAMS，FCGmA，
Kelly Ross 諮詢公司寶石學專家，
加拿大艾伯塔省，Kross5c@gmail.com

增強 DPMS 防制洗錢法規遵循能力

要想瞭解犯罪分子可能鑽的漏洞、洗錢發生的具體領域，就需要瞭解相關商品的業務、市場以及犯罪手法。不僅 DPMS 行業如此；面對任何其他報告機構，無論是賭場、房地產業或是貨幣服務業，均是如此。銀行業者可以透過增強 DPMS 行業知識、商業模式對應和交易分析能力，全面鞏固防制洗錢法規遵循與風險管理帳戶。

DPMS 業是相對小型的市場，雖然千年以來都是零售產業的一部分，但除了該行業從業人員（及相關銀行）之外，其他人對該行業知之甚少。針對 DPMS 交易評估制定一套專門工具，有助於提升調查、分析和交易監控能力。首先，全面瞭解珠寶行業對於深入剖析 DPMS 業務及其國內、國際市場至關重要。瞭解犯罪分子利用鑽石、寶石、貴金屬的方式，以及犯罪企業進入合法珠寶市場的模式，同樣重要。綜合運用上述知識，有助於全面瞭解 DPMS 行業提供的犯罪機會，犯罪涉及的商品，以及高風險點在於何處。

其次，充分運用行業與業務基礎知識，DPMS 帳戶審查的資深調查人員可審查現有的高風險 DPMS 帳戶。理想的審查方式，是根據業務模式、業務規模、地理位置、年度銷售週期、市場比較分析等因素開展交易對帳。此外，應鼓勵曾經分析 DPMS 行業，並具有相關業務知識的調查人員深入鑽研，致力於成為 DPMS 行業專家，就像深耕其他報告機構相關領域的專家一樣。

第三，堅定落實「了解您的客戶」綜合流程及預防措施，在開立相關帳戶之前，應進行專門的 DPMS 客戶開戶篩查。DPMS 行業十分特殊：相關企業應均已投保特定行業保險，進行特定行業登記，隸屬於特定行業協會，並且採用特定商業模式。此外，DPMS 零售商必須制定防制洗錢法規遵循制度體系。相關制度應經過審查、登記，並確定其符合現行法規遵循要求。開戶調查問卷的細節至關重要，因為調查人員需運用收集到的相關數據完整繪製出客戶業務模型，才能如前所述，順利進行交易比較分析。

結語

珠寶行業是一個奇妙的行業，作為全球商業的組成部分，擁有源遠流長、豐富多彩的歷史。然而，該行業性質特殊，商業模式繁多，業內買賣的商品五花八門，為犯罪分子洗白犯罪所得提供了不少機會。珠寶行業存在眾多風險點，讓犯罪分子能伺機洗白犯罪所得，相關資金流入珠寶行業後，再流入服務於珠寶行業的金融機構。珠寶行業處於一線，卻與銀行不同：後者擁有達到監管要求的防制洗錢知識、能力與資源；此外，銀行、防制洗錢調查員和分析師對大多數報告機構的相關交易分析高度敏感。如需改善這一狀況，培訓、調查 / 分析指導與專業化、客戶開戶篩查等均是實用工具，可加強 DPMS 的監管法規遵循能力。

1 Joseph B. Kuhns 等，“Understanding Decisions to Burglarize from the Offenders Perspective”（從犯罪分子角度理解行竊決定），*北卡羅來納大學夏洛特分校刑事司法與犯罪學系*，2012 年 12 月，https://www.researchgate.net/publication/268444817_Understanding_Decisions_to_Burglarize_from_the_Offender's_Perspective/link/546b48410cf2f5eb18091770/download

2 “2018 Crime in the United States”（2018 年美國犯罪報告），*美國聯邦調查局*，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 年美國每 10 萬居民犯罪量與犯罪率調查報告），美國聯邦調查局統一犯罪報告 (UCR) 計劃，https://ucr.fbi.gov/crime-in-the-u.s/2018/crime-in-the-u.s.-2018/topic-pages/tables/table-1

3 同上。

4 “Table 1: Police-reported crime for selected offences, Canada, 2017 and 2018”（表 1：2017 年和 2018 年加拿大警方報告的特定犯罪行為），*加拿大統計局*，https://www150.statcan.gc.ca/n1/pub/85-002-x/2019001/article/00013/tbl/tbl01-eng.htm

5 “Dealers in precious metals and precious stones”（貴金屬和寶石交易商），*加拿大金融交易與報告分析中心*，https://www.fintrac-canafe.gc.ca/re-ed/dpms-eng

6 “Financial Crimes Enforcement Network; Anti-Money Laundering Programs for Dealers in Precious Metals, Stones, or Jewels”（金融犯罪稽查局：貴金屬、寶石或珠寶交易商防制洗錢制度），*金融犯罪稽查局*，2003 年 2 月 21 日，https://www.fincen.gov/sites/default/files/shared/antimoneylaundering060305.pdf

ACAMS
公認反洗錢師協會

ACAMS 每年在全球舉辦 25 場活動

涵蓋您最為關切的重要議題，包括機構防制洗錢文化、防制洗錢領域的技術更新換代，以及對防制洗錢從業者不斷提高的執業要求。

一切盡在 ACAMS

瞭解您所在地區的最新情況：

如何通過稽核

俗話說，死亡和繳稅是人生必經之事。對法規遵循專業人士來說，這句話還可以加上一點——死亡、繳稅和稽核是人生必經之事。不過，正如死亡和繳稅一樣，稽核的具體情況可能因不同因素而大相徑庭，這些因素包括但不限於：具體所屬行業、稽核機構與人員、所在組織的風險、法規遵循制度體系等等。雖然法規遵循專業人士可能幾乎不受外部稽核因素影響，但往往可以改進或增強組織內部稽核流程，從而減輕稽核工作的負擔，緩解稽核工作帶來的損耗。本文將介紹稽核策略的準備、參與和回應措施，有助增進稽核流程的順暢。

沒有人喜歡驚嚇。因此，務必詳細瞭解法規遵循要求、風險因素和風險評估，以及（內部和外部）法規遵循制度體系的運作細節，這幾點至關重要，直接關乎稽核工作的成敗。稽核流程旨在找出現行政策與程序之間的差距，以期完善相關制度。有些稽核師對稽核工作抱著歡迎態度，因為展開稽核工作，有助於避免監管機構的介入。而更常見的是，有些人將稽核視為一種對抗關係，他們認為稽核師的唯一目的就是針對制度，在雞蛋裡挑骨頭，無論該評估是否合理得當。稽核的目的在於消除或顯著減少稽核流程中的潛在衝突。要做到這一點，關鍵在於如實自行評估相關制度，對法規遵循環境具有敏銳的察覺，提供完整全面的文件紀錄和資料管理。

顯然，組織越龐大，法規遵循責任就越錯綜複雜。舉例來說，許多監管行動展開的主因並非來自於故意瀆職，而是缺乏對法規遵循風險的全面指揮和控制。從這個意義上而言，良好的溝通和制度知識不僅能夠推動稽核流程順利進行，還有助於消除可能的監管後果，從而改善公司的聲譽、老舊制度及利潤率（這是高階管理層最看重的一點）。

要想通過稽核，在稽核流程正式開始就要做好準備。稽核準備是一個持續的過程，需要不斷地評估和打磨。因此，客觀進行內部稽核或聘請中立的第三方稽核師，至關重要。然而定期進行自省評估亦同等重要，因為商業環境、監管要求等並非一成不變。只要外部因素發生了巨大變化，幾年前無懈可擊的制度就可能存在嚴重問題。必須在稽核師發現這些問題之前，主動加以修正。

以下是一份基本活動核對清單，或許有助於提升您的稽核經驗。

通過稽核的必備清單

稽核準備

- 全面瞭解組織制度，並確保所有同事、員工均精通自身職責範圍。發現部分員工不完全瞭解自身職責，是稽核常見的觀察結果之一。
- 確保同事接受過全面和充分的培訓，並能夠提供此類培訓的證明。還需證明員工具備執行被分配任務的背景與能力。員工和主要承包商的簡歷應保持最新狀態且可供查詢。
- 確保組織中與稽核師溝通者或向稽核師提供書面資訊者，其意見一致；此外，其提供的稽核回覆不應超出其專業領域。例如，IT 技術員不應針對危險信號提出意見，除非涉及「法規遵循技術中應如何編寫危險信號程式」的事宜。任何錯誤的回覆均可能再次困擾您，哪怕時隔多年。
- 告知與稽核師互動的人員，務必直接回答稽核師的問題；回答任何問題時，不要超出該問題的範圍。否則，有可能造成混亂，導致意想不到的額外調查，進而讓稽核流程更加複雜且延長。總結：僅提供事實，不發表觀點。
- 定期進行風險評估和內部審查；或在出現全新因素（如推出新產品、新服務，或開拓新銷售管道）時進行前述活動。如有可能，聘請一位對您的行業瞭解透徹、不偏不倚的第三方稽核師，深入稽核您的組織制度。稽核師可能要求您提供相關審查報告的副本，以及您為解決審查結果所採取行動的相關說明。做好準備，及時提供這些文件。
- 確保您的政策和程序手冊完整，並適時更新。最重要的是：做好充分準備，證明您嚴格執行相關政策並遵守相關程序。稽核師通常不會同情這類毫無新意的缺失。您的組織既已制定了政策和程序，而不落實書面規定是受到監管處罰的常見理由。
- 進行全面的差距分析，並重視分析結果。如果忽略或輕視已發現的差距，很容易引起稽核師和監管機構的注意。
- 在風險評估的參數範圍內，盡可能修正、增補並加強現行政策與程序。準備詳盡的文件說明未彌補所發現差距的理由，或是提供彌補相關差距的計劃與時間表。始終努力制定或尋找解決方案。如有可能，制定臨時緩解措施，直至能夠實施長期解決方案為止。
- 及時瞭解行業最佳作法；如有可能，將其納入組織制度之中。稽核師會注意這一點。
- 必須承認，發現問題是稽核師的職責。要接受的是，即使是最理想的法規遵循制度體系，稽核師也能找到不妥之處。沒有法規遵循制度體系是完美的。即使是監管機構，也並不期望完美。欠缺完美就代表總是會有需要加強、增補或簡化的政策或程序。

稽核管理

- 稽核開始前，與稽核師就稽核範圍達成共識，記錄範圍並在文件上簽名。這樣做有助於防止稽核範圍擴大，避免與稽核師之間產生誤解。如果在稽核期間，稽核範圍發生變化，務必讓稽核師以書面記錄變更並留存備案。

稽核準備是一個持續的過程，需要不斷地評估和打磨

- 如有必要，傳授適當知識給稽核師，尤其組織制度具有獨特性或特殊規定時，就更需要這樣做。尤為重要的是，務必完整記錄不適用特定法規或最佳實踐的原因。若只表示其「不適用」，縱使您覺得原因顯而易見，卻往往無法令稽核師信服。
- 各行各業、許多組織都有自己的行話，其中有些可能與行業標準術語不符。最好的補救辦法是統一採用行業標準語言。如果難以實現，建議準備一份術語表，列出組織特有的術語及其常見的對應用語。應於稽核工作開始前準備好這份術語表，避免稽核過程中產生誤解。
- 承認有問題，總比忽視問題或試圖掩蓋問題要好。對於試圖掩蓋問題的人，稽核師不會手下留情。
- 密切配合稽核師的工作，對於任何不符合預期的數據，或出乎意料的文件要求，一一做出澄清。先確定同意測試內容和參數，再提供數據。若提供了不符合稽核師預期的資訊，稽核師可能認為這是在試圖拖延或掩蓋制度問題。在最壞的情況下，這會導致稽核過程延長，直至達到稽核師的要求為止。如果無法對稽核要求做出回應，就應準備好詳細解釋個中原因。探討是否有現成替代方案能滿足稽核師的要求。如果稽核範圍及流程均妥適，則在流程早期便應能發現難以回應的要求並妥善處理。另外，若稽核準備工作扎實，則應已涵蓋多數要求，並能隨時提供相關資訊。
- 僅根據稽核準備工作提供事實，不發表觀點。稽核過程中，關於政策或程序是否有效，或者政府法規是否合理的意見並不重要，發表此類意見卻可能出現問題。與稽核師進行溝通時，應保持專業、冷靜且有分寸。稽核的對象是制度，不是個人感受。
- 如果稽核師在稽核期間發現缺失，建議制定初步行動方案，並於稽核完成之前提交。

稽核後行動

- 每次稽核無論是例行公事或是痛苦差事，都應從中汲取經驗教訓。找出不盡人意的稽核因素，並積極改進；否則在後續稽核中，仍可能獲得同樣負面的稽核體驗。如發生最壞情況，組織會遭到罰款和處罰。謹記客觀評估團隊的表現。若放任對稽核流程產生挫敗感和負面情緒，可能影響任何稽核回應行動，甚至導致下一次稽核出現不良結果。
- 如果稽核開始前做足了功課，稽核結果應該不會有太多意外。亦即無需從頭瘋狂翻找資料，也能從容提供回應。若稽核結果中存在任何誤解或錯誤看法，務必加以更正。更正相關誤解或錯誤看法，並不表示稽核師會接受您的答覆；但如果不回應該問題，則可能被視為承認缺失，以致為未來的稽核埋下一枚未爆彈。
- 妥善計劃並落實必要的改正措施，不可等到下次稽核之前臨渴掘井。若只想在下次稽核之前臨陣磨槍，匆匆回應先前稽核中發現的問題，不僅會削弱稽核準備工作的作用，還可能導致相關緩解措施效力下降。任何稽核師若發現先前稽核中提出的建議未受到充分重視，都不會心慈手軟——無論是組織落實得不夠充分，還是苦苦解釋未落實建議的原因都不行。
- 確保將監管稽核結果和改正措施提供給後來的內部稽核師或第三方稽核師。他們的調查結果可能有助於確定組織對官方稽核的回應能否令監管機關滿意。
- 規劃過程中，應充分考慮稽核需求。對於任何法規遵循制度體系，稽核都是不可或缺的一部分，因此應將其納入年度計劃、預算，以及組織法規遵循文化。制定一套準備程序可能頗為實用，但應確保其與法規遵循程序分開，並且獨具特色。
- 面臨稽核時，準備、管理、回應與重複，缺一不可。

結語

要想成功通過稽核，既需優化管理流程，亦需團隊的密切配合。稽核，就像是要求嚴格的老師所出具的專業成績單。稽核結果不盡相同，可能是表揚工作出色（有效期至下次稽核前），也可能是坦率評估組織的法規遵循工作。事實上，通過稽核僅僅是最低的可接受結果。以開放的心態自信地接受稽核。本文中提出的建議措施並非稽核的金科玉律；就如同商界的其他眾多要求一樣，這些建議都基於業界常識，要求瞭解自身職責並盡己所能履行職責的敬業精神。與制定預算流程相同，凡扎實準備、明智地管理、密切跟進後續工作，就能有效節省精力，從容應對實際挑戰。

Ed Beemer，CAMS-FCI，efb@compliancecomm.com

Lauren Hughes，CAMS-FCI，laurenhughes81@gmail.com

資料洩露的最佳危機管理作法：（上）

近年來，許多公司的機密資訊接連遭受非法存取，令這些公司深陷危機，焦頭爛額。除了資料洩露外，各大企業或許還面臨其他危機。新冠疫情爆發後，各大企業不得不啟動危機管理計劃；若此前無相應計劃，就只得立即制定。設想一下，如果媒體突然報導，您有一家重要客戶與某一恐怖組織或不為人知的組織存在直接聯繫，試圖洗錢。儘管您先前已經採取了所有預防措施，但結果會如何？毫無疑問，您的「了解您的客戶」和風險管理流程均將受到嚴格審查。此外，新聞一旦公之於眾，又將帶來何種影響？

資料洩露事件代價巨大。Ponemon 研究院的一份報告指出，資料洩露事件的平均總成本高達 386 萬美元，其中包括：檢測與升級成本 111 萬美元、業務損失成本 152 萬美元、通知成本 24 萬美元、事後應變成本 99 萬美元。[1] 當中，與「收入損失」相關的成本佔比最高，約佔總成本的 40%。同一份報告還指出，如果企業設有事件應變團隊，進行過事件應變預演，平均成本則會降低 200 萬美元左右。

本文分為上、下兩篇，旨在介紹最佳危機管理作法，並探討一些值得深究的資料。文中提及的最佳作法，或許可以用於多種危機管理，但本文的關注重點是未經授權的資料洩露危機。

專家們在某些方面意見一致，在某些方面卻爭論不休。他們的首要結論是：必須未雨綢繆，做好準備。俗話說得好：防患於未然。重點不是資料洩漏事件是否會發生，而是何時會發生。

在針對資料洩露的風險方面，必須實施資訊安全、電腦安全、控制措施、隱私政策、培訓課程等舉措。事實上，成功打造出「安全文化」至關重要。[2] 本文對上述方面絕非置之不理，只是希望將重點放在探討危機管理流程的相關層面。

預防措施（危機前）

危機預防措施涉及眾多層面；影響眾多部門，自然也涉及高階管理層。有些預防措施偏重技術層面（適當的管理控制措施，或者特定的 IT 安全措施），有些偏重財務層面（購買網路保險 [3]），有些則偏重策略管理層面（整體風險管理與法規遵循）。

以下是預防危機的最佳作法：

- 建立危機管理團隊
- 制定危機管理計劃
- 制定公關計劃

建立危機管理團隊

如需進行危機管理，首要的預防舉措之一，就是建立一支多領域的危機管理團隊，並提前考慮到成員出差、度假等因素，準備好備援力量。[4] 要實現此目標，需要闡明每位團隊成員的職能與責任，並指定好負責人。[5] 這支團隊的主要任務是：[6]

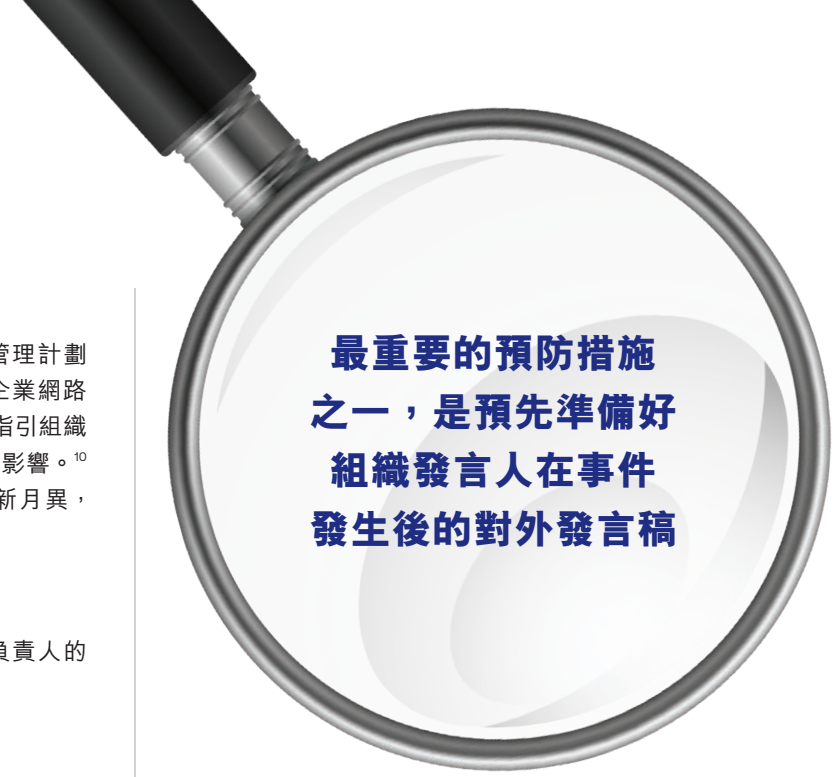
- 制定（或更新）危機管理計劃
- 針對危機管理計劃，為團隊成員和所有員工提供培訓
- 模擬不同的危機情境

鑒於危機管理的策略重要性，團隊裡應安排一名高階管理人員。[7] 此人除了從高階管理層的角度給予支持以外，也是高階主管與董事會成員的聯絡人。Experian 強調：「高階管理層的參與，對資料洩露應變計劃的成功與否有極大的影響……打造出網路安全文化。」[8]

危機管理團隊應由哪些人組成，相關人士的觀點不一。不過，就資料洩露方面而言，團隊中至少應有：

- 一位高階管理人員
- 一名 IT（或安全）專家
- 一名法律顧問
- 一位公共關係專家
- 一名人力資源負責人

此外，團隊應擁有可自由裁量的預算，能夠視情況諮詢或聘用外部資源。若危機真的發生，絕無時間協調相關資源，苦苦等待核准。



制定危機管理計劃

完成職能與責任的分配之後，下一步就是制定危機管理計劃(CMP)。正如 Experian 所述：「危機管理計劃是一切企業網路安全策略的重要組成部分。」[9] 危機管理計劃不僅能夠指引組織內部成員的行動，還有助於減少應變時間，降低財務影響。[10] 由於威脅因素、經濟環境等瞬息萬變，相關技術日新月異，危機管理計劃需要定期更新。[11]

危機管理計劃的主要構成如下：[12]

- 危機管理團隊成員的姓名與職能，後備人員、負責人的身分資訊
- 危機管理團隊成員的職能與責任
- 需要遵循的規程
- 外部利益相關者（如：徵信機構、執法機關人員、監管機構、外部法律顧問、專門從事資料洩漏調查的調查公司、可能受影響的業務合作夥伴等）的聯絡人
- 公關計劃（見下文）
- 業務持續性應急方案

鑒於商業勒索有增無減，企業機構應針對此類威脅制定危機管理計劃，並對可能面臨此類情況的員工展開培訓。[13] 此外，建議開設加密貨幣帳戶，因為加密貨幣是此類犯罪的首選支付方式。[14]

上述所有步驟，均有助於組織機構節省寶貴時間，儘快恢復正常運作。最後，要求危機管理團隊成員在某些策略性位置保存危機管理計劃的書面備份，因為若網路駭客發起阻斷服務攻擊，組織內部人員有可能長時間無法進入系統。

制定公關計劃

最重要的預防措施之一，是預先準備好組織發言人在事件發生後的對外發言稿。[15] 文稿的措辭、語調，以及組織發言回應的速度，均具備重大策略意義。在這些方面做得妥帖，有助於保護組織的聲譽，而且有可能減少財務影響。

公關計劃至少應包含：

- 公關團隊成員、後備人員和負責人的姓名與職能
- 組織的官方發言人（應為公共關係專家）
- 公關團隊成員的任務與職責

公關計劃還應包括：[16]

- 設立一個危機網站，並預先獲取核准。若發生危機，能啟用、完善並更新該網站
- 準備好高階管理層的新聞稿草案，並預先獲取核准。若發生危機，根據具體情況進行相關修訂後再行發佈
- 準備好符合監管法規遵循要求的（監管）公告，並預先獲取核准
- 正如 Communispond 執行長 Bill Rosenthal 所言：「做好準備，才能從容回答棘手問題。」[17]

公關計劃應涵蓋在發生資料洩露危機時，應如何通知組織員工、個人資訊遭洩露者、媒體、相關機構和業務合作夥伴，包括主要徵信機構（Equifax、Experian、TransUnion 等）：

- 如需聯繫員工，最好經由內部網路聯繫。若發生危機，應儘快通知員工，尤其是客服中心的員工。[18] 根據 Coombs 的說法，「瞭解情況的員工，就如同一條額外的公關管道，可以透過這些員工聯繫其他利益相關者。」[19] 此外，還可以通過內部網路聯繫業務合作夥伴。
- 至於（疑似和潛在）受害者，可採取多種途徑通知：新啟用的網站、其目前的帳戶、電子郵件、個人信件、傳統媒體、社交媒體等。建議「採取 [所有] 必要措施，維護客戶的信任度和忠誠度。」[20]

總之，資料洩露代價高昂，其影響難以消弭。本文（上）至此接近尾聲。本篇主要闡明，組織必須為資料洩露事件做好準備。要想實現這目標，就需建立一支職責明確的危機管理團隊，制定健全的危機管理計劃（包含公關計劃與應急計劃，列清程序、外部聯絡人等）並適時更新。

本文（下）將介紹應對資料洩露危機的最佳作法，探討後續措施，並提供若干建議。

Claude Mathieu，博士，教授，舍布魯克大學打擊金融犯罪研究生課程負責人，加拿大 ACAMS 蒙特利爾分會聯合主席，Claude.Mathieu@USherbrooke.ca

William Poisson，行政學碩士，CISSP，CISA，CISM，CFE，加拿大舍布魯克大學行政學碩士研究生，攻讀打擊金融犯罪課程

Yves Trudel，博士，教授，加拿大舍布魯克大學工商管理碩士及普通碩士課程主任，Yves.Trudel@USherbrooke.ca

1 “Cost of a Data Breach Report 2020”（2020 年資料洩露成本報告），*IBM*，2020 年 7 月，https://www.ibm.com/security/data-breach

2 Ramakrishna Ayyagari，“An Exploratory Analysis of Data Breaches from 2005-2011: Trends and Insights”（2005-2011 年資料洩露事件初探：趨勢與洞察），*Journal of Information Privacy and Security*，https://www.tandfonline.com/doi/abs/10.1080/15536548.2012.10845654；“Protecting Personal Information: A Guide for Business”（保護個人資訊：企業指南），*美國聯邦貿易委員會*，2016 年 10 月，https://www.ftc.gov/tips-advice/business-center/guidance/protecting-personal-information-guide-business

3 “Cybersecurity Insurance”（網路安全保險），*美國網路安全與基礎設施安全局*，https://www.dhs.gov/cisa/cybersecurity-insurance（訪問日期：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：您的公司準備好應對大量資料洩露了嗎？），*Experian and Ponemon Institute*，2018 年 2 月，https://www.experian.com/data-breach/2018-ponemon-preparedness?ecd_dbres_blog_2018_ponemon

4 同上；Theodore J. Kobus III，“2019 Data Security Incident Response Report: Managing Enterprise Risks in a Digital World”（2019 年資料安全事件應變報告：數位世界企業風險的管理），*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/

5 “PwC’s Global Crisis Survey 2019”（PwC 2019 年全球危機調查），*PwC*，2019 年，https://www.pwc.com/ee/et/publications/pub/pwc-global-crisis-survey-2019.pdf；Jena Valdetero 和 David Zetoony，“Data Security Breach Handbook for Hotels, Venues, & the Hospitality Industry”（旅館、會場和飯店業資料安全漏洞手冊），*Bryan Cave*，2016 年，https://www.lexology.com/library/detail.aspx?g=d26e57fb-a72e-4d35-a147-1a5bb913b7f0

6 Theodore J. Kobus III，“2019 Data Security Incident Response Report: Managing Enterprise Risks in a Digital World”（2019 年資料安全事件應變報告：數位世界企業風險的管理），*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”（網路安全事件受害者應變與報告的最佳作法），*美國司法部*，2018 年 9 月，https://www.justice.gov/criminal-ccips/file/1096971/download；“Data Breach Response Guide”（資料洩露應變指南），*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”（企業有效危機管理的最佳作法：透過案例分析細究危機的各個階段），*加州理工大學*，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

7 “Fifth Annual Study: Is Your Company Ready for a Big Data Breach?”（第五次年度研究：您的公司準備好應對大量資料洩露了嗎？），*Experian and Ponemon Institute*，2018 年 2 月，https://www.experian.com/data-breach/2018-ponemon-preparedness?ecd_dbres_blog_2018_ponemon

8 “Data Breach Response Guide”（資料洩露應變指南），*Experian*，2018-2019 年，https://www.experian.com/assets/data-breach/white-papers/experian-2018-2019-data-breach-response-guide.pdf，6。

9 同上，註 4。

10 “Best Practices for Victim Response and Reporting of Cyber Incidents”（網路安全事件受害者應變與報告的最佳作法），*美國司法部*，2018 年 9 月，https://www.justice.gov/criminal-ccips/file/1096971/download

11 同上；“Data Breach Response Guide”（資料洩露應變指南），*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：您的公司準備好應對大量資料洩露了嗎？），*Experian and Ponemon Institute*，2018 年 2 月，https://www.experian.com/data-breach/2018-ponemon-preparedness?ecd_dbres_blog_2018_ponemon

12 “Crisis Management and Communications”（危機管理與危機公關），*公共關係研究所*，2007 年 10 月 30 日，https://instituteforpr.org/crisis-management-and-communications。「Barton (2001)、Coombs (2007a) 和 Fearn-Banks (2001) 發現，危機發生時，危機管理計劃有助於節省時間：它能夠幫助人們預先分配部分任務、預先收集部分資訊，並將收集到的資訊作為參考。」

13 Theodore J. Kobus III，“2019 Data Security Incident Response Report: Managing Enterprise Risks in a Digital World”（2019 年資料安全事件應變報告：數位世界企業風險的管理），*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”（網路安全事件受害者應變與報告的最佳作法），*美國司法部*，2018 年 9 月，https://www.justice.gov/criminal-ccips/file/1096971/download

14 “BakerHostetler 2017 Data Security Incident Response Report Based on 450 Incidents”（BakerHostetler 2017 年資料安全事件應變報告，基於 450 起事件），*BakerHostetler*，2017 年，https://www.databreaches.net/bakerhostetler-2017-data-security-incident-response-report-based-on-450-incidents/

15 Bokyung Kim、Kristine Johnson 和 Sun-Young Park，“Lessons from the five data breaches: Analyzing framed crisis response strategies and crisis severity”（五次資料洩露事件帶來的教訓：結構化危機應變策略與危機嚴重程度分析），*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”（企業有效危機管理的最佳作法：透過案例分析細究危機的各個階段），*加州理工大學*，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

16 “Data Breach Response Guide”（資料洩露應變指南），*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：您的公司準備好應對巨量資料洩露了嗎？），*Experian and Ponemon Institute*，2018 年 2 月，https://www.experian.com/data-breach/2018-ponemon-preparedness?ecd_dbres_blog_2018_ponemon

17 Nate Lord，“Data Breach Experts Share the Most Important Next Step You Should Take After a Data Breach in 2019 & Beyond”（資料洩露專家分享重要後續步驟，助您從容應對 2019 年及未來的資料洩露危機），*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

18 Katelyn Smith，“Best Practices for Effective Corporate Crisis Management: A Breakdown of Crisis Stages through the Utilization of Case Studies”（企業有效危機管理的最佳作法：透過案例分析細究危機的各個階段），*加州理工大學*，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

19 “Crisis Management and Communications”（危機管理與危機公關），*公共關係研究所*，2007 年 10 月 30 日，https://instituteforpr.org/crisis-management-and-communications/

20 “Fifth Annual Study: Is Your Company Ready for a Big Data Breach?”（第五次年度研究：您的公司準備好應對巨量資料洩露了嗎？），*Experian and Ponemon Institute*，2018 年 2 月，https://www.experian.com/data-breach/2018-ponemon-preparedness?ecd_dbres_blog_2018_ponemon，2。

了解您的客戶所需的正確資料

在當今的金融犯罪法規遵循世界中，監管機構齊心協力，把了解您的客戶 (KYC) 要求不斷推向新高——至少在許多 KYC 和防制洗錢 (AML) 從業人員看來是如此。越來越多人期望能夠運用客戶相關的大量可取資料。然而，單純增加資料要求並不能保證實現最終目標——建立強大的防制洗錢法規遵循制度，對金融機構而言，這一制度應能滿足監管要求且無礙業務成長。

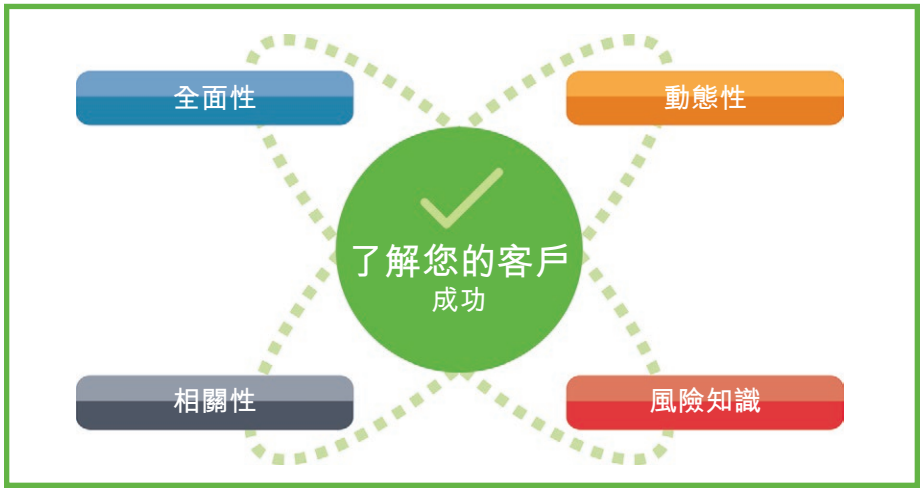
為實現這個最終目標，必須徹底轉變「了解您的客戶」的實施方式。具體而言，防制洗錢專業人士不僅應關注個別資料元素的收集和彙整，還應注重缺失的資料元素，而只有通過深入研究圍繞每個資料元素的人員決策過程，以及資料元素之間的關係，才能找出缺失的資料元素。

在討論「了解您的客戶所需的正確資料」之前，首先應從目前及未來的角度定義何謂「確實了解您的客戶」。

目前如何定義「確實了解您的客戶」？

迄今，「確實了解您的客戶」似乎都以收集到的資料量來衡量。在某些情況下，可能會重視資料的彙整與呈現方式。此外，也曾根據資料收集與彙整的速度和效率來下定義。看起來，古老的「力度測試法」似乎被運用在「了解您的客戶」領域——資料越多，越遵循法規。而這正是問題所在：人們歷來關注的都是法規遵循與法規遵循成本問題，卻未充分關注「對正確的客戶做出正確的決定，以增加企業收入」。

圖 1：「確實了解您的客戶」要素



未來又如何定義「確實了解您的客戶」？

未來「確實了解您的客戶」的定義取決於四大制度要素：必須具備整體性、動態性和相關性，必須清楚風險及所有制度要素之間的相互影響（見圖 1）。「確實了解您的客戶」將有助於更瞭解潛在客戶和現有客戶。要想實現這一點，就需要將收集到的資料以動態、即時的方式全面彙整。這意味著，我們需要瞭解在目前各種不同系統和流程中，資料元素之間存在的運用與流程關係；也要瞭解客戶帶來的風險，以及這些風險在客戶生命週期中將產生何種變化。

有人可能會說：我們已經在做這件事了，但實際上，目前仍著重於收集供決策使用的完整、準確、及時的資料，而非關注決策過程。更具體點說，正在收集的資料元素之間的關係，以及這些資料元素與資料關係如何影響客戶風險判定，都還未受到確切的關注。

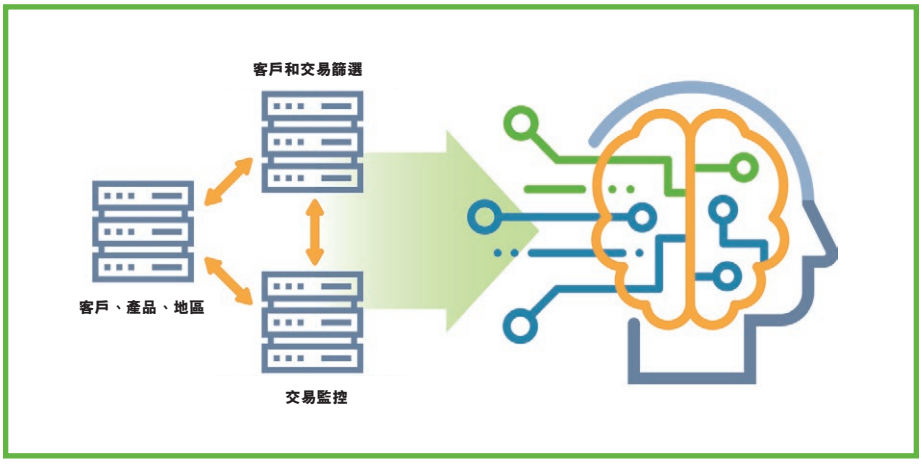
未來「了解您的客戶」是否奏效不再取決於資料量多寡，而是擁有可理解且可供參考的資料。此種資料具有整體性、動態性和相關性，能幫助您識別希望接納的客戶或希望拓展關係的客戶。

如何從目前邁向未來

如今，防制洗錢領域孤島林立。在人類決策的背景下，首先應研究、確定並理解所有資料元素在三大防制洗錢領域（制裁名單篩查、交易監控和了解您的客戶）中如何共同描繪客戶畫像（見圖 2）。

第一步應查看各孤島系統個別收集的資料元素，然後研究資料特徵或是資料元素之間的關係，不僅從孤島內部觀察，還要觀察各孤島之間的資料關係，這非常重要；實現之後，才有助於形成整體視角。顯然，要完成此項工作，即使沒有最優質的資料，也應使用良質的資料，但其相關性必須從人類決策角度進行定義。

圖 2：防制洗錢的三大領域



舉一個基本的例子：在預期正常活動的情況下，該活動與處境相似的客戶之間的關係，以及該活動與問題客戶交易及處境相同客戶交易的關係。目前收集資料的方式，通常是與客戶或潛在客戶面談，詢問客戶期望的活動。此類資料將忠實地記入「了解您的客戶」文件，還會在方框上打勾，表示已取得該類資訊。接下來就要靠「了解您的客戶」分析師（可能是領域專家，也可能不是；但大概不是客戶、行業和交易類型的專家）判定預期的「正常活動」究竟是否確實正常。

在此情境中，並無收集和評估其他資料元素的機制，用以證實或以其他方式支持客戶提供的資訊，完全依賴「了解您的客戶」分析師或案件調查員，尋找和評估此情況下的活動。

但事實是，「了解您的客戶」文件中可能已經提供了大量資料。例如：對於大型客戶，可能已經取得其年度、季度或其他報告可「證實」公司狀況。從這些報告當中，可以蒐集到哪些資料來證實或預測「預期正常活動」？其中的挑戰在於：如何讀取、識別、擷取並分析這些額外資料元素，形成更深入、更全面的客戶活動藍圖。

對「了解您的客戶」資料的觀念轉變將是一種典範移轉

「了解您的客戶」不僅應從資料收集與作業方面做出改變，還應提出有關「了解您的客戶」資料的新問題。新問題應比監管要求更深入，更著重「了解您的客戶」資料的價值——可以是有關信用、行銷視角等預測重點。

例如，若從貸款（即信用）等角度看待「了解您的客戶」，就應全面審視客戶，評估客戶的實力和可靠性，以及其拓展業務的可行性。從客戶已完成的事項來觀察客戶，作為預測客戶未來可能行事的指標。此外，應從行銷角度審視「了解您的客戶」，例如，詢問客戶喜歡什麼或未來想做什麼，因為客戶目前的行事可能是未來行動的指標。應當將此觀點融入「了解您的客戶」防範金融犯罪思維之中，因為客戶想要做的事可能會超出正常範圍，值得調查，也可能需要提交報告。

新型防制洗錢專員

為達成上述典範移轉，防制洗錢專員必須轉變思維方式。新思維應融合目前所有可用資料，更重要的是，融合涉及目前資料元素關係的所有資料；還應當瞭解目前的決策過程，以及進一步瞭解資料與決策過程的關係。只有這樣，才能將正確的資料呈現給「了解您的客戶」分析師，供他們在決策過程中使用——或更重要的是，讓人工智慧技術可運用並產生可能的決策，供「了解您的客戶」分析師確認。

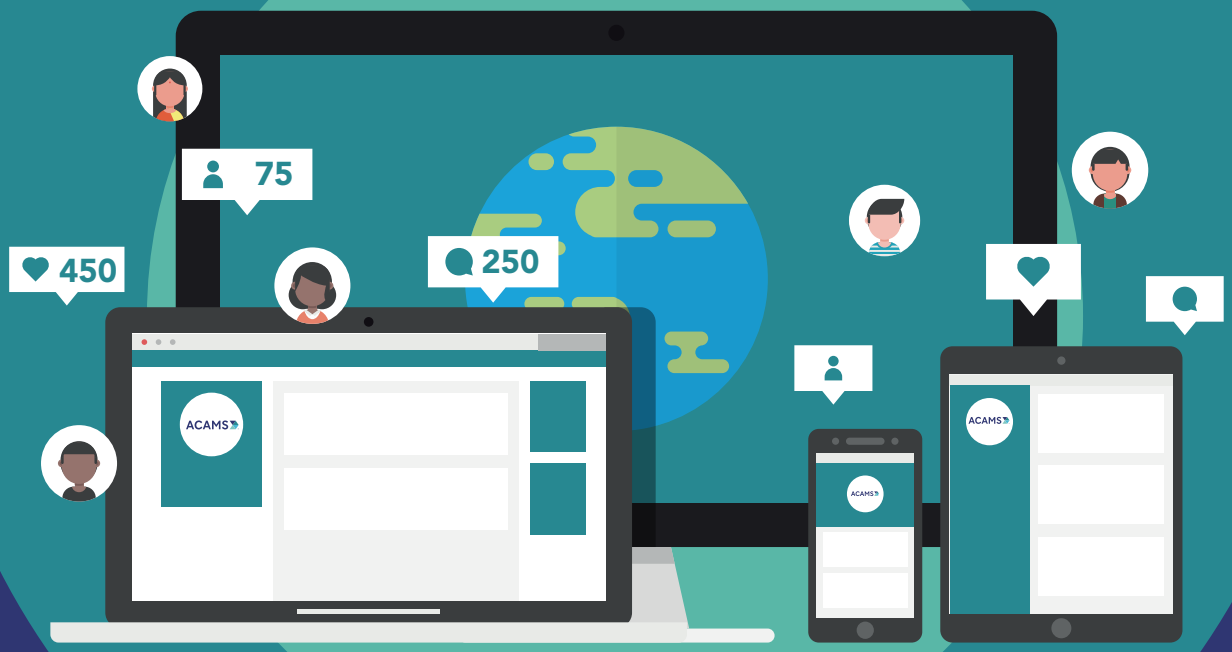
此外，「新型」防制洗錢專員應想得更深遠，不應局限於滿足當今的監管要求。獲取並運用正確的「了解您的客戶」資料確實需要投入資金。新型防制洗錢專員必須站在企業角度思考問題，理解正確的「了解您的客戶」資料是企業的利器，而非視為另一項窒礙的要求。

只要新型防制洗錢專員擁有了正確的思維方式，防制洗錢專業人士最終可實現理想——「我來自法規遵循部門，我是來幫忙的！」

Steve Marshall，
FinScan 集團 / Innovative Systems, Inc.
暨 FinScan 顧問服務協理，
美國賓夕法尼亞州，
smarshall@innovativesystems.com

ACAMS™
公認反洗錢師協會

讓我們來交流吧！



關注我們

掃碼 →

20 年風雨，20 個變化

《今日 ACAMS》將點出 20 年來最具顛覆性的 20 件防範金融犯罪 (AFC) 大事，為 ACAMS 20 週年慶活動掀開序幕。編輯團隊徵求 ACAMS 顧問委員會聯合主席 Rick Small (CAMS) 和 ACAMS 前顧問委員會成員 Lauren Kohr (CAMS-FCI) 的意見。

Small 是 Truist 防範金融犯罪團隊負責人，職責包括管理防制洗錢 (AML) 法規遵循事務、控制和調查、詐騙管理以及網路事件所致金融調查等。他於 2016 年加入 BB&T（現為 Truist），擔任首位金融犯罪制度總監。

Small 在公營和私營機構工作超過 35 年，經驗豐富。加入 BB&T 之前，他在安永擔任防制洗錢和防範金融犯罪資深顧問；在美國運通任全企業防制洗錢、反貪腐和國際監管法規遵循資深副總裁；在通用電氣旗下部門 GE Money 任防制洗錢負責人。Small 在私營機構的任職經歷始於花旗集團，擔任全球防制洗錢董事總經理。

在私營機構任職之前，他曾在美國政府歷任過多個職位，首先是美國司法部反壟斷部門的聯邦檢察官，後來任職於打擊有組織犯罪工作組，再後來在美國財政部任執法機關的資深法律顧問。最近的政府職位是在聯邦儲備系統理事會任監督與監管處副處長。

Kohr 工作經歷豐富，在防範金融犯罪部門工作超過 16 年，在銀行保密法 / 防制洗錢 (BSA/AML) 和制裁法規遵循方面有豐富經驗，同時曾管理複雜的監管問題及補救專案，以及促進公私合作以制定有效策略打擊非法金融活動。她現任 ACAMS 美洲防制洗錢部門資深總監，專注於建立全球防範金融犯罪工作組，專門促進公私合作，協助執行全球執法策略，同時是防制洗錢 / 打擊資恐 (AML/CTF)、監管政策和防制洗錢制度優先事項的領域專家和技術專家。此前，她曾在維吉尼亞州泰森斯角的歐道明國民銀行（Old Dominion National Bank，

簡稱 ODNB）擔任資深副總裁、風險長和銀行保密法主管。任職期間，Kohr 負責該行的企業風險管理制度，包括領導該行建立銀行保密法 / 防制洗錢及海外資產控制辦公室 (OFAC) 制度。

加入該行之前，Kohr 曾在賓夕法尼亞州哈裡斯堡的 Metro 銀行擔任副總裁 / 總監，負責防制洗錢 / 銀行保密法 / 海外資產控制辦公室工作。在此期間，她負責制定、實施和監督《銀行保密法》法規遵循制度體系各方面的工作，包括美國《愛國者法案》、防制洗錢和海外資產控制辦公室相關法規。Kohr 是 2016 *「ACAMS 年度防制洗錢專業人士」*的獲獎者，也是 2016 *《今日 ACAMS》年度文章獎*得主，2019 年獲 *「美國首都分會公私合作獎」*。她經常在公私營機構舉辦的國內和國際大會上發言，主題遍及防制洗錢、《銀行保密法》、海外資產控制辦公室和打擊資恐等。Kohr 現為 ACAMS 美國首都分會理事和防制洗錢合作論壇理事，也是「共同賦能：防制洗錢女性」倡議發起人之一。她之前還曾在 ACAMS 諮詢委員會任職。

作為各大領域的專家和防範金融犯罪領域的知名演說家，Small 和 Kohr 向 *《今日 ACAMS》*分享了過去 20 年裡最重要的 20 件防範金融犯罪大事。討論時，Small 和 Kohr 在他們的清單裡提到了類似的事件。*《今日 ACAMS》*採納了他們的寶貴意見，結合他們的清單，為您帶來過去 20 年裡最具顛覆性的 20 件大事：

1. 2001 年 911 事件
2. 美國《愛國者法案》
3. 聯邦金融機構檢查委員會《銀行保密法 / 防制洗錢檢查手冊》
4. 提升公私合作關係
5. 金融機構參與行業活動，共同打擊人口販賣，幫助人口販賣的倖存者
6. 防制洗錢範圍擴大，納入打擊資恐
7. 防制洗錢範圍擴大，納入網路犯罪
8. 防制洗錢範圍擴大，納入詐騙活動
9. 金融機構參與行業活動，與非營利組織合作，為非政府組織和非營利組織提供指導和銀行服務
10. 客戶盡職調查的監管
11. 受益所有權規定
12. 2020 年《防制洗錢法》
13. 首次發佈防制洗錢國家優先事項
14. 替代傳統銀行的金融科技公司興起，提供銀行相關服務
15. 數位貨幣納入加密貨幣、虛擬貨幣和非正式資產移轉體系
16. 防制洗錢技術納入大數據、人工智慧、機器學習和自動交易監控系統
17. 辨識社會影響問題（如環境犯罪）相關的資金流向
18. 貿易洗錢
19. 規避制裁陰謀的複雜性
20. 新冠疫情

最後，Small 和 Kohr 就未來 20 年對防範金融犯罪行業的影響分享了看法。Small 表示：「在接下來的 20 年裡，我預計新興技術將蓬勃發展，為防制洗錢風險管理提供尖端技術解決方案。」

Kohr 補充說：「未來 20 年的重點工作是：

- 繼續創新增效，打擊洗錢、資恐和資助武擴活動
- 加強公私合作，增加資訊共享機會
- 促使防範金融犯罪社群在打擊令人髮指的罪行上，既能主動出擊也能積極應變
- 超越自我，超越本職工作，拓展思路，打破常規

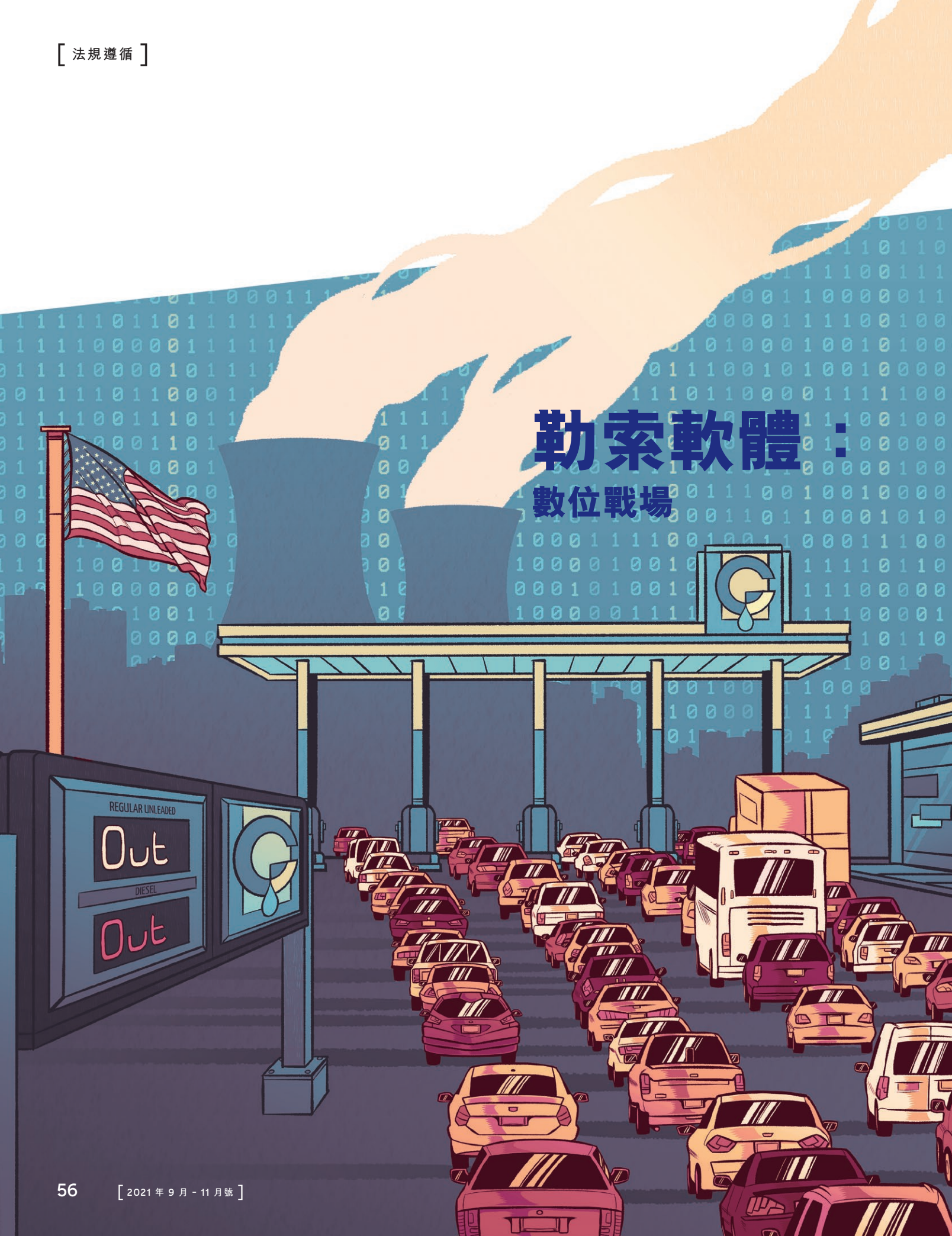
我們都要發揮自己的功能，想辦法推動防範金融犯罪社群的發展，推進各項倡議和計劃；不找藉口，因為我們不能讓障礙和挑戰阻止我們奮進的步伐。我們做得到的。」

在啟動 ACAMS 20 週年慶活動之際，我們也希望銘記和緬懷在美國本土發生最可怕的 911 恐怖攻擊中喪生的 2,977 條生命。此外，我們也要銘記並感謝在那個可怕日子不畏危險、拯救同胞的救難人員，向他們的敬業精神致敬。

作為努力終結金融犯罪及相關犯罪活動的社群和行業的一員，*《今日 ACAMS》*充滿感激。希望您能加入我們，從現在開始一起慶祝 ACAMS 的 20 週年並邁入 2022 年。

Karla Monterrosa-Yancey，CAMS，ACAMS《今日 ACAMS》雜誌總編輯，美國佛羅里達州，kmonterrosa@acams.org

Stephanie Trejos，CAMS、編輯、ACAMS，美國佛羅里達州，strejos@acams.org



勒索軟體：
數位戰場

在網際網路時代，駭客攻擊意味著丟失個人身分資訊 (PII)。在 2018 年駭客對 Facebook 發起的攻擊中，5,000 萬用戶發現，自己的生日、教育背景、位置等個人身分資訊容易受到網路犯罪者攻擊；[1] 連 Facebook 執行長 Mark Zuckerberg 的帳戶也被盜。他表示，攻擊者可以查看被盜帳戶的私人訊息或貼文，但無法存取財務資料。

現在快轉到加密貨幣時代（金錢網路），駭客攻擊意味著不只是可能丟失個人身分資訊，還可能喪失畢生積蓄——想想以網際網路的速度行竊。同時，也顯示勒索軟體即服務 (RaaS) 供應商、恐怖分子線上籌資、程式化洗錢行為和民族國家行動者的網路攻擊，以前所未有的速度和規模擴散。2021 年 5 月，針對 Colonial Pipeline 的勒索軟體攻擊不僅導致美國東海岸進出加油站的道路陷於癱瘓，還導致美國國家安全政策發生轉變，讓執法機關和政策制定者意識到：戰鬥的硝煙已經轉移到網路上。

Colonial Pipeline：案例分析

2021 年 5 月 7 日，Colonial Pipeline 慘遭勒索軟體攻擊，該公司經營一條 5,500 英里長的輸油管，向美國東海岸輸送 45% 的汽油和航空燃料。為應對這次攻擊，Colonial 主動關閉了業務點，導致燃油短缺，人們從邁阿密到紐約的加油站排著長隊等待加油。一些學校甚至利用網路教學以應對此次攻擊。

5 月 10 日，*《紐約時報》*報導，美國聯邦調查局證實，DarkSide 勒索軟體是導致 Colonial Pipeline 網路癱瘓的罪魁禍首。[2]

DarkSide 是一家勒索軟體即服務供應商，在暗網上銷售惡意軟體，從買方透過惡意軟體獲得的利潤中分得一杯羹。什麼是勒索軟體和勒索軟體即服務？勒索軟體是一種惡意軟體，網路犯罪者利用此類軟體阻斷受害者存取自己的資料。此類網路犯罪者會進入受害者的系統並對文件加密，將資料當成「人質」，收到贖金後再解密。初次感染之後，勒索軟體可能試圖經由受害者的網路傳播至共享硬碟、伺服器、連接的電腦及其他可存取的系統。勒索軟體即服務讓（無編碼經驗的）不法分子也可以發起勒索軟體攻擊。不妨將其想像成一家網路犯罪麥當勞餐廳，在這裡，「加盟者」可以購買勒索軟體即服務套件。在暗網上，人們可以通過 Tor 瀏覽器輕鬆獲得此類套件。勒索軟體即服務的開發人員收取一筆加盟費，其中包括一定比例的利潤（通常為 20%-30%）。然後，勒索軟體即服務的開發人員提供品牌、培訓、設備和全天候支援服務作為回報。不法分子不需要任何專業知識。受害者通常被要求以比特幣等加密貨幣支付贖金。

但勒索軟體早在加密貨幣出現之前就已存在。早在 2005 年，不法分子就設立空殼公司接受信用卡、預付現金卡和禮品卡的付款。雖然加密貨幣並非勒索軟體形成的原因，但加密貨幣具有成本低、速度快和匿名的特點，成為網路犯罪分子的首選貨幣。

在 Colonial Pipeline 遭到攻擊後，負責網路與新興技術的副國家安全顧問 Anne Neuberger 5 月 10 日在白宮舉行了簡報會。她將此次攻擊描述為「勒索軟體即服務的變體」，其中，「犯罪組織進行攻擊，然後與勒索軟體的開發人員分享犯罪所得，」並證實聯邦調查局 10 月以來一直在調查 DarkSide。[3] 除了封鎖 Colonial Pipeline 的電腦系統，包括公司的計費系統，使公司無法跟蹤燃油配送情況、無法計費，DarkSide 還竊取了超過 100 GB 的公司資料。[4]

5 月 13 日星期四，也就是攻擊發生近一周後，有報導稱 Colonial 支付了 75 個比特幣的贖金（價值高達 500 萬美元），可以在 5 月 12 日星期三恢復服務。[5] 5 月 8 日，有人從美國的一家交易所提取了 75 個比特幣，不久後將其轉入 DarkSide 勒索軟體支付地址。[6] 這筆資金很快就洗白，進入 DarkSide 的比特幣錢包。

5 月 14 日星期五這天，對 DarkSide 來說，可謂禍從天降。據 Intel 471 網站消息，Darkside 告訴附屬組織，其失去存取本身基礎設施的權利，很快就會關閉服務，因為執法機關進行干預，美國也施加很大的壓力。DarkSide 補充說，他們付款伺服器上的資金被轉入一個未知帳戶，成為「扣押」行動的一部分。[7] 5 月 13 日，有人從 Darkside 錢包裡取走了 113.5 個比特幣，存入另一個錢包。

6 月 7 日，Colonial 遭到攻擊一個月後，美國司法部宣佈成功地從存放贖金的加密貨幣錢包裡扣押了 63.7 個比特幣（合 230 萬美元）。扣押令由加利福尼亞州北區法院出具。[8]「今天早些時候，美國司法部已經找到並收回 Colonial 支付給 DarkSide 網路的大部分贖金。勒索軟體攻擊始終都是不能容忍的，如果它們要針對重大基礎設施，我們將不遺餘力地反擊，」副總檢察長 Lisa Monaco 在新聞發佈會上這樣說。[9] Monaco 在一份新聞稿中表示：「資金線索追蹤能力仍然是我們最基本，也是最強大的工具之一。支付的贖金是驅動數位勒索引擎的燃料，今天的公告表明，美國將使用所有可用工具，使犯罪組織付出更高的代價，使其攻擊行為變得無利可圖。」[10]

可是僅靠追蹤資金線索，執法行動只能到此為止。區塊鏈分析是非常強大的工具，讓執法機關能採用劇烈變革的金融犯罪調查方式，追蹤開放區塊鏈上的資金流動情況。然而，雖然透過

區塊鏈分析能追蹤加密貨幣的動向，但這些工具無法扣押非法資金。當美國司法部在新聞稿中宣稱，「透過審查比特幣公開帳本，執法機關能追蹤到以特定地址為目的地……的多筆比特幣轉帳交易，而聯邦調查局則有該地址的『私鑰』」，[11] 大家不禁想問，「聯邦調查局是如何破解私鑰，扣押非法所得的？」

可能性有多種——從運用技術破解到依賴人為情報。正如《*紐約時報*》報導稱，「加密貨幣專家表示，聯邦調查局依靠的似乎不是區塊鏈技術的基礎漏洞。比較可能的是依賴老式的警察調查工作。」《*泰晤士報*》稱，「聯邦探員獲得 DarkSide 私鑰的方式可能是在 DarkSide 網路內部安插臥底，駭入儲存 DarkSide 私鑰和密碼的電腦，或者使用搜索票或其他方式，迫使持有其私人錢包的服務機構交出 DarkSide 的私鑰。」[12] 歸根結底，這次扣押要歸功於出色的偵察工作。無論是高科技還是人為，這次成功扣押很可能是幾個月來出色調查工作的結果。正如白宮在有關 DarkSide 的首場新聞發佈會上所提，聯邦調查局自 10 月以來一直在調查 DarkSide。雖然這次迅速地追回比特幣，但這很可能是跨部門經年累月的努力及全球通力合作，建立起勒索軟體供應商和網路犯罪分子網路的成果。

Colonial Pipeline 案對美國未來的國家安全政策有什麼意義？

在 Colonial Pipeline 網路攻擊發生後，聯邦調查局局長 Christopher Wray 比較了 911 事件與最近對 Colonial 及全球最大肉品供應商 JBS Foods 等發生的網路攻擊。他告訴《*華爾街日報*》，「這些事件有許多相似之處，我們非常重視打擊和預防工作。」[13] 就在前一天，美國司法部將網路入侵提升到反恐調查的級別，指示美國各地的檢察官辦公室與新成立的勒索軟體和數位勒索任務小組合作，協同調查涉及勒索軟體、網路攻擊、防毒反制服務、非法線上論壇或市集、加密貨幣交易所、防彈主機服務、僵屍網路和線上洗錢服務的案件。[14] 執法機關的轉變可能顯示著 20 多年來國家安全政策的首次轉向——承認「911」已經成為過去，恐怖分子、網路犯罪者和流氓國家行為者已進入數位戰場。

法規遵循團隊和私營機構可以採取哪些措施防止網路攻擊

可以說，最有用的教訓來自 1980 年代的偉大電影，網路防禦也不例外。Ronald Reagan 總統看了法規遵循部門必看的一部電影《*戰爭遊戲*》——上世紀 80 年代的經典影片，由 Matthew Broderick 主演，他無意中侵入了一台軍用超級電腦並差點引發了第三次世界大戰——過後不久，他就做了件著名的事，就是責成美國國家安全局加強全國政府、企業和個人系統的網路防禦能力。[15] 目前這項工作仍在實施。

討論有關對付從事勒索軟體和其他網路攻擊的不法分子，則需探討全球公私合作的問題。[16] Colonial Pipeline 和 JBS Foods 等關鍵基礎設施由私營機構實體控制。2021 年 6 月 2 日，副國家安全顧問 Anne Neuberger 給私營機構寫了一封公開信，敘述私營機構加強對勒索軟體攻擊防禦能力的方式。[17] 具體而言，公開信敦促私營機構立即採取圖 1 中描述的行動。

無論是主動或被動應對勒索軟體，企業必須上下齊心，共同作為。首先要教育員工，不要點擊垃圾郵件中的連結或未知網頁。勒索軟體攻擊最常見的來源是釣魚郵件。[18] 電子郵件的攻擊方式通常利用社交工程——利用人類心理而非技術攻擊——來取得電腦系統的存取權。攻擊者依靠社交互動而非高科技駭客技術誘騙員工交出系統存取權。員工一旦點擊連結，惡意軟體就會接管系統，散播至連接的系統，搜尋有價值的資料。

雖然私營機構大多能積極主動地實施網路衛生措施，強化電腦系統和通訊協議，但隨時做好準備、從容應對攻擊也很重要。在最近的一次採訪中，Hunton Andrews Kurth 網路安全實踐部門負責人 Lisa Sotto 這樣解釋：

> 「在發生安全漏洞問題時，公司減輕傷害的一個重要方式是主動作為，防患於未然。至關重要的是，要制定最新的事件應變計劃，運用桌上演練反復練習。公司要組建訓練有素的事件應變團隊，在發生安全問題時，團隊成員知道自己的職能與責任。」

Sotto 繼續說明：

> 「一旦公司獲知發生了網路攻擊，就必須迅速召集適當的專家協助解決問題，包括經驗豐富的法律顧問、鑑識調查公司、勒索軟體談判專家（如果遭到勒索軟體攻擊）和外部公關公司（若適用）。強烈建議公司與執法機關合作，及時發現入侵指標或與威脅行為者相關的其他資訊，加快恢復進度。」[19]

最重要的是，私營機構 IT、法規遵循和金融犯罪專家可以發揮極大功能，主動和被動地應對勒索軟體和網路攻擊的威脅。有一件事情是清楚的：各國政府、私營機構甚至個人必須在全球範圍內密切合作，避開和應對威脅。換句話說，我們可以從《*戰爭遊戲*》中學到很多東西。

圖 1：美國政府針對防範勒索軟體威脅提出的最佳作法建議

落實拜登總統在「改善國家網路安全」行政令中提及的最佳作法：這些作法包括：(a) 使用多因素身分驗證而非單獨依賴密碼；(b) 使用網路檢測和回應技術主動檢測和搜尋網路上的惡意活動，在惡意活動破壞網路或系統之前加以阻止；(c) 如果勒索軟體不僅透過加密將資料作為人質，還威脅揭露敏感資訊，甚至在已恢復備份資料時仍威脅揭露資訊，試圖獲取更多贖金，則可使用加密技術將損害降至最低；(d) 委託有適當及合資格的系統安全團隊監控可用資訊，檢測是否存在新的威脅，即時修補和維護企業的 IT 系統、防範此等威脅。

將系統映像、組態和資料備份至離線儲存設備上，定期測試備份：勒索軟體會定期嘗試加密和刪除可從業務網路存取的備份。因此，應將備份儲存在離線設備上，使企圖加密攻擊企業 IT 系統的勒索軟體無法存取資料。此外，建議企業定期測試備份，確定備份是否足以在發生攻擊時恢復系統。

及時修補和更新系統：隨著新漏洞的發現，修補是防止勒索軟體攻擊的關鍵舉措。組織機構應考慮部署修補管理系統，採用風險為本的評估策略決定修補作業系統、應用程式和韌體的時機。

測試事件應變計劃：企業應制定事件應變計劃，運用桌上模擬演練定期測試這些計劃，及時發現和解決計劃中存在的任何缺陷。在審查事件應變計劃時，企業應自問幾個核心問題，包括 (a) 哪些是企業持續營運不可或缺的系統；(b) 在沒有特定系統的情況下，企業可以持續營運多長時間；(c) 如果特定業務系統（例如計費系統）受到勒索軟體攻擊，企業是否會被迫停止製造業務。企業根據上述問題適當調整事件應變計劃。

檢查安全團隊的工作：公司應運用滲透測試和其他漏洞測試，檢查其系統的安全性。

網路隔離：勒索軟體攻擊可能竊取資料，干擾公司營運。對於從事製造和生產業務的企業，如果勒索軟體能進入製造和生產控制系統，勒索軟體攻擊就會產生重大影響。本函建議，控制製造和生產作業的電腦網路應與用於公司業務功能的網路分開，企業要確認這些網路之間的連接，並仔細過濾和限制這些網路之間的網際網路存取。此舉可確保隔離製造和生產網路，當企業網路被攻擊時，製造和生產作業能繼續進行。企業應定期測試應急計劃，例如手動控制，確保在勒索軟體攻擊期間關鍵的安全功能可以正常運行。

資料來源：“What We Urge You To Do To Protect Against The Threat of Ransomware”（關於防範勒索軟體威脅的建議），白宮，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

除勒索軟體之外：恐怖份子籌資和程式化洗錢

雖然勒索軟體近來最受關注，但其他威脅也轉到了網路。2021 年 7 月 1 日，以色列國家反恐籌資局 (NBCF) 發佈行政令，扣押哈馬斯代理人控制的比特幣、Doge、Tron 和其他加密貨幣地址。[20] 不到一年前，美國司法部發佈公告稱，美國國稅局刑事調查處、國土安全調查局和聯邦調查局成功扣押 150 多個加密貨幣帳戶，這些帳戶涉嫌洗錢，且與屬哈馬斯軍事部門 al-Qassam 旅的帳戶有資金往來。[21]

2021 年 2 月，美國司法部公佈了一份長達 33 頁的聯邦起訴書，指控三名北韓電腦程式人員，稱他們參與了大量全球犯罪陰謀，發動了一系列惡意網路攻擊，從全球金融機構和其他公司盜取高達 13 億美元的加密貨幣和法定貨幣。[22] 起訴書內反覆提及有關惡意軟體、首次代幣發行騙局及針對加密貨幣企業的網路釣魚攻擊。比行為本身更令人擔憂的也許是北韓駭客團隊 Lazarus Group 的專業性和軍隊般的精准度，為進入受害電腦系統的後門，該團隊開發了惡意加密貨幣應用程式。

勒索軟體即服務供應商、恐怖分子資助者和國家支持的網路犯罪者轉向了數位戰場之際，執法機關亦逐步趕上。從 Colonial Pipeline 扣押、以色列機構對哈馬斯相關加密地址的識別以及對北韓網路犯罪分子的指控來看，執法機關能利用加密貨幣的力量和前景——依靠公開帳簿運作——追蹤並最終追回被盜資金。就像《悲慘世界》中尚萬強 (Jean Valjean) 與賈維 (Javert) 之間的精彩對決一樣，執法機關與不法分子之間貓捉老鼠的遊戲轉到了線上，威脅與應變之道亦以網際網路的速度改變。

Ari Redbord，TRM Labs 法律和政府事務主管，華盛頓特區，ari@trmlabs.com，Twitter 帳號：@ARedbord

[1] Mike Isaac 和 Sheera Frankel，“Facebook Security Breach Exposes Accounts of 50 Million Users”（Facebook 安全漏洞導致 5,000 萬用戶的帳戶資料外洩），*《紐約時報》*，2018 年 9 月 28 日，https://www.nytimes.com/2018/09/28/technology/facebook-hack-data-breach.html

[2] 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”（美國聯邦調查局證實，勒索軟體組織 DarkSide 是駭客攻擊美國主要輸油管的幕後黑手），*《紐約時報》*，https://www.nytimes.com/2021/05/10/us/politics/dark-side-hack.html

最重要的是，私營機構 IT、法規遵循和金融犯罪專家可以發揮極大功能，主動和被動地應對勒索軟體和網路攻擊的威脅

[3] “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”（美國白宮新聞秘書 Jen Psaki、國土安全顧問兼副國家安全顧問 Elizabeth Sherwood-Randall 博士以及網路和新興技術副國家安全顧問 Anne Neuberger 聯合新聞發佈會，2021 年 5 月 10 日），*白宮*，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/

[4] Jordan Robertson 和 William Turton，“Colonial Pipeline hackers stole data on Thursday”（攻擊 Colonial Pipeline 的駭客週四竊取了公司資料），*彭博新聞*，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

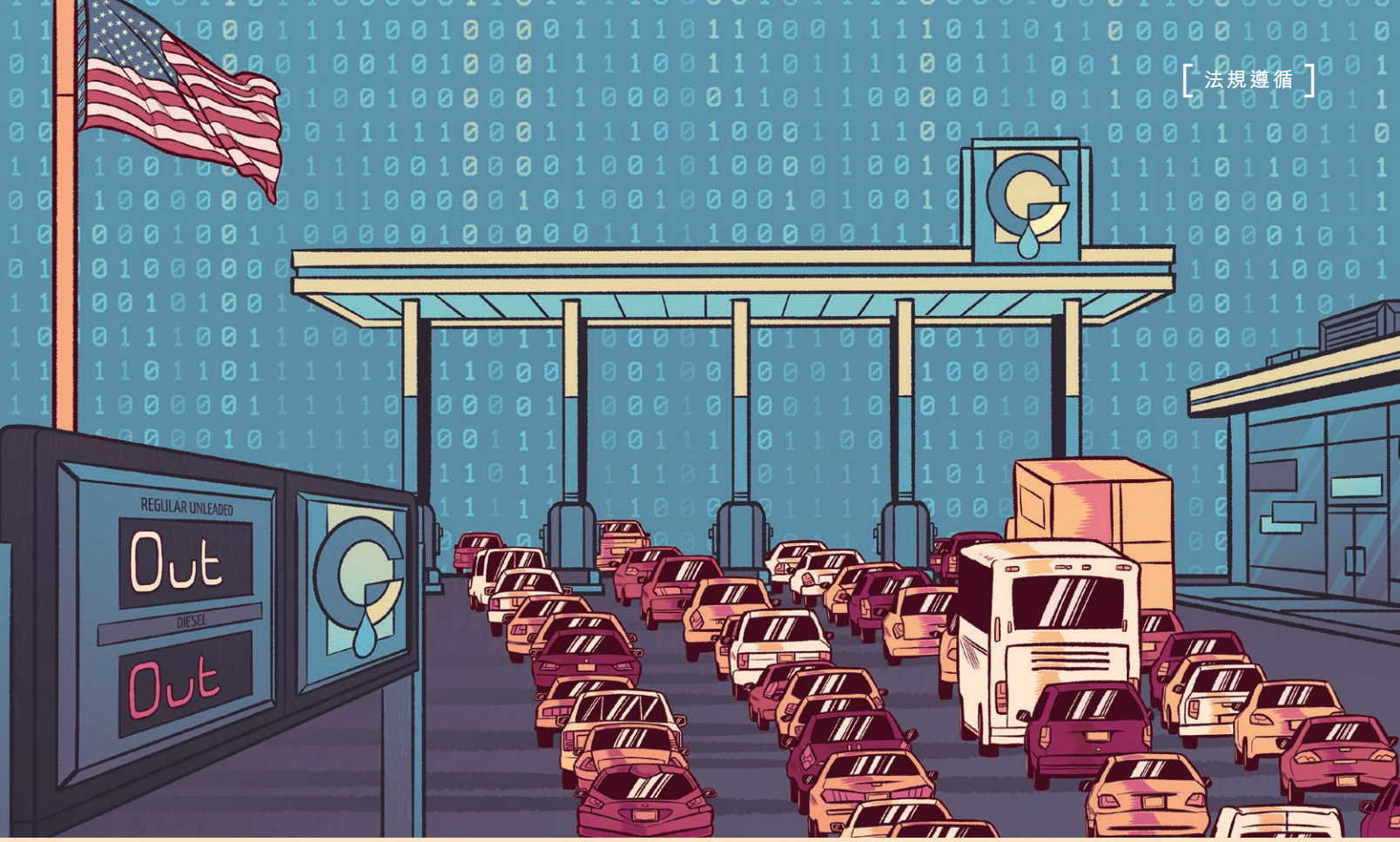
[5] William Turton、Michael Riley 和 Jennifer Jacobs，“Colonial Pipeline Paid Hackers Nearly $5 Million in Ransom”（Colonial Pipeline 向駭客支付近 500 萬美元贖金），*彭博社*，2021 年 5 月 13 日，https://www.bloomberg.com/news/articles/2021-05-13/colonial-pipeline-paid-hackers-nearly-5-million-in-ransom

[6] “Digging into the Darkside Ransomware Payment”（深究 Darkside 勒索軟體付款），*TRM Labs*，2021 年 5 月 14 日，https://www.trmlabs.com/post/darkside-ransomware-report

[7] “The moral underground? Ransomware operators retreat after Colonial Pipeline hack”（講道德的地下組織？勒索軟體營運商在 Colonial Pipeline 駭客攻擊事件後開始撤退），*Intel 471*，2021 年 5 月 14 日，https://intel471.com/blog/darkside-ransomware-shut-down-revil-avaddon-cybercrime

[8] “Darkside Seizure Warrant”（Darkside 扣押令），*美國加州北區地方法院*，2021 年 6 月 7 日，https://www.justice.gov/opa/press-release/file/1402051/download

[9] “DAG Monaco Delivers Remarks at Press Conference on Darkside Attack on Colonial Pipeline”（檢察副總長 Monaco 在新聞發佈會上就 Colonial Pipeline 遭 Darkside 攻擊案件發表評論），*美國司法部*，2021 年 6 月 7 日，https://www.justice.gov/opa/speech/dag-monaco-delivers-remarks-press-conference-darkside-attack-colonial-pipeline



[10] “Department of Justice Seizes $2.3 Million in Cryptocurrency Paid to the Ransomware Extortionists Darkside”（美國司法部追回了支付給勒索軟體敲詐者 Darkside 的 230 萬美元加密貨幣），*美國司法部*，2021 年 6 月 7 日，https://www.justice.gov/opa/pr/department-justice-seizes-23-million-cryptocurrency-paid-ransomware-extortionists-darkside

[11] 同上。

[12] Nicole Perlroth、Erin Griffith 和 Katie Benner，“Pipeline Investigation Upends Idea That Bitcoin Is Untraceable”（對 Pipeline 駭客攻擊案的調查顛覆了比特幣不可追蹤的觀念），*《紐約時報》*，2021 年 6 月 9 日，https://www.nytimes.com/2021/06/09/technology/bitcoin-untraceable-pipeline-ransomware.html

[13] Aruna Viswanatha 和 Dustin Volz，“FBI Director Compares Ransomware Challenge to 9/11”（聯邦調查局局長將勒索軟體與「911」進行比較），*《華爾街日報》*，2021 年 6 月 4 日，https://www.wsj.com/articles/fbi-director-compares-ransomware-challenge-to-9-11-11622799003

[14] “Guidance Regarding Investigations and Cases Related to Ransomware and Digital”（勒索軟體與數位相關的調查和案件指南），*美國司法部副檢察長辦公室*，2021 年 6 月 3 日，https://www.justice.gov/dag/page/file/1401231/download

[15] Fred Kaplan，“‘WarGames’ and Cybersecurity’s Debt to a Hollywood Hack”（《戰爭遊戲》與好萊塢駭客影響對網路安全的貢獻），*《紐約時報》*，2016 年 2 月 19 日，https://www.nytimes.com/2016/02/21/movies/wargames-and-cybersecuritys-debt-to-a-hollywood-hack.html

[16] “The United States, Joined by Allies and Partners, Attributes Malicious Cyber Activity and Irresponsible State Behavior to the People’s Republic of China”（美國聯合盟友譴責中華人民共和國從事惡意網路活動和不負責任的國家行為），*白宮*，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/

[17] “What We Urge You To Do To Protect Against The Threat of Ransomware”（關於防範勒索軟體威脅的建議），*白宮*，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

[18] Joseph Johnson，“Most common delivery methods and cybersecurity vulnerabilities causing ransomware infections according to MSPs worldwide as of 2020”（截至 2020 年導致勒索軟體感染最常見的攻擊方法和網路安全漏洞：全球管理服務供應商），*Statista*，2021 年 2 月 16 日，https://www.statista.com/statistics/700965/leading-cause-of-ransomware-infection/

[19] Jason Remillard，“Lisa Sotto of Hunton Andrews Kurth: ‘Relationships are incredibly important’”（Hunton Andrews Kurth 公司 Lisa Sotto：「關係不容小覷」），*ThriveGlobal*，2021 年 7 月 30 日，https://thriveglobal.com/stories/lisa-sotto-of-hunton-andrews-kurth-relationships-are-incredibly-important/

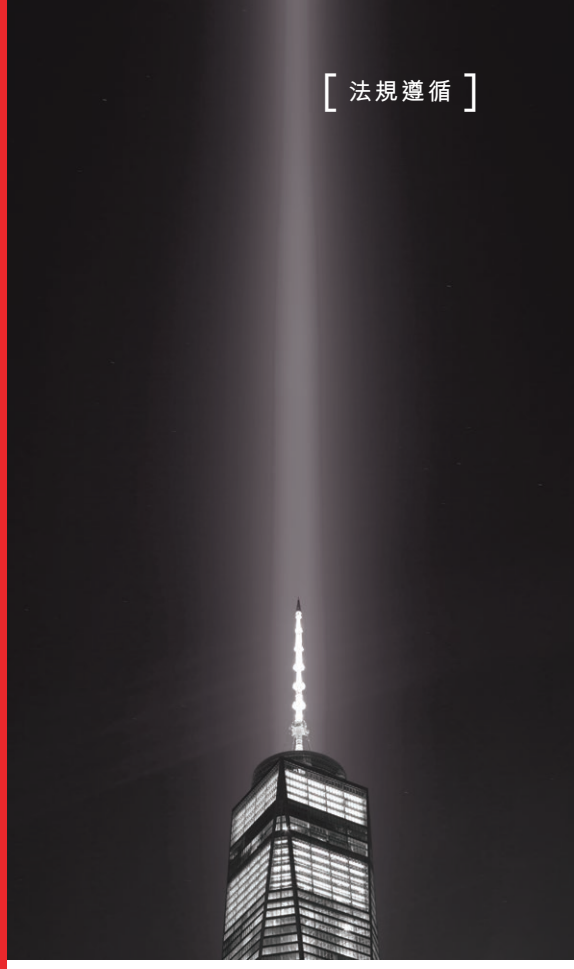
[20] “Seizures of Cryptocurrency”（扣押加密貨幣），*以色列國家反恐籌資局*，https://nbctf.mod.gov.il/en/seizures/Pages/Blockchain1.aspx

[21] “Global Disruption of Three Terror Finance Cyber-Enabled Campaigns”（全球成功破解三起恐怖分子網路金融活動），*美國司法部*，2020 年 8 月 13 日，https://www.justice.gov/opa/pr/global-disruption-three-terror-finance-cyber-enabled-campaigns

[22] “Three North Korean Military Hackers Indicted in Wide-Ranging Scheme to Commit Cyberattacks and Financial Crimes Across the Globe: Indictment”（三名北韓軍隊駭客被控參與多起詐騙，在全球實施網路攻擊和金融犯罪：起訴書），美國加州中區地方法院，https://www.justice.gov/opa/press-release/file/1367701/download

911：
20 年的旅程

有些事件會永遠銘刻在我們的腦海裡。對於 2001 年 9 月 11 日在公營或私營機構工作的人來說，蓋達組織 (al-Qaida) 對美國的攻擊顯然是銘刻於我們腦海的歷史性時刻之一。對於在那個可怕日子之後進入職場的人來說，911 事件 20 周年是回顧與反思的陰鬱時刻。



2001 年 9 月 11 日，美國東海岸正緩緩展開平靜而美好的一天。美國東部標準時間上午 8 點，人們準備開始一天的忙碌，他們並不知道，不久後一場災難正在波士頓機場、紐華克機場和維吉尼亞北部機場的四架飛機上徐徐展開。上午 8 點 19 分，其中一架飛機上的空服員通知航空公司航班被劫持，暗示有問題的第一信號出現了。上午 8 點 46 分，那架飛機撞向世貿中心北塔。開始時，多數人認為這是一場悲慘的意外事故。後來，上午 9 點 03 分，第二架飛機撞向世貿中心南塔。那一刻，人們感到一陣麻木，意識到這並非意外事故。那是一個人們永遠無法忘記的時刻。上午 9 點 37 分，更加令人震驚，第三架飛機撞向了五角大樓。在接下來的半個小時裡，據報導第四架飛機被劫持並飛往華盛頓特區，加劇了人們的恐懼。上午 10 點 03 分，由於機上乘客的英勇反抗，這架飛機突然墜毀在賓夕法尼亞州尚克斯維爾的一塊田地裡。

知識與教訓

我們知道蓋達組織是活躍在阿富汗且受塔利班保護的一個恐怖組織。其領導人 Osama bin Laden 對美國懷有強烈的仇恨。有大量警告信號顯示，bin Laden 抱持在全球攻擊美國利益的野心和意圖。不幸的是，作為一個國家，美國有一種錯誤的安全感和無敵感，不擔心國際恐怖分子會攻擊美國本土。

我們謙卑地學習到，面對恐怖主義，像美國這樣的開放社會異常脆弱，而蓋達組織在找出和利用系統漏洞方面可謂駕輕就熟。相反，在對 911 攻擊事件展開即時調查後，美國很快發現蓋達組織與恐怖分子主要有兩個弱點：通訊和金融。攻擊發生數週後，美國聯邦調查局繪出了此次攻擊的通訊和財務資訊時間表，以便追根溯源，挖出攻擊源頭的蓋達組織。

911 攻擊發生後，美國國會成立了 911 委員會，展開調查。調查結果發佈在《911 委員會報告》當中。這份報告是對 911 事件最權威、最全面、最客觀、最可靠的說明。報告中詳細描述了蓋達組織策劃並成功實施此次攻擊的過程，美國政府存在且使蓋達組織得逞的弱點、不足和失敗，以及美國對此採取的反制措施。重要的是，報告提出了 41 條建議，敦促政府制定最佳作法並盡量地減少將來的威脅。

911 委員會發佈了一份報告卡，用於監督美國政府反恐措施的實施進度。最高等級為 A-，是對回應資恐措施的評等。獲得評等的一項基本理由是根據「資恐政策協調委員會」工作組所進行的跨部門合作程度，以及 911 委員會《資恐專題研究報告》中描述的金融界「卓越合作」水準。

911 事件之前的威脅環境

由於對國家安全存在錯誤的認識，美國政府並沒有把反恐工作擺在首位。結果造成政府反恐資源不足、人力情報資源短缺、資恐調查缺乏且不協調、制裁效果不佳。美國執法機關和情報機構之間缺少資訊共享，進一步擴大了這些缺點。從金融情報的角度來看，需要建立更強大的《銀行保密法》條例和報告制度。

911 恐怖攻擊的第一個警示信號出現在 1993 年 2 月，當時有人首次在世貿中心發動炸彈攻擊。一枚巨大的卡車炸彈在世貿雙子星大樓的停車場被引爆。那次事件的目的是炸塌雙子樓。雖然造成了嚴重破壞和傷亡，但攻擊並未達到預期效果。這次攻擊的主謀是 Ramzi Yousef，他是 Khalid Sheikh Mohammed (KSM) 的侄子，而後者正是 911 事件的主謀。

從 1993 年到 2001 年，還出現了許多其他警示信號。1994 年，Yousef 和 KSM 在菲律賓策劃了「馬尼拉航空」攻擊計劃（又稱「波金卡」計劃），目的是在從亞洲飛往美國的多個航班上同時引爆炸彈。菲律賓警方成功地阻止了計劃。1996 年和 1998 年，bin Laden 針對美國下達了兩道教令。第一道教令是號召穆斯林殺害美國士兵，第二道教令是呼籲殺死美國人。蓋達組織 1998 年轟炸了美國駐東非的兩個大使館，2000 年轟炸了科爾號導彈驅逐艦。除了這些活動，還有大量的零碎情報稱可能有人對美國發動恐怖攻擊。

在 911 事件發生之前，資助恐怖活動並非情報界的重點工作。同樣，執法機關尤其

是聯邦調查局，也沒有認真對待資恐問題。然而，中央情報局在 911 之前提交的情報稱，蓋達組織在此期間的現金流穩定且安全。

911 恐攻

1996 年，KSM 在阿富汗托拉博拉會見了 bin Laden，建議在美國劫持 10 架飛機，攻擊東海岸和西海岸的目標。KSM 的計劃過於宏大，被 bin Laden 拒絕了。後來，在 1999 年初，bin Laden 在阿富汗坎大哈會見了 KSM。這次會見，bin Laden 同意了 KSM 的計劃，劫持大型商用飛機，以飛機為導彈攻擊美國境內目標。此後不久，有人組織了一系列的會議，參會人包括 bin Laden、KSM 和蓋達組織軍事領導人兼 bin Laden 高級顧問 Mohammad Atef。這些會議制定了 911 恐攻計劃，包括初始目標的選擇。儘管 911 恐攻的種子在 1993 年就播下，但直到 1999 年他們才想出攻擊計劃。bin Laden 的組織負責領導，蓋達組織提供資金和行動支援，KSM 負責策畫和執行，這些因素共同保證了攻擊計劃的可行性。

911 攻擊計劃的核心參與者分為三種角色：領導者、協助者和 19 名劫機者，劫機者又分成兩組，即 4 名飛行員和 15 名魁梧劫機者。從 1999 年春天開始，bin Laden、Atef 和 KSM 就一直在遴選協助者和劫機者。前兩名劫機者於 2000 年 1 月抵達美國。他們最初被選為飛行員，但無法適應西方文化，於是成了魁梧劫機者。後來，四名比較熟悉西方社會的人被選為飛行員。他們於 2000 年春夏進入美國。這些飛行員在接下來的一年裡進行了大量飛行訓練，並對飛行中的跨境飛機進行監視，確定最佳劫機時機。剩下的 13 名魁梧劫機者於 2001 年春夏進入美國。在攻擊發生前的幾天裡，19 名劫機者組成了四支飛行隊伍。9 月 11 日上午，劫機者成功執行了計劃。

對於 911 恐攻事件，有一點是無法辯駁的。攻擊計劃需要資金，成本在 40 萬美元到 50 萬美元之間，其中大約 32.6 萬美元由金融機構經手處理。bin Laden 向 KSM 提供了 911 恐攻需要的大部分資金，KSM 則把這些錢直接給劫機者，或者通過三個協助者把錢間接拿給劫機者。19 名劫機者每個人都在美國開立了可存提款的銀行帳戶，使它們便於執行攻擊計劃。他們還使用了外國銀行帳戶、貨幣服務業和外匯。協助者和劫機者之間大約有 20 筆電匯，其中包括未使用的資金，劫機者又透過電匯把這部分的錢還給了協助者。

背後的資金線索。先查明劫機者的購票方式，識別銀行帳戶，追蹤電匯，然後確定並建立起銀行交易活動和通信時間表。金融服務業強大的回應能力對調查工作發揮了極大的作用。

911 事件後的影響

近 3,000 人在攻擊中喪生。在那個悲慘日子之後的幾年裡，有數百名第一線救災者因在這四個撞機地點接觸到毒素而喪生。此外，911 事件也暴露出多方面的間接問題：情報系統存在系統性的問題，過度自滿，缺乏資訊共享，對資助恐怖活動重視不夠，需要加強《銀行保密法》報告要求，更加鞏固公部門之間及公私部門的合作。蓋達組織成功地利用了所有這些漏洞。

針對 911 事件，美國政府啟動了大規模的應變行動，開始解決此次恐攻暴露出來的現有系統性問題。包括軍事行動、情報和調查行動，以及監管和制裁行動，還建立了可持續的「公公」和

「公私」合作關係。此外，包括聯合國在內的國際社會團結起來支持美國，採取廣泛措施，將恐怖主義和資助恐怖活動定為刑事犯罪。

在911事件後，從多方面建立起重要對策。在往後的日子裡，這些對策不斷被完善和強化，力求將類似911攻擊的風險降至最低。除了成立911委員會以外，美國國會在2001年10月通過美國《愛國者法案》，增加相關法律條款以應對恐怖主義威脅。美國《愛國者法案》裡的財務相關條款大幅提高了《銀行保密法》有關要求。2001年10月，防制洗錢金融行動工作組織就資助恐怖活動問題在華盛頓特區舉行了一場特別全體會議，會中制定了《打擊資助恐怖活動特別建議》。2002年10月，防制洗錢金融行動工作組織發佈了有關資助恐怖活動的分類和指引。此後，防制洗錢金融行動工作組織持續就打擊資助恐怖活動定期提供指導意見。

當前的威脅環境

911事件以來的20年裡，恐怖主義威脅環境不斷變化。2001年至2019年初，主要威脅都是由組織推動的。各組織歷經興衰變化。911之前，尤其是在911事件前後，蓋達組織是主要威脅。2013年，隨著敘利亞和伊拉克哈里發國的發展，伊斯蘭國(IS)成為最大的恐怖威脅。2019年，哈里發國垮臺，伊斯蘭國變成叛軍。

蓋達組織和伊斯蘭國憑藉著網際網路招募和激化極端分子的能力，開始培養本土暴力極端分子(HVE)，將組織威脅轉變成個人威脅。本土暴力極端分子受到外國伊斯蘭恐怖組織意識形態蠱惑。在本土暴力極端分子形成威脅的同時，從2019年開始，國內暴力極端分子(DVE)的威脅

一方面，美國和志同道合的國家或地區把本土暴力極端分子和國內暴力極端分子構成的威脅擺在首位，但另一方面，也不能忽略來自外國恐怖組織的威脅

亦不斷增大。國內暴力極端分子是以推動種族偏見、反政府情緒等國內意識形態為目標，進而實施犯罪的個人。這些人當中最大威脅來自於有著種族或民族動機的暴力極端分子(RMVE)。

2021年，最嚴重的恐怖主義威脅來自本土暴力極端分子和國內暴力極端分子。1月6日的美國國會大廈騷動彰顯了國內暴力極端分子的影響力，令人震驚不已。一方面，美國和志同道合的國家或地區把本土暴力極端分子和國內暴力極端分子構成的威脅擺在首位，但另一方面，也不能忽略來自外國恐怖組織的威脅。儘管他們目前還沒有這個能力，但蓋達組織和伊斯蘭國都渴望對美國發動類似911的攻擊。

從資助恐怖活動的角度來看，以組織為中心的威脅環境轉變為以個人為中心，此環境具有去集中化和去領導化的特點，意味著資助恐怖活動趨向本地化。因此，與911事件不同，資金不大可能從組織流向恐怖分子，恐怖分子更有可能自己從本地資源籌措資金。無論是本土暴力極端分子或國內暴力極端分子發起攻擊，孤狼式攻擊都不需要很多資金。這種攻擊需要的資金更少，複雜度較低，規模較小，成功率更高。

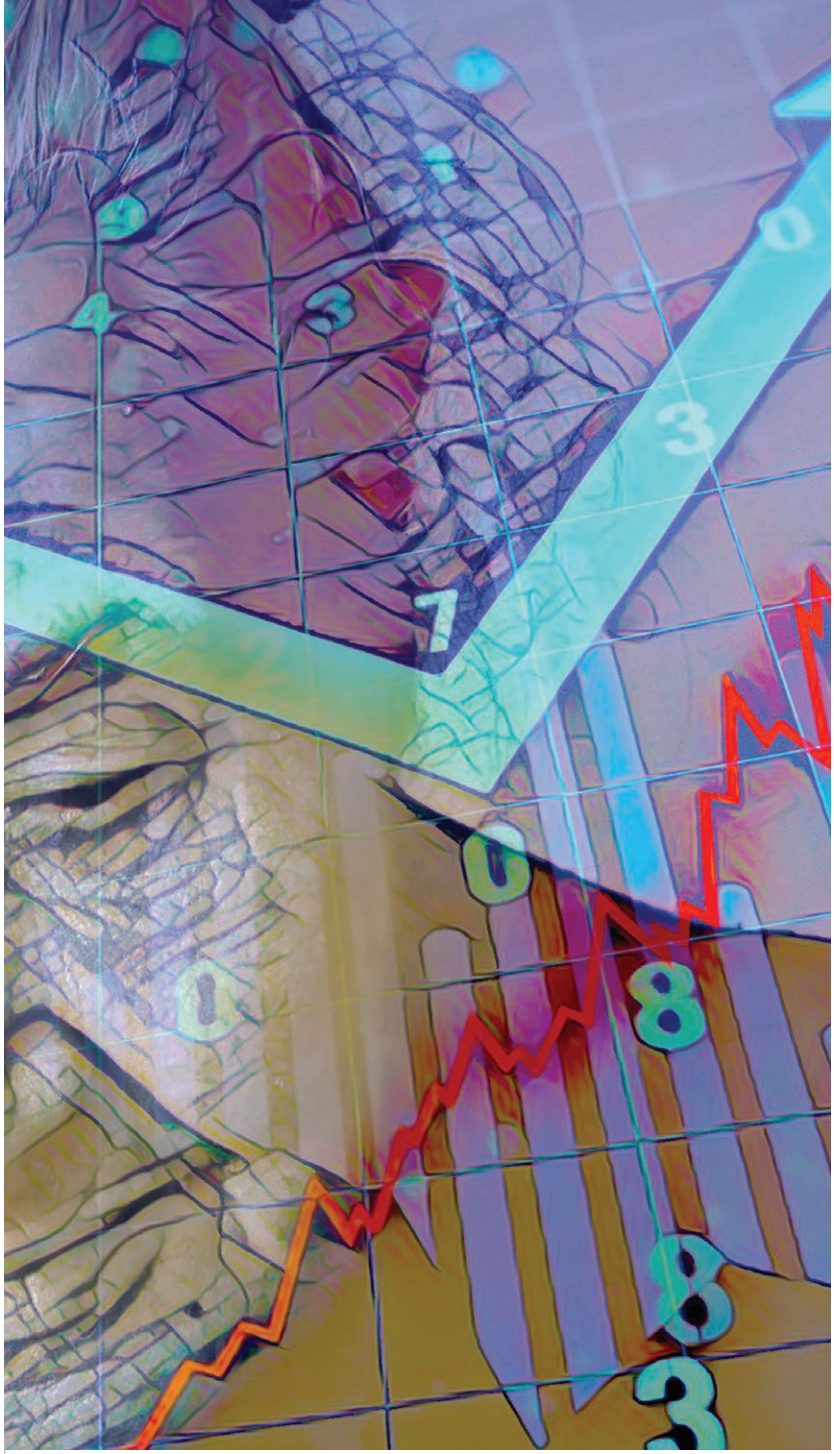
結語

911恐攻由策劃到行動用了兩年多的時間。這兩年裡，大量的資金被用於準備和執行911恐怖攻擊。在這期間，恐怖分子頻繁與銀行和貨幣服務業接觸。即使有了兩年的接觸時間，劫機者的交易活動並不引人注目，也不可疑。然而，在大多數情況下，劫機者及其協助者用的是真實身分，留下了資金線索。利用資金線索，聯邦調查局摸清了資金流動軌跡，發現了劫機者與協助者的關係，最終直接追溯到KSM，間接追溯到bin Laden。由於得到了金融部門前所未有的支持，聯邦調查局只用了幾個星期就確定了911事件的資金流向。但正如國會大廈的騷動可證，威脅形勢已經轉變。資金需求已從組織轉變為孤狼或個人群體。如果說最佳作法教給了我們什麼，那就是自籌資金的恐怖分子帶來更巨大的挑戰，公營和私營機構需要攜手共進，展開可持續、有意義的合作。

Dennis M. Lormel，CAMS，國際公認打擊資恐專家，DML Associates LLC總裁兼執行長，美國維吉尼亞州，dlormel@dmlassocllc.com

老年人錢財詐騙：巨大危機

老年人錢財詐騙這一巨大危機，由眾多因素共同促成：新冠疫情爆發，迫使人們在家隔離；人們對電話、電腦等通訊手段的依賴日益增加；成人保護服務機構 (Adult Protective Services) 的工作人員無法家訪，削弱了社會對老年人的保護；有些人因疫情失去唯一收入來源，陷入絕望；社會老齡化，每天有 1 萬人年滿 65 歲；犯罪嫌疑人積極尋找易於利用的目標；此外，許多老年受害人本身也是一大因素——不是太要面子，不願舉報，就是有認知障礙，不清楚發生了什麼事情。這些因素正好成就了老年人錢財詐騙的發生。多年以來，詐騙老年人錢財的罪行氾濫全美，如今已惡化成巨大的社會與經濟危機，極需積極有力應對。



1996-2018 這 22 年間，我有幸擔任聖地亞哥地區檢察官防止虐待老人小組的負責人。任職期間，全美各地不斷有人致電給我，請我為當地執法機關工作人員、檢察官、社會工作者等進行培訓。當時經過一番深思熟慮，我終於下定決心，把接力棒交給更年輕的檢察官。因此我才有時間與機會向更多人分享有關虐待老人的法院公訴案件。

在我起訴的虐待老人重罪案件中，有 65% 涉及不同形式的錢財詐騙行為。無論此等詐騙行為屬何種類型（不論涉及現金、不動產、投資還是個人資產），檢方面臨的困難始終如一，那就是：檢方應如何證明，嫌疑人是在未經受害者同意的情況下，剝奪了老年受害人的財產，且具有永久剝奪財產的意圖？

具體可分為四種情形。其中前兩種情形一目了然，但第三、第四種卻極難證明。

第一種情形是，受害人有充分作證能力，表明被告未經其同意剝奪其財產。

第二種情形是，受害人因重度失智或其他極端精神障礙，無法作證；而且詐騙行為發生前，受害人已有該疾病症狀。在此情形下，檢方可基於資產轉移證據，採信醫療執業醫師的證詞，證明受害人不具備同意資產轉移的能力。

第三種情形是，詐欺罪行揭露時，受害人已去世。按照慣例，在這種情況下，執法機關會立即做出判定，不再調查此事，因為無法證明受害人未同意。但我發現，如果具備第二種情形中所述的醫學證據，則仍有可能基於提出受害人紀錄在案的無行為能力證明，從而輔證詐騙罪行的發生。如果相關詐騙罪行涉及偽造文書，可考慮透過司法筆跡專家的鑒定來定罪。還有，如果受害人去世前曾經「激動陳述」，表明自己未同意轉移資產，則檢方可能成功說服法庭基於傳聞證據規則，破例採信此庭外陳述。

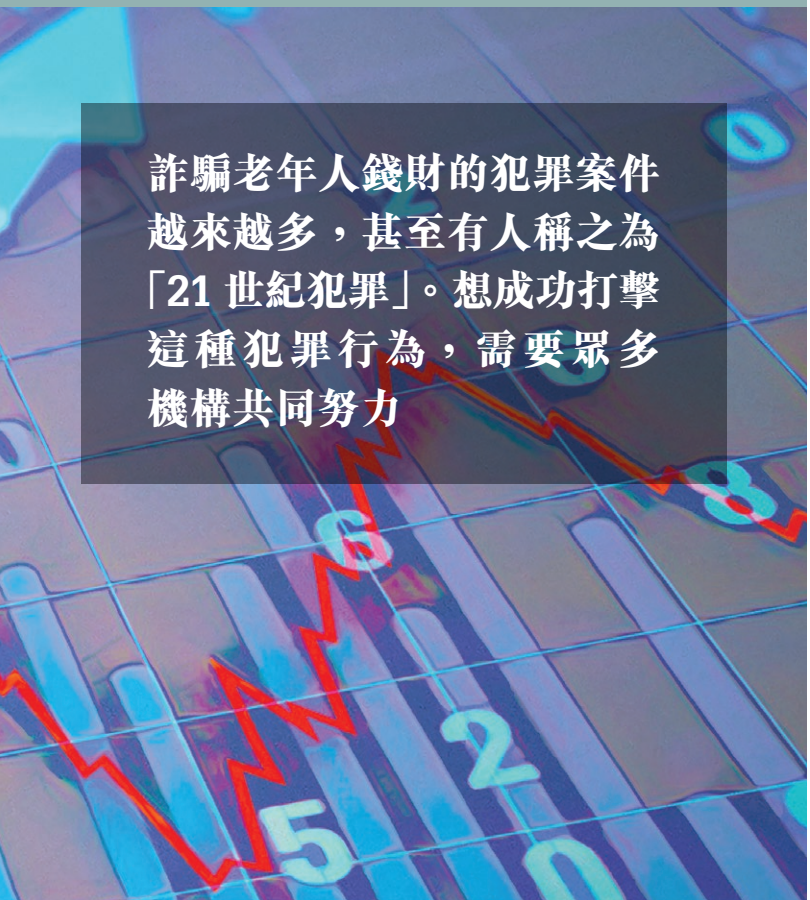
第四種情形是，有證據證明受害人存在記憶損害，受害人只能勉強作證。此種情形下，乍看受害人似乎是自願將資產轉移給被告，而被告通常也會將被轉移的資產解釋為贈禮或借貸。針對此種情形的案件，執法機關往往拒絕展開調查，理由是不存在明顯的犯罪行為。最後的結論往往是：嫌疑人未使用武力或脅迫而是經由巧妙的操縱，以不正當的方式影響受害人，讓受害人放棄了財產。但我們發現，這種情況必須根據以下重點事項展開調查：

- 受害人和嫌疑人的會面方式、會面地點和時間？
- 受害人在遇見嫌疑人之前，消費習慣是什麼樣的？如果可以確定受害人一向節儉，就可能合理推測出，該資產轉移完全不符合受害人的性格特點。
- 嫌疑人影響受害人的具體方法：嫌疑人是否切斷受害人與親朋好友的聯繫，或者偽造「身分」迎合受害人？嫌疑人是否做出某些行為，使受害人越來越依賴與嫌疑人的關係？

若能將老年人錢財詐騙案件歸入上述情形之一，肯定有助於對案件進行評估，以便後續提起公訴。不過，將此類案件提交法官或陪審團，需要多領域專業人士的通力合作。

採取多領域團隊合作法

詐騙老年人錢財的犯罪案件越來越多，甚至有人稱之為「21 世紀犯罪」。想成功打擊這種犯罪行為，需要眾多機構共同努力。值得慶幸的是，許多司法管轄區已陸續建立金融剝削專家團隊 (FAST)。那麼，此種團隊需要哪些專業人士？



詐騙老年人錢財的犯罪案件越來越多，甚至有人稱之為「21 世紀犯罪」。想成功打擊這種犯罪行為，需要眾多機構共同努力

顯然，需要當地執法機關、郡縣檢察官辦公室、成人保護服務機構、長期照護監察員、公共監護人等相關崗位的人員，還應邀請州檢察長辦公室和美國聯邦檢察官辦公室的代表，以及郵政檢查局、社會保障管理局、聯邦調查局、遺囑檢驗法庭調查員、建築承包商執照委員會等機構的成員。此外，銀行、信用合作社、投資經紀人和其他金融機構的反詐騙調查員也很重要。最後別忘了，司法會計師、老年病學專家、當地老年服務業的代表，也可以為團隊帶來寶貴的見解。

詐騙老年人錢財案件的報告，往往遞不到法庭之上。有時候，執法機關會宣稱「這只是民事問題」；如果嫌疑人持有授權書，更是如此。有時候，相關機構會告知受害人或受害人親屬「犯罪行為並不在本司法管轄區發生」，或者「嫌疑人可能在海外，我們無法確定其身分。」有些時候，檢察官還會暗示，受害人因年齡或殘疾無法提供有效證言，使受害人心生退意，打消繼續調查的念頭。

犯下此類投機罪行的嫌疑人往往心存僥倖，認為自己的操作經得起執法機關或檢察官的任何審查。而疫情的影響，更進一步助長了這些掠奪者的膽量。

結語

要迎接這一挑戰，務必認清「年齡歧視」誤解可能會形成阻礙，瞭解團隊合作方式的重要性，並洞察整合各種資源解決此類陰險犯罪的價值。

詐騙老年人錢財，是一種粗暴的罪行。不僅會影響老年人的財務安全，還會損害老年人的身心健康，更可能導致老年人生活方式的急劇惡化。老年人錢財詐騙案的受害者中，許多人都屬美國「最偉大的一代」。我們不僅應感激他們曾經做出的奉獻，還應當為他們爭取正義。

如果您還未成為防止虐待老人工作組的成員，不妨考慮加入此類工作組；如果您所在地區還沒有這樣的組織，或許可以考慮主動發起一個？

Paul Greenwood，美國聖地亞哥郡退休副地方檢察官，Greenwood 律師事務所，顧問兼培訓師

防制洗錢專業人士需要瞭解的新舉報人制度

2020 年《防制洗錢法》是美國防制洗錢法十多年來最重大的變化，其中有項規定擴大了《銀行保密法》舉報人制度，金融機構和防制洗錢專業人士需要特別予以關注。現在，舉報人可以匿名舉報違反《銀行保密法》的行為，並可從政府施以金錢制裁的金額中獲取最多 30% 的獎勵，而制裁總金額有時可達數億美元。目前實施的高額激勵措施有可能導致舉報事件急劇增加，就像美國證券交易委員會 (SEC) 在 2010 年建立獨立制度後所經歷的那樣。《銀行保密法》要求金融機構實施有效的防制洗錢制度體系，檢測和報告可疑交易。[1] 如果金融機構違反此要求，則每筆標的交易將面臨 25,000 至 100,000 美元的罰款。[2] 雖然《銀行保密法》之前有所謂的「線人」獎勵制度，但獎勵金額上限統一為 150,000 美元。[3] 此外，《銀行保密法》就匿名檢舉違規行為未作出任何規定。

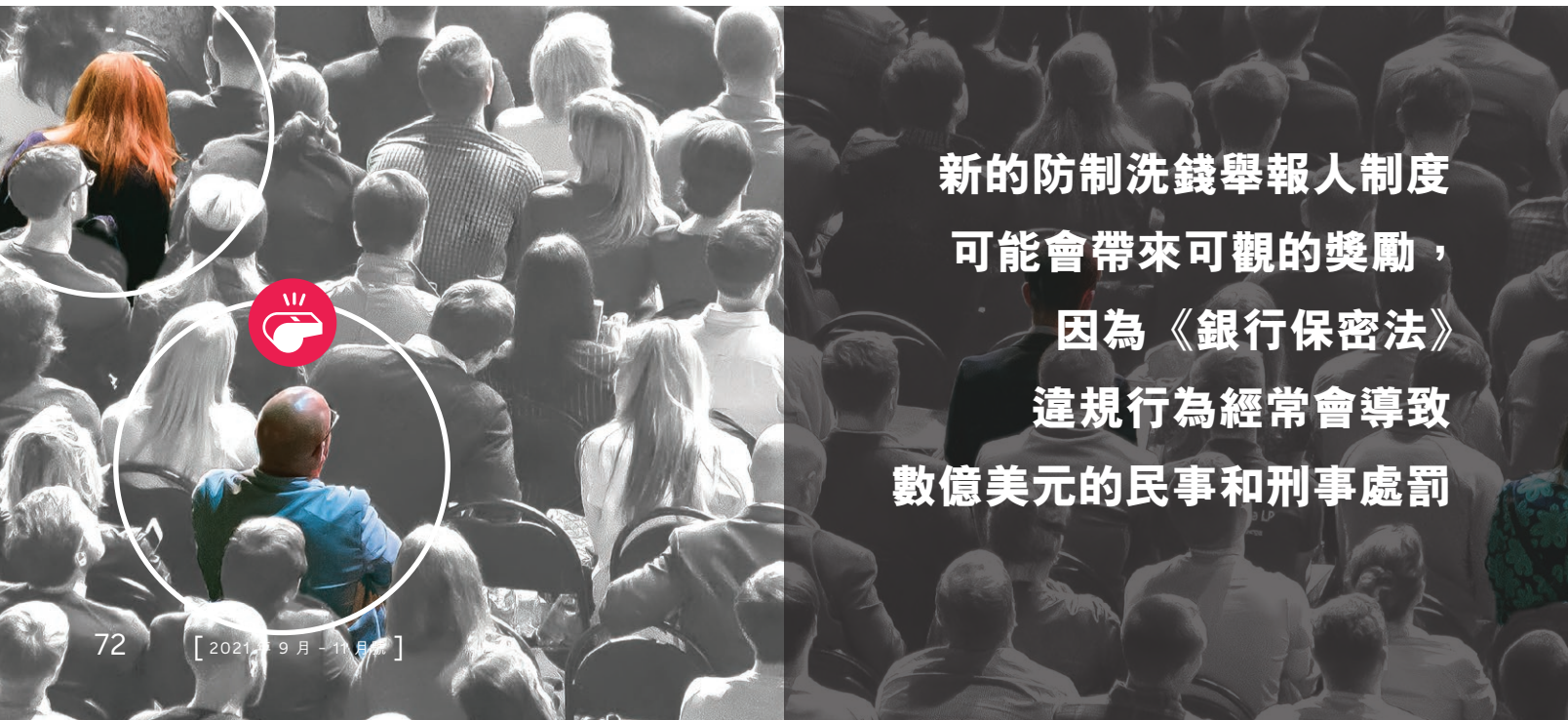
《防制洗錢法》對《銀行保密法》舉報人制度進行了幾項重要調整，顯著提高揭露《銀行保密法》違規行為的獎勵金額，增加防範報復措施，建立匿名舉報程序。現在，提供「原始資訊」以檢舉《銀行保密法》違規行為的「舉報人」，可就政府追回超過 100 萬美元的任何金錢制裁，獲得高達制裁金額 30% 的獎金。[4]

舉報人可以是「任何個人」或「聯合行動」的群體。[5] 不需要美國公民身分，因為洗錢活動經常跨越國界。舉報人提供的「原始資訊」可以來自舉報人的獨立知識或分析，只要政府尚未知曉或公共記錄中不存在即可。[6] 同時，也不需要舉報人直接向政府報告資訊。[7] 相反，舉報人可以將其作為工作職責的一部分，向雇主匯報資訊。美國財政部長有權決定給舉報人的獎勵金額，但必須考慮原始資訊對後續執法行動的重要性，以及舉報人或其律師對此類行動的協助程度。[8]

新的防制洗錢舉報人制度可能會帶來可觀的獎勵，因為《銀行保密法》違規行為經常會導致數億美元的民事和刑事處罰。例如，2021 年 1 月，金融犯罪稽查局 (FinCEN) 對美國銀行協會第一資本銀行 (Capital One) 處以 3.9 億美元的民事罰款，[9] 原因是該銀行在一家支票兌現的子公司未實施有效的防制洗錢控管措施。第一資本銀行在防制洗錢方面的缺失導致其支票兌現分支機構未提交可疑活動報告，這些分支機構後來承認犯有放高利貸、非法賭博、逃稅、洗錢等罪行。

同樣，2018 年，美國銀行與紐約南區美國檢察官辦公室達成暫緩起訴協議，支付了 5.28 億美元的罰款。[10] 尤其美國政府指責美國銀行雇用防制洗錢人員數量不足，使他們「嚴重分身乏術」，因而減少審查潛在可疑交易的數量。根據《防制洗錢法》，對第一資本銀行和美國銀行的處罰可能給提供原始資訊的舉報人帶來超過 1 億美元的獎勵。

《防制洗錢法》還制定了針對報復的重要保護措施，[11] 即任何舉報人揭露其合理相信違反《防制洗錢法》的行為後，禁止雇主解雇、降級、停職、列入黑名單或以「任何其他方式」歧視該舉報人。即使只是將違規行為揭露給舉報人的上司而非政府，該禁令也適用。受到歧視的舉報人可以向勞工部長提出申訴。



《防制洗錢法》允許舉報人通過律師「匿名」舉報

經驗豐富的法律顧問可以幫助專業人士和金融機構跟上新的發展，分析其影響，制定有效的行動方案。

Caleb Hayes-Deats，
MoloLamken 律師事務所律師，
美國華盛頓特區，
chayes-deats@mololamken.com[15]

如果勞工部長未在 180 天內發佈最終決定，舉報人可以向聯邦法院提起訴訟。可能的補救措施包括復職、雙倍賠償欠薪和其他補償性損害賠償，包括律師費。

最後，《防制洗錢法》允許舉報人通過律師「匿名」舉報。[12] 在這種方式下，政府只會收到律師的姓名和聯繫資訊，任何後續詢問都透過律師轉達舉報人。在取得獎勵之前，舉報人必須揭露其身分。這一條必不可少，因為政府雇員等特定群體不能獲得舉報人獎勵。[13] 但在舉報人身分資訊揭露後，《防制洗錢法》要求政府對該資訊保密，並對揭露設有具體限制，包括《隱私法》規定的限制。

《防制洗錢法》可能會使防制洗錢執法機構收到舉報人報告數量大幅增加。上述規定與 2010 年《多德 - 弗蘭克法案》建立的美國證券交易委員會舉報人制度非常相似。該制度頒佈以來，美國證券交易委員會收到的舉報人報告數量逐年增加，現在總計超過 40,000 份。2012 年至 2020 年，美國證券交易委員會向舉報人支付了 5.62 億美元的獎勵。[14]

《防制洗錢法》對《銀行保密法》舉報人制度的擴展，將為防制洗錢專業人士和金融機構帶來重大影響。獲知《銀行保密法》違規行為的防制洗錢專業人士有更強烈的動機向政府揭露所知道的資訊，況且現在他們可以匿名舉報了。正如美國證券交易委員會舉報人制度所證明的那樣，這些激勵措施可能會促使舉報數量大幅增加。

此新的現實情況也會給金融機構帶來風險，即使他們完全符合《銀行保密法》的規定。舉報人提交的報告即使缺乏基礎，也可能引發調查，而此類調查針對的金融機構將需要投入大量資源進行回應。金融機構可以採取多種措施，鼓勵內部舉報，降低意外調查風險。第一步是實施匿名熱線等內部舉報機制，但光有舉報機制是不夠的。還需要讓員工相信，所在機構會認真對待此類投訴，不會進行報復。金融機構可以透過最高管理層鼓勵舉報，制定強有力的反報復保護措施，儘量提高投訴調查透明度，由此培養員工上述信念。如果員工認為舉報制度可信，則機構有機會積極主動地解決問題，而非被動應對調查。《防制洗錢法》將內部舉報人列入合格獎勵對象，也有鼓勵內部舉報的作用。

防制洗錢專業人士和金融機構，若對新的舉報人制度有任何疑問或疑慮，最好諮詢律師。雖然《防制洗錢法》規定了舉報人制度的界限，但從多方面而言，該制度的未來將取決於執法機構及其發佈的監管規定或其他指導方針。

1 31 U.S.C. §5318。

2 *同上*。§5321。

3 31 U.S.C. §5323(b) (2020)。

4 31 U.S.C. §5323(b)(1)。金錢制裁包括「罰款、追繳和利息」，但不包括「沒收」、「歸還」或其他「受害者賠償」。*同上*。§5323(a)(2)。

5 *同上*。§5323(a)(5)。

6 *同上*。§5323(a)(3)。

7 *同上*。§5323(a)(5)。

8 *同上*。§5323(c)(1)。

9 "Assessment of Civil Monetary Penalty Number 2010-01"（對 2010-01 號案件民事貨幣罰款的評估），*金融犯罪稽查局*，https://www.fincen.gov/sites/default/files/enforcement_action/2021-01-15/Assessment_CONA%20508_0.pdf

10 "Manhattan U.S. Attorney Announces Criminal Charges Against U.S. Bancorp For Violations Of The Bank Secrecy Act"（曼哈頓美國檢察官宣佈對美國銀行違反《銀行保密法》提起刑事指控），*紐約南區檢察官辦公室*，2018 年 2 月 15 日，https://www.justice.gov/usao-sdny/pr/manhattan-us-attorney-announces-criminal-charges-against-us-bancorp-violations-bank

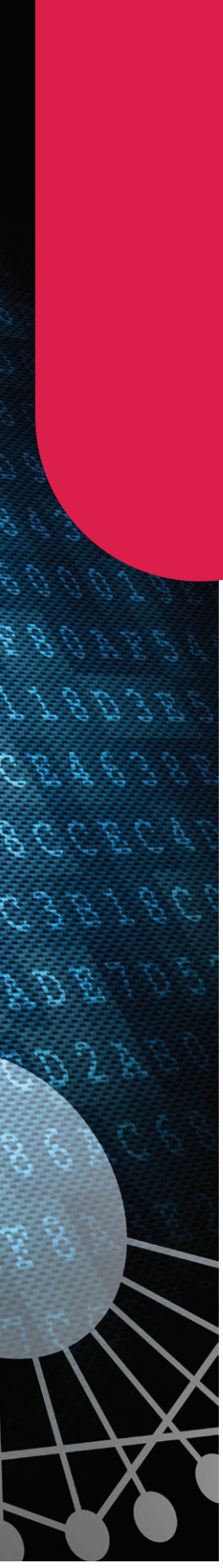
11 31 U.S.C. §5323(g)。

12 31 U.S.C. §5323(d)。

13 31 U.S.C. §5323(c)(2)。

14 "2020 Annual Report to Congress Whistleblower Program"（國會舉報人制度 2020 年度報告），*美國證券交易委員會*，https://www.sec.gov/files/2020%20Annual%20Report_0.pdf

15 Hayes-Deats 之前曾在紐約南區美國檢察官辦公室工作，參與了金融犯罪稽查局對美國銀行防制洗錢處罰的評估工作。本文表達的觀點僅代表作者本人觀點。



歐洲網路安全生態系統：一場打擊網路犯罪的戰爭

6月23日，歐盟委員會發佈消息稱，計劃成立聯合網路部門，以應對網路犯罪相關的大規模安全事件。[1]

歐盟和歐盟委員會針對打擊網路犯罪，不斷提出大量的提案、指南、策略和立法，此提案只是其中一部分。數量浩繁並非故意為之，只是展現出網路犯罪的性質。物聯網[2]現已成為全球互聯網基礎設施的一部分，形成了沒有邊界的虛擬空間。在這個空間裡，網路犯罪分子可以從全球任何地方攻擊任何行業、任何個人。

歐盟目前有27個成員國。因此，若想有效打擊和起訴網路犯罪，需要協調歐盟各國法律、文化和憲法規定。

從起訴的角度來看，電子證據的搜查和扣押是打擊網路犯罪的核心。國家法律不僅要符合搜查和扣押法，還要符合《歐洲人權公約》(ECHR)規定的公認人權條款。

有鑑於諸多複雜性，歐盟開發了一個錯綜複雜的「生態系統」，供歐盟成員國在其中有效打擊網路犯罪（見圖1）。

圖 1：歐洲網路安全危機管理框架

生態系統：歐洲網路安全危機管理框架

搜查和扣押立法與《歐洲人權公約》

《歐洲人權公約》是歐盟所有搜查和扣押立法（以及其他人權利益）的監督框架和標準。《歐洲人權公約》的各項原則由歐洲人權法院 (ECtHR) 執行。

《歐洲人權公約》適用於歐洲理事會的 47 個成員國，[3] 於 1950 年 11 月 4 日在羅馬簽署，1953 年 9 月 3 日在歐洲理事會大會上通過並正式生效。[4]

公約締約國受歐洲人權法院裁決約束。該法院有權審理國家間和個人的請願或投訴，而無需經地方政府事先核准。[5]

《歐洲人權公約》是歐盟所有搜查和扣押立法（以及其他人權利益）的監督框架和標準

歐盟網路與資訊安全局

歐盟網路與資訊安全局 (ENISA) 成立於 2004 年，宗旨是「在整個歐洲共同實現高水準的網路安全。」[6] ENISA 是歐盟協調應對網路犯罪事件和危機管理的一部分，並在必要時協助歐盟委員會開展工作。[7] ENISA 是根據綜合政治危機因應 (IPCR)「框架」所完成。[8] ENISA 與成員國共同制定「歐盟級網路危機管理程序，在發生跨境網路事件時提高狀態認知，幫助國家和歐盟決策者做出正確的決定。」[9]

網路安全法案

ENISA 條例為第 (EU) 2019/881 號條例，[10] 稱為《網路安全法案》。《網路安全法案》為產品和服務建立了網路安全認證框架。[11] 該法案加強了對 ENISA 的授權，令其可支援成員國處理網路安全威脅和攻擊。同時責成 ENISA 支持成員國建立全歐盟網路安全認證框架，ENISA 將在其中發揮關鍵作用。[12]

NIS 指令和 NIS2

2016 年發佈的 NIS 指令 (EU 2016/1148)[13] 是《歐盟數位十年網路安全戰略》的一部分，也是全歐盟網路安全立法工作的第一項成果。該指令說明成員國應採用的國家網路和資訊系統安全框架。[14]

NIS 指令分為以下三個部分：[15]

「1. 國家能力：歐盟成員國須具備歐盟各國特定的國家網路安全能力，例如：必須設立國家電腦緊急應變小組 (CSIRT)、展開網路演練等。

2. 跨境協作：歐盟國家之間的跨境協作，如歐盟 CSIRT 網路、NIS 戰略合作小組等。

3. 國家對關鍵行業的監督：歐盟成員國須監督本國關鍵市場營運者的網路安全事務：對關鍵行業（能源、交通、水力、衛生、數位基礎設施和金融行業）進行事前監管，對關鍵數位服務供應商（線上市集、雲與線上搜尋引擎）進行事後監管」[16]

指令旨在「加強整個歐盟的網路安全水準」，[17] 因該指令為歐盟指令，各成員國均已開始實施。

該指令第 23 條要求歐盟委員會定期審查指令的運作情況。審查結束後，於 2020 年 12 月 16 日提交 NIS2 予歐盟。[18] NIS2 將廢止現行的 NIS 指令。NIS2 宣稱使現行法律框架現代化，「考慮到內部市場數位化程度近年來不斷提高，網路安全威脅型態亦不斷變化。」[19]

歐盟網路安全戰略

歐盟委員會和歐盟外交與安全政策高級代表於 2020 年 12 月 16 日提出了新的歐盟網路安全戰略。[20] 歐盟網路安全戰略「敘述歐盟應該如何利用和強化所有工具和資源，維護技術主權。」[21] 該戰略是一項普遍適用的工具，當中說明可以「部署」的「三大工具」，即監管、投資和政策措施。這三大工具旨在解決以下問題：

- 彈性、技術主權與領導力
- 預防、遏制和應對行動的能力
- 合作推進全球開放網路空間 [22]

多項措施（如聯合網路部門）共同構成歐盟網路安全戰略的一部分。

歐盟安全聯盟戰略：「連接新安全生態系統中各個點」

2020 年 7 月 24 日，歐盟委員會制定了 2020-2025 年的新版歐盟安全聯盟戰略。與歐盟網路安全戰略一樣，歐盟安全聯盟戰略是一項普遍適用的工具，其中亦規定必須在歐盟層面實施的原則，或在該戰略稱為「四大戰略重點」。[23]

四大戰略重點如下：[24]

- 面向未來的安全環境
- 應對不斷演變的威脅
- 保護歐洲人民免受恐怖主義和有組織犯罪的傷害
- 強大的歐洲安全生態系統

圖 2 更詳細地描述了這四大戰略重點。

聯合網路部門的宗旨，是彙集歐盟所有的資源和專業知識，預防、遏制並應對大規模網路事件及危機

聯合網路部門

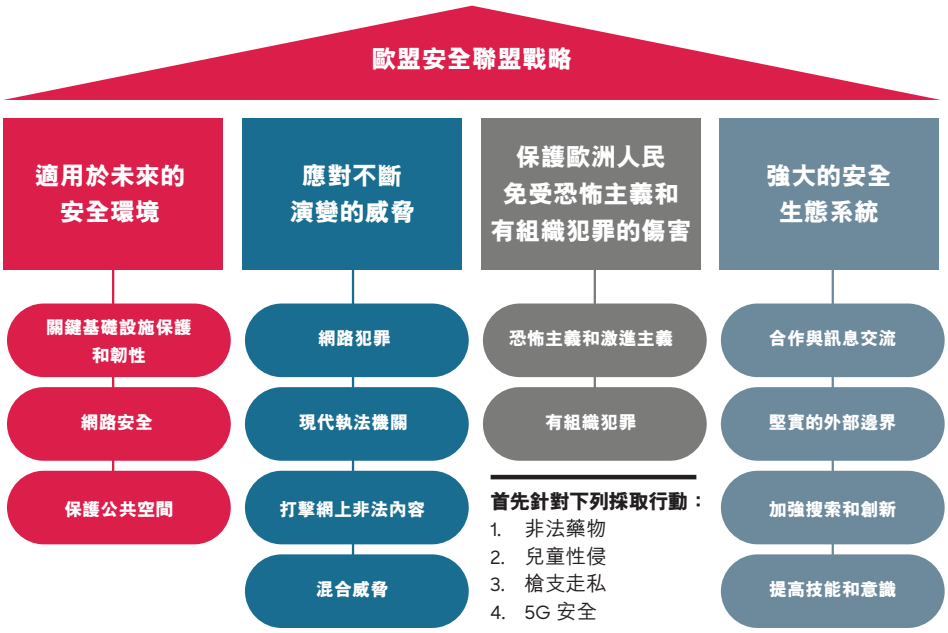
6 月 23 日，歐盟委員會提出建立一個新的聯合網路部門，以「應對影響公共服務及全歐盟企業和公民生活，且不斷增加的嚴重網路事件。」[25]

聯合網路部門的宗旨，是彙集歐盟所有的資源和專業知識，預防、遏制並應對大規模網路事件及危機。該部門也是歐盟網路安全戰略和歐盟安全聯盟戰略的成果。[26]

歐盟的資金支持

據稱，在未來 7 年裡，歐盟網路安全戰略將獲得「前所未有的投資」。[27] 此項投資將納入 2022 年歐盟長期預算。影響歐盟長期預算的機制是數位歐洲計劃、[28] 展望歐洲 [29] 和歐洲復甦計劃。[30] 除了歐盟長期預算之外，歐盟還制定目標，透過歐盟、成員國和行業的聯合投資，投入 45 億歐元（相當於 53 億美元）。[31] 歐盟將透過網路安全能力中心和協調中心網路 [32] 實現這一目標，確保大部分資金流向中小企業。

圖 2：歐盟安全聯盟戰略



資料來源：“EU Security Union Strategy: connecting the dots in a new security ecosystem”（歐盟安全聯盟戰略：連接新安全生態系統中各個點），歐盟委員會，2020 年 7 月 24 日，https://ec.europa.eu/commission/presscorner/detail/en/ip_20_1379

歐洲網路安全生態系統的影響和現狀

目前，生態系統只是一個構想，尚未落實到實際組織構成，因此可稱為具有前瞻性的網路安全框架，而不是現行框架。

歐盟將從 2022 年開始對網路安全戰略給予資金支持。聯合網路部門是歐盟委員會的一項提案，尚待實施。因此，該新生態系統對網路犯罪顯然尚未產生影響。

歐盟打擊網路犯罪的行動，現狀如何？自 2004 年以來，ENISA 一直是歐盟打擊網路犯罪的重要機構，而 NIS 指令發佈於 2016 年。

這份具有前瞻性的網路安全框架的影響，可能還要過幾年才會顯現出來。資金支持將從 2022 年開始入場，但其相關提案在 2023 年之前是否可執行，仍在觀望中。歐盟委員會預計於 2022 年 6 月 30 日展開聯合網路部門的運行階段，並於 2023 年 6 月 30 日全面獨立運作。[33]

歐盟委員會網站上發佈了如下聲明：「歐盟網路安全生態系統廣泛而多樣。有了聯合網路部門，不同群體和領域將享有一片合作共事的空間，屆時將可令現有網路充分發揮其潛力。這一生態系統的基礎，是從 2017 年開始的各項工作……」[34]

總之，目前看來歐洲網路安全生態系統是一份出色的可行戰略，似乎具備所有成功要素，即資金支持、成員國的合作以及必要的技能和專業知識。

Gideon Bouwer，Cyberlawforensics 資訊技術律師，南非，
gideon@cyberlawforensics.co.za

[1] “EU Cybersecurity: Commission proposes a Joint Cyber Unit to step up response to large-scale security incidents”（歐盟網路安全：歐盟委員會提議成立聯合網路部門，加強應對大規模安全事件），*歐盟委員會*，2021 年 6 月 23 日，https://ec.europa.eu/commission/presscorner/detail/en/ip_21_3088

[2] “What is IoT?”（什麼是物聯網？），*甲骨文*，https://www.oracle.com/za/internet-of-things/what-is-iot/。「物聯網 (IoT) 係指嵌入感測器、軟體及其他技術的實體物件（『物』）網路，其目的是通過網際網路連接其他設備和系統及交換資料。」

[3] 歐洲理事會成立於 1949 年，47 個歐洲國家為其成員國。

[4] Dietrich Schindler，“European Convention on Human Rights in Practice”（歐洲人權公約），*Washington University Law Quarterly*，1962 年 1 月，https://openscholarship.wustl.edu/law_lawreview/vol1962/iss2/2

[5] “European Convention on Human Rights: Europe [1950]”（歐洲人權公約：歐洲 [1950]），*大英百科全書*，1950 年 11 月 4 日，https://www.britannica.com/event/European-Convention-on-Human-Rights-Europe-1950（訪問日期：2020 年 9 月 17 日）。

[6] “About ENISA - The European Union Agency for Cybersecurity”（關於 ENISA——歐盟網路安全局），*歐盟網路安全局*，https://www.enisa.europa.eu/about-enisa

[7] “EU-level Cyber Crisis Management”（歐盟級網路危機管理），*歐盟網路安全局*，https://www.enisa.europa.eu/topics/cyber-crisis-management/eu-cooperation

[8] “How does the Integrated Political Crisis Response (IPCR) mechanism work?”（綜合政治危機因應 (IPCR) 機制的運作方式），*歐盟理事會*，2018 年，https://www.consilium.europa.eu/en/documents-publications/publications/ipcr/。「IPCR 是歐盟理事會的危機因應機制，是握在主席國手中的『工具』，用於協調對重大跨部門複雜危機（包括恐怖主義行為）的政治回應。」

[9] “EU-level Cyber Crisis Management”（歐盟級網路危機管理），*歐盟網路安全局*，https://www.enisa.europa.eu/topics/cyber-crisis-management/eu-cooperation

[10] “ENISA Mandate and Regulatory Framework”（ENISA 的授權和監管框架），*歐盟網路安全局*，https://www.enisa.europa.eu/about-enisa/regulatory-framework

[11] “The EU Cybersecurity Act”（歐盟網路安全法案），*歐盟委員會*，https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-act

[12] “The EU Cybersecurity Act is Now Applicable”（《歐盟網路安全法案》現已實施），*眾達律師事務所*，2019 年 6 月，https://www.jonesday.com/en/insights/2019/06/the-eu-cybersecurity-act-is-now-applicable

[13] “NIS Directive”（NIS 指令），*歐盟網路安全局*，https://www.enisa.europa.eu/topics/nis-directive

[14] 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”（歐盟新版網路安全框架：NIS 指令、ENISA 的作用及一般資料保護規則），*Computer Law & Security Review*，35 卷，第 6 期，2019 年 11 月，https://www.sciencedirect.com/science/article/pii/S0267364919300512（訪問日期：2021 年 8 月 11 日）。

[15] “NIS Directive”（NIS 指令），*歐盟網路安全局*，https://www.enisa.europa.eu/topics/nis-directive

[16] 同上。

[17] 同上。

[18] “NIS Directive”（NIS 指令），*歐盟委員會*，https://digital-strategy.ec.europa.eu/en/policies/nis-directive

[19] 同上。

[20] “The EU’s Cybersecurity Strategy for the Digital Decade”（歐盟數位十年網路安全戰略），*歐盟委員會*，2020 年 12 月 16 日，https://digital-strategy.ec.europa.eu/en/library/eus-cybersecurity-strategy-digital-decade-0

[21] “The Cybersecurity Strategy”（網路安全戰略），*歐盟委員會*，https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-strategy

[22] 同上。

[23] “EU Security Union Strategy: connecting the dots in a new security ecosystem”（歐盟安全聯盟戰略：連接新安全生態系統中各個點），*歐盟委員會*，2020 年 7 月 24 日，https://ec.europa.eu/commission/presscorner/detail/en/ip_20_1379

[24] 同上。

[25] “EU Cybersecurity: Commission proposes a Joint Cyber Unit to step up response to large-scale security incidents”（歐盟網路安全：歐盟委員會提議成立聯合網路部門，加強應對大規模安全事件），*歐盟委員會*，2021 年 6 月 23 日，https://ec.europa.eu/commission/presscorner/detail/en/ip_21_3088

[26] 同上。

[27] “New EU Cybersecurity Strategy and new rules to make physical and digital critical entities more resilient”（新的歐盟網路安全戰略，以及提升實際與數位重要實體彈性的新規則），*歐盟委員會*，2020 年 12 月 16 日，https://ec.europa.eu/commission/presscorner/detail/en/ip_20_2391

[28] “Commission welcomes political agreement on €7.5 billion Digital Europe Programme”（歐盟委員會歡迎就 75 億歐元的數位歐洲計劃達成政治協議），*歐盟委員會*，2020 年 12 月 14 日，https://ec.europa.eu/commission/presscorner/detail/en/ip_20_2406

[29] “Commission welcomes political agreement on Horizon Europe, the next EU research and innovation programme”（歐盟委員會歡迎就下一項歐盟研究與創新計劃「展望歐洲」達成政治協議），*歐盟委員會*，2020 年 12 月 10 日，https://ec.europa.eu/commission/presscorner/detail/en/IP_20_2345

[30] “Recovery plan for Europe”（歐洲復甦計劃），*歐盟委員會*，https://ec.europa.eu/info/strategy/recovery-plan-europe_en

[31] “New EU Cybersecurity Strategy and new rules to make physical and digital critical entities more resilient”（新的歐盟網路安全戰略，以及提升實際與數位重要實體彈性的新規則），*歐盟委員會*，2020 年 12 月 16 日，https://ec.europa.eu/commission/presscorner/detail/en/ip_20_2391（訪問日期：2021 年 8 月 11 日）。

[32] “Commission welcomes political agreement on the Cybersecurity Competence Centre and Network”（歐盟委員會歡迎就網路安全能力中心與網路達成政治協議），*歐盟委員會*，2020 年 12 月 11 日，https://ec.europa.eu/commission/presscorner/detail/en/IP_20_2384

[33] 同上。

[34] “EU Cybersecurity: Commission proposes a Joint Cyber Unit to step up response to large-scale security incidents”（歐盟網路安全：歐盟委員會提議成立聯合網路部門，加強應對大規模安全事件），*歐盟委員會*，2021 年 6 月 23 日，https://ec.europa.eu/commission/presscorner/detail/en/ip_21_3088

ACAMS™
公認反洗錢師協會

成為擁有防制洗錢或制裁法遵領域全球資格認證的專業人士

CAMS
CERTIFIED ANTI-MONEY LAUNDERING SPECIALIST

防制洗錢認證的國際黃金標竿

CGSS™
CERTIFIED GLOBAL SANCTIONS SPECIALIST

瞭解並解讀不斷變化的制裁制度

到訪 **www.acams.org**
開啟您的旅程

韓國「N號房」案例分析

2020年，全球封鎖導致線上兒童性虐待內容(CSAM)的供需雙雙增長；希望交換和提供非法內容的用戶，透過社交媒體、即時訊息工具、聊天室和線上遊戲存取這些內容，歐洲刑警組織將這種行為稱為「利用隔離」(Exploit Isolation)。

特別令人擔憂的是，這些非法內容大部分是未成年受害者自己製作的，而犯罪分子在試圖擴大參與者和倖存者範圍時，以脅迫方式取得這些內容。[1] 兒童和未成年人性剝削的最新案例是韓國「N號房」事件。

我們將在下文分析「N號房」一案，使人們加強認識此類犯罪行為，並提供防範金融犯罪專業人士可識別、標記和報告此類犯罪行為的知識；同時為執法機關和檢察官提供相關的工具和知識，協助他們逮捕和起訴涉及兒童性虐待內容的犯罪分子。

兒童性虐待內容不斷進化，難以預防、識別、追蹤和報告。兒童性虐待內容的交易方式特殊，因此不容易確定調查的司法管轄區，難以取得起訴所需的充分資料/證據。如果涉及加密貨幣，就可能涉及多個司法管轄區。根據所用加密貨幣的性質，也可能降低追蹤犯罪分子的難度。

建立信任

犯罪分子把兒童性虐待內容當作流通貨幣使用，為了獲得這種內容，他們首先會進行網路誘騙。犯罪分子透過搜尋受害者的社交媒體內容或線上遊戲玩家，確定容易上當的攻擊目標。鎖定目標後，他們會經由 Telegram 等即時訊息工具結識受害者。

犯罪分子會透過多種方式誘騙兒童性虐待內容的目標對象，包括假冒金主、星探、真愛或好友。誘騙活動往往分步實施，類似傳統的「線下」人口販賣活動，犯罪分子與受害者持續對話或允諾給予獎勵，與之建立信任。他們可能假扮金主或星探，向目標對象許諾金錢或名聲，或提出真愛諾言。

羞恥因素

隨著誘騙的發展，如果越來越成功，目標對象就會陷入騙局、無法脫身，犯罪分子會脅迫他們提供私密細節、照片、影片、財務資訊、個人資訊等。無論是透過網路詐騙，[2] 或是無意間洩漏或被脅迫揭露，犯罪分子一旦獲得這些私密細節，就會利用「羞恥因素」[3] 開始勒索，威脅把圖片內容散布到網上，讓所有人都能看到。

除此之外，在「N 號房」一案中，部分兒童性虐待內容是未成年人的家人

兒童性虐待內容不斷進化，難以預防、識別、追蹤和報告

提供的，為了獲得信任、受邀進入各種聊天室，他們自願上傳照片和影片。[4] 這是「N 號房」運作方式的一部分——採用會員制服務模式，在不同主題的聊天室裡交換性剝削內容。例如，「哥譚室」(Gotham Room) 是會員們共享兒童性虐待內容的行銷室，「羅莉室」(Loli Room，源自“Lolita complex”（羅莉塔情結）一詞）則提供物化年輕女孩的影片。兒童性虐待內容提供者被稱為「醫生」，向「醫生室」(Doctor's Room) 上傳影片可獲得報酬。[5] 為了能存取更多違禁內容，有些人同時扮演兩個角色（內容買家和提供者）。

殘酷的統計數據

「N 號房」內容的買家用比特幣付款，支付金額從 25 萬韓元（合 217.32 美元）到 155 萬韓元（合 1,347.39 美元）不等。[6]

令人厭惡的是，「N 號房」自 2018 年開播以來，上傳的兒童性虐待內容中除了色情內容外，還包括慘不忍睹的自殘內容。

迄今為止，已發現 3,700 多個色情短片，[7] 逮捕了 100 多名犯罪嫌疑人。Telegram 上的 56 個受監控聊天群似乎有超過 26 萬用戶。令人不安的是，「N 號房」得到很多人的支持，他們打招呼不說「你好」，而是「我們強姦吧」。[8]

了解您的客戶

幸好「N 號房」被兩名韓國女大學生曝光了，她們 2019 年聽說有這種剝削現象，[9] 於是著手調查以參加一項新聞專題報導比賽。她們在文章《你賣兒童色情內容嗎？ Telegram 大量滋生犯罪活動》中，描述了二人臥底發現的色情聊天室，最終導致「N 號房」幕後主使被捕。外號「GodGod」的韓國男子被判 34 年監禁。[10] 諷刺的是，據消息透露，GodGod 要求潛在會員提供「了解您的客戶」文件，篩查並驗證他們的身分，通過後才能參與交換兒童性虐待內容。

戀童障礙

對兒童性虐待內容的需求助長了此類內容的供應和獲利力。防範金融犯罪和執法機關專業人士通常認為，兒童性虐待、人口販賣和現代奴隸制屬於犯罪，必須予以起訴和懲罰。然而，要從全球徹底根除兒童性虐待內容，需要傳授並讓人們認知有關戀童障礙等疾病及可能的治療方式。戀童障礙的特點是反覆對未成年人（通常是 13 歲以下）出現強烈的性幻想、性衝動或性行為。患者必須年滿 16 歲以上，且比其性幻想或性行為的對象年長 5 歲以上，才能被確診患有戀童障礙。

對戀童障礙患者的治療方式包括心理治療和藥物治療（如抗雄激素）；然而，這些人可能不會尋求治療，因為法律要求臨床醫生和治療師必須向有關當局報告疑似兒童性虐待或身體虐待行為。這些要求因國家 / 地區而異。此外，確診年齡指導原則可能適用於西方文化，但許多文化允許未成年人從事性活動、婚姻和生育，並不見得適用。[11] 基於上述理由，許多兒童剝削案件遭到忽視，沒人提出報告，也無任何處理。由於一些金融機構具有國際影響力，我們可以利用其平臺，宣傳戀童障礙知識和相對應治療方案，在全球提高人們的認識，擴大文化影響，防範兒童剝削行為。

在打擊兒童剝削犯罪行為方面，首先必須教育並協助兒童認識和報告剝削行為

教育的重要性

在打擊兒童剝削犯罪行為方面，首先必須教育並協助兒童認識和報告剝削行為。棘手的是，在某些文化中，服從父母或長輩比兒童權利重要。因此，人們可能把兒童性剝削行為視為「家庭問題」而非法律問題。在壓力較大的家庭環境、自尊心較低且科技設備使用不受限制的情況下，兒童遭受性虐待的可能性更大。[12]

金融機構不僅能發現和報告潛在的兒童剝削行為，還可以利用其平臺啟動青少年呵護計劃，增進他們的心理健康和技術風險意識。金融機構可以結盟，支持從事兒童權利與安全的地方或國際組織。金融機構和國家或地區可以加入 WeProtect 全球聯盟等組織，共同打擊全球線上兒童性剝削活動。[13] 虛擬全球特別工作組 (VGT) 則是旨於解決線上兒童性剝削問題的國際執法機關聯盟。[14] 跨信仰聯盟結合世界各地的宗教領袖、執法機關、監管機構和科技行業，共同打擊兒童剝削活動，增進兒童尊嚴。[15]

與執法機關合作

傳統金融機構和加密貨幣交易所可以追蹤到兒童性虐待內容的潛在收益，並向執法機關報告或與其合作。在「N 號房」一案中，一些加密貨幣交易所為執法機關提供了寶貴的協助。[16]

兒童性虐待內容提供者和消費者採用不同的交易模式，金融機構必須制定特定的偵測規則，才能識別交易雙方。消費者交易金額小，利用各種貨幣服務企業來掩蓋資金的目的地。提供者可能會使用類似商業帳戶的帳戶，但業務性質

從誘騙、製作性內容到收款的過程中，線上兒童性剝削內容的提供者在各階段皆高度仰賴網際網路

和資金來源可能不明。有時候，提供者可能會使用多個個人帳戶從事活動。

根據加拿大金融交易和報告分析中心對線上兒童性剝削相關揭露和可疑交易報告的分析，消費者交易主要是透過貨幣服務企業對外轉帳，將資金轉移到兒童性剝削高風險司法管轄區，包括菲律賓、泰國、哥倫比亞、美國、加納、烏克蘭、多明尼加共和國、羅馬尼亞、牙買加和俄羅斯。[17]

可疑活動指標

從誘騙、製作性內容到收款的過程中，線上兒童性剝削內容的提供者在各階段皆高度仰賴網際網路。綜合各種情況，潛在犯罪分子的相關可疑活動指標包括線上購物、購買應用程式、線上遊戲和賭博、使用線上影音和通訊技術、使用線上文件儲存服務等一種或多種行為。這些交易可能涉及支付處理商。[18]

有些提供者可能會用加密貨幣提供線上兒童剝削內容銷售服務，Welcome to Video 即是本文撰寫時，內容最多的兒童性剝削市場。[19] 該網站使用比特幣進行交易，執法機關可以進行追蹤。相信提供者可能會轉而使用匿名加密貨幣以逃避追蹤，因為這些代幣加入了第三方交易處理商，可以隱藏交易記錄。在「N 號房」一案中，為方便透過 Telegram 存取，提供者接受比特幣付款。[20]

在可能使用匿名幣來混淆來源和活動目的的情況下，即可以將交易模式、交易金額以及用戶相關的負面新聞作為指標。例如，在調查 Welcome to Video 時，某些交易金額（如 0.04 個比特幣或 39 美元）出現的頻率比其他交易金額高，這些金額可能是某些內容的固定費用。透過特定金額的等價匿名幣可以洞察出交易目的。

儘管可以使用任何類型的加密貨幣帳戶購買兒童虐待內容，但更有可能專為此類購買交易開立加密貨幣帳戶，利用這些帳戶從事其他交易活動的機會很小。韓國非常勇敢，能與全球分享「N 號房」案件及其細節。透過該案件，我們可以更深入瞭解線上兒童剝削及其可能的偵測和防範方法。其他國家或地區需要效仿韓國，為保護公眾尤其是兒童的安全，披露犯罪分子的身分。

社交媒體的作用

全球疫情使得線上兒童虐待內容增多，犯罪分子利用「適合兒童」的應用程式結識和剝削兒童。[21] 兒童剝削問題不是某個平臺特有的問題，而是存在於所有社交媒體。對於社交媒體公司在監管或規定用戶發佈內容方面需要承擔多少責任，人們仍然爭論不休。[22] 加拿大等五眼聯盟國家（其他四個為美國、英國、澳洲和紐西蘭）發表聲明稱，將推動全球科技公司採納一套自願原則，就線上兒童性剝削內容的識別、揭露和刪除作出規定。此外，這些國家還努力提高追查和起訴兒童剝削犯罪分子的能力，立法強制社交媒體公司改進對兒童剝削內容的監管。[23]

社交媒體的作用與歐洲聯盟

為響應上述自願原則，歐洲議會也通過了一項新的臨時立法，允許根據歐洲聯盟電子隱私指令的規定，利用掃描技術偵測線上

兒童剝削問題不是某個平臺特有的問題，而是存在於所有社交媒體

誘騙活動。授權官員對違規實體（此例中為電子服務提供商）進行制裁或約束，強制政府提供保護，這非常重要。[24]

根據 7 月 24 日「歐盟委員會致歐洲議會公函」，[25]「……歐洲刑警組織無法從私營機構直接收取個人資料，支援成員國的能力受到窒礙……」這表明，受現行立法所限，歐盟和其他司法管轄區只能被動期望電子服務提供商能自願揭露相關資訊。在不揭露的情況下，經營兒童性虐待內容服務以及協助傳播兒童性虐待內容的特定電子服務提供商仍可繼續業務，無任何阻礙和懲罰。可以理解當今社會不能缺少資料隱私。然而，如果在兒童性虐待內容傳播方面依賴自願揭露，結果會造成巨大的真空，受到保護的只有犯罪分子。因此全球必須建立起強制、鼓勵揭露的機制，且對不揭露行為進行懲罰和追責，使這種自願揭露政策變得既有益也有意義。

結語

人口販賣（最近被歸為現代奴隸制）已經存在很長時間，隨著網際網路和現代通訊的出現，出現了顯著增長。

近來，各種形式的網路犯罪已演變為一種有利可圖的威脅。在新冠疫情的助威下，受害者自己所發佈而歐洲刑警組織將之稱為「自我剝削」的內容，網路犯罪也變得更加複雜，因為犯罪分子會利用一切機會，獲取非法利益，同時盡可能降低對自己的風險。

「N 號房」一案和相關參考資料提供了有用的真實案例，使我們可以從亞洲和歐洲角度瞭解最新的犯罪方法，深入探討更多可疑活動指標和這些案例的運作方式。

在研究和撰寫本文時，筆者不禁自問，ACAMS 會員該如何阻止這種剝削？

ACAMS 專業人士要同心協力，對此類犯罪活動的存在提高警覺，瞭解其運作方式，向執法機關報告可疑活動，繼續在打擊此類犯罪方面發揮積極作用。

歡迎會員和讀者提出寶貴意見。筆者研究過受害鏈，從預防網路釣魚和誘騙、識別犯罪分子、偵測付款方式，以及從服務和經營角度，考慮各種可能的解決方案。

金融機構亦可參與預防、偵測和報告兒童性虐待內容的工作。也可以利用金融機構的平臺，提高對兒童性虐待內容主題和預防方法的認識。

Shann Lu，法學碩士，CAMS，
Bitfinex 防制洗錢和金融詐欺調查管理

Fara Fallah，CAMS，CGSS，CBP，
CCI，Bitfinex 法規遵循顧問

編輯和其他內容：Peter Warrack，
CAMS、CBP、CCI、CFE，
Bitfinex 首席法規遵循專員

[1] “Exploiting isolation: sexual predators increasingly targeting children during COVID pandemic”（利用隔離：性掠奪者在新冠疫情期間逐漸瞄準兒童），*歐洲刑警組織*，2020 年 6 月 19 日，https://www.europol.europa.eu/newsroom/news/exploiting-isolation-sexual-predators-increasingly-targeting-children-during-covid-pandemic

[2] “Internet Fraud”（網際網路詐騙），*聯邦調查局*，https://www.fbi.gov/scams-and-safety/common-scams-and-crimes/internet-fraud

[3] Nicole de Souza，“The Nth Room case and modern slavery in the digital space”（「N 號房」案件與數位空間裡的現代奴隸制），*The Interpreter*，2020 年 4 月 20 日，https://www.lowyinstitute.org/the-interpreter/nth-room-case-and-modern-slavery-digital-space

[4] Yoon So-Yeon，“The spark that ignited the ‘Nth room’ fire”（點燃「N 號房」之火的火花），*韓國《中央日報》*，2020 年 3 月 31 日，https://koreajoongangdaily.joins.com/2020/03/31/features/The-spark-that-ignited-the-Nth-room-fire/3075527.html

[5] Ron Kim，“Victim Of Telegram Nth Room Case Speaks Up About The Horrors She Faced As A Middle School Student”（Telegram「N 號房」案受害者講述身為一名中學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/

[6] 同上。

[7] Choe Sang-Hun，“South Korean Man Gets 34 Years for Running Sexual Exploitation Chat Room”（韓國男子因經營性剝削聊天室被判 34 年），*《紐約時報》*，2021 年 4 月 8 日，https://www.nytimes.com/2021/04/08/world/asia/korea-sex-crime-chat-rooms.html

[8] Haeryun Kang，“South Korea’s ‘nth rooms’ are toxic mixture of tech, sex and crime”（韓國「N 號房」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

[9] Yoon So-Yeon，“The spark that ignited the ‘Nth room’ fire”（點燃「N 號房」之火的火花），*韓國《中央日報》*，2020 年 3 月 31 日，https://koreajoongangdaily.joins.com/2020/03/31/features/The-spark-that-ignited-the-Nth-room-fire/3075527.html

[10] Choe Sang-Hun，“South Korean Man Gets 34 Years for Running Sexual Exploitation Chat Room”（韓國男子因經營性剝削聊天室被判 34 年），*《紐約時報》*，2021 年 4 月 8 日，https://www.nytimes.com/2021/04/08/world/asia/korea-sex-crime-chat-rooms.html

[11] 醫學博士 George R. Brown，“Pedophilic Disorder”（戀童障礙），*Merck Manuals Professional Edition*，https://www.merckmanuals.com/en-ca/professional/psychiatric-disorders/paraphilic-disorders/pedophilic-disorder

[12] “11 Factors That Increase the Risk of Child Sexual Abuse”（增加兒童性虐待風險的 11 個因素），*Defend Innocence*，https://defendinnocence.org/child-sexual-abuse-risk-reduction/proactive-parenting/reduce-risk/11-factors-that-increase-the-risk-of-child-sexual-abuse/

[13] *WeProtect 全球聯盟*，https://www.weprotect.org/

[14] *虛擬全球特別工作組*，http://virtualglobaltaskforce.com/

[15] “Areas of Focus”（重點關注領域），*Interfaith Alliance for Safer Communities*，https://iafsc.org/areas-of-focus/child-dignity-online

[16] Felipe Erazo，“Huobi Korea Delists XMR Amid Nth Room Sexual Exploitation Case Rumors”（「N 號房」性剝削案謠言四起，火幣韓國交易所下架門羅幣），*Cointelegraph*，2020 年 4 月 12 日，https://cointelegraph.com/news/huobi-korea-delists-xmr-amid-nth-room-sexual-exploitation-case-rumors

[17] “Operational alert: Laundering of proceeds from online child sexual exploitation”（營運警報：洗白線上兒童性剝削所得），*加拿大金融交易與報告分析中心*，2020 年 12 月，https://www.fintrac-canafe.gc.ca/intel/operation/exploitation-eng

[18] 同上。

[19] “South Korean National and Hundreds of Others Charged Worldwide in the Takedown of the Largest Darknet Child Pornography Website, Which was Funded by Bitcoin”（警方關閉使用比特幣交易的最大兒童淫穢資料暗網，對一名韓國人及數百位多國人員提起訴訟），*美國司法部*，2019 年 10 月 16 日，https://www.justice.gov/opa/pr/south-korean-national-and-hundreds-others-charged-worldwide-takedown-largest-darknet-child

[20] Scott Ikeda，“South Korea’s New Crypto AML Law Bans Trading of “Privacy Coins” (Monero, Zcash)”（韓國新加密貨幣防制洗錢法禁止「匿名幣」（門羅幣、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/

[21] “Online Child Sexual Exploitation”（線上兒童性剝削），*加拿大政府*，https://www.canada.ca/en/public-safety-canada/campaigns/online-child-sexual-exploitation.html

[22] Aaron Barr，“Social Media Regulation: The Line Between Privacy and Protection”（社交媒體監管：隱私與保護間的界限），*Security Boulevard*，2021 年 6 月 9 日，https://securityboulevard.com/2021/06/social-media-regulation-the-line-between-privacy-and-protection/

[23] Karen Pauls，“New rules on removal of illegal online content could help in battle against child pornography”（非法線上內容刪除新規則有助於打擊兒童色情），*CBC*，2021 年 1 月 4 日，https://www.cbc.ca/news/canada/manitoba/canada-illegal-online-content-child-porn-1.5847695

[24] “Five Country Statement to EU to prevent child abuse online”（五國發表聲明，呼籲歐盟防範線上兒童虐待行為），*澳洲內政部部長*，2021 年 1 月 13 日，https://minister.homeaffairs.gov.au/peterdutton/Pages/five-country-statement-EU-prevent-child-abuse-online.aspx

[25] “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”（歐盟委員會致歐洲議會、歐盟理事會、歐洲經濟和社會委員會及地區委員會的公函——歐盟有效打擊兒童性虐待策略），*歐盟委員會*，2020 年 7 月 24 日，https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020DC0607

如何將洗錢風險納入風險管理：（上）

相關規則已將洗錢和資助恐怖活動風險（以下簡稱「洗錢風險」）納入金融機構整體風險管理的範疇。這些規則包括防制洗錢金融行動工作組織 2014 年發佈的《銀行業風險為本方法應用指南》、巴塞爾委員會 2017 年發佈的《防制洗錢及資助恐怖主義相關風險的健全管理指導》指南、中國銀行保險監督管理委員會 2019 年發佈的《銀行業金融機構防制洗錢及資助恐怖活動管理辦法》等。

中國人民銀行印發的《法人金融機構洗錢和恐怖融資活動風險管理指引》（銀反洗發 [2018] 19 號）就法人金融機構加強實踐風險為本方法作出了詳細規定。這些指引還包括貫徹落實《國務院辦公廳關於改善反洗錢、反資助恐怖主義、反逃稅監管體制機制的意見》，加強法人金融機構的防制洗錢 / 打擊資恐工作，以及有效防範洗錢和相關犯罪活動。然而，許多機構對於如何將洗錢風險納入金融機構整體風險管理工作仍存疑慮，甚至在實踐中可能繞了遠路。筆者將基於監管實踐和金融機構的實際情況，利用系列文章就以下三方面提出一些指引建議：洗錢風險的評估與衡量；洗錢風險管理策略的制定；高階管理人員職責的落實。

這是系列文章的第一篇，將討論洗錢風險的評估和衡量。雖然上述指引和規則已將洗錢風險納入了金融機構的整體風險管理框架，但並未提供評估和衡量風險的方法，也未說明如何衡量該風險給金融機構帶來的損失。

洗錢風險的評估與衡量

在大多數情況下，洗錢風險本身不會給金融機構帶來直接風險或直接經濟損失，有時甚至會產生收入，卻會產生間接風險或損失。正如巴塞爾委員會所說：「如果洗錢 / 資恐風險管理制度不健全或是欠缺該制度，則會使銀行面臨重大風險，尤其是聲譽風險、經營風險、法規遵循風險和集中風險。」[1] 值得注意的是，這些風險有相互關聯性。然而，對金融機構的任何處罰都有可能同時帶來巨大的風險（例如，批量融資和貸款終止成本、對銀行的索賠、調查成本、資產凍結和貸款損失）。此外，為解決洗錢風險帶來的問題，投入有限且寶貴的管理資源與營運資源，也會產生成本。《法人金融機構洗錢和恐怖融資活動風險管理指引》（銀反洗發 [2018] 19 號）：「任何洗錢風險事件或案件的發生都可能帶來嚴重的聲譽風險和法律風險，並導致客戶流失、業務損失和財務損失。」

如果金融機構未能認真實施適當的風險管理政策、程序和控制措施，除了「強監管、嚴問責」帶來的防制洗錢罰款外，還會增加洗錢風險帶來的直接或間接成本。如果金融機構能繼續實施有效的風險為本防制洗錢 / 打擊資恐政策和程序，則可以減少或避免此類成本和損失。因此，金融機構需要評估洗錢風險，衡量洗錢風險造成的直接或間接損失，積極反省其洗錢風險狀況，使制定的洗錢風險管理策略能符合洗錢風險狀況及機構的系統重要性程度。下文分別介紹歷史模擬法和情景分析法，用於衡量洗錢風險所致直接或間接損失。

衡量法規遵循風險造成的損失

監察部負責監督金融機構代表公眾利益履行防制洗錢義務、降低洗錢活動對社會危害的情況。如果金融機構未能履行防制洗錢義務，監管機構（包括其他司法管轄區）將對金融機構進行處罰。監管部門不僅可以罰款，還可責令金融機構停業整頓，暫停或停止特定業務，不核准新業務，提高各類基金（存款保險基金、投資者保護基金、保險保障基金等）的適足率等。

假設法規遵循風險損失以 T1 表示，罰款損失以 t11 表示，發生機率以 p11 表示；金融機構被責令停業整頓，損失以 t12 表示，發生機率以 p12 表示；暫停或停止業務所致損失以 t13 表示，發生機率以 p13 表示；新業務損失以 t14 表示，發生機率以 p14 表示；增加各類資金的適足率，損失以 t15 表示，發生機率以 p15 表示；則公式為：$T1 = t11 \times p11 + t12 \times p12 + t13 \times p13 + t14 \times p14 + t15 \times p15$。各金融機構可根據其註冊地、分支機構所在地和境外分支機構所在國家或地區的防制洗錢監管力度、頻率和實際處罰情況，特別是對同類機構的處罰情況，結合本身洗錢風險的自評結果和發現的潛在違規事實，確定 t11 和 p11 的值；同樣，可以結合實際數據或歷史數據確定 t12、p12、t13、p13、t14、p14、t15、p15 的值。

衡量聲譽風險造成的損失

聲譽風險造成的損失很難評估。如果在遭到重大防制洗錢行政處罰後，金融機構暴露在洗錢醜聞或出現負面新聞，結果可能導致（新舊）客戶流失。這不但令營收減少，甚至可能導致銀行擠兌。此外，銀行將謹慎處理該金融機構帶來的業務（通匯業務、跨境匯款等），這會加大業務開發的「摩擦係數」，消耗金融機構寶貴的有限管理資源和營運資源，導致潛在損失，甚至與銀行的合作關係終止。假設聲譽風險造成的損失以 T2 表示，客戶減少造成的損失以 t21 表示，發生機率以 p21 表示；業務損失以 t22 表示，發生機率以 p22 表示；則有公式 $T2 = t21 \times p21 + t22 \times p22$。各金融機構可以根據其現有客戶或潛在客戶的實際情況設計調查問卷，抽樣評估客戶獲悉金融機構捲入洗錢醜聞或負面新聞，而後受到重大防制洗錢行政處罰時會採取的措施，然後評估相關損失。這樣就可以確定 t21 和 p21 的值；業務損失——t22 和 p22 的值——可以根據各種憑單和資訊的成本，以及處理各種銀行同業業務所需要的各種憑單和資訊導致的工作效率下降來確定。

經營風險和集中風險有可能直接造成損失；然而，經營風險和集中風險有可能放大法規遵循風險、聲譽風險和法律風險

衡量法律風險造成的損失

法律風險所致的損失主要是指特定客戶群或受害客戶在金融機構發生洗錢案件後採取的法律行動，以及金融機構為避免陷入索賠或賠償程序而承擔的損失。例如，一家銀行因海外洗錢案而被提起法律訴訟，因此支付了數百萬美元的律師費。假設法律風險造成的損失以 T3 表示，客戶賠償以 t31 表示，發生機率以 p31 表示；律師費以 t32 表示，發生機率以 p32 表示；則有公式 T3 = t31 × p31 + t32 × p32。

衡量經營風險和集中風險造成的損失

經營風險和集中風險有可能直接造成損失；然而，經營風險和集中風險有可能放大法規遵循風險、聲譽風險和法律風險。金融機構經營風險和集中風險會增加其他風險的發生機率，很可能導致法規遵循風險、聲譽風險、法律風險，進而造成損失。具體而言，如果金融機構存在經營風險，很可能造成內部防制洗錢控管制度失效，甚至產生「內外合謀」，使內部防制洗錢控管制度形同虛設。

例如，某銀行櫃員應客戶要求辦理「假現金」業務，最終導致洗錢案件發生，造成監管部門對該行罰款 500 萬元人民幣（約合 773,167.95 美元）。如果金融機構存在集中風險，洗錢風險可能有五種表現：一，交易對象集中在洗錢風險高的國家和地區；二，客戶集中在洗錢風險高的國家和地區；三，交易量集中於洗錢風險較高的業務或產品；四，交易量集中於洗錢風險高的客戶；五，同一受益所有人控制的法律工具或法律安排構成代理規模和資本優勢，或者構成大量關聯交易。

綜上，假設金融機構因洗錢風險承擔的總損失表示為 T，則有 T = T1 + T2 + T3。在一定時期內，這些損失需要金融機構動用資本甚至提前動用儲備金來彌補。

為了評估和衡量洗錢風險造成的損失，本文只考慮實務中常見的風險因素。這些風險因素會相互作用，一個風險要素的發生會影響另一風險要素的發生機率。此外，本文未考慮金融機構的溝通協調能力和輿論的影響，也未考慮其他洗錢風險因素造成的損失。

本文探討的洗錢風險評估和衡量方法還有待改進，業內人士可以研究探索其他更先進的方法。

下一篇文章將討論洗錢風險管理策略的制定問題。

Liu Lihong，中國人民銀行業務辦公室

[1] “Guidelines: Sound management of risks related to money laundering and financing of terrorism”（指南：防制洗錢及資助恐怖主義相關風險的健全管理指導），*巴塞爾銀行監管委員會*，2017 年 6 月，https://www.bis.org/bcbs/publ/d405.pdf

《隔離帶來的深思》第3章：求職者的反擊

欲閱讀《隔離帶來的深思》第1章和第2章，請前往 ACAMSToday.org 網站「職業指南」專欄查看。

13年來，我一直在防制洗錢、法規遵循和監管領域從事人才招聘工作，期間經歷過兩次經濟衰退。我學到的最寶貴一課就是經濟衰退是可預測的，與其他週期一樣——至少從招聘的角度來看。我上班的第一天，是2008年7月15日。我之所以記得這麼清楚，是因為兩個月後，我才剛剛熟悉的一家大銀行破產了。2008年9月15日，雷曼兄弟倒閉。自那之後，多米諾骨牌開始坍塌。銀行與公司合併，申請破產，向政府求助……壞消息紛至沓來，令人備受煎熬。開始時（也是經濟

衰退最嚴重的時候），首當其衝的便是工作，尤其是低收入工作。2008 年底，我的電話開始響個不停，直到 2010 年初才算消停。來電數量從零星到越來越多，然後突然就是一連串集體解雇的故事。2009 年，美國運通一次又一次在大禮堂裡召集員工，然後一下子把員工統統解雇。實際上，這樣也無可厚非：5 萬人，要如何一個一個地裁？

經濟衰退的影響，往往出人意料地深遠。一家又一家公司接著破產。您會意識到，經濟只是一座紙牌屋，最輕微的風也能將它吹翻。裁員是大多數公司必選的止血方案，透過減少營運成本來節省現金。大規模裁員越來越多，令人們陷入巨大的痛苦和深層的焦慮，最終逼得政府不得不干預。政府干預後，各種紓困金和現金從四面八方奔湧入場。諷刺的是，即使解雇了

一半的員工，企業也從未停止過招聘。在經濟大衰退，以及新冠疫情所致的衰退期間，市場上均還有數百萬個職缺。因為在經濟衰退期間，買方控制了市場，公司可以精挑細選最佳求職者。這也有道理，畢竟供大於求嘛。數百萬人退出了就業市場，因為就業市場處於休眠狀態。紓困金幫助失業者度過經濟衰退期（希望如此），而在職者則緊緊抓住自己的工作不放，仿佛生命離不開工作一樣。這樣，人們就能夠在一段時間內（通常為一兩年）保持動態平衡。然後，在這條漫長隧道的盡頭出現了亮光。

人們開始活躍起來，從各個方面慢慢擺脫疫情帶來的經濟、公共衛生和社會束縛。我在 2021 年上半年走的路，就已超過了 2020 年全年；至於就業市場的當下狀況也比 7 月盛夏裡加州死亡谷的仙人掌還來得更熱。在美國，2021 年 3 月至 7 月期間，市場上增加了超過 329 萬個職缺，失業率降至 5.4%。[1] 然而，還需要有 760 萬員工進入私人企業工作，就業率才能達到 2020 年 2 月的水平。[2] 人們說，經濟大衰退是經濟大蕭條以來最嚴重的經濟危機。但事實上，比起新冠疫情導致的蕭條與衰退，大衰退只不過是小事一樁。

然而，反彈也更為明顯。2021 年 4 月，市場上有 930 萬個職缺。[3] 2020 年 4 月，有近 500 萬個職缺。[4] 而大衰退期間的反彈情況是：到 2012 年 1 月，市場上有 350 萬個職缺。根據美國勞工統計局的數據，在 2009 年 11 月，市場上只有 240 萬個職缺，降至最低點。[5] 美國的現狀（截至 2021 年 6 月），讓我想起了大衰退最黑暗時期過後的情況。因此，求職者，無論是目前在職還是待業的人員，可以考慮利用經濟衰退的有機週期。

大衰退之後，有《多德 - 弗蘭克法案》來力挽狂瀾；新冠疫情所致衰退之後，有疫苗來扭轉乾坤。2010 年，《多德 - 弗蘭克法案》出爐後，在市場上憑空湧現大量有關法規遵循和防制洗錢的新職缺。2021 年，新冠疫苗接種讓人們得以走出家門，重啟經濟。除了創造的數百萬個新職缺外，公司企業紛紛宣佈，計劃當下和未來將雇用數十萬員工。[6] 與過去一樣，這次經濟衰退過後的就業市場是賣方市場。這次求職者占上風，因為他們會收到多個工作邀請並可加以挑選。

還有一些其他因素也加劇了當下的招聘熱潮，尤其是在法規遵循、防制洗錢和監管領域。第一個因素是金融科技的復興。去年，銀行和金融服務被迫走向數位化。大多數人都在家裡辦理銀行業務和投資。替代性匯款體系、加密貨幣錢包和交易所以及機器人顧問全面增加員工。防制洗錢和法規遵循團隊當然也要壯大。第二個因素則更能顯現出疫情所致衰退的一個細微差別。與大蕭條不同，這次衰退不是經濟基本缺陷導致的結果。由於員工必須迅速適應新的生活方式和工作方式，以致專案被擱置。而這些專案現在開始重啟，需要立即招聘額外人員。最後一個因素是政府。美國政府現由民主黨執政，通常表示監管和強制執行會增加。綜合這些因素後，自然就有了招聘熱潮。今後 12 - 18 個月會非常有意思，因為現在有很多的職位空缺，卻沒有足夠的人來填補，而這種狀況會持續一段時間。所有行業皆是如此，防制洗錢和法規遵循領域也不例外。

至理名言

許多人在防疫期間可謂收穫豐碩。他們減肥成功，健康達到最佳狀態，發現了新的愛好，事業蒸蒸日上，或是統統達成。另一些人的狀況則不太理想。他們失去了工作、家園、健康、家人和親人。2020 年將因新冠疫情記入史冊，新冠疫情也迅速地改變了人們的生活。現在，人們開始逐步恢復疫情前的日子。生活中那些我們認為理所當然卻頓時失去的小確幸：隨意走訪親友，去吃速食店，在當地酒吧喝杯啤酒。但願我們不再把這些事視為理所當然。

就業市場正在恢復原狀，那就好好把握機會吧。作為求職者，如何才能善加利用經濟衰退結束的時機？具體來說，如何把握疫情衰退結束的時機？

1. **現在就開始找：**防制洗錢和法規遵循領域的專案和全職工作只會有增無減。但並非您想工作就一定能找到工作。您無法想像，我面試過多少頭撞南牆的人，只因為他們得不到預期的面試和工作機會數量。最終他們失去動力，沮喪地退出了就業市場。那些能堅持下去並尋找正確職位的人，卻遇到截然不同的問題：收到了太多工作機會，卻不知道該選哪一個。

2. **多思考能否提升技能，而非只看高薪：**從開始為《*今日 ACAMS*》撰稿以來，我一直秉持這一理念。掌握更多技能等於更高的薪酬；或者至少可以說，更多技能等於更多選擇。技術和人工智慧日益成為傳統銀行業防制洗錢和法規遵循制度體系的重要部分，金融科技和監管科技公司都希望招到精通技術的法規遵循專業人士。利用這段時間和機會找一份能提供更多可能性的工作，學習執行法規遵循制度的新方法，以及管理有效法規遵循部門的新方式。
3. **給自己一個機會，不要指望所有工作都能 100% 遠距工作：**即使沒有明說可以 100% 遠距工作，也不要馬上拒絕潛在工作機會。混合式工作及遠距工作已成為人們生活的一部分，但不要以為所有職務都能選擇 100% 遠距工作。在某種程度上，人們最終還是會回到辦公室。早在 2020 年 3 月，人們突然被迫轉向遠距工作。這並不是公司的順勢轉型；高階主管仍希望員工回到辦公室。
4. **拓展人際網路：**大衰退期間，人們有很多機會：午餐、會議、咖啡、雞尾酒等，能夠輕鬆拓展自己的人際網路。在新冠疫情所致的社交距離限制結束之前，人們只能透過 Zoom、Microsoft Teams 和 Google Hangouts 會議的方式互動。猜猜結果如何？這兩者並無區別。聯繫以往的同事和老闆，聯絡 LinkedIn 上新的和潛在的連絡人，參加網路會議。最後，一切回歸正軌時，不妨考慮參加地方分會主辦的 ACAMS 會議和活動。
5. **職涯道路並非一成不變：**經濟衰退之後的時期，是考慮換工作、改行、換居住地的最佳時機之一。在賣方市場下，求職者不僅可以掌握正規的求職程序，還能夠兼顧自己的目標與價值。如果法規遵循和防制洗錢工作讓您感覺不錯，但直覺（甚至可能是內心）告訴您，人生已到了分岔路口，該怎麼辦？在炙手可熱的就業市場，公司迫切需要人才。好好利用公司求賢若渴的心理！公司樂於透過具有創造力的方式招募人才。2021 年和 2022 年，職缺數量會多於符合條件的求職者數量，是人們走出舒適區的絕佳時期。
6. **好好利用招聘專家（免費）：**我不是在給自己打廣告。機構招聘人員是免費的資訊來源，不妨透過他們瞭解就業市場狀況、共同行業、用人趨勢、熱門技能組合需求，當然還有職缺需求。無論您是主動尋求建議，還是被動瞭解情況，這些值得信賴的專業顧問都可為您提供參考資訊。不妨將機構招聘人員視為自己不斷壯大的工作人際網路中的一員。

到 2021 年底，可能會有數十萬人重新進入就業市場。找工作的人群中，有很大一部分是之前因需照顧在家上學的孩子而退出勞動市場，或是因為之前從州和聯邦政府獲得的補貼比工資高。疫情將告結束，孩子們將重返學校，聯邦和州政府也會停發補貼。於是，經濟將重新變得熾熱，失業率將降至疫情前的水平。諷刺的是，由於勞動力短缺，很多全職工作暫停招人。公司一邊聘請約聘人員和顧問展開專案，一邊等待新的求職者湧入。在已開放的數百萬個工作職缺以外，還會新增成千上萬個工作。賣方市場短期內不會結束。

結語

當下正是求職者找工作的最佳時機。建議保持靈活彈性的心態，持續充電學習，擴大人際網路，利用賣方市場優勢，掌控自己的未來，做到這些，就能夠找到最佳工作機會，滿足自己的需求。誰知道呢？您也許能找到疫情前想都不敢想的理想工作。

Sanjeev Menon，《ACAMS 職業指南》專欄作家，Infinity Consulting Solutions, Inc. 法規遵循、法律和隱私事務資深經理，美國紐約州，smenon@infinity-cs.com

撰稿人及編輯意見：Karla Monterrosa-Yancey，CAMS，ACAMS《今日 ACAMS》雜誌總編輯，美國佛羅里達州，editor@acams.org

[1] “Civilian unemployment rate”（美國平民失業率），*美國勞工統計局*，2021 年 8 月 6 日，https://www.bls.gov/news.release/empsit.nr0.htm

[2] Scott Horsley 和 Andrea Hsu，“Hiring Picked Up Last Month, But The Economy Still Needs More Workers”（上月聘僱數回升，但經濟仍需要更多勞動力），*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

[3] Jeff Cox，“Job openings set record of 9.3 million as labor market booms”（隨著勞動力市場的繁榮，職位空缺創下紀錄，達 930 萬個），*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

[4] “Job openings, hires, and separations levels, seasonally adjusted”（職位空缺、聘用人數和離職數（經季節性調整）），*美國勞工統計局*，https://www.bls.gov/charts/job-openings-and-labor-turnover/opening-hire-seps-level.htm

[5] “Job Openings and Labor Turnover Survey News Release”（職位空缺和勞動力流動調查新聞稿），*美國勞工統計局*，2012 年 3 月 13 日，https://www.bls.gov/news.release/archives/jolts_03132012.htm

[6] “Amazon to hire 100,000 more workers in its latest job spree this year”（亞馬遜今年將再招 10 萬名員工），*CNBC*，2020 年 9 月 14 日，https://www.cnbc.com/2020/09/14/amazon-to-hire-100000-more-workers-in-its-latest-job-spree-this-year.html；Jessica DiNapoli，“PwC to Create 100,000 New Jobs to Help Clients Grappling with ESG Reporting”（PwC 將創造 10 萬個新工作崗位，幫助客戶應對 ESG 報告需求），*Insurance Journal*，2021 年 6 月 16 日，https://www.insurancejournal.com/news/international/2021/06/16/618744.htm

有效運用事件觸發審查的方法

事件觸發審查 (ETR) 或事件驅動審查，是持續監督或持續審查防範金融犯罪 (AFC) 控制措施的一部分。與週期性的定期審查不同，事件觸發審查具有臨時性的特點。此外，事件觸發審查與防制洗錢 (AML) 調查不同，前者通常由業務部門而非法規遵循部門實施。

本文將探討如何有效運用事件觸發審查，加強金融機構 (FI) 的客戶風險管理。

監管期望

監管機關的期望非常明確。在事件觸發審查期間，金融機構必須更新客戶資訊，查核是否需要審查客戶的風險狀況。例如：

> 「建立業務關係後，金融機構必須透過定期審查或事件觸發審查，維持對客戶現狀的正確認知。如果評估認為存在較大風險，則會視情況提高與客戶溝通的頻率和強度。」[1]

事件觸發審查是定期審查的補充，以確保客戶資料維持最新狀態。然而，一些金融機構完全依賴事件觸發審查，將其作為「風險為本方法」的一部分，用於更新客戶盡職調查和風險狀況。但事件觸發審查在這方面的效果似乎並不明顯。例如，在荷蘭銀行近期的刑事調查事實陳述中，荷蘭檢察官[2]提到銀行在以下方面未取得成效：

- 在私人銀行業務中，很少執行事件觸發審查，亦即未能持續監督私人銀行業務關係。
- 如下例所示，銀行系統和程序本應產生資訊以啟動事件觸發審查，但卻未發揮正常作用：
  - 在 2018 年 9 月之前，銀行針對負面媒體報導的篩查流程未自動化，而是採用人工方式。此外，在處理篩查配對及重新評估受影響客戶資料方面，存在積壓問題。2019 年，稽核師發現客戶篩查流程「差強人意，需要改進」。
  - 交易監控 (TM) 系統因其使用的風險分類與設定方式，導致錯失若干信號。另外，至少在 2019 年之前，所產生的交易監控警報在處理上都存在積壓問題。因此，可能導致事件觸發審查的警報未能及時處理。

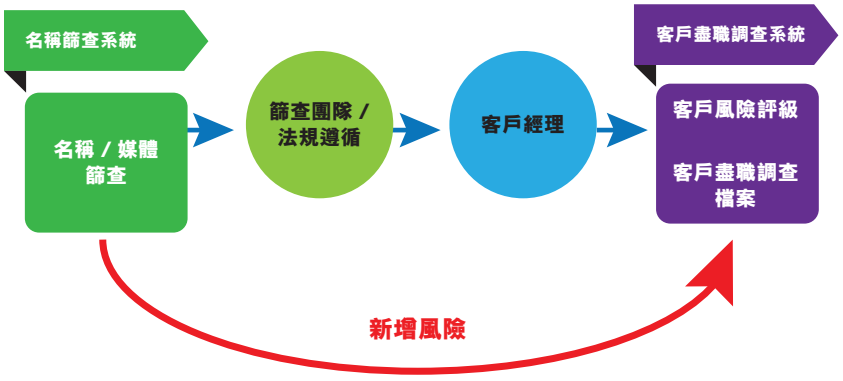
新風險和增量風險的評估

客戶開戶後，後端名稱或媒體報導篩查系統會定期根據供應商資料庫和內部黑名單，篩查金融機構的客戶資料庫，發現新風險或增量風險。此類風險包括新的政治公眾人物(PEP)、重大負面新聞，或者針對客戶或其關聯方的潛在制裁關係。對大多數組織機構而言，這些風險的識別與升級，似乎是標準的事件觸發審查工作（參見圖1）。

但必須明確定義升級協議和客戶風險評估準則。識別出新風險或增量風險時，必須在金融機構的客戶盡職調查系統中迅速標記新風險，同時進行評估並申請特准以留住目標客戶。

除篩查符合項目（或篩選命中）的審查工作存在積壓問題之外，真正的風險在於：業務部門及法規遵循部門探討新風險或增量風險時，可能不會將客戶標記為高風險。例如，客戶是政治公眾人物嗎？負面新聞嚴重嗎？制裁關係是否相當遙遠？另一種風險是，由於仍在徵求高階管理層的核准，則未將客戶標記為高風險，以期保留客戶關係。然而，只要未在金融機構客戶盡職調查系統中標記客戶，客戶就不會受到增強監控。金融機構客戶盡職調查系統的風險指標將根據風險定義門檻，匯入交易監控系統以便監控，因此規則應該是先標記、後決定。

圖1：新風險和增量風險的評估



交易監控循環

交易監控期間，為回應來自交易監控團隊的資訊請求(RFI)，客戶可能會提供資訊以消除對警示交易的疑慮。例如，客戶的交易對象可能是其新雇主或新供應商，也可能是客戶的其他私人投資公司或親屬。客戶解釋警示交易目的時，也可能揭露新的財富或資金來源。在金融機構的客戶盡職調查檔案中找不到此新資訊，因而提出資訊請求。然而，在金融機構交易監控案例管理系統中，此類資訊有多常出現在已關閉的警報稽核日誌中？

有效的循環機制，能夠觸發從交易監控到客戶關係經理的事件觸發審查。收到事件觸發審查要求後，客戶關係經理應進行審查，並將附加資訊納入客戶的客戶盡職調查檔案中。客戶關係經理還應評估是否需要重新分析客戶風險等級，是否需要修正客戶盡職調查檔案中聲明的帳戶預期用途和預期帳戶活動，這些均為事件觸發審查的一部分。借助金融機構盡職調查系統中修正後的客戶盡職調查檔案，交易監控團隊能夠快速評估同一客戶下一次交易監控警報的風險關聯性（參見圖2）。

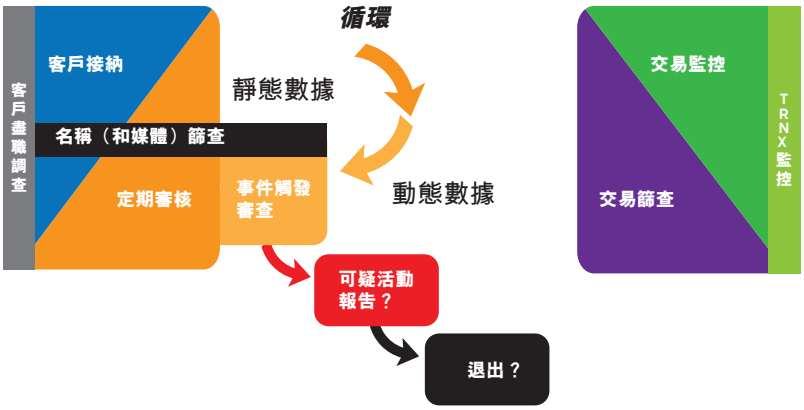
由於客戶回應資訊請求時可能揭露新資訊，以解釋潛在的交易篩查符合項目（或篩查命中），因此應制定循環機制，將資訊從篩查團隊傳回給客戶關係經理，啟動事件觸發審查程序。由於交易篩查符合項目通常牽涉客戶或其交易對象的潛在制裁關係，因此需將客戶對資訊請求的回應納入客戶的客戶盡職調查檔案。新資訊亦應構成客戶制裁盡職調查的一部分，尤其當新資訊可能將客戶或其交易對象的潛在符合項目被當成錯配。

觸發財富來源和資金來源的複審程序

對於私人銀行客戶和較高等級的零售客戶，在客戶接納過程中必須證實或驗證財富來源(SOW)和初始資金來源。此規定是讓銀行評估客戶總財富（即淨值）和資金來源(SOF)的合法性。完成客戶接納和定期審查後，客戶關係經理通常會要求對客戶聲明的財富來源或資金來源進行更改（如有）。但若傳入交易的規模（單獨或合計）超過客戶聲明的淨值，銀行是否有機制會啟動事件觸發審查？或者，若資產管理規模(AUM)超過客戶淨值，是否有機制啟動事件觸發審查？交易規模和資產管理規模增加，表明銀行可能不清楚客戶的財富總額或資金來源。

銀行應設立季度或半年儀表板，若匯入大額款項或客戶資產管理規模大幅增加，該儀表板能夠自動提醒客戶關係經理。

圖 2：循環機制



當客戶成為大客戶或重要關係（即資產管理規模等於或超過既定門檻）時，儀表板亦能給予提示。儀表板是交易監控及其偵測情境套件的附加控管工具。

作為事件觸發審查的一部分，客戶關係經理應審查客戶聲明的淨值是否超額；若超額，應向客戶詢問其新的財富來源和資金來源。此外，當客戶成為「大客戶」或「重要關係」時，事件觸發審查基本上就是對客戶財富來源和資金來源進行重新審查，以及重新評估新的或增加的客戶風險（如有）。新的財富來源和資金來源需要記錄並驗證。若客戶風險有所提高，防範金融犯罪政策應制定特准程序，以保留客戶關係。儀表板如圖 3 所示。

圖 3：淨值審查觸發器儀表板

客戶名稱				
帳號				
聲明的淨值（截至年 / 月 / 日）		$X		
	YYYY 年一季度	**YYYY 年二季度**	**YYYY 年三季度**	**YYYY 年四季度**
交易規模 ($,000)	500	50	2,000	
資產管理規模（增量百分比）	3	無變化	5	
資產管理規模（大客戶）				是

註：防範金融犯罪政策根據聲明的淨值，定義大額交易規模和資產管理規模的顯著增量。該政策亦根據資產管理規模定義組織的大客戶。

整合最佳作法，提升事件觸發審查效果

- 金融機構的防範金融犯罪政策應闡明什麼是事件觸發審查，審查客戶盡職調查檔案的觸發事件或動因，以及重新評估客戶風險的時機。
- 闡明事件觸發審查的職責與責任，包括升級協議。
- 設計系統流程，將觸發事件（和資訊）自動傳給客戶關係經理，以實施事件觸發審查工作。
- 確保具備足夠的資源，以便及時審查並處置警報和配對項目，進而及時實施事件觸發審查。
- 追蹤事件觸發審查工作，直至完成為止，其中包括：檢查是否已修正客戶風險評級，是否已更新金融機構盡職調查系統中的客戶盡職調查檔案（如適用）。

結語

有效的事件觸發審查程序，是有效「風險為本防範金融犯罪制度」中不可或缺的部分。因此，金融機構應設計良好的事件觸發審查流程並嚴格落實法規遵循。完成事件觸發審查後，及時更新客戶的客戶盡職調查檔案和風險檔案，有助於加強防範金融犯罪風險管理工作。

Rosalind Lazar，CAMS，
ACAMS 亞太地區防制洗錢法規遵循總監，
rlazar@acams.org

[1] “Guidance For Effective AML/CFT Transaction Monitoring Controls”（有效防制洗錢 / 打擊資助恐怖主義活動交易監督措施指南），*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

[2] “Statement of Facts and Conclusions of the Netherlands Public Prosecution Service”（荷蘭公共檢控服務部事實陳述與結論），*國家嚴重詐欺、環境犯罪與資產充公辦公室 (Functioneel Parket) 和國家辦公室 (Landelijk Parket)*，https://assets.ctfassets.net/1u811bvgvthc/4e UXF7eCnLthKp95RNnMnz/645730a7cd044da33ef4 ad1545470f12/Statement_of_Facts_-_ABN_AMRO_Guardian.pdf

ACAMS GREATER PHOENIX Chapter

大鳳凰城分會：
調整、發展與適應！

今年 6 月，ACAMS 大鳳凰城分會以「加密貨幣時代的資恐行動：監管與執法框架」為題舉辦了一場網路研討會。此次研討會大獲成功，超過 500 名註冊會員參加。研討會伊始，美國國稅局網路犯罪小組探員 Chris Janczewski 以三個真實的犯罪案例開場，說明恐怖組織如何「調整、發展與適應」其融資方式，尤其是使用加密貨幣。Janczewski 探員展示了美國執法機關如何成功查獲與哈馬斯、蓋達組織、伊斯蘭國有關的組織網站和貨幣資產！

一個組織利用網站進行比特幣籌資活動，為「巴勒斯坦抵抗運動」尋求捐款；另一組織則利用其 Telegram 管道尋求捐款以資助恐怖攻擊，支持「敘利亞聖戰者」。一名服務於伊斯蘭國的人員建立了一個網站，聲稱有 N95 和其他個人防護用品出售，可幫助人們應對危機。受害者以信用卡支付，購買不存在的商品，結果導致信用卡被盜刷。總計 10 萬美元的犯罪所得隨後通過比特幣洗白，此人最終遭逮捕！值得慶幸的是，美國政府經行動查獲的加密貨幣隨著時間而升值——這當然是錦上添花。

接著發言的是來自 TRM Labs 的 Ari Redbord。Redbord 介紹了 TRM 的使命，即「防範加密貨幣詐騙與金融犯罪，為數十億人建立更安全的金融體系。」他強調，加密貨幣有望出現爆炸性成長，犯罪分子很可能利用新技術來規避檢測——如跳鏈 (chain-hopping)、隱私技術、程式化洗錢等技術。他的演講重點探討了加密貨幣當前的監管環境：即使只有不到 2% 的比特幣鏈上交易涉及非法實體，但監管重點仍放在加密貨幣的非法利用，極少關注加密貨幣的合法使用。

Redbord 指出，美國財政部（包括金融犯罪稽查局）依然重點關注加密貨幣的非法使用，目前對虛擬資產服務提供商的監管要求，便可證明這一點——許可證、「了解您的客戶」、增強盡職調查、交易監控、遵循轉帳規則等。他指出，這些要求與金融機構的要求非常相似，是一大考驗！金融機構作為中介機構，負責收集金融情報，並編列成有組織結構的報告送交執法機關。然而，加密貨幣具有去中心化的特點，其結構與典型組織不同。犯罪分子利用跳鏈、隱私技術等讓情報收集工作難上加難。監管業要如何調整、發展與適應，還有待觀察。

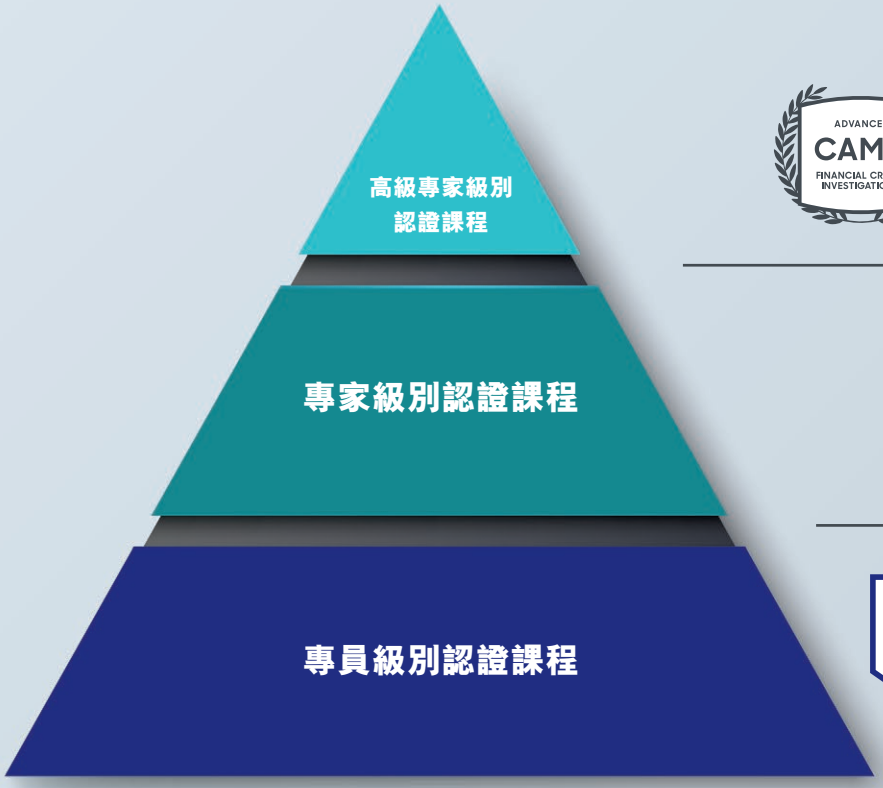
顯然，互動環節是研討會的亮點！問答環節持續了近一個小時，仍有許多問題來不及回答。在後續討論中，與會者就廣泛議題展開了探討，如利用古董資助恐怖主義、美國國內恐怖主義案件的細微差別、利用更短的交易時間搶佔加密貨幣新市場等，還舉辦了線上腦力激盪會議，討論如何降低整個行業的風險。Janczewski 探員提及完全瓦解恐怖組織與破壞恐怖組織融資 / 運作等看似影響不大的作為，兩者之間的區別，令筆者印象最為深刻。參加這場網路研討會，實在受益匪淺！

Caryn Langolf，
註冊監管合規經理、CAMS、
ACAMS 大鳳凰城分會聯合通訊主管，
carynlangolf@gmail.com

ACAMS 公認反洗錢師協會 Certifications

通過 ACAMS 認證課程，提升員工在防範金融犯罪方面的專業知識和技能。

www.acams.org



ADVANCED CAMS FINANCIAL CRIMES INVESTIGATIONS

ADVANCED CAMS AUDIT

ADVANCED CAMS RISK MANAGEMENT

黃金標竿

CAMS CERTIFIED ANTI-MONEY LAUNDERING SPECIALIST

CGSS CERTIFIED GLOBAL SANCTIONS SPECIALIST

CERTIFIED CKYCA KNOW YOUR CUSTOMER ASSOCIATE

CERTIFIED CTMA TRANSACTION MONITORING ASSOCIATE

CERTIFIED CAFCA AML FINTECH COMPLIANCE ASSOCIATE

Winnie Yuen：

以有效協作為目標的傳播

本期《今日 ACAMS》中，我們採訪了全球行銷營運經理 Winnie Yuen，瞭解她多年以來累積的行銷經驗及行銷活動成功的關鍵。Yuen 從事行銷傳播工作已有 10 多年。加入 ACAMS 前，她在遊戲和生活時尚行業工作多年，擁有精湛專業的行銷技能。本月，Yuen 將迎來在 ACAMS 工作的五周年紀念日。她是 ACAMS 亞太地區行銷部聘請的第一位員工，見證了 ACAMS 香港辦事處的發展壯大，迎來越來越多充滿活力的同事。

過去五年，從產品發佈到現場會議，從促銷郵件到活動贈品，Yuen 監督亞太地區的所有行銷推廣活動。2019 年，她榮獲 Adtalem Global Education 頒發的 TEACH 大獎，表揚她在 ACAMS 會員和業務合作夥伴服務的傑出貢獻。最近，Yuen 晉升全球行銷營運經理，作為各行銷團隊不同部門之間的溝通橋樑，並參與多項跨部門專案。

***《今日 ACAMS》*：今年，您在 ACAMS 任職已滿五年，祝賀您！想請教一下，您如何將在遊戲和生活時尚行業獲得的行銷經驗，融入 ACAMS 的行銷工作？**

Winnie Yuen：非常感謝！真難以相信，我在 ACAMS 已經工作五年了。遊戲、生活時尚與金融法規遵循行業看起來截然不同，但基本行銷原則並無二致。先前取得的工作經驗讓我更有自信地應對各種行銷挑戰。分享一個有趣的故事，我在美國辦公室見到 ACAMS 全球營銷總監 Fernando Beozzo Salomao 本人。交談過程中，我們發現他認識我以前的一個老闆，因為他們曾在同一家公司、同一部門工作。世界真小啊！

***《今日 ACAMS》*：您是亞太地區行銷部門的第一位員工，也是當時唯一的員工。從那時至今，該部門有何發展？**

Winnie Yuen：我 2016 年加入 ACAMS 時，是亞太地區唯一的行銷人員，負責亞太地區所有的行銷推廣工作。當時，我們一年內舉辦了 10 場現場研討會和 1 場現場國際會議；在亞太地區推出了四種語言的公認反洗錢師認證課程，同時還從事其他行銷專案——可以想像，對於只有一個人的團隊來說，有多少工作要做。幸運的是，我的辛勤工作（和繁重的工作量）得到了管理層的肯定，ACAMS 開始擴張亞太區行銷部門，2018 年，部門員工人數增加到 4 名。現在，我們有三名同事常駐香港，一名同事常駐北京。我們擁有不同的背景與經歷，我覺得這樣的混合搭配非常好。

***《今日 ACAMS》*：行銷活動取得成功的關鍵是什麼？**

Winnie Yuen：在我看來，行銷的核心就是在消費者與產品 / 服務之間搭建橋樑。行銷活動的成功關鍵就是應瞭解潛在消費者需要什麼，他們的痛點是什麼。這非常重要。ACAMS 不是零售公司，因此非常依賴資料分析、調查回饋，以及非常倚重與銷售代表的溝通，因為他們直接接觸客戶。此外還應隨時瞭解行業 / 市場新聞和動向。

***《今日 ACAMS》*：作為全球行銷營運經理，您對跨部門、跨地區的協作有什麼建議？**

Winnie Yuen：重視溝通！無溝通，不成事。這一點放之四海而皆準，對 ACAMS 尤為重要，因為 ACAMS 是一支龐大的全球團隊。每個人都有自己的優勢、經驗和立場，因此，溝通對於實現共同目標至關重要。

***《今日 ACAMS》*：迄今為止，您印象最深刻的 ACAMS 行銷專案是什麼？**

Winnie Yuen：我印象最深刻的有兩個專案，一個是我負責的第一場國際會議，另一個是推出 ACAMS 微信與 LINE 社交媒體管道。2017 年，我是亞太地區唯一的行銷人員，有大量的會前準備工作要做；而微信和 LINE 是華語用戶用得最多的社交媒體管道。那是我首次處理 app 上架活動、發佈規劃工作，因此整個流程中有很多地方需要學習。

***《今日 ACAMS》*：您在空餘時間喜歡做些什麼？**

Winnie Yuen：閒暇的時候，我喜歡健行、跑步、看電視。最近在學習家居維修和泰語。我始終孜孜不倦，不斷探索新的愛好——沒有什麼固定的標準，只要有趣、實用就行！

採訪者：Stephanie Trejos，ACAMS，CAMS、編輯，美國佛羅里達州，strejos@acams.org

進階認證課程
畢業生

亞美尼亞
Emil Abrahamyan, CAMS-RM

巴哈馬
Sinead Bethel, CAMS-RM

開曼群島
Christopher Green, CAMS-RM

德國
Manuela Drachenberg, CAMS-RM

香港
Kit Wah Flora Liu, CAMS-RM
Siu Long Wong, CAMS-RM

日本
Yasutomo Haruki, CAMS-RM

拉脫維亞
Khaled Almustafa, CAMS-RM
Kalvis Bambals, CAMS-RM

黎巴嫩
Katia Marrouche, CAMS-RM

澳門
Ching Chi Percy Wong, CAMS-RM

荷蘭
Henri Korkalainen, CAMS-RM
Luciano Riccioli, CAMS-RM
Marcin Wasilewski, CAMS-RM

挪威
Adis Crnalic, CAMS-RM

卡達
Faheem Razzaq, CAMS-RM

沙烏地阿拉伯
Malcolm Sandesh Lewis, CAMS-RM

韓國
Yoon Sang Seong, CAMS-RM

阿拉伯聯合大公國
Kartik Sharma, CAMS-RM

英國
Yoe Strous, CAMS-RM

美國
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
公認反洗錢師協會

ACAMS 網絡研討會高級訂閱帳號

您的網絡研討會通行證

新版 ACAMS 網絡研討會高級訂閱服務是一個全年通行證，您可瀏覽 ACAMS 即時和隨選網絡研討會資料庫，次數不限。

9+ 平均**每月舉辦**
場全新即時網絡研討會

40+ 每年**探討**
個防範金融犯罪 (AFC) 主題

800+ ACAMS 資料庫收錄
小時防範金融犯罪培訓

如需詳細資訊並訂閱，請至

acams.org/en/premium-webinar-subscription

此訂閱服務包括ACAMS 網絡研討會，企業會員亦可使用

國際公認反洗錢師 (CAMS) 畢業生：

5 月 - 7 月

阿富汗

Atal Bahand
Izatullah Hafizi
Aimal Mangal

亞美尼亞

Gevorg Khachatryan

阿魯巴

Kelvin Osmond Halley
André Carmelo Kelly
Sandy Odor
Albertico Gregorio Willems

澳洲

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

奧地利

Amaury Crucy

阿塞拜疆

Tural Imamaliyev

巴哈馬

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

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

巴貝多

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

比利時

Eduard Hovsepyan
Roger Kaiser
Anne-Dorine Ligthart
Thomas Mareel

貝里斯

Salvador M. Awe
Lissa A. Lord

百慕達群島

Claire Loxley
Pui Shan Ma

波札那

Malebogo Hirschfeld
Masego Matjola
Gorata Moipolai

巴西

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

汶萊

Mary Chiew Horng Ong

保加利亞

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 Azubuike
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 Mechkour
Mohsin S. Mukaddam
Aarti Naidu
Karin Lourdina Nanayakkara
Khurram Nawaz
Morounfoluwa Oduwole
Ademola Ogungbemile
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

開曼群島

Edgar Ogville Bennett
Deepal Bhandarkar
Ashley Borde
Kayla Bush
Elizabeth Byrne
Melissa Nastasia Durrantt
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

中國

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
Yunyun 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
Guoju 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 冯嘉铙
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 高光键
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
Zhoulu 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
Xiujing Guo 郭绣晶
Yuli Guo 郭宇力
Yuzhen Guo 郭宇蓁
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 李从瑢
Fang Li 李方
Guanzhong 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 李锶溱
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
Xiyan 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 李鸢
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 刘川绮
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 刘旎
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 刘烨暄
Yijie Liu 刘奕颉
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
Ruilin 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 佘宇英
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
Liwen 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 苏小蕤
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 孙泠珂
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 田雨鑫
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 王笳铭
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 魏鹊巍
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 吴彬绉
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
Xiaoou 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 杨赟颖
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 尹艳
Zhen Yin 尹桢
Zhidi You 尤智迪
Changrong Yu 余长蓉
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 岳垚
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 查洧阳
Fangyuan Zhai 翟方源
Xu Zhai 翟栩
Boyan Zhang 张渤岩
Chunyue Zhang 张春月
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
Yuzhong 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 郑钰浈
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

哥倫比亞

Jose Eduardo Rojas
Kimberly Suarez-Contreras

象牙海岸

Cyriaque Towanoun Hounsa

克羅埃西亞

Anton Kohut
Maja Kovač

賽普勒斯

Marina Agathangelou
Kalia Charalampous
Theodoros Stavrou

捷克共和國

Marek Bocanek
Petra Capkova
Gabriela Kindlova

丹麥

Charlotte Rose Lowry

埃及

Yousri Mounir L. Showeitar

愛沙尼亞

Evelin Ruus

芬蘭

Lisa-Maria Altenberger
Karola Koivula
Wilhelm Lindstrom

法國

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

德國

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

迦納

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

希臘

Zinon Chatziantonoglou

圭亞那

Chandan Kumar
Melissa Tashana Smith
Faith June Taylor

洪都拉斯

Gerardo I. Midence Zúniga

香港

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 Miu 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 Goswani
Nitin Kumar Gupta
Poorani Ilango
Anurag Jain
Smriti Jajodia
Jiten Shivram Joshi

ACAMS™
公認反洗錢師協會

邁出第一步

CERTIFIED CKYCA
KNOW YOUR CUSTOMER ASSOCIATE

CERTIFIED CTMA
TRANSACTION MONITORING ASSOCIATE

CERTIFIED CAFCA
AML FINTECH COMPLIANCE ASSOCIATE

ACAMS 最新社群集結大量通過認證的專業人士，如果您是剛進入瞭解您的客戶 / 客戶盡職調查、交易監控以及金融科技企業防制洗錢法規遵循領域的人員，熱烈歡迎您的加入！

趕快瀏覽 **www.acams.org**
展開您的旅程

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

印尼

Febrina Aruan
Anthoneus Ismoyo Djati
Candra Putra

愛爾蘭

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

牙買加

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

哈薩克

Gaukhar Akina

肯亞

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

拉脫維亞

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

盧森堡

Laurent Dao
Giedrius Drulia
Feng Du
Luis Esparza
Cristina García Berenguer
Sybille Giriens Rakintsev
Galit Goldman-Malka
Yadie Li
Andrés Santamaría Alvarez
Maria Isabel Carolina Vago
Siwei Xiong
Xin Zhao

澳門

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

馬拉威

Tisunge Tiwonge Phiri

馬來西亞

Mogan Chanderan
Guan Yu Ng
Nurhidayah Binti Abdul Razak
Poh Cheong Seow
Chin Leong Tsai

馬爾他

Margherita Alessandri

模里西斯

Gowree Roopnah-Dusoruth

墨西哥

Federico Cano Robert
Manuel Arturo Vazquez Torres

納米比亞

Menfret Melk

荷蘭

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
Kasım Emre Türk
W. R. S. van de Steeg
Piet-Hein van Zijl
Liudmila Vegter-Boroshko
Emily Verwaal
Marcin Wasilewski
Daehan Wi

紐西蘭

Kit Chiu
Louise Coad
Charis Danieli
Md Shafiul Azim Faruqui
Kannitha Kaing
Christelle Launay
Lucas Joseph Mansell
Warden Tamuka Nyawo
Owen Bruce Turner

奈及利亞

Taiwo Adeniyi
Olufunke Ajani
Bright Chinweotuto Anyanwu
Ajibola Sunday Fakorede
Abisola Gbadebo
Adefunke Ibironke
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

巴拿馬

Helene Tison

巴拉圭

María Teresa González Fretes
Oscar Ramon R. Melgarejo

秘魯

Ingrid Del Solar
Armando Martin G. Vasquez

菲律賓

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

波蘭

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

卡達

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

俄羅斯

Vladislav Anadikt

盧安達

Ubald Sesonga

沙烏地阿拉伯

Essam Abdullah M Al Nasayn
Abdulrahman K. Alruwaished
Ibrahem 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 Zimmel
Chen Hong
Yin Lin Jacqueline Houng
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
Jenalynn 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

斯洛維尼亞

Sebastijan Peterka
Masa Zalar

南非

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

韓國

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
Jiyoon 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

斯里蘭卡

Ramith Bandara Ranathunga
Janani Sriskandarajah

聖克里斯多福及尼維斯

Keishara C. Liburd
Mark Mangan

瑞典

Emil Bexenius
Carl-David Sukrit Lundström
Hanna Lüttschwager
Emil Richloow
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

台灣

Kuo Chieh Chao 趙國婕
Hsinyi Chen 陳心儀
Li-Tang Chen 陳立唐
Ying Chien Chen 陳穎蒨
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 謝甯伃
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 鄧宇玹
Pei-Chen Tsai 蔡吝真
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

千里達及托巴哥

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

土克斯及開科斯群島

Soreka Sharonda Brown

烏干達

Mugisha Habib
Kenneth Natukunda

烏克蘭

Marta Babyak
Ivan Paramonov

阿拉伯聯合大公國

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 Zoueineh
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 Nikesh 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

英國

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

美國

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

ACAMS
公認反洗錢師協會

制裁領域

為組織提供全面的解決方案，
促使其員工遵守複雜的制裁法規。

- 國際制裁合規師 (CGSS) 認證
- 線上培訓
- 大師班系列
- 月度制裁報告
- 思維領導力
- 聯誼活動

瀏覽以上內容，請進入
acams.org/sanctions

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 Grzyboski
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
Cylenthia Drinkard Jones
Amrita Vijay Joshi
Namita Karunakaran
Anna Elizabeth Kasparek
Asher Keam
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 Momberg, 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
Ndidi C. Obicheta
Lauren O'Brien
Henry Ododah
Sakine Oezcan
Jacqueline Ogden
Julien Ogden
Muyiwa 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 Shelbaya
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

葉門

Osama Omer Ali Mohammed
Hussein A. AlMehdhar

尚比亞

Sibeso Mutumweno

國際制裁合規師 (CGSS) 畢業生：

5 月 - 7 月

亞美尼亞

Zaruhi Badalyan

澳洲

Say Pheng (Sophia) Foo
Jun Li
Venkatesh Nathilvar
Qiang Sun

巴林

Imtiaz Ahmad
Rajnish Ranjan
Muhamad Nizam Bin Shaidon

孟加拉

Mohammad A. Al Mamun

比利時

Frederic Jadot
Geoffrey Max Lepage

加拿大

Jinhe Li

中國

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 江姈
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

丹麥

Jeffrey Nielsen

埃及
Noha Ashraf M. A. Megid

芬蘭
Mark Bossmann

法國
Alberic Botella
Julien Gallo

德國
Ruiya Fu
Antonio Stoyanov

希臘
Anna Damaskou

香港
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

拉脫維亞
Laura Kalnina

黎巴嫩
Rita Fares
Khaled Haidar
Myriam Khairallah

墨西哥
Tania Balanzario Meraz
Miriam Guillermo Blancas
Benjamin Serra Cruz

荷蘭
Inbal Djalovski
Ruofei Shen
Erdem Tascilar
Annemarie Verkerk

紐西蘭
Jatin Kumar Mistry
Rani Pillay
Minyu Zheng

奈及利亞
Babatunde Olaoluwa Macaulay

挪威
Eva Helena Deinoff
Eivind Parr Ohme

巴基斯坦
Nasir Mehmood

菲律賓
Frances Lynette Sayson

波蘭
Wenbin He

波多黎各
Luis Miguel G. Hernández
Natalia Rodriguez

卡達
Muhammad Shahid Farid
Neil Scully

俄羅斯
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

韓國
Dongyeop Hyun
Ping Ji
JaeKyung Kim
Jeongeun Park
Zongrui Yin

瑞士
Xavier Charles Didier Béard
Aliaksandra Hurynovich

台灣
Chih-Feng Chung 鍾至豐

土耳其
Melik Bagis Bilici
Bilal Ertogrul

阿拉伯聯合大公國
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

英國
Jane Alimonda
Julie Choudhury
Clare Anne Davies
Monica Handoo
Kevin Penter
Mark Sallis

美國
Julio Gabriel Borras
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

ACAMS™
公認反洗錢師協會

進階的 CAMS 資格認證

ADVANCED CAMS AUDIT

公認反洗錢稽核師 (CAMS-AUDIT) 進階資格認證是一項高級專業認證，專門為執行反洗錢稽核工作，以及獨立檢測防範金融犯罪控制措施的專業人士所設計。

瞭解更多
www.acams.org/cams-audit

ACAMS
公認反洗錢師協會

企業方案: 防範金融犯罪工作團隊所需的致勝工具。

ACAMS 企業方案是專門為從事防範金融犯罪工作的組織而提供的優質專業會員配套。

為什麼要選擇企業方案？

- 為您的團隊提供 ACAMS 個人會員的所有好處，且可以使用 moneylaundering.com 及網路研討會資料庫，次數不限
- 透過企業方案使用報告追蹤團隊的訓練情況，向監管機構說明法規遵循狀況
- 可以 ACAMS 訓練及活動的優惠價，制定最佳訓練預案

詳情如下:

www.acams.org/zh-hant/會籍/acams企業方案