NICE
ACTIMIZE

2021 年亞洲趨勢和展望：

對抗未來的金融犯罪

白皮書

Kapronasia

區域重大發現

新加坡

- 2020 年第一季因電子商務詐騙案增加，損失達 4130 萬新幣。
- 新加坡當局封鎖進行詐騙行銷的公司數量持續增加。
- 「無底洞 (Rabbit Hole)」式詐騙，是瞭解詐騙精心策畫過程的絕佳例子
- 對新加坡而言，隨著數位銀行執照發出，加上銀行預計於 2021 年中正式啟用，發展有效的數位犯罪對防範策略至關重要

澳洲

- 在 COVID-19 疫情爆發前，退休金 (Superannuation) 詐騙是一項日漸嚴重的問題
- 詐騙者假扮政府機構的情況增多
- 疫情期間線上賭博數量增加，須謹慎觀察
- 虛擬銀行正式啟用，合規疑慮加深
- 內線交易偵查與判刑數量雙雙攀升

台灣

- 自 2016 年爆發兆豐金弊案後，台灣近年來的反洗錢管理體制大幅改善，在亞太洗錢防制組織 (APG) 的排名也進步了
- 相較於許多其他國家，台灣在新冠病毒疫情控管成效良好，產業仍相對得以持續穩定運作，銀行及其客戶受到 COVID-19 相關詐騙的風險隨之降低
- 不過，2021 年有三家數位銀行即將開張，而且除了支付之外，領軍的科技公司對銀行業務毫無經驗

日本

- 線上金錢轉帳詐騙在 2019 年急遽上升
- 有超過 1,000 個假網站在疫情期間出現
- 日本數位轉型的進度，在金融服務方面進展相對緩慢，造成線上詐騙與其他金融犯罪的風險上升
- 遠端工作的挑戰

NICE · ACTIMIZE

目錄

執行概要

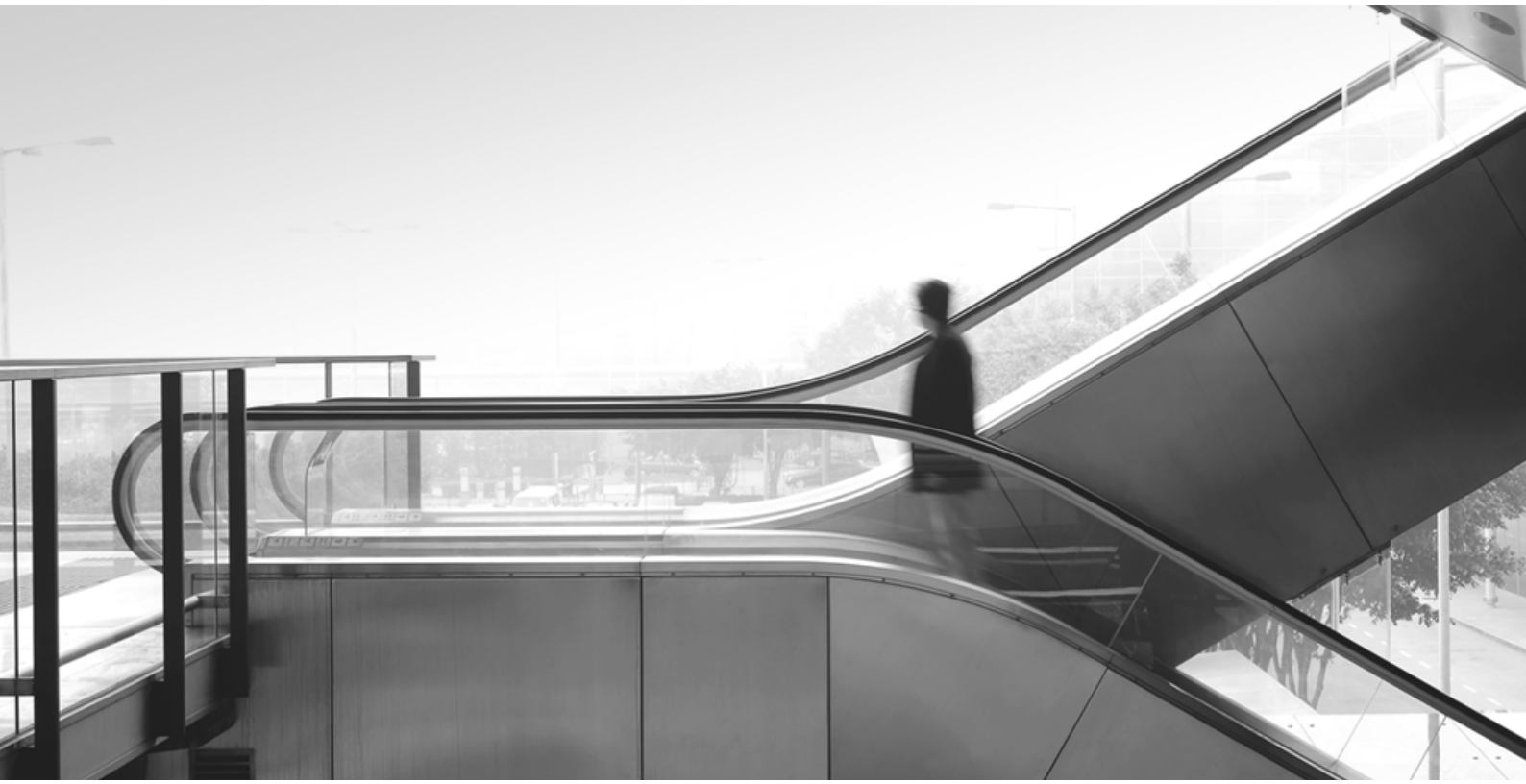
受新冠病毒疫情影響，由於個人及企業紛紛轉向線上服務，亞太金融機構數位化進度亦隨之加速。這項新的機會也帶來新的風險，金融罪犯跟著金流走向線上犯罪。在基於安全性與衛生考量，面對面接觸的情況減少之下，金融機構要如何防範假冒與洗錢罪犯，是前所未有的困難考驗。

在亞太地區，地區金融中心如新加坡特別容易成為目標。除此之外，澳洲、台灣、和日本等國仍與不斷增長的國內詐騙、洗錢、及部分內線交易案件奮戰。罪犯為保護非法資金流動的源頭，其中部分犯罪是採跨區域活動。銀行業由於傾向個別進行合規調整，致使無法有效共享資訊的特性，經常被跨國境金融犯罪加以利用。

近期金融犯罪執法網路 (FinCEN) 檔案外洩事件，顯示這種獨立做法在本質上的風險：金融機構可能無法看見金融犯罪風險的全貌。在馬來西亞一馬公司醜聞（1MDB）弊案中確實如此，並讓新加坡的銀行深陷其中。金融犯罪執法網路檔案也同時揭露澳洲與日本銀行的違規交易行為。

在風險潛伏的環境中，四大重要趨勢將決定亞洲能否成功對抗亞洲金融犯罪：資料管理、數位轉型、預測分析、及異常偵測日漸增加的重要性。在這四項趨勢中，科技都是不可或缺的一環，能強化金融機構保護客戶與自身的能力，遏止金融罪犯的持續侵擾。另外，人員因素也同等重要：金融機構的合規團隊內需要更有效的合作互助，乃至於各銀行、各金融機構與監管單位間的配合。

綜合以上考量後，亞洲金融產業應能順利從受疫情影響的逆境中恢復，隨著世界在未來幾年逐漸形成後疫情常態，變得更加穩健茁壯。



關鍵轉折時代的調適

2020 年，全世界面臨到許多世代以來最巨大的公共衛生和經濟挑戰。國際貨幣基金組織預測 2020 年全球經濟將縮減 4.9%，是自 1930 年代大蕭條以來最惡劣的經濟表現。經濟有可能在 2021 年復甦，但很大可能是不均衡的復甦。[1]

有個「新常態」已近乎確定，即生活將會受到週期性疫情引發的破壞，直到冠狀病毒得到有效遏制。該病毒不僅善變、難以捉摸，且會爆發，犯罪分子一定會試圖利用這些混亂局勢。在線上快速遷移的經濟，為罪犯提供了前所未有的目標對象。

現在正是金融機構最需要強大合規能力的時刻。不僅是由於上述的種種漏洞，也為了因應經濟變動期間在投資策略上的各種變化。投資人正在對資產進行重新分配，包括大筆資金轉移、清算投資組合、大幅增加現金持有量、對資產、房地產、與虛擬貨幣進行避險。「金融交易模式的重大變更可能會掩蓋犯罪活動，特別是當資產轉換成更不透明、更無法追蹤的形式時。」美國國會研究處表示。[2]

防制洗錢金融行動工作組織（FATF）認為對金融機構的威脅，將隨著疫情延續至 2021 年。「FATF 於 2020 年 10 月的聲明中表示，「失業率攀升、遠距交易的利用率提升、以及經濟振興計劃的加速實施，都是犯罪分子在未來幾個月可能利用的漏洞。由於經濟不穩定，經濟體中的現金流通量增加，加上邊境的關閉，都可能會影響洗錢活動。[3]

NICE · ACTIMIZE

金融業界有幾個特定的漏洞：

- 許多現行金融機構仰賴過時的資訊系統 (IT) 基礎架構，這些超過十年的系統很難升級，且設計上無法處理大筆線上交易。這通常會限制運作中的銀行無法徹底執行應符合規範，致使自身與其客戶暴露在金融犯罪的風險中，像是洗錢與詐騙。
- 數位銀行一般對客戶盡職調查流程非常熟稔，且擁有較為靈活具彈性的技術，但在面對來自投資人的快速成長壓力時，可能會為了積極增加客戶數量而犧牲金融犯罪防制與合規作為代價。只要出現一次重大安全漏洞，對數位銀行的信任與聲譽就可能付之一炬。

[1] 國際貨幣基金組織，世界經濟展望快訊，2020 年 6 月，“A Crisis Like No Other, An Uncertain Recovery,” https://www.imf.org/en/Publications/WEO/Issues/2020/06/24/WEOUpdateJune2020

[2] 國會研究處，COVID-19 與新興金融犯罪全球模式，https://fas.org/sgp/crs/misc/IN11496.pdf

[3] FATF 總裁聲明，在 COVID-19 疫情期間投資足夠資源至 AML/CFT 管理體制的重要性，https://www.fatf-gafi.org/publications/fatfgeneral/documents/covid-19-impact-oct-2020.html

善用科技強化金融犯罪防制

亞太地區的金融犯罪數量，正隨著銀行數位化與區域經濟同步成長中。新加坡、澳洲、台灣、與日本正努力和與日俱增的線上詐騙和洗錢案件對抗。新加坡與澳洲亦同時必須面對內線交易的問題。

然而，面對金融犯罪產生的風險，許多金融機構還沒有準備好進行控管，特別是和洗錢防制有關的部分。根據 FATF 估計，直到 2019 年底前，僅 25% 國家具備合適的洗錢防制 (AML) 監管機制。

在金融犯罪風險不斷增加的年代，亞洲金融服務產業務必及早調整適應。不論是傳統或數位銀行，都必須透過合宜的科技強化第一道與第二道防線。如此一來，才能在犯罪活動猖獗的網路上保護客戶資產與資料，同時降低成本並提高營運效率。

金融機構必須先獲得可最佳化資料情報的技術，才能取得這些成果。將來自各方面的第三方資料來源，包括國際制裁、PEP 進度、企業所有權、強制執行名單、負面新聞等資料，整合成單一可採取行動的情報，讓金融企業更有效地評估風險並進行調查。如此一來，在與外部頂級資料來源整合時，將能做出更有效的決策判斷。

金融業界使用人工智慧 (AI) 的例子越來越常見，以便從龐大的資料中收集重要的洞見觀察。其中一項人工智慧技術的重要類型「認知運算」，在作為合規工具時特別有幫助。認知運算系統能辨識自然語言和圖像、辨認並解讀重複模式，包括在可疑金融交易內的活動－即使資訊亂無章法。認知運算的一項重要優勢，就是能隨著經驗累積不斷改善，從錯誤中學習並隨時間提高效能。

透過認知運算，自然語言處理 (NLP) 在金融犯罪控制上有許多應用程式可使用。NLP 應用程式可用來掃描與收集文件、段落文字、網路、與暗網內的重要情報，並按關聯性與內容進行分類。這些功能讓 NLP 成為相當實用的工具，可進行比對姓名、交易篩選、貿易融資、分析、分類監管文件、並產生可疑活動報告 (SAR) 與分析。

內容分析是合規工具包內另一項實用的附加功能。內容分析可監控所有的客戶已知資訊，將 KYC 資料與交易資料進行比對，包括第三方資料。金融機構對客戶越理解，越容易確定何時會出現問題。

最後，透過整合金融犯罪中心的啟用，讓金融機構得以將所有分散的資訊整合成統一的偵測與調查策略，以強化監控風險並進行調查的能力。

「合適的職員、領導方式及科技，可確保大家在不犧牲品質與一致性的情況下，維持靈活應變能力。」NICE Actimize 反洗錢部門亞太區市場主管 Matthew Field 表示。「我們應定期對瞬息萬變的威脅指標進行風險評估，並藉此調整營運方式，確保能有效控管這些威脅，維持堅實的第一道犯罪防線。」

對抗亞洲金融犯罪

I. 新加坡

在東南亞金融中心遽增的線上犯罪案件

新加坡身為亞洲首要金融中心之一，多年來一直在努力對抗與之俱來的金融犯罪。隨著金融服務產業加速數位化的腳步，對該國帶來新的挑戰，且並未因疫情爆發隨之減緩。新加坡計畫在 2021 年中啟用四家數位銀行，其必須制定有效的策略，遏止金融犯罪出現在數位領域中。

「經過 COVID 後，新加坡表示網路犯罪已成長達 1,000%，由於大家都在上網，罪犯也將無可避免地跟著金流移到網路上。」以東南亞為基地的金融犯罪與法遵科技專家在對談中表示。

根據新加坡警方於 2020 年 1 月至 3 月的彙整資料顯示，新加坡因詐騙損失的年度累計金額達 4130 萬新幣，相較去年成長約 28%。其中以電子商務與假冒貸款詐騙最為普遍。罪犯有時亦透過電子郵件、簡訊或通訊應用程式發送假廣告，冒充星展銀行、新加坡郵政儲蓄銀行、大華銀行及聯昌銀行等銀行向受害者提供貸款，並成功詐得 160 萬新幣。[4] 在新加坡，持有執照的貸款方僅能透過官方網站、辦公室物業範圍內，以及企業與消費者黃頁等處宣傳商品。

部分詐騙方式是精心策畫的成果。一種稱為「無底洞 (Rabbit Hole)」的詐騙方式，誘使受害者參加經設計的問卷調查，並藉此取得敏感的私人及付款資訊。受害者可能因為點選假冒知名大公司（如新加坡電信或新加坡郵政或名人的假廣告，進而卸下心防並詳實填寫問卷。有份問卷宣稱只要花費新幣 1 元手續費，就有機會贏得新的手機，受害者便填入所需信用卡資訊以支付手續費。起初，這份新幣 1 元手續費會出現在帳單上，但在一個月內，受害者的信用卡會出現新的授權交易。[5]

新加坡當局接獲至少 40 名新加坡人投訴後，於 2020 年 5 月封鎖了 Arotrade 這個據信於貝里斯註冊的未經授權交易平台。Arotrade 聲稱將為股票、外匯、商品、加密貨幣和指數等資產類別提供價差合約 (CFD)。由於 Arotrade 在新加坡沒有資本市場服務許可證，因此其活動違法該國的證券期貨法。[6]

---

[4] Cara Wong，「第一季詐騙受害損失達 4,130 萬美元；電子商務與借貸詐騙最為常見」，《海峽時報》，
https://www.straitstimes.com/singapore/courts-crime/scam-victims-lost-413-million-in-first-quarter-of-2020-e-commerce-and-loan

[5] David Sun，「詐騙集團透過當地品牌及『贈品』，以無底洞手法鎖定新加坡人進行詐騙」，《海峽時報》，
https://www.straitstimes.com/singapore/courts-crime/fraudsters-target-singaporeans-using-local-brands-and-freebies-in-rabbit-hole

[6] 亞洲新聞頻道，「新加坡當局封鎖線上交易平台 Arotrade，疑與詐欺行銷策略有關」，
https://www.channelnewsasia.com/news/singapore/arotrade-trading-platform-website-blocked-fraudulent-marketing-12779798

新加坡警方發現，Arotrade 涉及詐欺行銷活動，試圖說服新加坡人透過網站進行投資。在該網站封鎖前，受害者已轉帳超過新幣 33 萬元予 Arotrade。根據警方與新加坡金融管理局 (MAS)、資訊通信媒體發展管理局 (IMDA) 的共同聲明表示，Arotrade 網站使用「假新聞文章使人誤信知名人士，包括新加坡警方高層，對加密貨幣之投資背書，隨後將使用者導向 Arotrade 網站中。」[7]

內線交易雖然不如詐欺和洗錢常見，但仍不時會在新加坡發生。在 2019 年 7 月，該國將三名男子定罪入監，其在超過七年期間透過內線交易不法獲得超過 8 百萬新幣。他們被起訴共 333 項內線交易。這是新加坡首起因超前交易被內線交易罪名起訴的案例，其罰則遠比單純超前交易要重得多。「三人共謀濫用機密資訊謀取個人利益，從而破壞市場誠信，」新加坡金融管理局政策、付款與金融協理 Loo Siew Yee 在一篇聲明中表示。[8]

在此同時，線上詐欺仍是新加坡最普遍的金融犯罪類型，特別是在金融詐騙方面。從 2020 年 1 月至 6 月期間，與銀行業相關的釣魚詐騙案件年增率超過 2,500%（自 34 件增至 898 件），而貸款詐騙從 650 件成長到 1,014 件，相較 2019 年同期增長 56%。[9]

預計將在 2021 中期啟用的新加坡數位銀行，在線上詐騙活動激增的情況下，必須特別留意合規性。

---

[7] 亞洲新聞頻道，「新加坡當局封鎖線上交易平台 Arotrade，疑與詐欺行銷策略有關」，https://www.channelnewsasia.com/news/singapore/arotrade-trading-platform-website-blocked-fraudulent-marketing-12779798

[8] 新加坡金融管理局，「三人涉內線交易遭定罪，法院命令沒收不法所得，https://www.mas.gov.sg/news/media-releases/2019/court-convicts-three-individuals-for-insider-trading-and-orders-forfeiture-of-criminal-proceeds

[9] 亞洲新聞頻道，「2020 年上半銀行相關釣魚詐騙暴增逾 2,500%」，https://www.channelnewsasia.com/news/singapore/online-scams-increase-police-crime-social-media-impersonation-13053822

II. 澳洲

最知名的貸款機構涉及與新冠肺炎相關的退休金詐騙及大型洗錢活動

與新加坡類似，澳洲的線上詐騙數量也隨著疫情爆發升溫，使犯罪份子得以利用民眾對金融安全的顧慮。澳洲當局在 2020 年 5 月揭露，詐騙者試圖取得約 150 名澳洲人的退休金帳戶。這些帳戶內含民眾退休後可使用的儲蓄金，但作為疫情時期的紓困方案之一，帳戶持有人可在政府核准下提前取用。至今已核准約 1 百萬澳幣的申請。澳洲當局表示，進行調查時，警方已凍結據信是從這些帳戶竊取的 12 萬澳幣。[10]

在其中一個案例中，詐騙集團似乎透過一對夫妻的名義建立重複的 myGov 帳戶（澳洲政府服務線上入口網站），並且利用竊取的身分資訊申請到 2 萬澳幣左右。所幸該夫妻發現遭竊，阻止犯罪者從他們的帳戶提領現金。[11]

澳洲聯邦警局 (AFP) 在 2020 年 7 月攻堅犯罪集團並逮捕 12 人，該集團涉嫌自澳洲稅務局 (ATO) 騙取超過 1,700 萬澳幣。當局表示，該集團鎖定金融業專家進行招募，為其犯罪行為提供所需知識以順利進行詐欺。法新社 (AFP) 將在法庭上指控，該集團透過旗下公司雇用勞力應支付予 ATO 的稅金，是透過嫌犯擁有的薪資公司支付，進而以此洗錢。超過 1 百萬澳幣的金額被移轉到位於新加坡的銀行帳戶。當局在破獲後已凍結 65 個銀行帳戶。[12] 至今尚未有澳洲主要銀行涉及此案，但調查尚未結束。

一位澳洲法遵科技專家指出，澳洲最大的銀行正在進行大規模洗錢違法行為，「他們打造自己的技術平台，以便對發展中國家的民眾提供低價值貸款。他們不把這視為洗錢行為。過時的 IT 系統將產生反洗錢的漏洞。

該銀行最後因違反反洗錢及反資助恐怖主義條款達 2,300 萬件，遭判罰 13 億澳幣。這項罰鍰為澳洲史上最大宗，超過 2018 年另一家澳洲銀行為解決一起民事訴訟，違反反洗錢及反資助恐怖主義條款情事共計 53,000 件，遭罰澳幣 7 億元之金額。[13]

---

[10] SBS 新聞，「詐騙集團鎖定疫情下的澳洲退休金帳戶」，
https://www.sbs.com.au/news/fraud-scheme-targeted-australian-superannuation-accounts-during-pandemic

[11] Pat McGrath 與 Alison McClymont，「檢查您的退休金結餘。透過新冠病毒提前發放方案，成千上萬的澳洲人遭詐騙，」ABC 新聞，
https://www.abc.net.au/news/2020-06-01/scammers-stealing-thousands-through-coronavirus-super-scheme/12301010

[12] 澳洲聯邦警察，「組織犯罪調查結果，12 人進行多層次詐騙遭起訴」，
https://www.abc.net.au/news/2020-09-24/westpac-money-laundering-austrac-fine-explained/12696746

[13] Michael Janda，「Westpac 破紀錄 13 億 AUSTRAC 洗錢罰款的理由」ABC 新聞，
https://www.abc.net.au/news/2020-09-24/westpac-money-laundering-austrac-fine-explained/12696746

澳洲交易報告分析中心 (AUSTRAC) 同時發現，由於銀行未盡客戶盡職調查之責任，遂有人利用此管道將錢匯往菲律賓，並從事涉及已知兒童剝削風險的交易。不僅如此，AUSTRAC 指出貸款方未能提供十天內的交易報告（按法律規定），自 2013 年 11 月至 2018 年 9 月為止，有近 75% 的匯入款項來自澳洲境外銀行。這些交易共計 1,950 萬筆，金額超過 110 億澳幣。[14]

銀行於 2020 年 6 月反洗錢 / 反資助恐怖主義合規報告中公布內部調查結果。銀行整理出合規失敗三大主要原因：銀行未充分瞭解銀行特定反洗錢 / 反資助恐怖主義風險、不清楚管理反洗錢 / 反資助恐怖主義合規之完整責任制度、缺乏反洗錢 / 反資助恐怖主義專業知識與資源。[15]

新加坡金融犯罪專家與科技產業高階主管表示，澳洲銀行界缺乏反洗錢 / 反資助恐怖主義合規知識情況非常普遍，這裡提到的四大銀行「並非異數」。

除詐騙與洗錢外，部分專家認為內線交易在澳洲非常盛行。澳洲國立大學在 2019 年 9 月公布一項研究，其調查自 2005 至 2015 年間澳洲股票交易所 (ASX) 的交易結果，發現澳洲上市公司的董事經常使用內線交易策略。其中以礦業公司最為常見，另外還有醫療保健、製藥及消費產品。[16]

指導該研究之金融學教授 Dean Katselas 向澳洲股市情報網站 Small Caps 表示，「我發現這些獲知內情的人，尤其是董事，是炒短線的交易者。他們根據公司先前的收益表現，提前逢低買進，逢高賣出。」根據法律，這絕對形同內線交易；如果該公司是績優股，情況則更嚴重。」[17]

---

[14] AUSTRAC，「AUSTRAC 對 Westpac 提出民事懲罰令」，https://www.austrac.gov.au/about-us/media-release/civil-penalty-orders-against-westpac

[15] Westpac 集團，「Westpac 公布 AUSTRAC 索賠聲明書問題調查結果」https://www.westpac.com.au/content/dam/public/wbc/documents/pdf/aw/media/westpac-releases-findings-into-austrac-statement-of-claim-issues-media-release.pdf

[16] 澳洲國立大學，「研究揭露澳洲股票市場內線交易」https://www.anu.edu.au/news/all-news/study-exposes-insider-trading-on-australian-stock-market

[17] Imelda Cotton，「澳洲國立大學研究指出，ASX 涉及大量內線交易」，https://smallcaps.com.au/insider-trading-asx-australian-national-university-anu-study/

在此同時，澳洲銀行在展望未來之際需進一步加強洗錢管控，否則將損及財務與商譽。澳洲最大的貸款方已因涉及洗錢遭罰破紀錄的罰鍰，並確認它與波多黎各一家離岸銀行有關係銀行的關係，而且這間銀行是國際洗錢與逃稅調查的核心。[18]

在與澳洲媒體《世紀報》*The Age* 訪談中，任職於某大型澳洲銀行的前合規官表示，澳洲銀行往往將銷售看得比風險管理還重要，導致未經適當審查便建立合夥關係。[19]

[18] Charlotte Grieve 與 Nick McKenzie，「Westpac 與波多黎各 Euro Pacific 銀行有所關聯，呼籲金融犯罪改革聲起」，https://www.theage.com.au/business/banking-and-finance/westpac-s-ties-to-puerto-rico-bank-euro-pacific-spark-calls-for-financial-crime-reform-20201019-p566bh.html

[19] Charlotte Grieve 與 Nick McKenzie，「Westpac 與波多黎各 Euro Pacific 銀行有所關聯，呼籲金融犯罪改革聲起」，https://www.theage.com.au/business/banking-and-finance/westpac-s-ties-to-puerto-rico-bank-euro-pacific-spark-calls-for-financial-crime-reform-20201019-p566bh.html

III. 台灣

洗錢問題獲控管，但線上詐騙仍難防

相較於新加坡與澳洲，台灣金融界較小而集中，程度上發生金融犯罪情況較少。但是，台灣的洗錢控管長久以來不夠充足，直到近年來才有所改善。其中促成改革的催化劑，是 2016 年兆豐銀行紐約分行遭紐約州金融服務署 (NYDFS) 重罰 1 億 8 千萬美金，指控其違反反洗錢與反資助恐怖主義法。NYDFS 發現兆豐銀行紐約分行與其他兩間位於巴拿馬的分行之間有可疑交易，而巴拿馬屬於洗錢的高風險國家。[20]

自此之後，台灣開始採取規範方法對抗金融犯罪。為更有效打擊洗錢行為，台灣於 2017 年 6 月通過一項新法規，要求銀行進行更全面的客戶盡職調查，報告可疑交易並保留紀錄。該法還特別針對超過特定門檻的現金與黃金，制定強制性的海關申報單，在財產或空殼公司交易中使用所有者以外的他人姓名，將被視為刑事犯罪，並允許執法機構更迅速開展洗錢調查，沒收違法資金。[21]

2019 上半年，台灣沒入 37 億新台幣（折合 1 億 1800 萬美金）涉嫌洗錢案件的資金，是前一年的八倍。違法資金的目的地多半是中國、接著是香港與澳門。有些案件也牽涉馬來西亞、菲律賓、越南及印尼。[22]

台灣對抗洗錢犯罪的努力終於開花結果。2019 年底，澳洲的亞太洗錢防制組織 (APG) 將台灣列為「一般追蹤」名單中，與香港、澳門、印尼及庫克群島並列。在此之前，台灣名列「加強追蹤」名單內，代表該地區有較高的洗錢風險。

[20] Samiel Rubenfeld，「銀行違反反洗錢法遭罰，與巴拿馬文件有關」，《華爾街日報》，https://www.wsj.com/articles/BL-252B-11007

[21] 中華民國法規資料庫，洗錢防制法，https://law.moj.gov.tw/ENG/LawClass/LawAll.aspx?pcode=G0380131

[22] Jason Pan，「政府於對抗洗錢方面大有斬獲」，《台北時報》，https://www.taipeitimes.com/News/taiwan/archives/2019/08/09/2003720190

在強化對抗金融犯罪的能力方面，台灣仍有進步空間。台灣的金融監督管理委員會 (FSC) 於 2020 年 3 月向金融機構發出公開信，描述在幾個合規領域的不足之處。其中包括風險評估、交易監控、客戶盡職調查、以及客戶風險評估系統。金管會認為，台灣的機構對客戶背景缺乏深入瞭解，有些個案甚至未取得足以判別受益人的相關文件，也未留存遭拒客戶的紀錄。

這些合規漏洞雖不嚴重，但最終仍可導致無法察覺及預防的金融犯罪。有鑑於此，金管會告知金融機構強化對帳戶與交易的監控，以及戶名查驗。

在管控詐騙方面，台灣也面臨難題。在 2020 年 3 月，一位台灣女性遭控向 9 家台灣銀行詐得 386 億新台幣（折合 13 億美金），並自美國引渡至台灣待審。在該夫妻的指示下，潤寅實業有限公司員工自 2011 年 1 月至 2019 年 5 月持續偽造不實交易文件、資金轉移及假投資內容，以向銀行進行詐貸。該夫妻與其他 34 名涉案人遭控違反台灣銀行法、洗錢防制法、商業會計法。[23]

上述重大案件僅為特殊個案，並非常態。台灣多半詐騙案件皆為特定幾種小規模線上詐騙。近年最轟動的個案之一，是台灣高等法院因一位女子於 2014 至 2016 年間，透過 Facebook 進行 439 起詐騙案，上百名受害者向其購買商品遭騙，遂判處 14 年有期徒刑。該名女子以平均市價 7 折至 5 折的價格，誘使受害者上當。她經常違反約定寄貨日期，並拒絕提供退款。在躲藏一陣子後，她最終向警方自首。她共向 439 名受害者詐得 2 億 5,200 萬新台幣（折合 810 萬美金）之不法所得，法院因此判處漫長的徒刑。[24]

另一個近期案件，是台灣警方破獲一個線上賭博詐騙活動，半年內共計從 69 萬名賭客身上詐得 20 億新台幣（折合 7,100 萬美金）。[25]

有鑑於台灣電子商務產業正蓬勃發展，加上高速網路普及，智慧型手機普及率達 97%，因此在未來幾年間，線上詐騙應仍是主要的金融犯罪類型之一。

---

[23] Chiu Chun-chin、Lin Chang-shun 與 Chiang Yi-ching，「銀行詐欺案嫌犯遭遣送回台灣」，Focus Taiwan，https://focustaiwan.tw/society/202003080004

[24] Focus Taiwan，「網路賣家詐騙遭判 14 年有期徒刑」，https://focustaiwan.tw/society/201907250014

[25] Focus Taiwan，台灣破獲線上賭博詐騙集團，共 95 名嫌犯遭捕，https://focustaiwan.tw/cross-strait/202011040021

IV. 日本

亞洲加密貨幣中心面臨金融犯罪威脅攀升

東京是舉足輕重的區域金融中心，但日本自古以來未曾成為金融犯罪的溫床。但是近年來根據警方調查指出，國際犯罪網路已進入日本國內。2019 年警方白皮書顯示，2018 年警方調查共 511 起洗錢案件，這是破紀錄的單年案件量，而上次超過 500 起案件是在 20 多年前。日本當局表示，犯罪組織可能將日本許多擁有國際通路之中小企業，視為進行洗錢的方便管道。組織犯罪成員佔所有洗錢案件的 12.7%。[26]

獲報的洗錢案件數量，在 2019 年進一步上升到 537 件。日本國家警察局表示，2019 年非法交易事件報告破紀錄達 440,492 件。其中銀行佔絕大多數，是整體案件之 80%；但另一方面，加密貨幣也出現約 6,000 件非法交易。[27]

日本的線上詐騙數量也在增加。根據國家警察局指出，網路金融轉帳詐騙在 2019 年達 1,872 件，是前一年的 600%，累計損失金額達 25 億 2 千萬日圓，是 2018 年的 550%。許多犯罪份子偽裝成銀行發送簡訊給被害人，試圖引導至假冒網站輸入資訊，藉此取得使用者的網路金融資訊。企業在此類詐騙損失合計 7,500 萬日圓，而一般民眾損失合計高達 24 億 4 千萬日圓。[28]

---

[26] Akinobu Iwasawa，「國際犯罪集團進駐，日本洗錢案件飆升。」《日經亞洲評論》，https://asia.nikkei.com/Business/Finance/Money-laundering-spikes-in-Japan-as-global-crime-moves-in

[27] Turner Wright，日本國家警察局：「2019 年 537 人因洗錢遭捕」，Coin Telegraph，https://cointelegraph.com/news/japans-national-police-537-arrests-for-money-laundering-in-2019

[28] Nippon.com，「2019 年日本線上金融詐騙案件激增」，https://www.nippon.com/en/japan-data/h00695/

同時，日本開放加密貨幣的政策，使其成為網路罪犯的目標。自從比特幣於 2008 年誕生起，日本就一直是活躍的貨幣交換中心。日本人是最早開始使用比特幣的族群之一，即便在當時幾乎沒有任何實質價值。第一家大規模加密貨幣交易所 Mt. Gox 即為一家日本公司。Mt. Gox 自 2010 年開始營運，直到 2014 年遭逢史上最大宗比特幣駭客事件後宣告破產：犯罪者獲得等同於市值 4 億 6 千萬美金的比特幣。[29]

儘管 Mt. Gox 遭駭的驚人金額，但是在接下來幾年內，日本對虛擬貨幣交易的限制依舊相對地微不足道。日本在 2017 年 4 月成為第一個引進加密貨幣交換登記系統的國家。但是，直到駭客於 2018 年 1 月，從 Coincheck 交易所竊得價值 5 億美元的加密貨幣後，日本金融服務管理局 (FSA) 才終於挺身對抗數位貨幣的金融犯罪。「FSA 以大動作向其他六家營運商發出改善命令，要求他們改善洗錢防制與其他方面的不足之處。在部分案例中，客戶在身分驗證不足情況下，仍得以透過郵務信箱作為個人地址進行註冊。」*《日經亞洲評論》*表示。[30]

加密貨幣成為日本幾十年來最備受關注的刑事案件之一，即前日產執行長 Carlos Ghosn 於 2019 年 12 月從日本潛逃案。據傳，Ghosn 之子 Anthony Ghosn 以 63 枚比特幣（市值 50 萬美金），透過加密貨幣平台 Coinbase 轉交給 Peter Taylor，亦即 Carlos Ghosn 雇用協助他從日本潛逃的兩人之一。Carlos Ghosn 因涉嫌金融犯罪而被起訴。[31]

日本若要按計畫成為亞洲首選加密貨幣交易中心，就勢必要持續強化對應的監管能力。在便利友善與充分管控之間，日本需要拿捏適當平衡，方能遏止針對虛擬貨幣的犯罪。

[29] Robert McMillan，「Mt. Gox 的內幕，比特幣價值 4 億 6 千萬美金的災難」，Wired，https://www.wired.com/2014/03/bitcoin-exchange/

[30] Takero Minami，「日本針對加密貨幣加強洗錢防制」，《日經亞洲評論》，https://asia.nikkei.com/Spotlight/Cryptocurrencies/Japan-eyes-cryptocurrencies-as-it-toughens-money-laundering-laws

[31] David Yaffe-Bellany 與 Janelle Lawrence，美國：「Ghosn 之子支付 500,000 美元給被告逃犯的共犯」，Bloomberg，https://www.bloomberg.com/news/articles/2020-07-23/ghosn-son-paid-500-000-to-accused-escape-accomplice-u-s-says

對抗未來的亞洲金融犯罪

亞洲金融服務的數位化發展迅速，成為一把兩面刃：其為金融產業同時帶來更多機會與風險。儘管一些投機犯罪分子正以環境特有的詐騙利用疫情引發的焦慮不安，但數位金融犯罪的上升則是長期趨勢，並與產業轉移至網路的趨勢息息相關。

有四大主要趨勢將決定能否成功對抗亞洲金融犯罪：資料管理、數位轉型、預測分析、及異常偵測日漸增加的重要性。在這四項趨勢中，先進科技都是不可或缺的一環，能強化金融機構保護客戶與自身的能力，遏止精通數位技術金融慣犯的持續侵擾。除此之外，金融機構合規團隊的合作互助亦同等重要，乃至於各銀行、各金融機構與監管單位間的相互配合。

資料管理

為最佳化資料管理，金融機構應透過整合詐欺防制與反洗錢資訊，以更全面的方式對抗金融犯罪。整合的反詐欺與反洗錢團隊將能更流暢地分享重要資訊，藉此提升評估客戶風險、辨識可疑交易、協同進行調查的能力。結果來說，合規成本將降低，而客戶滿意度將有所提升。在即時交易數量持續上升的年代，全面式的金融犯罪防制前所未有地重要。的確，客戶希望付款和其他業務能輕鬆又便利。

但同時，金融機構應與其他同業進行資料共享。現今銀行業各自獨立作業的方式，常導致無法以更宏觀全面的角度評估金融犯罪風險。犯罪份子深知這項弱點，並極力在不同銀行之間加以運用，移動不法所得。

近日的金融犯罪執法網路文件外洩事件也指出了這點。檔案指出，與逃亡者 Jho Low 家族與企業有關的數十億美元，幾年來一直在美國各家銀行中流竄。據傳，他是 1MDB 弊案的主謀。即便明知事有蹊蹺，例如無法找到資金源頭，銀行仍未能阻止資金流動。儘管數家銀行最終申報可疑交易，但已經是在交易發生許久之後。屆時要阻止不法資金流動為時已晚。[32]

金融犯罪執法網路文件外洩案也同時揭露，東京奧運競標委員會的一名顧問將 37 萬美金轉給一位舉足輕重的國際奧委會成員之子。資金移轉的路線迂迴曲折，從日本轉到新加坡，最後進入俄羅斯與塞內加爾的銀行帳戶。[23]

[32] Aidila Razak，「解密文件揭露，美國銀行對劉特佐「可疑的」1MDB 相關轉帳採取行動時，早就為時已晚」MalaysiaKini，https://www.malaysiakini.com/news/543389

[33]《朝日新聞》，「FINCEN 檔案解密：東奧競標顧問與 IOC 成員有金錢往來」http://www.asahi.com/ajw/articles/13746177

數位轉型

數位轉型能幫助強化資料管理流程。金融機構使用人工智慧技術如認知運算與自然語言處理 (NLP) 強化反洗錢能力，提供足夠資料供演算法分析獲得有效情報。一位新加坡法遵科技與金融犯罪專家指出，「如果您有豐富的資料庫，就有能力運用這項科技。如果您想透過人工智慧防制洗錢，就需要大量資料來進行剖析，這項技術才能使用。」

他同時表示，澳洲最大的貸款方之一「正使用人工智慧等技術迅速識別銀行對監管機構的義務，並且加速整個流程的進度。唯有如此才能持續領先。」

在反詐欺與反洗錢解決方案轉換至雲端的過渡期之中，數位轉型相較於過時的 IT 基礎架構，能提供更細膩、更具彈性的偵測能力、辨識能力、以及回報能力。以雲端為基礎的整合式反洗錢、反詐欺解決方案，結合單一窗口個案管理器與強大的分析能力，能協助銀行改善偵測準確度、減少誤報情形、並提升營運效率。

預測分析

預測分析是由機器學習支援的一種資料分析技術，讓合規團隊得以評估未來事件的風險程度。預測是根據交易資料、顧客及交易對手情報、以及行為活動進行分析。

預測分析是一項強大的反洗錢創新技術，搭配規則建立法使用，可提升警報的準確性，讓金融機構按照預先制定的條件，自動將警報轉發給合適單位。舉例來說，高預測分數事件在工作流程出現時，將自動呈報給資深案件處理者。相對來說，低預測分數事件將被移入休眠佇列，減少在警報光譜兩端進行初級調查的壓力。

異常偵測

客戶身分調查過程中的異常偵測，是另一項對抗未來金融犯罪的重要趨勢。異常偵測對合規團隊日趨重要。此功能可檢測某些危險警訊，像是獨特項目、事件、或資料與其他內容不符的可疑觀察，以及其他以規則為基礎的交易監控系統可能會漏掉的警訊。異常偵測透過機器學習與統計分析運作，紀錄每天所有交易活動並逐步發展出個別的帳戶活動模式。

接著，每日、每週與每月的活動會與帳戶的歷史資料進行比對，以及與該帳戶相似族群的其他資料比對，找出非典型行為。任何明顯不尋常的活動都將被標示進行進一步分析。

在客戶身分調查流程中，進階區隔也很重要。相較於傳統單就客戶身分調查或行為模式建立的「硬性區隔」方法，進階區隔是透過分析客戶金融交易的匯總所得。其根據不同類型對客戶進行分類，並放入不同風險級別的群體中。

一位跨國界付款亞太地區金融犯罪防制高階主管表示，「我們必須儘可能縮短蜜月期，儘快辨識出危險分子，金融機構都知道，更快、更精確進行客戶身分調查與驗證，將是一項競爭優勢。生物辨識技術的大量採用，反映出政府在實名化上的趨勢。他們能利用 API 取得政府資料。」

該執行長表示，與其他地區相比，這方面在亞洲是一項優勢。在亞洲，金融機構和監管機構都利用技術來強化合規流程，「監管機構和被監管單位之間合作密切」，程度遠高於美國，他表示。

未來發展

展望未來，亞洲的金融機構預期將浮現 Wirecard 弊案後續連鎖效應，因為金融界範圍遍布全球，而且與數位技術關聯性越來越高。Wirecard 自新加坡金融管理局於 2020 年 9 月 30 日發出命令後，已停止在新加坡的所有活動。自從該公司陷入財務危機，無法再為許多新加坡店家處理交易後，新加坡金融管理局命令 Wirecard 關閉在新加坡所有金流服務。約有 1,900 間新加坡店家受到波及。[34]

在充滿挑戰的商業環境中，傳統銀行和數位銀行很快就意識到，擁有強化合規能力的合適技術這件事至關重要。2020 年 2 月，總部位於新加坡的 TONIK 已獲准在菲律賓設立受監管銀行，並選用 NICE Actimize 的雲端 AML Essentials，包括交易監控與客戶盡職調查，以及制裁篩選功能。

「我們相信，相較於傳統銀行，數位銀行的運作能夠達成更高的金融合規等級，而與 NICE Actimize 的合作則充分顯示，我們期望能在東南亞地區的數位銀行領域奠定更高的信任、可靠度與合規標準。」TONIK 執行長暨創辦人 Greg Krasnov 表示。

到最後，新時代銀行將不受過時 IT 系統的限制，從數位時代科技自然具備的靈活性中取得充分優勢，在面對新興數位金融犯罪威脅時更能從容以對。他們不需像傳統銀行那樣苦苦追趕。為了在面對威脅方面保持領先，他們必須將合規放在優先考量，不僅將之視為監管責任，更要將它當成為客戶提供允諾卓越體驗的必要一環。

[34] Joyce Lim，Wirecard 在新加坡終止營運：「波及商家的其他方案。」《海峽時報》，https://www.straitstimes.com/business/banking/alternative-options-for-merchants-affected-by-wirecard-ceasing-its-services-in

NICE
ACTIMIZE

關於 NICE Actimize

NICE Actimize 是最大型且範圍最廣泛的金融犯罪、風險與合規解決方案供應商，為區域性及全球性金融機構以及政府監管單位提供服務。NICE Actimize 的專家運用創新科技來揪出金融犯罪，避免詐欺發生並提供監管合規服務，藉以保護機構、捍衛消費者及投資人資產，也因此持續被排名為業界第一。

公司提供即時、跨管道的詐欺防制、洗錢防制的偵查以及交易監控解決方案，解決如付款詐欺、網路犯罪、交易監控、市場濫用、客戶盡職調查與內線交易等問題。

請前往 www.niceactimize.com、@NICE_Actimize 或者 Nasdaq:NICE 了解更多資訊。

隨時接收更新
Matthew Field
反洗錢部門亞太地區市場主管
NICE Actimize
matthew.field@niceactimize.com

關於 Kapronasia

Kapronasia 是市場研究方面的頂尖供應商，包括金融科技、銀行業、付款及資本市場。我們的辦公室以及位於上海、香港、台北、首爾及新加坡的代表處，為區域內的客戶提供把握亞洲價值最高商機所需的的深入洞見，並且幫助客戶在市場實現並維持競爭優勢。

請瀏覽 https://www.kapronasia.com

Kapronasia