行政院及所屬各機關因公出國人員報告

（出國類別：考察）

新加坡智慧財產保護及打擊詐欺犯罪業務
考察報告

服務機關：法務部

姓名職稱：鄭鑫宏主任檢察官（臺灣高等檢察署）

黃彥琿檢察官（臺灣高等檢察署）

劉怡君檢察官（臺灣高等檢察署智慧財產分署）

林彥均主任檢察官（臺灣臺北地方檢察署）

陳信郎主任檢察官（臺灣臺中地方檢察署）

羅韋淵檢察官（臺灣臺北地方檢察署）

黃啟祥檢察事務官（臺灣高等檢察署）

派赴國家：新加坡

出國期間：113 年 4 月 8 日至 4 月 12 日

報告日期：113 年 5 月 28 日

摘要

新加坡採取對重要研發成果，在法律政策採取較為寬鬆之保護及保密方式，吸引外國企業及人才進入。而新加坡政府就國內及國外專利申請部分，採取國安審查政策，此類制度係以保護國家安全及民眾利益為基礎，就專利申請涉及不宜公開之國家安全或產業技術資訊，列入專利准否之考量。

新加坡政府對非組織性之微罪智財案件，採取權利人自行委任律師蒐證及撰寫起訴狀，並由檢察官審查認情節程度應採刑事追訴者，准許權利人自行委任律師向法院提起刑事訴訟，可視作「經檢察官審查之自訴程序」。

新加坡 Law Enforcement and Other Matters Bill 及（Corruption, Drug Trafficking and Other Serious Crimes (Confiscation of Benefits) Act 1992, CDSA）新法極具參考價值，透過立法假設的方式，對於符合特定客觀不法態樣的行為，透過立法方式將主觀犯意的舉證責任轉換於被告，由被告對於自己缺乏犯罪意圖負舉證責任。

本文除針對考察目的、內容進行說明外，另就新加坡智慧財產保護及打擊詐欺策略等面向提出心得與建議，期供我國相關政策擬定之參考。

目錄

壹、拜訪駐新加坡台北代表處

民國 113 年 4 月 8 日由臺灣高等檢察署兼智慧財產分署主任檢察官鄭鑫宏率臺灣高等檢察署查緝詐欺及資通犯罪督導中心檢察官黃彥琿、臺灣臺中地方檢察署主任檢察官陳信郎、臺灣臺北地方檢察署主任檢察官林彥均、檢察官羅韋淵、臺灣高等檢察署智慧財產分署檢察官劉怡君、臺灣高等檢察署檢察事務官黃啟祥共七人，偕同甫於 112 年 8 月 30 日退休之前臺灣高等檢察署智慧財產分署主任檢察官陳文琪，於同日下午抵達新加坡後，隨即由我國派駐新加坡代表處之刑事局外事科警官王正和引導，參訪團一行共八人拜訪我國駐新加坡代表處，並獲童振源代表親自接見。

童代表首先了解本次參訪團主要任務及目的後，接著就新加坡各項政、經、科技及犯罪偵防實況作了扼要介紹，並與參訪團成員進行意見交流及互動。令人印象深刻的是參訪團甫抵新加坡樟宜機場， 即對機場自動通關的設備感到好奇；對照我國目前僅開放事先至移民署辦妥自動通關相關必要手續後始得使用自動通關的措施，新加坡係不分本國或外籍人士一律開放使用自動通關，在通關效率上實在值得我國借鏡。

童代表並介紹新加坡大量使用科技設備於民眾生活的結果，民眾出門只要攜帶手機，幾乎所有關於民眾日常生活的證照、社會保險資料、金融帳戶、支付工具等，一臺手機即可搞定，和之前我國原擬推行數位身分證所產生的爭議相比，新加坡顯然更懂得運用科技及大數據的益處，尤其運用科技執法的結果，一般公共場所幾乎看不見警察，治安卻沒有因此惡化，與我國動輒要求增加警力及見警率以換取良善治安的政策大相逕庭。

雖然新加坡近年亦受詐騙集團橫行之苦，但今年以來陸續推動若干新法，例如個人客觀上持有逾十個電信門號即構成刑事犯罪，不論持有者之主觀意圖為何，從行政前端管制電信門號，避免遭詐騙集團濫用之強力防詐作為，亦值得我國省思。整個拜訪行程歷時一個小時結束，成員均表示獲益良多，對接下來的參訪行程多有助益。

貳、考察目的

1. 智慧財產保護：

智慧財產保護是先進國家努力的課題，也是外商貿投關心之事項。近年來營業秘密保護及數位侵權問題尤受關注。新加坡政府於 110 年公布《新加坡智慧財產權戰略 2030》(Singapore IP Strategy 2030,SIPS 2030)，是一個將新加坡打造成全球無形資源(IA)和智慧財產權(IP)樞紐地位(A Global Hub for IA/IP)的十年藍圖。包括：(1)大數據運用。(2)營業秘密保護。(3)人工智慧 AI 與智慧財產權保護之銜接。透過考察參考學習新加坡在法制框架、執法技巧及司法實務案例之發展與作為。

2. 打擊詐欺犯罪：

隨著電信、網路之自由化與全球金融交易多元化，詐欺集團利用資、通訊科技發達及金融便利性，不斷衍生新型態之詐欺手法，詐欺民眾財產，政府近年來雖將打擊詐欺犯罪列為治安重點，全力執行各項偵防策略，但民眾對於詐欺犯罪仍感威脅，復因詐欺集團據點已擴及到海外第三地國家，年輕人遭誘出國從事詐欺機房或領款車手等工作，甚至淪為國際人口販運被害人，影響我國國際形象。

我國為因應當前高發詐欺案類據以精進，行政院於 113 年 4 月核定「新世代打擊詐欺策略行動綱領 1.5 版」，共計新增了 4 項策略及 17 項行動方案及相關預算編列，俾賡續透過「宣導教育」、「犯罪通路」、「贓款流向」及「偵查打擊」等四大面向，整合各部會力量，群策群力研擬因應策略，以遏止詐欺發生，維護民眾安居樂業生活環境，提升治安滿意度[1]。

為持續調整、優化我國之打擊詐欺策略，遂擇定新加坡考察瞭解新加坡對於移工帳戶、門號及黑莓卡(持國外門號漫遊使用)之管理、對於電信網路詐欺之刑責、沒收及假釋是否有特別之規定，以及對於虛擬資產加密貨幣遭用於犯罪者洗錢之相關防堵措施。

[1] 引自「新世代打擊詐欺策略行動綱領」1.5 版(核定本)

參、考察內容

一、新加坡大學技轉及創新中心

1.新加坡大學技轉及創新中心（下稱技轉中心）係為將技術商業化並提供智慧財產權管理為目標而設立於新加坡大學內之部門，為達成設立目的，技轉中心透過設立海外學院培育創業人才，促進學院與當地產業結合，推動技術轉化至創新的服務，鼓勵人才創業，進而建立全球各地的據點，而達成擴建全球化門戶之目標。

2.技轉轉化至可商業化之智慧財產權

有關技術轉化至創新服務部分，技轉中心並提供相關資源及支援，促進新加坡大學的科研人員與外部企業合作，推動創新與經濟發展結合。首先新加坡大學內科研人員之研發成果，將先由技轉中心就該研發成果進行市場評估，確認市場需求性及潛在客戶意向，選出具有新穎性、非顯而易見且具有實用性之研發成果。

針對有市場發展潛力之研發成果，與科研人員建立聯繫，提供商業化相關建議及支援，由技轉中心提供智慧財產權相關規劃與布局，提供科研人員申請智慧財產權之相關書面草稿協助，並就該技術向新加坡技術許可辦公室（Singapore Technology Licensing Office, STLO）申請為期 90 日之評估審查，並確保評估審查階段的技術保密工作。待智慧財產權建制完成後，由技轉中心規劃智慧財產權轉化為商品服務之路線，並與科研人員建立合作，提供資金支持，協助產品開發，引入行業相關之參與者，讓科研人員與企業建立合作關係，將智慧財產權化的技術加以商業化。

3.智慧財產權轉化至商業：GPA 基金

非核心基金轉化基金將在技術許可辦公室管理下，依不同的清單項目，將提供最高 12 個月 20 萬新幣或 6 個月 5 萬新幣的資源，讓資助的技術價值提升至更適合商業化之狀態，該技術必須達最低之技術成熟水平後，由新加坡大學管理該技術之相關智慧財產權，並向技術許可辦公室提交商業化之計畫底稿。

核心基金係針對有潛力及影響力之技術項目，提供最長 2 年

200 萬新幣之資金支持，目的係將研發成轉化為可帶來經濟及社會效益之產品、流程及服務，並要求該技術於此期間必須達於更高水平，將智慧財產權交由新加坡大學管理，並發明揭露給技術許可辦公室，此階段尚不能准許技術團隊藉此技術成立公司。

國家健康創意中心為了開發具有臨床意義且可以商業化的醫療創新技術，提供最長 1 年半 30 萬新幣之資金支持，申請人必須為公共醫療機構或學術醫學院擔任重要職位，且團隊在臨床醫療具代表性，始符合申請資格。

新加坡大學另設有最小可行產品工作室（Minimum Viable Product Studio, MVP Studio），為初始創立企業開發可商業化產品之原型，促進新加坡大學的技術順利進入市場。

4.新創公司孵化

新加坡大學研發創新計畫為科研人員提供 12 個月之支援及指導，將具有國際競爭力的研發成果，孵化為可持續投資的科技新創公司。該計畫由具有經驗的商業領袖擔任指導者，逐步指導創業過程，提供建議及資源發展最小可行性產品，協助媒合技術互補的技術人員共同創業，並由新加坡大學提供最高 10 萬新幣之投資資金。

新創公司孵化後，商品及智慧財產權即進入商業化程序，新創公司可將智慧財產權授權給產業界，教授及學生均可從分拆成立的公司中獲利。

5.研發成果保護及管理

新加坡大學內之研發成果歸屬於發明人，保護及管理方式則採「棒子與胡蘿蔔」併行模式。

學校與發明人簽署保密協議，但學校作為學術機構，顯少以違反保密協議為由而訴諸訴訟，故保密實際上欠缺嚇阻效果。

但因發明人透過協議與學校共享研發成果，技轉辦公室則協助評估及布局智慧財產權，幾乎三成之智慧財產權可達成商業化使用，因商業化使用所生之授權金利益，將可由學校與發明人共享。再者，發明人有機會因重大研發成果，由技轉中心輔導而成立公司，成為公司經營者。

透過保密協議與共同商業化成果之「棒子與胡蘿蔔」方式，有望達成發明人與學校共同保護及管理研發成果之效。

6.關鍵技術保護議題

I.政府政策及措施

新加坡政府並未制定及公告關鍵技術清單或施行特殊之保護關鍵技術法律。因為新加坡政府以引世界各大企業在新加坡設廠或設立辦公室為主要政策，因此對技術流通採取開放態度，原則上未設任何限制。

依美國管制法規而禁止移轉技術之實體清單上企業或機構，政府會尊重美國法律，不會授權給實體清單上之企業或機構使用相關技術，但仍儘量維持與實體清單上企業或機構保持學術上之合作關係。

技轉中心主任另認為，因技術必須被用於商業用途，始會對市場產生影響，成為商業間諜問題。隨著人才流動，技術流通應在所難免，無法以管制人員出境方式控制技術之流失。

參訪人員認為此部分看法，應與新加坡之產業類別及國際經貿政策有關，是否可套用於我國國際經貿狀況及符合產業特性，恐有另酌餘地。

II.新加坡大學管理措施

新加坡大學針對重要技術有建立內部清單，清單係由設立之委員會決定，但委員會首先參考美國之關鍵技術清單。學校針對清單上技術會加強保護，針對接觸技術之人進行篩選，但無法保證接觸技術之人不會改變效忠對象的意向。

此部分技術清單僅係學校內部政策，並無相關法律規定或效果，但倚賴新加坡長期建立之守法文化與教育，多數新加坡人會遵守相關約定。然而，若簽署保密或其他協議之發明人違反契約，學校可能對該發明人解僱，但法律上責任十分輕微，實質上欠缺嚇阻效果。

二、新加坡律政部

1.律政部為新加坡政府內綜理政策發展及法制修訂機關職掌法律執業者執照核發、國際調解、法律服務、監督國土政策及智慧財產權部門發展，為新加坡智慧財產局（Intellectual Property Office of Singapore）之上級機關。

2.智慧財產權法制與執法

新加坡之智慧財產權法制係注重智慧財產創造，及運用智慧財產吸引外資投資，由海關協助邊境執法，刑事偵查局則負責其他智慧財產法制執法。

智慧財產權法制部分，可區分為需註冊之專利權及商標權，及不需註冊之營業秘密及著作權。

3.專利法制

新加坡專利法設有國家安全相關之專利審查規定。專利法第 33 條[2]係有關專利申請涉及國家安全問題之規範，申請人提出專利後，專利審查機關有 3 個月審查期間。若經審查發現該專利資訊公告可能妨害新加坡之國防者，該專利申請將不被允許；若經審查發現該專利資訊公告可能損害公眾安全者，則可禁止或限制該專利之公告或告知特定對象。

專利法第 34 條[3]規定，若新加坡公民欲向其他國家申專利，必須先取得新加坡專利審查主管機關授權允許，除非該專利已在新加坡提出專利申請 2 個月以上，因主管機關已有審查該專利之機會，故無需再次向主管機關申請至外國申專利之授權。

上開部分為新加坡專利法內有關國家安全及公眾安全審查制度，若違反上開規定者，將承擔罰金刑之刑事責任。

新加坡專利法亦有公平競爭之專利授權規定。專利法第 55 條[4]規定，若任何人請求專利授權，專利權人必須有合理理由才可不授權，若無正當理由不授權則可能造成不公平競爭，此時請求授權之人可向法院提出聲請，要求法院裁定專利權人為公平之

[2] Patent Act 1994 (Singapore) Article 33: Information prejudicial to defence of Singapore or safety of public.

[3] Patent Act 1994 (Singapore) Article 34: Restrictions on applications abroad by Singapore residents.

[4] Patent Act 1994 (Singapore) Article 55: Compulsory licences.

授權。

4.營業秘密保護

新加坡之營業秘密保護基礎為機密法（Law of Confidence），該資訊必須具有機密性，資訊取得者因契約負保密義務，或因情況知悉該資訊為保密資訊而負保密義務，該資訊取得者卻違反保密義務，此時即可依機密法追究其責任。營業秘密所有者，則會視該資訊特性，評估是否有繼續維持秘密性之需求。負有保密義務者違反保密義務，營業秘密所有人可採取暫時狀態處分、要求金錢賠償或請法院命令違約者銷毀或返還資料。

營業秘密同時有不同之法律體系可作為保護依據，包括電腦犯罪或契約責任。電腦犯罪相關法律非律政部主管法規範疇。

5.智慧財產權執法

新加坡之智慧財產執法機關則包括刑事偵查局、海關、移民與檢驗站等機關。執法分為四個面向：民事責任、刑事處罰、訴訟外紛爭解決機制及邊境執法措施。因為新加坡有知名之國際仲裁組織，因此盛行以訴訟外紛爭解決機制處理智慧財產權侵害糾紛。而刑事處罰部分大部分規定在著作權法及商標法。

因通路商販售未經授權之設備，將促使此類未經授權設備在市場流通，影響權利人權利，故凡未經授權之設備，均會被認定為仿冒品而追查。另外，基於商業目的而持有侵權複制品，及以破解密碼方式接觸原受保護著作權保護之商品，均屬刑事犯罪行為。

6.邊境執法

I.請求邊境扣押

新加坡海關可依權利人之請求而協助進行侵權違法商標之邊境扣押程序。若欲請海關執行邊境侵權違法物品之查扣，權利人會提供可供海關辨識侵權產品之資訊及方法。海關在邊境查扣疑似違法物品後，會通知權利人，由權利人則繳納保證金，由海關執行 60 日之扣押程序，而權利人則必須於 10 日內提起各類侵權民事訴訟。

II.請求檢驗扣押物品

新加坡商標法及著作權法均有權利人可針對扣押物品進

行查驗之規定[5]。海關於查扣侵權違法物品後，會發通知給權利人，要求權利人進辨識，權利人也可主動請求前往查驗確認扣押物品是否為侵權產品。若權利人欲前往辨識，必須於 48 小時內回應海關之通知，並提出權利證明文件及繳納保證金，海關則將相關資料交付給權利人，權利人加於查驗後採行民事訴訟程序。

因此類程序下，海關與權利人必須密切聯繫，權利人一般會提供侵權商品之辨識資訊給海關。雙方每年也會舉辦訓練活動，讓海關人員可與權利人接觸及瞭解辨識侵權產品方法，權利人也利用此機會介紹新產品之侵權辨識資訊給海關人員知悉。

7.警方主導及與權利人合作之不同犯罪查緝模式

新加坡智慧財產執法警察於 89 年後，開始執行偵查及起訴智慧財產犯罪之工作，主要係針對大規模及有系統散布仿冒知名品牌商標權之對象，進行商標權之執法。執法方式大致可區分為警方主導之執法及與權利人合作之執法。

警方主導之執法面向，新加坡因警力有限，僅針對大規模組織性犯罪方式主導執法，將侵權產品充公，避免影響新加坡之經濟發展。權利人則可自行決定是否另採取提出民事訴訟損害賠償訴訟或定暫時狀態處分等法律行為。

與權利人合作執法面向，係由權利人自行委請律師，向法院聲請搜索票，警方僅協助權利人執行搜索票，查扣侵權違反產品。嗣由權利人與侵權者洽談和解方案，若和解洽談無果或權利人認為侵權者犯行動大，可委請律師撰寫起訴狀並向總檢察署提出，總檢察署經審查後將回復是否准許權利人向法院起訴之決。權利人若獲得准許向法院起訴之函文，則可委由律師自行向法院起訴；反之，若總檢察署未准許權利人起訴，權利人僅能繼續與侵權者洽談和解方案。

8.電子商務及網路平台之執法挑戰

電子商務及社群平台崛起後，透過網路無國界商業交易成為常態，買方網購之貨品經常在國外，透過郵遞方式寄至新加坡境內，此時海關則會就輸入之貨品進行查驗，若發現有侵權商品情

[5] Trademark Act 1998 Article 93A (Singapore), Copyright Act 2021 Article 336-337 (Singapore).

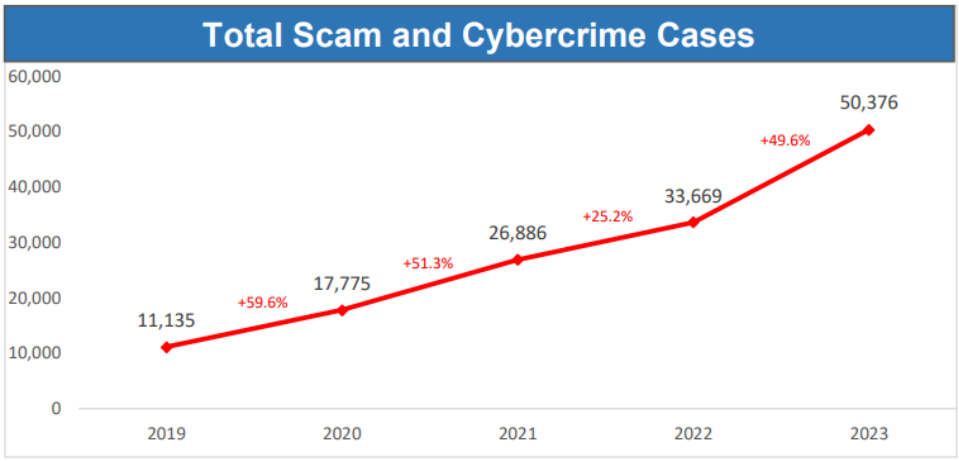
況時通知方處理，由警方裁量是否展開調查。一般而言，警方針對小型賣家案件較可能將資訊提供給權利人，由權利人自行委請律師向法院聲請搜索票執行；但若顯示為組織型犯罪時，警方則傾向自行偵辦。

3. 反詐騙指揮處

1. 新加坡警察部隊反詐騙指揮處（Anti-Scam Command,ASCom）於 111 年 9 月 6 日正式啟用，組織沿革最早為 106 年新加坡警方成立跨國商務犯罪小組 ，107 年針對網路購物詐欺成立特別犯罪調查小組 ，108 年 6 月成立反詐騙中心，此為反詐騙指揮處之前身，111 年 3 月 22 日起擴編為「反詐騙指揮處」，以調查所有類型詐騙案，並監督各警局成立的「反詐騙調查小組」。反詐騙指揮處有新加坡總檢察署之檢察官常駐，擔任法律諮詢之角色，於法律面協助警方查緝犯罪。
2. 新加坡詐騙犯罪現況

I. 犯罪數

新加坡詐騙及數位犯罪的案件數持續攀升，111 年全年 3 萬 3669 件，112 年全年 5 萬 376 件。成長率高達 49.6%。其中惡意軟體相關詐欺犯罪占 5 萬 376 件中的 92.4%。

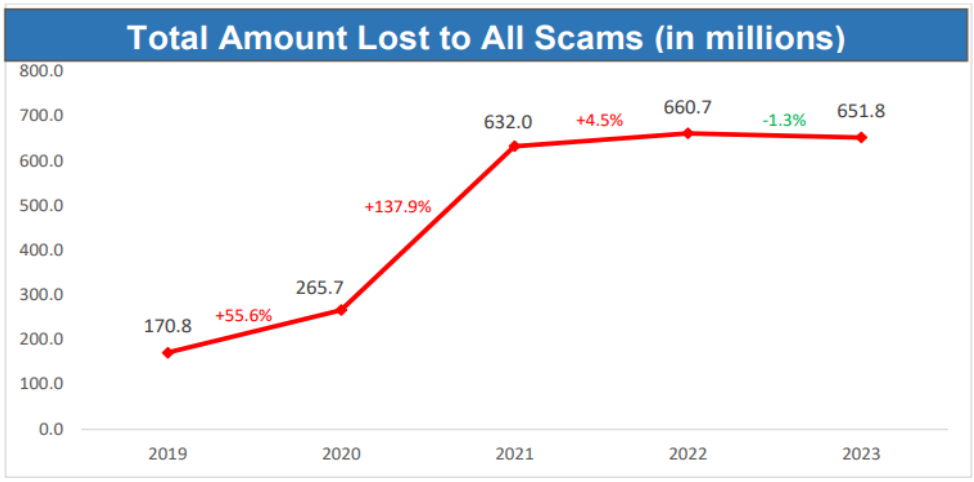


新加坡近 5 年詐欺及數位犯罪案件數統計表(引自新加坡反詐騙指揮處簡報內容)

II. 財損數

112 年全年詐欺財損為 6 億 5180 萬新幣，較 111 年全年詐欺財損之 6 億 6070 萬元略減少 1.3%，是近 5 年首次減少。單一詐騙案件的財損金額也從 111 年的 2 萬 824 新幣減少為 112

年的 1 萬 3999 新幣，降低幅度為 32.8%。反詐騙指揮處分析財損降低的原因，應可歸功於新加坡警察部隊與新加坡資通訊媒體發展局（IMDA）、數位安全局（CSA）金融管理局（MAS）及數位政府團隊（SNG）以及私部門的通力合作，建立預防及阻斷詐欺的架構，並且提供公眾防詐意識以避免詐騙。



新加坡近 5 年詐欺財損統計表（引自新加坡反詐騙指揮處簡報內容）

III. 犯罪態樣

新加坡前 5 大詐騙犯罪態樣依序為求職詐騙、網路購物詐騙、交友詐騙、釣魚式詐騙以及投資詐騙。其中又以冒充政府官員詐騙案件的單件財損最高，平均為 10 萬 3600 元新幣；投資詐騙次之，單件平均財損為 5 萬 700 元。

詐騙集團大多以社群媒體、通訊平台、網路購物平台及電話等方式聯繫被害者，前 5 大使用的工具依序為社群媒體平台、通訊平台、電話、網路購物平台以及其他網站。社群媒體平台在詐騙犯罪的使用率於 112 年是 13725 件，相較於 111 年的 7539 件明顯成長，其中 71.7%是臉書，18.5%是 Instagram。

3.反詐騙指揮處的一大特色為強調公私協力，尤其是推動共同辦公（CO-Location），自 111 年 7 月 25 日起，與新加坡金融管理局(MAS)合作，指定星展、華僑、大華、匯豐、渣打及聯昌國際等 6 大銀行派員 24 小時進駐指揮處，提供立即協助警方追查金流以及凍結帳戶之工作。112 年整年反詐騙指揮處共凍結 1 萬 9600 個銀行帳戶，追回超過 1 億新幣之詐騙贓款。若自 108 年反詐騙中心啟用迄今，共凍結超過 6 萬 600 個銀行帳號，追回詐騙贓款

金額高達 4 億 1090 萬新幣。新加坡在 108 年以前，凍結帳戶必須透過紙本公文，需耗時平均 14 至 60 天才能完成帳戶凍結。然目前已經做到 1、3、5（1 天凍結、3 天檢視問題帳戶、5 天提供交易明細），目前所有銀行都能配合上開期程。

4. 反詐騙指揮處為遏止詐騙犯罪，其主要策略包含「資訊管理」、「阻斷」、「調查」及「國際合作」，並專注於從「上游」開始介入，觀察銀行帳戶資金流向，並利用科技辨識潛在詐騙案件，在受害者意識到被騙前即提出警告，以阻止詐騙案發生。
5. 反詐騙指揮處為阻止被害者受騙，推動自動化 A.S.T.R.O.（Automation of Scam fighting Tactics & Reaching Out Astro），其方式是透過警方與銀行合作資訊共享，利用簡訊的大規模發送來提醒潛在被害人，早期介入避免被詐騙，以 112 年為例，反詐騙指揮處共發出超過 6 萬 8000 則簡訊，提醒超過 2 萬 8,500 名受害者，並以此方式阻斷超過 1.48 億美元的潛在損失。A.S.T.R.O 行動執行方式如下：
   I.擷取被害人匯款銀行帳戶：彙整報案資料中被害人匯款銀行帳戶，以 Excel 檔傳到反詐騙指揮處系統資料中。
   II.自動化發送 email 到受款行凍結帳戶：系統接受資料後，會自動發出 mail 給給銀行進行帳戶凍結。
   III.自動化發送 email 給合作銀行調查潛在被害人：該系統會另發送 email 通知其他銀行；其他銀行收到 email 後，會調查有無客戶匯款到被凍結的帳戶內，並將這些潛在被害人之相關資料彙整（包含姓名、身分證字號、電話號碼、銀行帳號、轉帳金額）回傳反詐騙指揮處。
   IV.反詐騙指揮處以簡訊通知潛在被害人：反詐騙指揮處會透過系統自動發送簡訊的方式通知潛在被害人，以達阻詐之效果。
6. 另外，為推動即時下架疑似涉詐的網路廣告及帳號，新加坡線上購物詐騙發生率第二大的旋轉拍賣平台（Carousell）自 113 年 1 月 30 日起派員進駐反詐騙指揮處共同辦公，以協助平台涉詐廣告及帳戶之即時下架及凍結。

7. 新加坡政府為打擊詐欺及數位犯罪於 112 年 7 月通過《網絡犯罪危害法》The Online Criminal Harms Act (OCHA)，本法自 113 年 2 月生效，新法授權政府（包含警察機關），當合理懷疑（when there is reasonable suspicion）網路上正在從事犯罪活動時，可依據犯罪事實發布以下 5 種具強制力之指令(Direction)給網路業者。5 種具強制力之指令包含：

I.

A.停止通訊（Stop Communication Direction：禁止於網路上傳播特定資訊）

B.內容屏蔽（Disabling Direction：強制線上服務提供商移除特定內容）

C.用戶限制(Account Restriction Direction：強制網路服務提供商限制或關閉特定平台帳號）

D.停止解析（Access Blocking Direction：強制互聯網服務提供商阻止訪問相關網站或域名）

E.刪除手機應用程式（App Removal Direction：強制要求應用程序商店將涉嫌不法之應用程式下架）

II.另外，為有效「主動預防詐騙及惡意網路活動（Proactive Prevention of Scams and Malicious Cyber Activities）」，本法訂有針對「詐騙」及「惡意網路活動」降低發動門檻之規定，授權政府只要在懷疑（when it is suspected）任何網站、網路帳戶或網路活動可能被用於詐騙或惡意網路活動時發布指令。相較於其他犯罪，採取較低的發動門檻，使政府能在實際詐騙犯罪發生前，有效提早預防。

III.本法規範對象包含本國公司及外國公司，違反上開指令者，主管機關得以限制業者其全部或部分業務，嚴重者可能會因不遵循指令（non-compliance of directions）而遭到起訴。值得注意者是於新法之下，新加坡警方針對疑似涉詐的網路廣告、帳號等，都可以強制要求業者下架，而既係針對疑似不法，故不需要有實際詐騙犯罪之發生，警方在執行

上也無須提出被害人報案紀錄等為佐證，大大提升預防詐騙犯罪之成效。

8. 外籍移工金融帳戶管制措施

新加坡有許多外籍移工，為解決外籍移工人頭帳戶之問題，除開戶數量本有限制以外，新加坡政府針對藍領移工實施離境時帳戶強制關閉之措施，實務操作上會給予一定關閉帳戶所需時間，超過時間後帳戶會自行關閉，若有存款則由銀行待保管，故新加坡外籍移工人頭帳戶的問題並不嚴重。

9. 門號管制措施

為防堵本地門號遭不法集團利用，新加坡政府規定每一個人最多僅能購買 3 張預付卡，此數量以足以供來新加坡觀光旅遊及工作之人使用。另外，後付費型的門號遭不法使用之狀況也日益增加，故 113 年 4 月 15 日所實施之新制，已限制每一個人至多只能持有 10 個門號，若在施行前已經持有超過限制數量的門號不受影響，然不能再申請新門號。

4. 總檢察署

1.詐騙仍是新加坡的一個主要問題。新加坡政府近年來制訂一系列法令用於打擊詐欺犯罪。

2.首先，就非法濫用行動電話 SIM 卡（含 e-SIM 卡）部分，依照新加坡現行法律規定，警方須證明犯罪嫌疑人有幫助他人使用自己名下 SIM 卡用於犯罪，若犯罪嫌疑人抗辯無幫助的不法意圖或故意，警方通常難以證明也不易控告此類濫用或不負責任的犯罪嫌疑人。新加坡於 113 年 3 月通過《執法和其他事項法案》（ Law Enforcement and Other Matters Bill）修正案，訂於 6 個月後開始施用[6]。本法案在 西元 1906 年《雜項犯罪（公共秩序和滋擾）法》(Miscellaneous Offences (Public Order and Nuisance) Act）中，第 6 部分之後插入一「第 6A 部分與濫用 SIM 卡有關的罪行（OFFENCES RELATING TO MISUSE OF SIM CARDS）」。本法案主要為防止不法份子濫用本地 SIM 卡(即在新加坡行動服

[6] https://sso.agc.gov.sg/Bills-Supp/14-2024/Published/20240307?DocDate=20240307

務提供者註冊的 SIM 卡，包括 e-SIM 卡）進行犯罪活動，以及採取措施防止 SIM 卡及個人資料遭濫用。新法賦予警察更多的權力，採取更嚴厲的措施打擊濫用 SIM 卡行為，本法案新增規定三種犯罪行為如下：

I.不負責任的 SIM 卡登記者（ Irresponsible Registration of Local SIM Cards）

民眾將登記自己個人資料的 SIM 卡交給他人，或允許他人使用其個人資料登記本地 SIM 卡，且符合下列情形之一者，即推定（presumed）實施或協助犯罪：

A.出於任何利益而交付 SIM 卡

B.未採取合理措施（reasonable steps）查明 SIM 卡收受者的身分、實際位置或其他詳細資料

C.未採取合理措施查明 SIM 卡收受者目的或其他詳細資料

例如，將自己的個人資料交給陌生人以註冊 SIM 卡，或出售以自己的個人資料註冊的 SIM 卡以換取金錢，均推定為實施或協助犯罪。

此類犯行將被處以最高 10,000 新幣罰金或最高三年有期徒刑，或兩者併罰。

但如果民眾有正當理由（legitimate reason）將其本地 SIM 卡或其個人資訊交給他人，則該人將不承擔犯罪責任。例如，代表家庭成員註冊 SIM 卡後交付家庭成員使用。

II.交易 SIM 卡的中間人（Middlemen Who Deal in Local SIM Cards）

無正當理由收受、提供或持有（Receive, supply or possess）他人名義或未經註冊的 SIM 卡，且符合下列情形之一者，即推定（presumed）實施或協助犯罪：

A.持有 11 張以上 SIM 卡；

B.所持 SIM 卡被用於犯罪；

C.若本地 SIM 卡已登記在他人的資料中，且有下列情形之一者：

i.為取得任何利益而接收或提供 SIM 卡

ii.在提供 SIM 卡時未採取合理措施查明 SIM 卡接收者的身分和實際位置

iii.在提供 SIM 卡時未採取合理措施查明收件人取得 SIM 卡的目的

例如：擁有 11 張或以上非以本人資料註冊的 SIM 卡（包括未註冊的 SIM 卡），或在電子商務網站平台上，出售以他人資料登記的 SIM 卡，以供他人使用。

此外，本法案還規定，在無需證明該人的犯罪意圖的情況下，購買、出售或租賃（buy, sell or rent）以他人個人資訊註冊的本地 SIM 卡均屬犯罪行為。

但若有正當理由收受、提供或持有他人名義或未經註冊的 SIM 卡，則該人將不承擔犯罪責任。例如雇主持有供員工使用的 SIM 卡。

III.不良零售商（Errant Retailers）

行動服務提供者或零售商（mobile service provider or retailer）在未經本人授權的情況下，使用該人的個人資料註冊本地 SIM 卡，或明知該個人資料是虛偽假，且符合下列情形之一者，即構成犯罪：

A.該行動服務提供者或零售商知道或有合理理由相信 SIM 卡將用於實施或協助犯罪，或造成他人不當收益或致他人損害。

B.SIM 卡已被證明隨後被用於實施或協助犯罪，或造成他人不當收益或致他人損害。

例如，明知 SIM 卡會被用於詐騙，但零售商卻在本人不知情的情況下使用該人的個人資料來註冊 SIM 卡。

上述（二）、（三）類型犯罪行為將處以最高 10,000 新幣的罰金或最高三年有期徒刑，或兩者併罰。對於第二次或後續違規之累犯，將處以最高 20,000 新幣罰金或最高五年有期徒刑，或兩者併罰。

上述三種新制訂的犯罪行為亦適用於公司和非法人團體，例如合夥企業和社團。由於這些實體不會被判處監禁，因此對這些實體的最高罰金將是個人罰金的兩倍。

3.《執法和其他事項法案》6A 於 113 年所增訂推定犯罪條款，大幅降低檢察官的舉證責任，檢警不用再去證明犯罪嫌疑人是否具有知悉或幫助他人犯罪之主觀犯意。新加坡總檢察署檢察官表示，該法案立法目的係分析新加坡電信詐欺犯罪統計數據，發現絕大多數電信詐欺犯罪所使用的 SIM 卡，均係來自上開「不負責任的 SIM 卡登記者」，而民眾若收受、提供或持有 SIM 卡數量超過 11 張（含），亦多係與電信詐欺犯罪有所關連，另外，過去該國對零售商僅能課處罰鍰，新法對公司或非法人團體之負責人、員工亦納為行為主體，並對法人或非法人團體課予兩倍罰金，將有助降低濫用 SIM 卡行為。

4. 又隨著科技發展，新型態支付服務應用不斷推陳出新，也增加了交易風險與威脅，有鑑於此，新加坡於 108 年 1 月 14 日通過《支付服務法》（Payment Service Act）[7]，於 109 年 1 月 28 日生效，擴大監管範圍，將虛擬貨幣交易所及電子錢包等支付服務提供商納入法規監管，由「金融管理局」（Monetary Authority of Singapore，MAS，下稱金管局）擔任支付服務提供商（payment service provider）的註冊及監管。金管局於 113 年 4 月 2 日發布新聞稿表示，該局將擴大對付款服務活動的管制，修訂支付服務法及相關附屬條規，要求「數位付款代幣」（digital payment token，簡稱 DPT）服務商應遵循反洗錢、打擊恐怖主義融資、用戶保護與金融穩定等相關規定。相關修訂將自本年 4 月 4 日起生效，欲繼續從事相關服務的商家，須在 30 天內（自 4 月 4 日起）通知金管局，並在 6 個月內提交執照申請書，以及業務活動皆遵守反洗黑錢及打擊恐怖主義融資等要求的鑑證報告，報告須由合格的外部審計師在 113 年 4 月 4 日起的 9 個月

[7] https://sso.agc.gov.sg/Acts-Supp/2-2019/Published/20190220?DocDate=20190220&ProvIds=P12-#pr5-

內完成。對於無法滿足要求的商家，在修訂法生效時就必須停止提供服務[8]。

5.支付服務法包括兩種監管框架

I.指定制度（designation regime）

指金管局基於確保金融穩定及市場效率，可指定支付系統或服務業者加入，避免單一支付服務提供商壟斷市場，以降低產業創新和競爭阻礙。

II.許可證制度（licensing regime）

指將帳戶發行服務（account issuance service）、國內匯款服務（domestic money transfer service）、跨境匯款服務（cross-border money transfer service）、數位支付型代幣服務（digital payment token service）、電子貨幣發行服務（e-money issuance service）、商業收購服務（merchant acquisition service）等七種支付業務納入監管範圍。支付服務提供商依其提供之支付服務類型、交易金額總值，向金管局申請並取得許可證。

6.支付服務法第 6 條規定，許可證制度分為三類

I.貨幣兌換許可證（a money-changing licence），

僅限提供貨幣兌換服務。

II.標準支付機構許可證（a standard payment institution licence），

可以提供一種或多種前述七種支付業務

III.大型支付機構許可證（a major payment institution licence），符合以下條件，應申請大型支付機構許可證：（1）僅提供一項交付服務，月平均交易金額超過 300 萬新幣或等值外幣；提供二項或多項支付服務，月平均交易金額超過 600 萬新幣或等值外幣機構。（2）提供電子貨幣帳戶發行服務，日平均電子貨幣帳戶餘額超過 500 萬新幣或等值外幣。（3）提供電子貨幣發行服務，日平均發行電子幣總價值超過 500 萬新幣或等值外幣的機構。

金管局並要求支付服務提供商皆須遵守防制洗錢及打擊資恐相關規定，防止支付服務被用於任何非法活動，例如：用戶須

[8] https://www.roc-taiwan.org/sg/post/42770.html

經認證、資料加密及預防伺服器遭受攻擊等，並透過信託等方式保障客戶款項免受損失。

7.支付服務提供商須符合法規要求才能在新加坡營運。依據支付服務法第 5 條，未經許可在新加坡提供任何類型支付服務的業務者，個人部分將被處以最高 12 萬 5,000 元新幣罰金、或最高三年以下有期徒刑，或兩者併罰；對於第二次或後續違規之累犯，按日科處 1 萬 2500 新幣罰金。對於法人或其他團體，處以最高 25 萬新幣罰金；對於第二次或後續違規之累犯，按日科處 2 萬 5000 新幣罰金。同法第 9 條並禁止未取得許可證之支付服務業者在新加坡從事招攬行為，違反者個人部分將被處以最高 12 萬 5,000 元新幣罰金、或最高三年以下有期徒刑，或兩者併罰；對於第二次或後續違規之累犯，按日科處 1 萬 2500 新幣罰金。對於法人或其他團體，處以最高 25 萬新幣罰金；對於第二次或後續違規之累犯，按日科處 2 萬 5000 新幣罰金。

8.《貪腐、毒品販毒及其他嚴重犯行》（Corruption, Drug Trafficking and Other Serious Crimes (Confiscation of Benefits) Act 1992, CDSA）新法介紹

新加坡檢察官過去在偵辦詐欺集團 money mules（我國俗稱為車手），面臨主觀犯意舉證之困難，導致許多被告無法成功起訴與定罪，國會在 112 年 5 月 9 日三讀通過 CDSA 修正案（113 年 2 月 8 日施行），其中包含增訂過失及魯莽的洗錢犯罪（Negligent and Rash Money Laundering）以及增訂第 55A 條舉證責任之具體犯罪態樣。

第 55A 條是透過法律的假設，在符合本條 4 種法定要件之事實證明時，將證明缺乏犯罪意圖的責任歸於被告。而此 4 種要件包含:1. 所處理的財產與已知收入來源顯不相當；2、允許他人存取、操作或控制支付帳戶，但沒有採取合理措施查明其使用目的；3、使用自己的支付帳戶接收或轉帳資金，但未能採取合理措施查明資金來源或去向；4、從另一個人或多個人處收受金錢或向他人轉賬，但未能採取合理措施查明該人的身分和實際所在位置。

在檢察官證明 CDSA 第 55A 條規定的 4 項要件之一後，除非被告能夠證明缺乏犯罪意圖，否則犯罪成立。違反第 55A 條犯罪之法定刑為 3 年以下有期徒刑或科或併科新幣 5 萬以下罰金。

另外值得注意者是，此處所規範的並非僅限於金融帳戶，而是包含 108 年 Payment Service Act 第 2(1)條定義內的「payment account」，依照之前新加坡的說明，虛擬通貨帳號等具有支付性質的工具，均涵蓋在內。

9.新加坡對於從事虛擬貨幣等匯兌服務業務，自 108 年後即以支付服務法規範，須取得金管局之許可證，違者即依支付服務法處罰。而且取得許可證的門檻嚴格，至少要辦理公司登記然後依規定檢附會計師審計報告、法遵聲明等文件提出申請，自然人無法取得許可證。

10.新加坡依前述新制定「執法和其他事項法案」中之「第 6A 部分與濫用 SIM 卡有關的罪行」，將針對提供外籍人士離境後所遺留之電話門號（即外勞卡）之行為人進行處罰，然目前並無針對外勞卡、國外電信公司在本國境內發行之國際漫遊門號（即黑莓卡）有何詐欺案發生前之前期行政管制措施。由此觀之，我國為降低電信詐騙案件發生，要求主管機關通傳會研擬相關外勞卡、黑莓卡管制措施，遠較新加坡為先。

肆、心得及建議

一、我國與新加坡之重要產業類型及產業發展政策有顯著差異，新加坡採取對重要研發成果，在法律政策採取較為寬鬆之保護及保密方式，吸引外國企業及人才進入，從我國產業之國際競爭力角度觀察，應不適合逕予採用。況竊取營業秘密行為刑事責任化為國際趨勢，我國在營業秘密及研發成果保護政策上，更不宜貿然採行與國際趨勢相背之政策。

二、新加坡政府就國內及國外專利申請部分，所採取之國安審查政策，為我國所欠缺。衡諸此類制度係以保護國家安全及民眾利益為基礎，就專利申請涉及不宜公開之國家安全或產業技術資訊，列入專利准否之考量，應有參考價值。至於專利申請因國安理由而不予准許情況，應否採行相關補償措施，則仍有進一步研求餘地。

三、有關透過網際網路交易輸入侵害商標權商品，透過網際網路經營拍賣購物網站，陳列販賣侵害商標權商品，或以侵害他人著作財產權圖片經營網拍網站之輕微商標法及著作權法犯罪，甚至著作財產權團體追訴小本經營之商家於店內播放未經授權之影音之惡性非鉅案件，近年有不少權利人透過大量提告刑事責任方式，對犯罪嫌疑對象施加支付和解金壓力，造成大量刑事案件湧入司法系統，成為司法系統被海量刑事案件癱瘓原因之一。新加坡政府對此類非組織性之微罪智財案件，採取權利人自行委任律師蒐證及撰寫起訴狀，並由檢察官審查認情節程度應採刑事追訴者，准許權利人自行委任律師向法院提起刑事訴訟，可視作「經檢察官審查之自訴程序」。此類制度屬於將小規模私人智財權侵害案件，由權利人自行負擔追訴成本，避免權利人大量利用公權利實現自己權利卻無需繳付任何費用之情況，應可有效減輕大量智財微罪案件壅塞司法體系之困境，我國應有借鏡相關法制之空間。

四、我國現正面臨有效將詐欺集團定罪之困境，對於詐欺集團刻意製造斷點，而使用主觀犯意作為抗辯之困境，一直力求透過修法來突破困境，新加坡 Law Enforcement and Other Matters Bill 及 CDSA 新法極具參考價值，透過立法假設的方式，對於符合特定客觀不法態樣的行為，透過立法方式將主觀犯意的舉證責任轉換於被告，由被告對於自己缺乏犯罪意圖負舉證責任，應可有效提升此部分之定罪率，並提高民眾對於個人帳戶、SIM 卡使用以及交易行為之注意義務，實具參考價值。

五、除上述 112 年、113 年增訂或修訂之法律外，新加坡在《刑法》（Penal Code 1871）第 420 條、CDSA 第 51 條亦分別訂有詐欺罪（最高判處 10 年以下有期徒刑）、洗錢罪（最高判處有期徒刑 10 年以下，或 50 萬新幣以下罰金，或兩者併罰）。因此，對於新興科技犯罪，諸如利用虛擬貨幣、利用 apple store 點數進行詐欺、洗錢，新加坡政府均已有相關之規範，值得我國借鏡及參考。