

出國報告(出國類別:進修)

金融情報中心之法制與實務運作

服務機關:彰化地方檢察署

姓名:陳詠薇

派赴國家:美國

出國期間:民國 111 年 8 月 3 日

至 112 年 8 月 2 日

報告日期:民國 112 年 11 月 1 日

摘要

現今金融犯罪手法不斷推陳出新，如何面對此情景，有效順應局勢，甚至站在時代前方率先一步蒐集相關金融情資，成為打擊金融犯罪之基本要務。本文以美國法制為主，細繹美國法制系統以及國際金融情報組織下之各個金融情報蒐集網。期望能藉由此讓讀者，對於美國金融情報蒐集中心能有初步架構式了解與掌握。筆者更進一步舉出該等政府機構具體運作或案件，希望能讓讀者對於美國金融情報中心體制，以及其等實務運作上效果，能有更清楚的理解。筆者亦期盼上開分析研究方法，能對我國未來立法或修法上，產生有裨於我國打擊金融犯罪之效能。

目錄

壹、	研究目的及過程-----	1
貳、	概說經濟犯罪-----	1
參、	美國金融情報中心機構-----	3
肆、	美國實務運作-----	11
伍、	心得與建議-----	19

壹、 研究目的及過程

所謂得先機者，得天下，現今政府在不論在監管或是追究刑責上，動輒得咎，主要原因除礙於現行法規範不足以因應目前時勢所需之外，另一原因即為欠乏足夠情報資訊蒐集網。從而，如何藉由外國比較法研究，以彌補我國所欠乏者，並仿效外國機構發揮正常運作效能，實為我國現今迫切所需。筆者希望能從分析美國之金融情報中心之方式，詳述其等政府機構、國際組織所扮演之腳色，並深而探究此些機構實務上運作效果。希望本文能略對我國產生「他山之石，得以攻錯」之俾益。

貳、 概說經濟犯罪

經濟犯罪是指以非法手段獲取經濟利益，損害公私財產、經濟秩序的犯罪行為。經濟犯罪的類型繁多，根據犯罪行為的具體特徵，可以分為以下幾類¹²：

(1) 詐欺類經濟犯罪：是指以欺騙手段非法獲取他人財物的犯罪行為。

常見的詐欺類經濟犯罪包括冒貸詐欺、投資詐欺、破產詐欺、票據

¹Bruce L. Benson, DeVoe Moore and Distinguished Research Professor of Economics, Economics Department Chair and Courtesy Professor of Law, Florida State University, US and Paul R. Zimmerman, Economist in Antitrust I, United States Federal Trade Commission, Handbook on the Economics of Crime, Publication Date: 2010, ISBN: 978 1 84720 954 2
<https://www.e-elgar.com/shop/gbp/handbook-on-the-economics-of-crime-9781847209542.html>

² 許永欽，經濟犯罪實務，2008年5月1日。

詐欺、保險詐欺等。

(2)侵占類經濟犯罪：是指違反國家規定，侵吞公私財物的犯罪行為。

此類經濟犯罪包括公務侵占、業務侵占、挪用公款、挪用資金等。

(3)重利類經濟犯罪：是指以高利放貸為目的，違反國家規定，收取高額利息的犯罪行為。

(4)走私類經濟犯罪：是指違反國家規定，逃避海關監管，非法進出口貨物的犯罪行為。

(5)偽造類經濟犯罪：是指偽造、變造貨幣、有價證券、稅票、會計憑證等，以非法牟利為目的的犯罪行為。

(6)電腦類經濟犯罪：是指利用電腦技術，侵犯他人財產權益，危害社會經濟秩序的犯罪行為。常見的電腦類經濟犯罪包括網路詐騙、網路盜竊、網路勒索等。

(7)其他經濟犯罪：除了上述類型之外，還包括違反證券交易法、違反稅捐稽徵法、違反銀行法、違反公平交易法、違反期貨交易法等，違反管理外匯條例、危害經濟秩序等的犯罪行為。

經濟犯罪的對於社會之危害性不言可喻，不僅會造成個體經濟損失，還會破壞整體經濟秩序，影響社會安定。因此，如何完善法律法規，加強對經濟犯罪的打擊力度，同時並健全金融監管體系，防範金融風險乃是維護社稷的重要工作。

參、美國金融情報中心機構

美國有許多政府機構單位負責蒐集不法經濟金融活動情資。以下分述之：

一、Financial Crimes Enforcement Network(簡稱 FinCEN)³

通常被稱為「金融犯罪執法網絡」或「金融犯罪執法網」。FinCEN 是美國財政部的一個部門，負責收集、分析和傳播金融情報以支援執法和國家安全。FinCEN 可收到來自金融機構和其他受監管實體的可疑活動報告。所謂可疑活動是指任何可能與洗錢、恐怖主義或其他金融犯罪有關的交易或活動的報告⁴。FinCEN 也向執法機構和其他政府實體傳遞金融情報。這些情報可用於調查金融犯罪、破壞資金流向犯罪分子、保護國家安全。所以 FinCEN 是美國打擊金融犯罪和恐怖主義努力的重要政府機構。它旨在保護美國金融體系和美國人民金融交易安全⁵。另外，此特別提及，國際間也有類似 FinCEN 之組織，此即是 Financial Intelligence Units (FIU)，中文常譯為「國家金融情報中心」，負責收集、分析並向

³ 相關資訊可查 FinCEN 官網 <https://www.fincen.gov/>

⁴ 2023 年 1 月 18 日該機構直接於官網上發布新聞稿：FinCEN 認定虛擬貨幣交易所 Bitzlato，涉及參與俄羅斯非法金融的“主要洗錢問題”。參見官網 <https://www.fincen.gov/news/news-releases/fincen-identifies-virtual-currency-exchange-bitzlato-primary-money-laundering>

⁵ 我國行政院洗錢防制辦公室亦在官網敘明 FinCen 之建議與指引。參網站 <https://www.amlo.moj.gov.tw/1461/30914/30921/Lpsimplelist>

執法部門和其他主管機關傳達(disseminate)有關可疑(suspicious)金融交易的資訊。他們在打擊洗錢(money laundering)、恐怖主義資金(terrorist financing)和其他非法金融活動(other illicit financial activities)方面發揮著至關重要的作用。大多數國家都有一個國家金融情報中心(FIU)，該機構負責監督其境內的洗錢行為，並與國際上的類似組織共用相關不法金融情報。160 多國之國家金融情報中心組成了國家金融情報中心埃格蒙特小組(Egmont Group)，這是一個於 1995 年成立的國際組織，旨在為傳播最新的反洗錢和反恐融資業務、相關數據和見解提供一個論壇。該小組成員努力執行聯合國安理會、金融行動特別工作組 FATF (Financial Action Task Force on Money Laundering) 和 G20 財長的 AML(Anti-Money Laundering Program)和 CFT(Combating the financing of terrorism)相關決議。埃格蒙特小組作為一個國際組織，埃格蒙特小組認為其主要作用是分享資訊，防止洗錢和恐怖主義的擴散，並確保國家金融情報中心遵守反洗錢和反恐融資的國際標準。它促進金融情報機構之間的國際合作，提供「一個安全交流專業知識和金融情報的平臺，以打擊洗錢和恐怖主義融資」。

二、 Law enforcement agencies 執法政府機構

此處包含警察機關、FBI(the Federal Bureau of Investigation，中文多譯為聯邦調查局)⁶、United States Attorney(聯邦檢察官)⁷、CIA⁸(Central Intelligence Agency，中文多譯為中央情報局等)。CIA 雖然其主要工作目的是針對國外政府、公司、政治、文化、科技等方面的情報，並調查其他國內情報機構的活動，再把此些情報彙整並分享予美國政府其他部門，但筆者仍將其列為重大經濟犯罪之情報蒐集機構之一。主要原因是因為 CIA 現任局長 William Burns 曾受訪表示，CIA 內部早在前任局長在位時就啟動數個加密貨幣⁹「研究項目」，旨在打擊勒索軟體採用加密貨幣作為贖金)，CIA 類同上述其他機構均有針對非法經濟行為之刑事偵查權限，並與國家金融情報中心(FIU)密切合作，並聯合追溯並打擊經濟罪犯。

三、Regulatory agencies 監管機構

包括 Securities and Exchange Commission (SEC，中文常譯為美國證券交易委員會) 和 the Commodity Futures Trading

⁶ FBI 是美國司法部下之其一調查機構。組織架構圖請參照該網頁之 All Components and Agencies 圖，網址 <https://www.justice.gov/about>。

⁷ 美國另外有代表州政府之檢察官(District Attorney，簡稱：DA)，泛指在美國各州之司法轄區內，代表州政府提出刑事訴訟。

⁸ 相關資料介紹請參考，官網 <https://www.cia.gov>。

⁹ 英文常稱為「cryptocurrency」，亦有「digital currency」稱呼之。但考量 digital currency，亦可以指一切以電子訊號形式存在並作為支付工具之貨幣，例如：遊戲公司所設計以購買電腦遊戲中寶物之金幣，或是現行之比特幣等，digital currency 與加密貨幣之共同點，是同樣不具備有形之方式存在，但是加密貨幣重要特徵在於，它是一種使用密碼學原理來確保交易安全及控虛擬資產個去中心化的加密貨幣，之後加密貨幣一詞多指此類設計。

Commission (CFTC，中文常譯為美國商品期貨交易委員會)，二者均是負責監管金融市場以及防範經濟詐欺。同樣地，他們也是具備調查不法經濟活動之權限。

四、 Tax authorities 稅務機構

例如 the Internal Revenue Service (IRS，中文常譯為”美國國家稅務局”，此處以 IRS 代稱之)¹⁰，負責稅務課徵並且進行強制執行稅務債權。為了有效達到執行目標，IRS 亦可進行相關可疑經濟活動之調查(例如疑似逃漏稅、洗錢等)。

五、 消費者金融保護局(The Consumer Financial Protection Bureau，通常簡稱為 CFPB)¹¹

CFPB 是一個獨立政府機構負責金融領域中之消費者保護。CFPB 是依據因應 2008 年金融風暴危機而生之 Dodd-Frank Wall Street Reform And Consumer Protection Act 法案¹²而建置之獨立機構。在 2007 年之前，由於美國寬鬆的金融監管制度導致了極度危險的貸款行為，而此房地產行業的泡沫，最終如蝴蝶效應般造成了全球危機，產生了對金融機構的公共救助需求以及全球金融衰退。The Dodd-Frank Wall Street Reform and Consumer

¹⁰ 因為美國採聯邦、州政府雙重稅制，所以若有符合州政府稅制情形下，州政府亦可課徵徵稅。

¹¹ 相關資料請參考官網 <https://www.consumerfinance.gov/language/zh/>。

¹² 相關資料請參考網址 <https://www.investopedia.com/terms/d/dodd-frank-financial-regulatory-reform-bill.asp>。

Protection Act 是在歐巴馬(Obama)政府時期於 2010 年所通過之大規模立法。CFPB 所負責業務內容主要為是防止掠奪性抵押貸款(predatory mortgage lending)，並幫助消費者在同意抵押貸款之前瞭解抵押貸款的條款。這反映了人們普遍認為次級抵押貸款市場(subprime mortgage)是 2007-2008 年災難的根本原因。CFPB 喝止(deter)抵押貸款經紀人(mortgage brokers)以更高的費用或更高的利率放貸來賺取更高的佣金。它要求抵押貸款者(mortgage originators)¹³不得引導潛在借款人(potential borrowers)去借貸將導致該抵押貸款者獲得最高總付款金額的貸款。CFPB 還管理其他類型的消費貸款(consumer lending)，包括信用卡(credit cards)和簽帳卡(debit cards)，並處理消費者投訴(consumer complaints)。CFPB 要求貸款人(lenders)（不包括汽車貸款人 automobile lenders），須以消費者易於閱讀和理解的形式披露資訊。例如，在信用卡申請的簡化條款(the simplified terms now on credit card applications.)。在 CFPB 官網上，可發現其為了服務廣大美國移民民眾，有數種語言建置，例如西班牙文、中文、韓文、俄語等。CFBP 的執法辦公室(The Bureau's Office of Enforcement)有權在根據聯邦消費

¹³ https://www.investopedia.com/terms/m/mortgage_originator.asp

者金融法(Federal consumer financial law)在司法或行政裁決程序之前進行調查(conduct investigations)。消費者金融保護法(Consumer Financial Protection Act)亦授權 CFPB 去調查潛在的違法行為，並發出稱為民事調查要求 (CID, civil investigative demands) 的調查傳票 (investigational subpoenas)。一份有效 CID，是可以提出傳喚要求、要求提出文件、電子郵件、報告書、對於書面問題之回覆，和口頭之證詞 (demand, documents, emails, reports, answers to written questions, and oral testimony)。收到上開 CID 者，可以要求 (petition)、修改(modify demands)或撤銷請求(set aside demands)。但是若 CID 接收者(recipient)未能遵守 CID，所謂不合規行為(non-compliance)包括未能對 CID 做出全面回應以及未能在規定的期限內做出回應。該局可以向聯邦地區法院提交請求以執行該 CID。另在 CFPB 官網上，其亦告知民眾若覺遭受欺詐，可以向當地的員警或警長辦公室提出報告、或聯繫民眾所在州之州檢察長。假設受害者是一名老年人或殘疾人，尚可聯繫當地的成人保護服務機構。或是透過網上的老年人護理搜尋系統，或致電聯繫各州負責接收和調查涉嫌老年人財務剝削的舉報之機構。另外，若有關欺詐、騙局或財務剝削的受害者，亦可另向聯邦貿

易委員會 (Federal Trade Commission) 提出投訴。另外官網上亦說明若美國民眾致電予(855) 411-2372，美國民眾可以選擇中文等其他語言，總共多達180種語言服務。另外，其官網亦說明必要時會和其他調查機構共享民眾之檢舉報告資訊。

六、國際機構 International organizations

以 Financial Action Task Force (FATF，中文常譯為防制洗錢金融行動工作組織) 和 the United Nations Office on Drugs and Crime (UNODC，中文常譯為聯合國毒品和犯罪問題辦公室) 為例，因為美國是上開國際組織會員國，所以常以國際規模型式聯合各國共同打擊經濟犯罪。這些國際組織也提供訓練跟技術上協助給需要國家，俾以提升並實施國際打擊非法經濟行為之標準¹⁴。同前所述¹⁵，各國內有 FIU 負責監督、收集、分析國內之可疑金融交易資訊(特別是涉及洗錢、反恐等不法資訊)，並與埃格蒙特小組(Egmont Group)國際組織，分享上開不法訊息、數據，以確保國際間金融情報機構合作，資訊互通有無，以達致有效喝阻跨國洗錢和恐怖主義融資。

七、學術機構 Academic institutions

¹⁴ 根據政府間機構金融行動特別工作組 (FATF) 的說法，其建議說明指出，各國應建立金融情報機構，作為接收和分析可疑交易報告的中央收集點。此外，金融情報機構應收集「與洗錢、相關上游犯罪和恐怖主義融資相關的其他信息，並用於傳播分析結果」。

¹⁵ 參照參、一、

例如哈佛大學商學院在其頗具聲望之期刊(Harvard Business Review)常發表對於最新時事或經濟評論報導。在 2021 年 11、12 月份時，其發表一篇” Case Study: Should We Embrace Crypto?”，其內容頗引人省思¹⁶。政府情報蒐集單位可利用此些學術單位之觀察或實驗結果，去預先設想未來可能之新型態之犯罪模式，並從中先掌握先機。在此引用一篇美國聯邦儲備委員會(以下簡稱「美聯儲」)的研究報告¹⁷:「在早期，用大面額的美元支付是毒販最喜歡的支付方式。目前世界上所有美元現金中，100 美元面值的鈔票占現金總量的 80%，而日常生活中使用百元現鈔的人並不多，甚至連美聯儲都不知道這些錢流通到了哪裡。90 年代，美聯儲主席艾倫·格林斯潘專門成立了一個小隊，調查百元面值美金的去向。領隊的大姐叫露絲·賈德森，她花了幾年時間，帶著幾個特工滿世界尋找大額美鈔，但是效率太低。恰好，這個小隊裡有個組員是學生物出身的，他想起以前人們估算魚群數量的方法。這個方法是，先在湖裡抓 100 條魚，全部塗上標記之後放回湖裡，然後再隨機撈 100 條魚，看看帶標記的魚有多少。這

¹⁶ Charles C.Y. Wang, Case Study: Should We Embrace Crypto?, Harvard Business Review, Nov 2021。

<https://hbr.org/2021/11/case-study-should-we-embrace-crypto>

<https://www.hbrtaiwan.com/case-study/20700/should-we-embrace-crypto>

¹⁷Banegas, Ayelen, Ruth Judson, Charles Sims, and Viktors Stebunovs (2015). International Dollar Flows. International Finance Discussion Papers 1144.

<https://www.federalreserve.gov/econresdata/ifdp/2015/files/ifdp1144.pdf>

樣反覆統計幾次之後，就能大概知道帶標記的魚在捕撈上來的100條魚中的占比，也就能算出湖裡有多少魚了。於是，這個小隊在美元現鈔發行之後，利用技術手段追蹤其流向，他們發現竟然有2/3的百元美鈔流向海外，而海外銀行和換匯機構只保有其中極少的一部分，大部分百元美鈔成為地下交易的仲介。畢竟100萬美元的現鈔不並重，成年男子能憑一隻手就提起，且另一隻手還能拿槍，很符合電影中美國黑幫形象。筆者以為除反思過去偵查作為之外，精進學術技能，或可能如該小組成員般利用學術研究方法在未來犯罪偵防上發生意想不到之效果。

肆、美國實務運作

一、「加密貨幣¹⁸交易所之創始人認罪(plea guilty)違反銀行保密法」案：

依據紐約南區美國聯邦檢察官在官網上所發布之新聞稿¹⁹：據稱是“離岸”(off-shore)加密貨幣交易所或“BitMEX”的創始人和高階管理人 Arthur Hayes、BENJAMIN DELO 均承認違反【銀行保密法】(Bank Secrecy Act “BSA”)，故意未能在 BitMEX 建立、實施和維

¹⁸ 參註釋9關於加密貨幣解說。此處之所以翻譯為加密貨幣交易所，係因為其販賣之主要商品係以加密貨幣或是以加密貨幣進行之金融商品為主。

¹⁹ U.S. Attorney's Office, Southern District of New York, Feb 24, 2022
<https://www.justice.gov/usao-sdny/pr/founders-cryptocurrency-exchange-plead-guilty-bank-secrecy-act-violations>

護反洗錢（“AML”）計劃。根據其等各自認罪協議的條款，他們分別同意支付 10 萬美元的刑事罰款，代表犯罪各自所得的金錢收益，他們並已在美國完成認罪（其等所遭控訴之罪名苟若成立，最高可處 5 年有期徒刑監禁）。該案之聯邦檢察官，並在公開發布之新聞稿中，讚揚了聯邦調查局紐約洗錢調查小組的出色調查工作，並感謝商品期貨交易委員會的律師和調查人員，由於他們的專業知識和勤勉不懈完成了該份出色調查任務。本案由該辦公室的洗錢和跨國犯罪企業股處理起訴。另有美國助理檢察官 Jessica Greenwood、Samuel Raymond 和 Thane Rehn 一起偕同負責起訴。（The prosecution is being handled by the Office’ s Money Laundering and Transnational Criminal Enterprises Unit. Assistant U.S. Attorneys Jessica Greenwood, Samuel Raymond, and Thane Rehn are in charge of the prosecution.）。

二、司法部刑事部成立國家加密貨幣執法小組（NCET）²⁰：

國家加密貨幣執法小組（NCET）係隸屬於司法部刑事部門²¹²²。根

²⁰ US. Department of Justice, Office of Public Affairs , 06 Oct, 2021
<https://www.justice.gov/opa/pr/deputy-attorney-general-lisa-o-monaco-announces-national-cryptocurrency-enforcement-team>

²¹ 參司法部 DOJ organization chart, <https://www.justice.gov/agencies/chart/map>

²² NECT 之頂頭上司為負責刑事司的司法部助理部長 Kenneth Polite。刑事部門制定、執行和監督所有聯邦刑法的適用，但專門分配給其他部門的法律除外。該部門和 93 名美國檢察官負責監督刑事案件以及某些民事訴訟。刑事部門檢察官起訴了許多全國性重大案件。另外，除直接擔任訴訟職責外，該單位還制定和實施刑事執法政策，並就刑事事項提供建議和協助。例如參

據司法部官網 2022 年 2 月 17 日發布，嗣後再於 2023 年 8 月 14 日更新之新聞稿，可知因現今虛擬資產²³和分散式帳本技術的迅速創新，犯罪分子非法使用它們該等技術之情形大增。因為虛擬資產與分散式帳本之匿名性與迅速交易特性，犯罪者遂利用之以遂行網路攻擊(cyberattacks)、勒索(ransomware)、網路販運毒品之支付工具(traffic in narcotics)、駭客工具(hacking tools)、或進行竊盜和詐騙等犯罪態樣。而 NCET 的成立就是為了確保美國政府能應上開犯罪濫用所帶來的挑戰。該委員會之組成中之檢察官²⁴們不乏具有加密貨幣、網路犯罪、洗錢和沒收辦案經驗背景者。另，NCET 亦會負責識別、調查、支援和追蹤涉及虛擬資產犯罪的案件，並特別關注加密貨幣交易、混合服務、基礎設施提供者以及其他導致加密貨幣和相

與證人安全計畫和電子監控的使用、就刑法問題向檢察總長(Attorney General)、國會、管理和預算辦公室以及白宮提供建議；向聯邦檢察官和調查機構提供法律諮詢和協助；並領導協調國際以及聯邦、州和地方執法事務。參見官網 <https://www.justice.gov/criminal/about-criminal-division>

²³ Digital assets, 此處翻譯為虛擬資產，它可以是指企業或個人擁有或控制的，以電子訊號形式存在者。此虛擬資產，是透過電腦編碼而產生之文字內容、圖片或影像等多媒體。具體來說，虛擬資產包括網站及其內容、域名、應用軟體、代碼、電子文件、圖片內容、媒體內容、加密貨幣、NFT、電子郵件、遊戲帳號、帳號及其內容、社群網路帳戶、雲端服務帳戶及資料等。通常，虛擬資產都具備經濟價值，可以以法定貨幣取得之。

²⁴ 根據該份新聞稿，司法部亦言及任命 Eun Young Choi 擔任國家加密貨幣執法小組 (NCET) 的首任主任。該新聞稿中亦提到，Choi 在擔任副總檢察長 Lisa O. Monaco 的高級法律顧問之前，Choi 曾擔任紐約南區的助理美國檢察官，那時她擔任該辦公室的網路犯罪協調員，調查和起訴網路、複雜的欺詐和洗錢犯罪，並特別關注網路入侵、加密貨幣、暗網和國家安全調查。她曾在各種案件中擔任首席檢察官，包括調查一個負責駭客攻擊摩根大通公司和其他十幾家金融公司的跨國組織、Coin.mx（一家未經許可的虛擬貨幣交易所）的運營以及唯一與巴拿馬有關的起訴。此外，她還成功地對第一個暗網市場絲綢之路的創始人兼首席管理員 Ross Ulbricht 提起訴訟。在她職業生涯的早期，她曾擔任美國紐約南區地方法院 Naomi Reice Buchwald 法官和美國第二巡迴上訴法院 Reena Raggi 法官的法律助理。她學業優異，畢業於哈佛大學和哈佛法學院。<https://www.justice.gov/opa/pr/justice-department-announces-first-director-national-cryptocurrency-enforcement-team>

關產品濫用的個人及法人。活動的技術。筆者認為最特別是 NCET 除負起領導國內犯罪調查等事宜，尚負責與國際執法單位、國內主管機關、私人企業之合作協調事宜。NCET 亦會為聯邦、州、地方和國際執法單位提供支援和培訓，以打擊美國和世界各地涉及上開犯罪之不法活動。

NCET 亦整合司法部內所有之調查資源，例如檢察官、國家安全部門、聯邦調查局(Federal Bureau of Investigation，簡稱 FBI)等跨單位之合作。為了應付這波結合電腦犯罪、洗錢、加密貨幣詐騙、販毒等之猛烈攻勢，聯邦調查局亦成立一個 Virtual Asset Exploitation Unit 調查組織，該組織由多位加密貨幣專家組成，專心致力於替聯邦調查局提供分析幣流、相關調查、人員培訓等。

三、CFPB 發佈新公告，分析虛擬資產投訴的增加²⁵

根據 2022 年 11 月 10 日 CFPB 官網新聞公告，「虛擬資產投訴增加-屠豬、以及其他騙局在虛擬資產投訴案中名列前茅 “Pig butchering” and other scams lead list of crypto-asset complaints」。

在上開最新投訴公告中，CFPB 說明已經收到不少與虛擬資產有關的投訴。以往投訴案件，常係欺詐(frauds)、盜竊(theft)、帳戶駭

²⁵ CFPB 官網 <https://www.consumerfinance.gov/about-us/newsroom/cfpb-publishes-new-bulletin-analyzing-rise-in-crypto-asset-complaints/>

客(account hacks)和詐騙(scams)的受害類型。然現在關於虛擬資產，因為消費者在執行交易和在交易所之間轉移資產方面也出現問題。例如平臺故障、身份驗證問題、安全保留或平臺技術問題，許多消費者在使用其帳戶中的資金時遇到了問題。糟糕的客戶服務亦是與此相關之常見投訴。

CFPB 主任 Rohit Chopra 表示:依據我們對消費者投訴的分析，不良行為者正在利用虛擬資產對公眾進行欺詐(bad actors are leveraging crypto-assets to perpetrate fraud on the public)，在虛擬資產方面，美國人也報告了有交易上問題、帳戶凍結和儲蓄損失(Americans are also reporting transaction problems, frozen accounts, and lost savings when it comes to crypto-assets)。人們應該警惕任何尋求虛擬資產預付款的人，因為這可能是一個騙局(People should be wary of anyone seeking upfront payment in crypto-assets, since this may be a scam)。

詐騙者通常以虛擬資產為目標，因為很難確定許多虛擬資產地址背後的人(it can be difficult to determine the person or people behind many crypto-asset addresses)，並且詐騙者使用許多技術來掩飾虛擬資產向其他帳戶的轉移(there are a number of techniques scammers use to obscure the movement of crypto-

assets to other accounts)。這使監管機構和執法部門追蹤被欺詐者竊取的虛擬資產更加耗時。(more time consuming for regulators and law enforcement)

近年來，隨著價格波動和虛擬資產採用的增加，CFPB 收到的關於這些金融產品的投訴也有所增加。從 2018 年 10 月至 2022 年 9 月，CFPB 收到了超過 8,300 份投訴，其中大部分是在過去兩年投訴的。自 2018 年 10 月以來處理的虛擬資產投訴中，約有 40% 的消費者將欺詐和詐騙列為主要問題。另外虛擬資產的各種交易問題約占投訴比的 25%，而資產在未能依照約定使用之爭議約占投訴比 16%。該公告確定了分析虛擬資產投訴的幾個常見風險主題。另外，惡意行為者的駭客攻擊破壞了虛擬資產安全，並導致消費者遭受重大經濟損失，求償無門。

其亦一併在官網中公告羅列了的其他常見風險包括：

1. 浪漫騙局和“屠豬”：虛擬資產通常是浪漫騙局的目標，詐騙者利用受害者的情緒來榨取金錢。一些詐騙者採用「屠豬」技術，欺詐者花時間獲得受害者的信任和感情，以便讓受害者建立虛擬資產帳戶，但騙子最終卻竊取了他們所有的虛擬資產。此外，由於許多虛擬資產平臺缺乏客戶服務選項，攻擊者有機會偽裝成客戶服務代表來訪問客戶的帳戶並竊取虛擬資產。

2. 難以獲得賠償(Difficulty obtaining restitution)：在消費者被騙或帳戶遭駭客入侵的情況下，他們經常被告知無處可求助。此外，該虛擬資產平台和服務提供者往往要求強制仲裁(mandatory arbitration)和限制集體訴訟(limit class action)才能使用其服務。又關於使用服務的重要術語可能隱是藏在條款和條件中，並且很難讓消費者在平臺上找到。

3. 欺詐交易：投訴顯示，一些虛擬資產平台只是在收到客戶的投訴後才採取措施來驗證某人有代表客戶行事的權限，而且通常是在該客戶進行多次升級後才採取措施。例如：一個詐騙者向同一個電子錢包進行數百筆小額交易，就代表施詐術者故意逃避風控措施，以此規避洗錢和欺詐偵查。(suggest scammers may be aware of and purposefully evading controls to prevent money laundering and fraud)。

4. 更高的資產波動性(higher asset volatility)：特別是在最近幾個月，虛擬資產的價值波動明顯大於政府支持的貨幣。一些虛擬資產已經歸零或被交易所凍結。

5. 識別風險(risk of identification)：區塊鏈技術的一些用戶，因為對於區塊鏈技術能力認知不足，所以惡意行為人(malicious actors)可能將虛擬資產交易和電子錢包網址與其他消費者的身分或

其他交易連結起來，以完成”匿名性”之目的。

6. 該份報告並提請消費者亦應該注意某些惡意網站或程式，會詐欺性地暗示其是有經過政府認可或經保險公司保護之虛擬資產。例如：有不肖公司或業者，濫用 Federal Deposit Insurance Corporation(簡稱：FDIC，中文譯為：美國聯邦存款保險公司)的名稱或標章向消費者偽稱其公司之虛擬資產是享有上開聯邦存款保險保障。另外，自2014 年以來，CFPB 一直在處理投訴，並警告消費者有關加密貨幣的風險。

7. 針對經消費者投訴資料庫中發佈之投訴，必須將其發送給該被投訴公司並讓該公司進行回覆。但是，因為許多因加密貨幣遭訴之公司或業者並沒有存在於資料庫中(Consumer Complaint Database)，故該等投訴通常會變成轉介給其他監管機構處理(regulatory agencies)。CFPB 與 FTC Sentinel 會共用投訴，並通過 CFPB 的安全政府門戶將其提供給該政府機構。最後這些投訴也可供 CFPB 工作人員進行審查和分析。

伍、心得與建議

參考上開美國金融情報中心之概述，可知我國對於打擊虛擬資產(特別是加密貨幣)犯罪之法制化密度與專業性之建置仍有所不足。首

先，我國行政院消費者保護會對此常見之虛擬資產交易糾紛(不論是屠豬之感情詐欺或糾紛，或是交易所客戶服務程度不足)，我國之行政院消費者保護會仍未如同 CFPB 主動發布新聞稿，並在網站上詳細羅列可能之糾紛模式。筆者建議，在偵查前端，應由行政院消費者保護會，立於前哨站之腳色，積極呼籲消費者對於虛擬資產相關交易宜多加謹慎。畢竟，不是所有虛擬資產糾紛，都能符合刑事或是民事責任之構成要件，讓消費者能透過法律途徑尋得救濟。又，行政機關有其職能，既然目前我國金融監督管理委員會對於加密貨幣業者，係採取業者自律原則²⁶，則行政機關對於屢屢與客戶端或是用戶端發生交易或使用糾紛之業者，行政院消費者保護會宜仿 CFPB，整理分析上開資料，並於必要時公布周知。另，因為虛擬資產業者，其資產是數位化電磁紀錄，所以筆者可以預見未來某些業者有可能將來連公司實體、客服專線都沒有，所以宜儘早建置數位化公司管理系統，一方面可以有效快速讓我國之消費者保護機關迅速地將民眾投訴轉遞給該業者，另一方面行政機關亦可於此際去辨識該公司的網址或 logo，是否有偽稱假冒經過合法信託或保險之情。

另外，審酌目前地方檢察署多已遭大量詐騙案件瘋狂式轟炸以致於

²⁶ 參虛擬通貨平台及交易業務事業防制洗錢及打擊資恐辦法。

眾多檢察官們疲於應付該等案件，更遑論做好細緻偵查²⁷。針對多變之電腦金融犯罪案件，實難期望其等能針對耗時之”加密貨幣或虛擬資產”經濟犯罪進行高度、精緻性偵查作為。以筆者目前身處之彰化地方檢察署為例，雖然各檢察官有盡量抽空參與關於「加密貨幣犯罪偵查」之研修課程，但上開課程並不是強制性參與。另關於加密貨幣犯罪分案，在筆者任職之彰化地方檢察署而言，則與傳統案件(例如：恐嚇、毀損、傷害等)一同輪分，從而實難期待每位收案者能馬上具備該加密貨幣犯罪之偵查技巧與經驗。就目前利用加密貨幣進行詐欺案件而言，此等詐騙案件態樣之兩大主流分別是：

(1)詐騙集團向被害人詐稱可保證獲利之高額投資，並指定被害人將款項匯給詐騙集團之某車手掌控之銀行帳戶或電子錢包內，該車手再依照上游之指示，將各被害人被騙贓款匯入合法交易所(例如：MAX

²⁷ 第一線之地方檢察署檢察官們須應付例行性案件管考，除此之外，當現今每個月分案案件暴增約以前分案之百分之五十時，偵查能量早已呈現疲狀且難以負荷精緻偵查，並壓縮到其他案件辦案時間。此種現況是全台地檢署共同面臨之困境。參鏡周刊 2024 年 1 月 29 日專題報導「正義的成本 2：法官「我們快要被詐欺案淹沒了」案件暴增不休假也辦不完」之報導，並節錄其中一段【吳承學法官提供我們一份統計，以台北地方法院近 10 年為例，2013 年總案件量為 2 萬 7 千多件，2023 年增至 3 萬 5 千多件，10 年增 3 三成，讓本就過勞的他們，精疲力竭到幾乎難以負荷。其中，詐騙案件增加最多，10 年前 1 年僅 800 多件，2023 年已暴增至 1 年 3 千多件。法官鮑慧忠就說：「我們快要被詐欺案件淹沒了！」法官是後端，司法流程的前端是檢察官，檢察官偵查後決定起訴的案子，才會送到法院。法院案件量驟增，必定代表前端地檢署的案件量更加驚人。以近 5 年的案件量來看，統計資料顯示，2019 年時，全台地檢署一整年的新收案件量約 56 萬多件，到 2023 年，已暴增至 1 年 83 萬多件，短短 5 年，案件量增加了百分之 47。臺南地檢署檢察官蔡佰達的辦公室有一張行軍床，累的時候躺一下。他說話語速快，劈哩啪拉蹦出一堆數字：「以前我剛來臺南，每個月新收到的新案子大概 50 件，現在 80 幾件，例如我上個月新收 85 件，扣掉上個月結案 58 件，等於上個月又多了 17 件『未結案件』，就這樣每個月累積。如果我要讓未結案件量下降，1 個月是不是要結案超過 85 件？那我根本都不用睡覺啊。」案子多到永遠結不完，新案子還不斷像海嘯般湧來。每一件刑案都要先閱讀卷宗，然後思考、調查、開偵查庭，如此反覆蒐證，最後要撰寫不起訴或起訴書。每個月平均要辦八十幾件案子，而一個月就算都不休假也只有三十天，顯然任誰都不可能辦完。】。

網址 <https://www.mirrormedia.mg/story/20240122pol003>

平台、幣安平台)購買 USDT，之後再移轉至上游詐騙集團所指定之其他電子錢包迅速轉幣，以逃避追緝。

(2)詐騙集團車手，直接假裝成合法幣商，同時該集團透過網路方式向被害人稱需向該幣商購幣，並提供給被害人該幣商之聯繫方式，被害人遂依照該集團之指示交付現金或轉帳給該假幣商，之後該假幣商再透過合法交易所迅速轉幣，將不法所得移轉至國外。

不論(1)或(2)，往往該等詐騙集團均是有備而來，甚至準備好一套教戰手冊，一言以蔽之，大都是以：以合法交易來包裝非法詐騙洗錢行為²⁸。更有甚者，因為詐騙集團之金錢實力以及現在律師行業競爭激烈，不少律師已經前仆後繼為詐騙集團在偵查階段進行洩密、串證，其等不僅指導其當事人(亦即檯面上被告)如何趨吉避凶，甚至充當上游(尚未浮出水面之潛在被告)之保護傘²⁹。參現今實務，越來越多車手或是提供帳戶者，經法院派決無罪案件或經地檢署作不起訴，探究上開無罪判決、不起訴書之內容，大都是憑被告提供之對話紀錄³⁰。

然而在對話紀錄生成器³¹於網路上唾手可得之前提下，苟過於偏重該

²⁸ 參臺灣臺中地方檢察署(臺中地檢署)於民國 113 年 4 月 8 日發布之關於「阿福錢包」偵結起訴之新聞稿。<https://www.tcc.moj.gov.tw/295804/295830/657577/1163340/post>

²⁹ 參臺灣臺北地方檢察署(臺北地檢署)新聞稿 113-05-13

<https://www.tpc.moj.gov.tw/media/358910/1130513%E8%87%BA%E5%8C%97%E5%9C%B0%E6%AA%A2%E5%81%B5%E8%BE%A6%E9%84%AD%E5%A7%93%E5%BE%8B%E5%B8%AB%E7%AD%89%E4%BA%BA%E6%B6%89%E7%8A%AF%E6%B4%A9%E5%AF%86%E5%8F%8A%E7%B5%84%E7%B9%94%E7%8A%AF%E7%BD%AA%E6%A1%88%E5%81%B5%E6%9F%A5%E7%B5%82%E7%B5%90%E6%96%B0%E8%81%9E%E7%A8%BF.pdf?mediaDL=true>

³⁰ 參臺灣雲林地方法院 112 年度金訴字第 38 號、第 94 號無罪判決、臺灣桃園地方檢察署 113 年度偵字第 2434 號不起訴處分書、臺中地檢署 113 年度偵字第 16798 號不起訴處分書。

³¹ 如 Fake Line Message Generator 網址 <https://flmg.guychien11.dev/zh-TW>

等對話紀錄之證明力，是否恐有縱放真正詐騙集團車手與提供人頭帳戶者之情？筆者以為，檢察官基於客觀性義務要求，須斟酌所有有利與不利被告之事證並對之調查。有謂者可云：可利用加密貨幣之幣流分析以調查加密貨幣詐欺案件，筆者認為此充其量僅能證明被告與被害人間有轉幣之客觀事實，尚不足以證明被告主觀犯意。故，若欲探求被告主觀認知，尚需輔以其他證據調查³²。為突破被告以假對話紀錄所建築起來之防堵追緝屏障，身為第一線之檢察機關、司法警察，不僅要能掌握時間立即發現幣流詭異之處，並主動發掘其他事證，以釐清被告主觀認知。然棘手的是，此類加密貨幣詐騙案件現今如雪片般激增，又佔各檢察署案件之大宗。甚為可惜的是，往往負責最初偵辦的警察（以筆者目前經驗而言），大都欠缺加密貨幣之基礎常識，以致於在接手辦案時，其等手邊往往僅有被害人指訴之金流、被害人提供之交易明細、被告銀行開戶資料（且大都欠缺被告所申設交易所開戶資料、相關入出金、幣流分析等）。既然警方無法於最初被害人報案時找到案件之突破口（再加上其等也鮮少主動找科技偵查組偕同辦案，可能是礙於行政上組織之流程規定，或是科技偵查組案件繁忙。另科技偵查組在目前警察體系中，僅係扮演輔助一般分局或刑事警察

³²參臺灣臺北地方法院 112 訴字第 338 號刑事判決，其透過分析多個被害人幣流，始認定被告係集團成員之一，亦即被告與被害人間之僅為左手轉右手之交易。換言之，苟該案中檢察官僅發現一被害人，若欲破解被告辯詞，就需花費更多時間去查證其他證據，例如：發現潛在之被害人。

隊偵查之腳色，而非案件主導者)，則檢察官於收案時就要花費更多時間去補齊警察未能在第一時間補齊之客觀資料。此舉無異又是一種時間程序上耗費。簡言之，此種涉及加密貨幣詐騙犯罪，在目前組織運作之下，往往是由非具科技、區塊鏈專業背景之警察主導案件調查，等案件移送給地檢署時，此際業已喪失先機，來不及向法院申請對被告之搜索票。退步言，縱然聲請到搜索票，被告往往早已利用加密貨幣移動迅速特性，移轉其等犯罪所得，甚難期望能查扣該不法所得，更遑論發還不法所得予給被害人。基於以上實務困境，筆者以為或可參考美國司法部之 NCET 概念，由一個機驗豐富檢察官³³負責統籌、規劃各項偵查行動以及訓練未來小組成員(包含檢、警)。另外目前臺灣加密貨幣交易所向金融監督管理委員會申報已遵行洗錢防制法規定者已有 26 家³⁴，其中有交易所的可透過超商買幣，有交易所的還能進行 C2C(即所謂之場外交易)，有的交易所於申請會員註冊時尚需額外手持一張白紙記載申請何平台並同時提供自己與身分證件之合照(例如 MAX 平台，要求會員申設者須手持一張身分證件、一張白紙並記載僅供申請 MAX 平台使用以及日期)，有的交易所卻只要求申設者手持證件照即可。再參酌現今詐騙手法多元，有些人可能因需錢孔急，就

³³ 之所以建議檢察官主辦，係考量檢察官法律專業較能迅速判斷各項證據在法律上意義與重點。

³⁴ 參金融監督管理委員會之網址資料，目前已完成洗錢防制法令遵循聲明的加密貨幣平台共有 26 家。<https://www.sfb.gov.tw/ch/home.jsp?id=1053&parentpath=0,8>

在網路上輕易信對方而提供自己雙證件照片、金融帳戶資料，或是因貪圖小利而出賣自己加密貨幣交易所帳戶等情，是即便交易所有依法進行所謂「實名制」³⁵之驗證，仍無法有效防堵交易所淪為詐騙集團用以實施詐欺、洗錢之平台。從而加密貨幣交易所應如何落實真正“實名制”（此處要防堵者，包含提供個資讓詐騙集團用以申設人頭交易所會員帳號以及申設者以自己交易所會員帳號幫詐騙集團進行詐欺、洗錢者）實是目前極大難題。對此類犯罪，檢警不僅需分析幣流、核對金融交易紀錄，尚且須熟悉各家不同交易所之申辦流程。也因為各家交易所會員註冊方式互殊，檢警需花更多時間瞭解並據之以釐清被告之主觀認知。故筆者才會希冀，與其讓目前加密貨幣詐欺案件在全臺各處開花分案，讓各承辦檢察官自行調查摸索，或許能考慮以一條鞭式系統管理。首先將加密貨幣詐欺案件類型依照被告之答辯分類（例如：幣商、幣商仲介、因為網路找工作、網路借貸或幫網友代買加密貨幣等）並系統化案件管理流程。尤其是針對某位車手案件在各地檢署均有警察移送者，若我們能有一條鞭式的人員負責熟悉各類被告答辯之標準化流程處理、監控模式或有專屬電腦系統集中管理此種加密貨幣詐騙案件，相信檢警就可即早發現該某車手的詭異金流與不合

³⁵ 縱然上開平台除要求申請者須透過網路上傳送雙證件照片、申請者照片、提供申請者之金融帳號，並進行手機號碼、電子信箱之驗證，然目前已有地檢署對於被告辯稱遭冒用個資至交易所盜辦會員帳號部分，作出不起訴處分。

理答辯³⁶。此方式亦可避免目前車手或提供帳戶者常出現之在甲地檢署為不起訴處分，但在乙地檢署卻為起訴之不一致現象³⁷。相信藉由類似 NCET 之專業團隊，可迅速分析全臺加密貨幣詐騙案件類型，並進而模型化(pattern)，且利用大水庫匯聚效果，在第一時間發現該等詐騙集團成員在臺灣各地之詐騙階層關係與手法。筆者深刻希望此法制能有效提升現行打擊數位金融犯罪(特別是加密貨幣犯罪)模式之效能，並同時緩解因加密貨幣興起而生之詐欺案件對於地方檢察署上之重擔。

以上僅為筆者淺見，希冀能參考美國法制，率先掌握我國潛藏金融犯罪之各項情報，並在其發生重大損害前，逐一偵破，以保我國金融秩序穩定、人民財產及生活之安全。

³⁶ 關於加密貨幣案件偵查難度，尚涉及比起偵查機關而言，被告更是加密貨幣之專家。

參臺北地檢署 113 年 4 月 26 日關於王○桓之新聞稿。

<https://www.tpc.moj.gov.tw/media/357022/1130426%E8%87%BA%E5%8C%97%E5%9C%B0%E6%AA%A2%E5%81%B5%E8%BE%A6%E7%8E%8B%E4%BA%A4%E6%98%93%E6%89%80%E7%AD%89%E6%B6%89%E8%A9%90%E6%AC%BA%E6%A1%88%E5%81%B5%E6%9F%A5%E7%B5%82%E7%B5%90%E6%96%B0%E8%81%9E%E7%A8%BF.pdf?mediaDL=true>

³⁷ 目前就筆者偵查案件中，已經遇到被告主動提供其它地檢署之不起訴處分書，主張自己無罪。筆者亦曾發現某被告手機內有其他被告在其他地檢署之不起訴處分書。