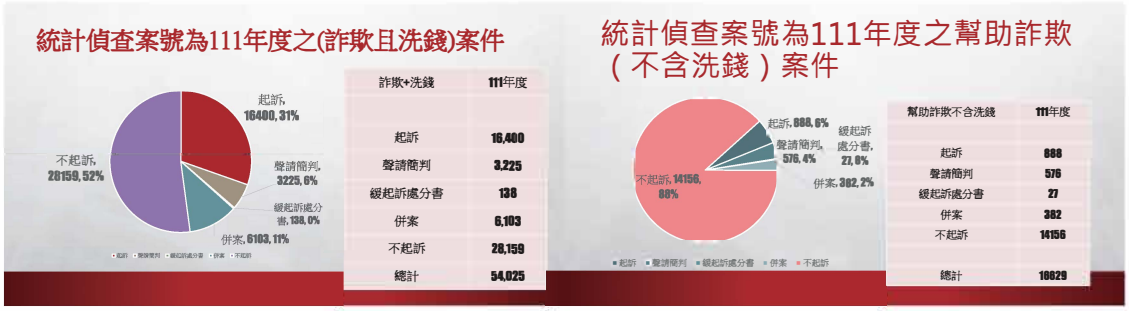
➢112.6.17 前線檢察官打詐實務與防詐策進研討會(一)

目前社會詐騙案件猖獗，人頭帳戶、網銀洗錢、假門號、冒名電子支付、Line 邀投資、個人幣商等等諸多亂象，致檢察官難以溯源，案量遽增！與其後端司法追查，不如前端公私部門積極管理防制。各機關部門是否有效防制？各處漏洞有無設計防堵？檢察官偵辦案件知之甚詳，研討會特別邀請第一線實務檢察官，檢討當前各項管制漏洞並提出策進建言，彙整供打詐國家隊參考。

警方重複移送之策進 / 橋頭地檢署楊翊妘檢察官

今天報告主題是關於警方報請指揮跟重複移送的問題。首先想一下，如果有一位同仁，查獲了一個集團，同仁很努力洗出詐欺案件金流去向而查獲重要共犯，是不是應該給他得到最多的獎勵呢？事實上，可能並非如此，比如說我們今天有甲同仁查到 2 個共犯，乙同仁查到 3 個共犯，丙同仁查到 3 個共犯，丁同仁最後收案找到一個被害人的時候就非常開心，因為甲同仁 2 個、乙同仁 3 個、丙同仁 3 個，丁同仁可以把甲乙丙搜獲的共犯湊一湊，再加上 2 個幫助詐欺湊成 10 個，向檢察官聲請核發拘票或向法院聲請核發搜索票，就會是這個案件的最大贏家，因此丁同仁就會湊成 10 人的一個犯罪集團，事實上這些同樣的共犯，也許之前就曾經被其他的同仁移送過，甚至詐欺集團的案件，在其他地檢全部的被告都已經被起訴，而警方辦完之後，仍以詐欺集團模式重複移送給地檢署，地檢署就必須要再將這些集團的成員重新再訊問過一次，可能起訴到法院去之後，法院也要再就相同的一些被告全部再重新審判一次。像這樣的情形，因被告在一個集團中，被告可能人數眾多，各個被告具有共犯關係，所以各署均有管轄權，若各別提起公訴，將導致法院亦需就相同集團全部重新審理，徒耗司法資源。

例如被害人 ABCD，他們可能因為詐騙匯款到第一層的帳戶，第一層帳戶又共同去匯到第二層、第三層，後續導入虛擬貨幣，譬如說第一層帳戶，他可能說我是辦貸款，第 2 層可能是說我有一個美國大兵男友想要來臺灣投資，第 3 層可能是網路平臺虛擬貨幣的投資，最後進到虛擬貨幣錢包。我們同仁在辦這樣的集團的時候，會不會把 ABCD 的被害人共同偵辦呢？不會的，檢察官可能會就 A 被害人，就一直追，追四五層，然後以偵結起訴或不起訴，接下來被害人 B，又到另外一個地檢署去重新報請指揮，再重新偵辦一次。所以這幾個共同正犯，可能高雄地檢辦一次、橋頭地檢辦一次、臺中地檢辦一次，可能屏東地檢又再指揮辦一次，這樣成效之下，也許部分會被不起訴好幾次。到最後的虛擬貨幣，是不是追到虛擬貨幣就會有成效呢？其實也未必，因為實務上非常多的真假幣商，現行法規上似乎無法界定這些幣商到底是真幣商還是假幣商，所以在認定上相當困難。如犯罪時間在 111 年 8 月的案件，檢察官已聲請簡易判決處刑，因又發現另一個被害人，所以另一單位的警方必須再為通知、拘提及移送程序，等於警方也有完全重複之辦案程序，因此案件如果是多位被害人，共同的集團成員下，這些成員可能要被不同的警方、被不同的檢察官、被不同的法官分別訊問、起訴、判決，造成司法資源耗損。就偵查案件為 111 年度之案件進行統計，因詐欺案件，很常與洗錢案件共同來做偵辦，所以以詐欺且洗錢的案件，類別為起訴、聲請簡判、緩起訴、併案意旨書及不起訴處分書之情形來做統計，已結案的案件書類總數約 54,025 筆左右。另外，因有一些案件移送進來，可能是幫助詐欺案件，但沒有移送洗錢的部分，檢察官結案書類也沒有寫到洗錢，再做另外統計，以幫助詐欺，扣除掉洗錢的部分，因這樣的一個統計，事實上有一些案件可能是不會進來的，就像是移送的是詐欺，但是沒有洗錢，我們結案書類也只寫到詐欺，並沒有提到洗錢，可能就不在我的統計範圍內，這樣的部分為 111 年度之結案件數 16,029 筆。從中再去挑出併案意旨書的部分到底有多少，所謂併案意旨書指案件實際上已經起訴過，是一個實質性相同的一個案件，另外又再重複送法院併案審理，就詐欺且洗錢的部分，總數量約 6,103 筆。



統計偵查案號為 111 年度之詐欺且洗錢案件，其中起訴部分約佔 31%，聲易簡判約佔 6%，緩起訴的書類比較少，併案意旨書大約佔 1 成，不起訴約 5 成以上。統計偵查案號為 111 年度之幫助詐欺（不含洗錢）案件，不起訴處分書結案量，居然高達了近 9 成，起訴及聲請簡易判決處刑佔的比例是比較少的。

比較上開兩者，不起訴的比例約佔 6 成，併案意旨書約佔 1 成，實際成效案件即被起訴、聲請簡易判決處刑、緩起訴處分，大概約佔 31%。事實上為何感覺辦了很多案件，辦了很多集團，但卻好像未達一個成效，也許是因實際上成效僅 3 成多的量。

111 年度之詐欺且洗錢且曾經判決確定案件，案件可能在移送進來後，檢察官偵結已有法院就這一部分事實下判決，因曾經判決確定而為不起訴處分，計 4,935 件。111 年度幫助詐欺（不含洗錢），因曾經判決確定而為不起訴處分，計 1,150 件。111 年度之詐欺且洗錢且前案不起訴的統計，例如說，甲檢察官為不起訴處分，後來又被送進來，我又再做一次不起訴處分，我們通常就會在書類中提到，已經有前案為不起訴，但是這樣的一個統計也是說檢察官自己有去提到前案不起訴的情形，若檢察官書類中未提到，就不在我們統計範圍內，統計的結果為 2,028 件，而 111 年度幫助詐欺（不含洗錢），且前案不起訴的統計是 1,118 件。

結論：不起訴處分書類，總計約 42,315 件，其中為曾經判決確定或有前案不起訴處分，約佔 1 萬件左右。因此 111 年度詐欺洗錢不起訴處分案件中，其中約有 1/4 為曾經判決確定或有前案不起訴，即 2 成 5 左右案件量，另外 111 年度幫助詐欺（不含洗錢）不起訴處分案件中，其中約有 16%為曾經判決確定或有前案不起訴。

111 年度上開 2 類案件總計，起訴結案的比例約佔 25 %，聲請簡易判決約佔 5%，而併案約佔 9%，曾經判決確定為不起訴處分約佔 9%，有前案不起訴而為不起訴處分約佔 4%，因此將併案及因曾經判決或有前案不起訴而為不起訴處分約佔 22 %。

這樣的統計不是說這些都是重複起訴的案件，有可能是因為正犯，如一個車手，提領了數個被害人款項的一個案件，而侵害數個被害人行為都必須要被處罰，假設這數個被害人是分別被移送，可能就會分別做處理，若說是合併一個案件移送，就是以一個案件來做處理，並不是說警方不能移送這樣的案件，而是說在各被害人分開移送情況下，可能會造成重複移送之情形。倘若司法資源多被耗費在重複及欠缺效益之案件上，可能減損檢察官辦案量能，且可能會嚴重影響司法公信力及案件品質。希望檢察官可以處理案件核心，並解決社會問題，而不是花費太多心力在處理這類案件。現在不只警方就連調查局也會移送這類案件，重複移送車手或幫助詐欺，例如提供門號、帳戶併在一起報指揮，但在檢察官看來，就是 1 件別人起訴過的案件，並非實質共犯的一個案件，檢察官卻要花費時間與司法警察溝通，為何無法准予向院方聲請搜索之具體原因。

建議：有關管轄及移送方式，若警方以被害人住所為管轄機關，可能多個被害人就會有多個案件，分由不同分局調查及移送，被告需多次接受詢問，可能與管轄地檢不同而不能拘提，之後由各分局移送到地檢，成為多個案號，而需分別偵審。若為集團案件，則可能相同被告，移送至不同地檢，再由不同法院審理。建議派出所製作完被害人筆錄，調取完明細後，逕分別移轉到該人頭帳戶之戶籍地或管轄地，以該戶籍地為管轄的分局，這樣同一個帳戶的行為人或數個行為人，將各個被害人集中在同一個地方做一次性移送，警方就可以累積數個被害人將之傳來詢問，就可以一次性的移送，檢察官亦可一次性處理，法院單一次判決。另就績效認定的部分，現行為什麼在集團上，司法警察同仁不願意就被害人去做清查，因為這部分清查可能沒有績效，若增加任何一個集團的成員會增加績效，可是增加被害人數可能不會增加績效，所以建議同一個案件，如同一集團，也可以依照被害人人數來增加績效，特別強調要增加該承辦人首功績效，因若沒有增加首功績效，可能會覺得拆案比較划算，拆成 2 案，我可以記兩次獎勵，但若選擇合併案件就沒有這樣的獎勵。因此司法警察可以就辦完集團後，把 ABCD 這 4 個被害人也一同訊問，地檢署就可一次性的解決，已經起訴過的集團，以相同被害人移送，希望可以不列績效，若是因為其他被害人而移送，希

望可以去減少其績效，對於非真實的集團就是湊幫助詐欺的或者湊非同團的人頭車手的，希望可以不要去認列這類集團績效。

警方重複移送之策進 / 雲林地檢署施家榮檢察官

楊翊妘檢察官偏重大數據的部分，我來講理論的部分。在講這個問題之前，我們學術派先做定義，我覺得很多時候檢警在對話是沒有對焦，因為大家把這個檢方的管轄或者警方的管轄都混在一起，我覺得偵查中管轄應該要分三個部分，第一個警方調查之管轄，通常就是指哪個警分局負責調查（鐵路、港口、機場我們姑且不論）。第二個警方移送（報告）至何地檢署，這個不一定跟調查的警分局在同一縣市。第三個由何地檢署起訴。舉例彰化分局受理一案件，是照 109 年高檢規定，你要移送這個被告所在地或者戶籍地，假設被告戶籍在臺中，警方就移送到臺中地檢，最後也許有併案，或移轉管轄之類，最後也許比如說雲林地檢起訴，你就會發現說這個問題是不太一樣，警方管轄時是彰化，可移送到臺中，光是 1 跟 2 就不一樣，更何況最後起訴是誰還不一定。談警方移送的共通法理基礎，因證據共通，以節省偵查資源，該法理基礎在 10 年前似乎不是那麼受大家重視，但當你詐欺案件量從 5、6 萬，一直到現在逼近 20 萬時，訴訟經濟可能是我們一個重要原則。避免偵查結果歧異、判決矛盾，譬如說人頭帳戶，我是第三位承辦檢察官，我發現前有兩名檢察官，一個檢察官將案件起訴，一個檢察官為不起訴處分，起訴理由可能認為怎麼可以隨便輕易交出帳戶，另一個不起訴處分理由認為被告說不定是被騙，被告要求職、貸款，因此被騙帳戶。我身為第三位檢察官，究要跟隨何檢察官，此時需要調前二案卷檢視。具體的措施就是我們搭配一開始講的三個管轄階段來處理。刑事訴訟法規定管轄都是講起訴之時，或者至少是聲押時，可我們現在要往前推，譬如 109 年高檢署跟警方開的會議，要將人頭帳戶移送都往前推到第二個階段，警方要移送何地檢這個階段。楊翊妘檢察官說明的部分，已經是又往前推到第一個階段，就是警察調查案件時就要合併管轄。今年媒體報導，內政部警政署 112 年 3 月 8 日提到「警署刑打詐字第 1120002186 號函，內容提到以犯罪被害人現住地」劃分警方管轄，但這只是處理第一階段警方調查的管轄問題，而媒體卻報導，警方政策走向好像跟高檢政策不一樣！說高檢以被告戶籍地來做總歸戶，可警方怎麼會以犯罪被害人現住地為主，其實媒體是雞同鴨講。所謂的警方由犯罪被害人現住地之警察管轄，指的是第一階段，就如上開所舉例彰化分局調查階段，但後續仍可能移送臺中地檢或其他地檢。按照目前收到的新案及向多名偵查隊長確認過，確認警署刑打詐字第 1120002186 號函文並無變更以前見解，移送至何地檢還是依照 109 年高檢會議決議，人頭帳戶案件仍移由帳戶開戶者居所或住所地之地檢署偵辦。管轄的問題只要在第二階段警方移送何地檢署能夠合併由同一地檢受理，即可節省檢方偵查資源、避免認定歧異。合併處理的概念，是否要往前推到第一階段警方調查之管轄，其實是可以做，但實益可能有限，有時是我們對警察期待，如果說今天第一個受理被害人之警分局，就要求該警分局要作清查並調一個月或調多久之交易明細，警方要調的資料要讓人看出你有在清查，然後對被告製作警詢筆錄時，已經發現有嫌疑人，是不是就要把有嫌疑之所有交易次數全部問該被告，身為偵查機關，既然認定被告有嫌疑，僅問被害人這一筆，而其他筆也很可疑卻不問，這不是很沒效率嗎？理想作法是第一個警分局就把該問的都問完畢，後面第 2 到第 10 甚至到第 100 個警分局，他就逕將第一個警分局警詢筆錄影印或列印，拿來附卷即可，如此一來較能即時偵查，而不是把 10 個分局都弄完，再統整到第 11 個分局，才想說不然來問一下被告，我不敢說這樣絕對不可行，這樣還是有好處，就是避免被告奔波，但如果第一受理的警分局，就願意去將該帳戶所有可疑交易明細一開始就做

清查，後續受理的警分局，只要附卷第一個警分局之警詢筆錄即可，或許這才是即時偵查，同樣也達到避免重複詢問被告之狀況。另外有個方式檢察官現在就可以做，只是比較少檢察官做，檢察官受理 10 個警分局的移送，而檢察官有權限將所有案件指定由某一個警分局為後續統整、調查。當然被指定的警分局什麼績效都沒有，這點影響檢察官在實務運作上比較少這麼做，惟法理上並無任何問題，因此警政署就這部分得設計績效獎勵措施因應。

過往臺高檢、最高檢察署或法務部檢察司，將管轄的問題，過於集中在人頭帳戶，其實人頭帳戶偵辦上從 109 年以來就做得不錯了。希望上級長官視野要廣一些，如說車手至多地領款，在臺灣西部一次就可以在很多縣市領款，每個都是正犯，每個地點都是提領地，提領地就犯罪地。例如在雲林虎尾提領，警方就移送雲林地檢，於彰化提領就移送彰化地檢，於臺中提領就移送臺中地檢。該車手辯解我以為這是打工，事實上被告在多地領款之辯解，難道不是證據共通？因每個案件中辯解都是一樣的，若要起訴，為什麼不能一起起訴？就同一個檢察官承辦就好，雖然這是數案件，但至少是牽連案件，可以期待高檢跟警政署溝通，不僅是這個車手的部分，其他像與被害人面交的車手，或到便利商店領包裹，包裹內就是會有存摺跟提款卡，還有一個幣商可能做 3 個月，就已經繫屬在數個地檢，到底是真幣商還是假幣商需要統一認定，不然地檢又得重複調查，既浪費司法資源也可能造成偵查結果歧異、裁判矛盾。以車手為例，套用一開始講的 3 個管轄階段，現在是連檢察官起訴之第三階段都沒有統整，各地各自起訴，我們現在希望至少要推到第二個階段，警方移送到地檢的階段，高檢署或最高檢要去統整。警方移送地檢署時，如發現係相近期之多次提領，且前已經其他警分局移送，則均移由第一個受理之地檢署合併偵辦、偵結，例如已有虎尾分局已經移送到雲林地檢，雲林地檢尚未結案，其他之彰化分局、桃園分局等分局，警方結案前要查前科，發現有一個提領的案件繫屬在雲林地檢，就都可以移送來雲林地檢。另外移轉管轄要設一個標準，若是警察沒有做，檢方在移轉管轄時，高檢署也要允許我們移轉管轄，把它併案到同一個承辦檢察官，因為車手在數個縣市提領，若時間很相近的話，你當然就是要做同樣認定，若未做同樣認定，不僅耗費檢方、院方資源，而且容易判決歧異。在判決執行上，每次有一個新的判決又得定一次刑。最後附帶提一個問題，一個案件，已被起訴多次，是否還要一直起訴？過往適用刑訴第 254 條時，可能是第一個罪是殺人罪判很重，第二個罪是竊盜罪預期會判很輕，因此改適用該法條。但在詐欺案件中，譬如說前案犯 20 次均判有罪，就應執行刑 2 年多，再起訴第 21 次有無實益？寫份起訴書，經法院一、二、三審，再到執行科再定刑，法院做定刑裁定，耗費心力後可能僅讓應執行刑多判 1 個月，該 1 個月還不是真的 1 個月，可能經假釋或透過累進處遇條例，最後多關的不知有無剩 20 日，故應考慮後案是否仍有起訴之實益？需要大家思考，也希望這問題能實際與司法警察溝通解決。

法務部檢察司/李仲仁主任檢察官

剛剛二位檢察官針對目前警方移送及管轄方面比較混亂的情形，先做一個簡短回應。於今年 3、4 月間，法務部長針對幫助詐欺案件，希望在移送到地檢署前，在前階段可以把這些案件可能重複的情形進行瘦身，

檢察司為此進行研議，而提出一個幫助詐欺被告全國總歸戶之計劃，該計畫希望在警方移送之前，可以將案件的同一個被告部分，不要再有重複調查、重複移送及重複偵查等情形。希望達到案件減量、程序簡化之核心目標，而具體措施藉此機會說明，目前法務部希望在打詐區塊，在幫助詐欺這部分簡化調查程序，將火力集中在較核心重要的詐騙案件進行偵查，簡化程序部分希望未來無論在警方管轄或檢方管轄，統一均歸由被告戶籍地、住所地作為管轄，目前警方的管轄是以被害人住所地為管轄，而檢方可能以被告戶籍地、現居地或羈押所在地為管轄，因此導致現在很多同一個被告重複調查、重複移送及重複實行偵查。目前規劃希望朝向所有同一被告幫助詐欺案件中，警方與檢方在管轄劃分上能統一，即均由被告戶籍地、住居所地進行管轄，該計畫臺高檢也相當支持，並且後續與警方進行研商。

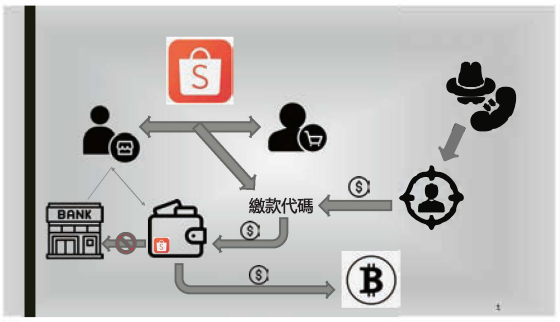
第二個策略部分，以被告的戶籍地為管轄後，在警方的承辦人部分，我們也希望可以單一化，因同一個分局裡面，如果不同承辦人，有可能同一個被告再重複進行調查、重複再移送，希望警方在這部分也可以統一由同一承辦人來進行調查。同一個幫助詐欺的被告，希望以一個案卷為主，因目前有可能是同一個被害人匯款給不同的被告，可能移送進來的在不同的、無共犯犯意聯絡的幫助詐欺案件帳戶中的被告，全部都出現在一個案卷，移送到地檢署後，檢察官承辦發現沒有管轄就會開始移轉，變成重複移轉，造成檢方很多重複偵查。希望透過以被告戶籍地為管轄，再以單一個被告、單一個案卷、警方承辦人單一這 3 個具體措施在前階段將這些案件減量、程序簡化。於後階段警方調查時，希望幫助詐欺的被害人報案後，因為被害人在全國各地都可能會報案，警方內部也可以有移轉管轄的概念，把這些被害人報案筆錄全部彙整到被告戶籍所在地的警分局，由該警分局統一進行，再移送給相對應地檢署。原則上同一個幫助詐欺被告，會由一個地檢署來負責管轄。在以警分局為中心的情況下，警方在移送前可以透過目前 165 反詐騙系統查詢，該同一個警示帳戶中，有哪些警分局已經進行了警示帳戶或被害報案次數，尤其警方亦可查詢目前有哪些被害人在各地的報案情形，於移送前可以彙整這些相關被害人筆錄，統一由該警分局進行移送，避免以前各地被害人到處報案、到處移送地檢署，造成地檢署對同一個被告一直重複偵查。這個部分法務部檢察司已進行研議中，臺高檢予以協助，也希望警政署就這部分共同努力，將所有的火力集中於較重大詐欺案件處理，對於幫助詐欺案，能程序簡化、案件減量，讓檢、警均可避免重複調查、偵查，藉著今天研討會的研討議題向各位說明法務部目前重要政策之推動。

臺灣大學法律學院/林鈺雄教授

如果一個公司，它明顯有某一種業務會癱瘓掉整個公司，甚至造成虧損的時候，通常會怎麼做？公司會把這個業務部門切割出去，至少讓其他部門業務可以正常營運。其實我們在面對很多比如說有些設施比較容易受到駭客攻擊的時候，基本上的處理方法也是這樣。今天最好的狀況是，我們行政管制的前置這些，都有聽進去而採取一些措施，慢慢讓詐欺案件量降下來，讓地檢署跟司法機關能夠正常運作，這是最好的狀況。但如果還沒等到那一天，有沒有另一種情況是，我們就承認詐欺案件我們沒辦法辦，案件這麼多怎麼可能辦啊？就從地檢署裡面分幾個敢死隊，給他們支援加班費去做，其他人就做正常的事情。如果這樣還不夠，那沒問題，高檢署讓所有的案件全部到這裡來，警察那邊也派人來，資源都分到這邊來，其他的地檢署就不要再碰這些案件，我覺得有很多種作法的。

門號簡訊亂象之策進 / 新北地檢署黃佳彥檢察官

《問題說明》



先從去年我跟刑事局合作偵辦一件簡訊驗證碼供應商的案件說起，在這個案件中，如圖示可以看到這是蝦皮賣場，然後蝦皮賣家跟蝦皮的買家，正常來說，蝦皮賣家會需要做實名認證，然後會有一個綁定對應的賣家個人金融實體帳戶。這個案件中，我們看到的狀況是怎樣？這上面所有出現的人都是人頭，沒有真正的行為人，詐欺集團用蝦皮買家跟蝦皮賣家之間去成立訂單產生的繳款代碼，然後話務機房這邊去詐欺被害人，讓被害人匯款到繳款代碼。正常的情況，錢循繳款代碼進到蝦皮錢包之後會解款到實體金融帳戶，但在這個案件中發現，這筆錢根本沒有進到實體金融帳戶，而是直接在蝦皮賣場上就買加密貨幣跑出去。

那為什麼他可以這樣做？他們全部都是人頭的會員帳號，其他實體資料、個人資料那些都是冒用的，都是被冒用。那下面一個問題就是，為什麼他們可以這麼方便的產出虛設的帳號？

我們在這案件中鎖定一個提供驗證碼的被告，後來還有鎖定到他的機房，搜索的結果在現場查獲持有SI M卡大概快 1 萬張，還有大量的企業社相關文件、行動通訊設備跟 Modem Pool。這個 Modem Pool 再跟大家講一下為什麼會有這個東西，我們國內在賣這個簡訊驗證碼其實有很多團，然後他們可能有一個時間的演進，過去他們的講法是當申請門號 SI M 卡之後，就賣到中國，然後在國外接收驗證碼。後來因為電信公司跟這些電商都有發現被濫用的狀況，所以他們有逐步的在增加監管，蝦皮的方式就是有時候會隨機傳送語音簡訊，而不是文字簡訊，變成說你在國外的 SI M 卡，就像你拿臺灣的 SI M 卡，在國外你沒辦法收語音，那就沒有用。所以，這個被告就更極端，直接在國內幫你收完簡訊再傳出去。從這個角度來看的話，也可以確認一件事情，就是這些集團唯一的業務內容就是在賣驗證碼而已，現場也有可以遠端操作的設備。

偵查過程中與電信公司詢問的結果，每一個企業社一次大概可以申請 2,000 到 4,000 個門號，申請之後，並不是這一批效期過了，才再申請，而是如果企業社申請後有需要，就可以再次提出需求，由電信公司去評估。然後我們看案件中查扣的相關東西，你看他們的廣告就專門在賣驗證碼，大概在 110 年 1 月的時候，他的廣告顯示已經出售 1 萬則，實際的數量遠遠應該是不止。然後我們在現場也可以看到他們跟中國那邊的團體聯繫的方式，中國端說我要什麼的社群軟體還是我要什麼電商，然後臺灣這邊就幫他收、發。持續收驗證碼、發驗證碼。

接著說明現在的困境，過去大家應該都很熟悉，就是車手還要去收集人頭帳戶後，拿個提款卡，然後拼命的領。現在就是剛剛提及的公司戶、網路銀行，然後辯解變得更困難，越來越難判斷。然後還有一個就是洗錢管道增加，詐欺之後錢從加密貨幣出去、遊戲點數出去、電子帳戶出去。現在蝦皮的錢包也可以利用。然後另一個困難，現在有好多層，所以我們今天面對的大概不是單一一種狀況，而是可能不同的帳戶層，會有不同的方式去混用，這是我們現在第一線檢察官實際面臨的狀況。

《架構解析》

我自己的理解，把詐欺結構定義成機房端、水房端，與中介的資訊流。資訊流重點在於，除了產生這些詐欺以及取錢的工具以外，另一方面也產生遮蔽真正行為人的效果。以我們這個簡訊驗證碼為例，如果循門號去找，永遠都只找到這個企業社，那其他的東西我們都找不到。另一方面，換個角度來想來講，虛設電子支付蝦皮錢包這些必要條件，其實把它拆解起來很簡單，就是個人的資料，這部分就牽涉到個資外流的問題，另一個就是電信門號跟驗證碼，這兩個東西現在大概就是合一，只要註冊帳號、變更設定、使用服務、要進行驗證就需要這個。所以，如果有一個團體不斷地在提供這些資料，那我們就會不斷地有查不完的人頭，但反面來講，我們只要能把這端截掉，他們產生人頭帳戶、人頭帳號的這些做法上就沒有那麼容易，這就是今天開會的目的，這些東西如果到最後詐欺被害人都已經產生之後，再由檢警來處理，那實在是疲於奔命，永遠都是預防勝於治療。

《制度失靈之處在哪？》

結論：前端企業與主管機關的把關可以有效限縮有心人違法行為的程度跟範圍。我的想法是人頭無敵，如果被告今天是自願要成為人頭，很多防治措施能產生的效果都有限。但是另一方面，如果是像我這個案件中，有心人是利用制度上某種漏洞去大量的產生人頭，不管是政府單位還是民間私部門，都應該要極力的去避免。

電信門號在現代社會，尤其是網路越來越方便的時候，因為我們現在網路的身分驗證就是都採用 OTP 隨機密碼的方式，如果在這個前提下，電信門號其實他會有屬人性的意義。

然後還有一個問題，什麼叫企業門號？或者他們美其名叫做企業客戶專案？我自己的理解企業門號比較像是，這個公司業務上會常常需要使用到電信服務，然後有一個比較優惠的費率。而不是像我們這個案件中被告這邊的團體可以持續的在賣這個簡訊驗證碼，這個我覺得是蠻奇怪的。還有，什麼是二類電信業？我覺得更極端的是電信法第 17 條規定，二類電信業者應向電信總局申請許可，但在這個案件中，那個企業社根本就不是什麼二類電信業者，但為什麼他可以持續大量地購買門號，且轉身就把它賣出去，儼然就像一個從事電信業的公司。這在整個制度上，我覺得很明顯是有問題。他可能比較扣得上邊的或許是 (二類電信業者從事的) 預付式電話卡的轉售業務，縱然我們認可他是電信業者，那也不應該在他都沒有獲得許可的時候就讓他從事這種業務。

但在個案中看到的是同一個人員他實際掌握數十間的企業社，持續找人來辦企業社，每間企業社每期持續地申請大量門號，這合理嗎？還有已經知道他申辦的門號持續牽涉詐欺等犯罪，但仍然持續讓他辦門號，這合理嗎？再來就是，這個是電信公司的人跟我抱怨，他們也有發現問題，也有不讓行為人申請過，那為什麼後來又開放申請？因為行為人去跟主管機關陳情，然後主管機關要處理客訴就又回頭問電信公司。在我來看，這個申請的行為人從來沒有具體改善過發生的問題，就因為陳情，又開放門號申請，這合理嗎？我覺得全都不合理。第一個就是訂約前的查核不力，甚至說是沒有查核。第二個是示警機制失效，然後第三個是未落實契約規範，我們這些電信公司的契約裡面，其實都有一些終止事由的條款或者限制使用服務事由的條款，但我們看到的狀況卻變成是全面的失守。

《建議》

第一點：電信公司在訂約前，關於申辦對象的門檻要提高，申辦的數量要降低，然後要有一個風險層級，就好像借錢一樣，你今天跟我借錢，我都不認識你的話，我不會一次大筆的借你錢，那應該要累積相當的合作經驗之後，才去逐步提高他能申請的門號啊。然後我昨天有確認一下，我們新世代打擊詐欺策略行動綱領 1. 5 版有提到一個目標「人頭門號停斷話 5,000 門」，這個數字或許可以再想一下，像我剛剛講的上述案件中，被告他每一個企業社可以申請 2,000 到 4,000 門，他有十間以上的企業社。那我要特別再強調一件事，就是說很多時候他沒有出問題並不是說沒有問題，譬如說他那個單一企業社 2,000 個門號，實際上都是潛在的人頭門號，他出去的流向完全沒控管，出去到底做什麼都不知道，他只要一個轉身，馬上就可以變成作為犯罪使用，所以這個停斷話數量的目標部分，我自己是覺得應該要更多。

第二點：電信公司應該要精進跟落實查核，目前我現在有看到 NCC 是強調說要去做實地查核，實地查核或許可以防止虛設公司，但如果說今天他就是自願成為人頭，他就是真的成立了企業社，這種狀況下，實地查核能有效的查覺異狀嗎？我是覺得這種業務應該要有一定的管制，轉售門號給不特定第三人行為應該要禁止。

第三點：契約條款應該要確實的執行。在電商的部分，我個人的建議是如果涉及處理金流的電商帳號，應該要求它使用註冊的門號必須以本人名義的電信門號，就好像我們用手機上網報稅一樣，會先透過電信公司去確認這個門號確實是你本人申辦，進而確認真的是你本人在報稅，這部分技術上應該是可以做得到。

接著，就是示警機制跟回饋，警察機關個案之情資傳遞，這個前面各位先進都有講過，就是介入的時點要往前。我覺得有一個具體的做法，可以統計五大電信公司門號違法使用的數據，如果這間電信公司的門號一直都在涉及這些犯罪的話，主管機關是有門號核配的控管權限，違規的情況多，核配的少，這些都可以有效地去改善這個狀況。

最後延伸兩個問題，第一個是詐欺簡訊可以全面取得個人資料跟個人門號，要怎麼處理？大家可以集思廣益。第二個，長遠的來說，個人覺得 OTP 驗證碼或許不是一個那麼有效安全的身分驗證方式，如果有一個更好的身分驗證方式的話，應該要修正以 OTP 簡訊驗證身分的作法。

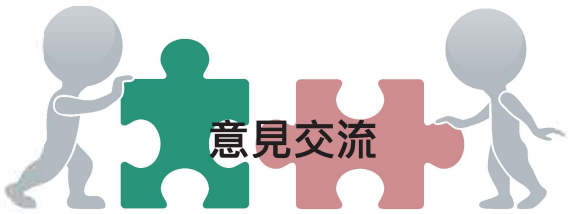
門號簡訊亂象之策進 / 雲林地檢署黃薇潔檢察官

今天跟大家報告關於人頭亂象的部分，剛剛提到關於黑莓卡，也有一些是電信公司大量申辦門號的案例，在這些情形下檢調單位，其實有一個武器可以使用，就是通訊監察保障法第 14 條，以及電信事業應該要建置監察的系統，相信這個規定是指電信事業，所以應該是包含第一類電信跟第二類電信。那我在偵辦偽基站跟研究一些現今詐欺集團運作的模式，可以發現說，現在出資的主謀大部分都在中國大陸，在偽基站的案件裡面，至少是可以看到這樣子。會由主謀提供大量的工具，無論是剛剛提到的驗證碼的部分，或是進口偽造的基地台的部分，或者是剛剛講到的黑莓卡的部分。也就是提供做一個斷點去阻礙檢調的查緝，做一個斷點的工具規避前開通訊監察的這些規定。也可以在很多的案件裡面看到被騙的一些錢，資金是回流到中國大陸，因為主謀就在大陸。所以我想剛剛講到的那個蝦皮，為什麼他會直接買 U 幣轉出去，還有用了那個黑莓卡轉四層之後錢就轉出去，然後要開設境外的一些帳戶，這個我們都可以再思考看看。在案件的人頭門號亂象，發現大概是分成下列三種，一種就是人頭預付卡的收卡卡商，這種就是一次申辦 10

幾個人頭門號的收卡集團，另外一種是企業客戶，剛剛黃佳彥學長講的就是企業客戶的部分，此部分也有第二類電信公司，企業客戶及第二類電信公司均會向一類電信申辦大量的門號，這個大量的門號，除了做簡訊、網卡使用，或者是作為承租電話線路供使用的部分，這都是屬於大量的門號。實務上，基本上案例就是上萬門號，甚至可以一次開通到 30 萬門收簡訊的部分。第三個部分就是一個形同託管的漫遊門號的部分，這個漫遊門號有網路、可以通話，可以收簡訊，以下採黑莓卡為例：人頭門號煉金術，就是預付卡的部分，或者是一般月租門號，卡商集團會專挑原住民、老人或者是遊民訛騙，或利誘去辦門號來換現金，如此新聞案例稱月入可以高達 50 萬，這部分就是人頭門號的案例。另外，這個企業客戶申辦大量門號案例就是已經非常的多了，從 1 萬門到 30 萬門。另外，黑莓卡可以躲避查緝，也可躲警監聽，所以黑莓卡現在大部分，就是被用來做販毒集團、詐欺集團、重利集團或不法的討債集團，不法集團成員都知道要買黑莓卡躲避檢調查緝。以下是個人偵辦案件時遇到的案例，這案也是一間第二類電信公司，是關於企業客戶申辦大量門號的部分，這案關於第二類電信公司其實是直接跟大陸的上游去做掛勾。那這個是什麼呢？這裡有一個理解，就是一般我們理解的黑莓卡，會佯裝成好像是合法的，所以不法業者會說：「這個黑莓卡是香港來的，這個是合法可以買到的。所以我們只是合法代理公司，我賣這些卡都是合法的。」那案例中查到的第二類電信公司，現場有大量的黑莓卡的外包裝，也有比特卡，還有 BK 卡，BK 卡就是可以接收驗證簡訊的卡片。那這邊比特卡、黑莓卡、BK 卡，等一下會統稱它是「漫遊門號」。這裡有一個理解，這個理解就是第二類電信公司，或者不需要是第二類電信公司，臺灣一般的公司也可以，他會賣這一些漫遊門號給臺灣人，然後佯裝，就是事實上用一台電腦連上國外網路，也就是連到大陸的網站去做一個嫁接，就是嫁接到大陸的網站，不管是大陸的電信公司還是第二類電信公司的平台，在大陸公司的後台直接幫臺灣人開啟這個比特卡的套餐、黑莓卡的套餐、BK 卡的套餐，可以直接由臺灣的公司賣給臺灣人去漫遊門號給臺灣人使用。那以下給大家參考一下這個數據，今年的 1 到 3 月，全球國家入境人數是 110 萬人，從大陸地區來臺人數是 29,779 人次，以下是我跟五大電信調的一些資料，就是五大電信今年 1 到 3 月開給中國大陸的漫遊門號，總數總共是 100 萬。那這個概念是什麼？就是有 97 萬門，97 萬的漫遊門號是在臺灣的公司直接開啟，或製作這些比特卡、黑莓卡、BK 卡，就是為了製造斷點，躲避檢方的查緝、檢警的查緝。那我想這個數字真的是蠻可怕的，這樣我們有沒有辦法去調閱這些 IP？無法，也就是我們只要去查他使用的網路的 IP，都會在中國大陸，那也有可能，香港也有可能開出來，所以不管你怎麼查 IP 他都在中國大陸或香港，那這代表什麼？就是我們現在全臺的檢察官去調閱 IP 就是一個笑話，不用再調了，因為都在大陸或香港嘛！另外就是，我們現在已經沒有辦法使用通訊監察這個武器了，那我想要呼籲說，科技偵查法真的要趕快通過，因為我們第一線的檢察官要作戰，我們不能只有用破銅爛鐵，而是需要一個武器。

統計今年 1 到 5 月，總共開出 875 萬境外門號，剛剛提到 1 至 3 月數字是 110 萬，所以，1 到 5 月開了 875 萬，那 1 到 5 月，就算旅遊人數大概是 200 萬，總共也是多開 6、7 百萬門號。那這是什麼概念？就是到今年的年底，我們總共多開的門號數可能會超過 1,500 萬，1,500 萬個門號數應該足以癱瘓我們的檢調系統了吧。109 年 8 月到 110 年 7 月，這段期間臺灣是禁止旅客進來臺灣的，那時候有旅客管制，但這期間亞太電信總共開給全世界 11 萬 9,000 個門號數，其中給中國的門號數近 11 萬 5,000，佔比高達 96%，這是什麼一個概念？亞太電信那個年度所有的漫遊收益幾乎來自於中國。我不知道這個部分，大家會不會覺得數據非常的可怕？我想請問一下 NCC，漫遊門號，到底歸誰管，有沒有辦法管？另外，我在 112 年 5 月 15 日請求 NCC 配合同年 5 月 16 日搜索，做一個行政檢查，他們說沒有這個往例。我問說申

辦門號要歸誰管？他說申辦的人頭門號，是我們人民的電信自由，我們不可以管人民的電信自由。另外，我說我這一案查到了第二類電信，第二類電信歸你們管了吧？然後說，我們電信管理法只管五大電信，第二類電信的部分交由第一類電信跟第二類電信之間的私法契約去約定。那我現在來是想問 NCC， 在這時隔一個月之後，NCC 跟高檢署開了多次會議，這一些沒辦法，現在都有辦法管。那接下來漫遊門號，到底還有沒有辦法去管理？這個是在電信管制鬆綁後，有一個規定，電信事業要不要登記？請業者自行考量，如果你們要自願辦理登記來給我們管，我們也會受理。這是電信管理法很明確的規定，依通訊保障監察法，提供我們通訊監察之紀錄。那我想這個是應該要由公私部門一起來努力，不管是 NCC，使用公權力，還是請五大電信業者，去做私法契約的約定，我想這個部分真的是足以動搖國本，所以這個部分是一定要想盡辦法去改善的。另外，現在違反電信法、電信管理法等行政刑罰規範密度是嚴重的不足，剛有說，詐欺案件一定要扣金流，我有案件扣到 1 億多的不動產。但被告很可能是無罪，因為現行的法律的規範不足，等於跟被告表明你們這樣做沒有違法。縱觀整部電信法跟電信管理法的規定，因為電信法已經在 7 月的時候就要落幕了，電信管理法的規定只有在第 72 條裡面有規範，就是毀損海纜登陸站，交換機房衛星通信，我是不知道這是一般人有沒有辦法做到的，相信這幾年可能是沒有辦法發生一件，只有這一條。另外，想要問 NCC，兩岸通信往返的統計，連打電話都要做統計，為什麼網站找不到我們開給中國的漫遊數？我希望把開給中國的漫遊數的數據，放在 NCC 的公開網站上，供一般人民還有記者去做監督。



橋頭地檢署/鄭子薇檢察官

有時候我們會去銀行端宣導洗錢防制，聽到很多銀行員的心聲，特別是針對主管機關金管會，我們的觀察是銀行，尤其是洗防部門 AML 的人員，他們非常的積極，甚至幫我們偵測出很多，比方說用不同的帳號，去約定同一個約定轉帳對象，但是來自不同的來源，甚至是有很多國外的 IP 正在測試轉帳中，準備可能未來會成為人頭帳號的這個帳號，他們都已經偵測出來，可是他們偵測出來之後，把它暫停交易，結果持有人或者是詐團的人跑來客訴，詐團的人講話特別大聲，客訴之後就去找金管會，金管會就會把他們被客訴的這個紀錄列成他們的缺失，要銀行去說明，所以銀行人員他們會覺得說，金管會要求我們要抓人頭帳戶，可是當我們被客訴的時候，主管機關又不挺，這時候會顯得非常左右為難，所以是不是有可能呼籲主管機關，至少就這個監管措施的部分當銀行積極地去做的時候，可不可以給第一線人員一些支持。再來也有遇到有銀行員表示說，偵測出一個可疑的帳戶，可能是詐騙集團準備要去洗錢的帳戶，可是這個帳戶目前還沒有錢進來，也就是可能即將會有錢，但是還沒有錢進來的時候，他們不知道該怎麼辦，好像也只能申報 STR，可是申報 STR 距離他實際被調查局洗錢防制處發現並且分送，甚至不見得會分送，這個過程要經歷好久的時間，那可能在這段時間內，這個帳戶早就已經被拿去用，錢也都洗出去了。那這個部分，如果說假設第一線的銀行人員已經有發現這個狀況，透過 AI 去發現一些潛在的人頭帳戶，有沒有可能讓他們可以儘速的去通報？如果在早期階段就可以去監控這些帳戶，甚至去找到背後的集團，也許就可以去預防很多的被害人被詐騙，或是可以即時把錢追討回來，這個機制或平臺有沒有可能去建立起來。

再來關於人頭公司戶的問題，其實現在不只是人頭門號的業者很多都是人頭公司，包含我們下午場會提到的蝦皮，其實很多賣家也是人頭公司，第三方支付用大量的人頭公司，臺灣在針對開公司戶幾乎是完全沒有任何的審查，也沒有任何的限制，所以就導致像有大量的包含第 3 層第 4 層帳戶，很多也都是用什麼企業社、人頭公司，他們一口氣去領了幾百萬，銀行也拿他沒轍，行員就說為什麼現在對於開公司這麼浮濫，主管機關都沒有任何的把關，甚至這個人頭公司的負責人要去開公司的時候，他對於公司在做什麼、在哪裡、賣什麼都完全不瞭解，還是讓他開。這個部分主管機關有沒有可能在開公司的這一端，針對這個人頭公司的部分去做一些監管。

基隆地檢署/劉星汝檢察官

關於人頭公司的部分，剛剛報告案例的詐騙集團主嫌，他當時籌組詐騙集團之資金來源，一部分就是他自己開了一個人頭公司去辦了新創貸款，也就是我們政府補助的新創貸款，他用這樣的方式自己創立了一個水房集團，所以我們政府也是間接的補助了詐騙集團、提供他資金，所以其實人頭公司的管控，應該也會是我們之後要討論跟精進的部分。

臺北地檢署/蕭永昌檢察官

我們透過大數據的分析，分析帳戶的使用習慣，以及這個帳戶的登記名義，相關財經背景資料來判斷目前帳戶使用是否異常，進而在過程中限縮使用，我覺得這件事情是可行的。提供一個個人的經驗分享：我是使用玉山銀行的國旅卡，有使用玉山銀行國旅卡玩手遊，然後儲值，曾經就不小心買太多，就是在短時間內買的很頻繁，多了好幾筆交易，可能頭兩筆還 OK，但是第 3 筆就刷卡失敗，然後我就收到一個簡訊，簡訊內容就是跟你說，你的使用狀況似乎有一些情形，請向銀行這邊進行聯繫，於是我為了要買(儲值)，我就打電話給玉山銀行，告知那是我買的，銀行端也會確認說，請問你到底是消費什麼？以及你今天做的交易好像是外國的手遊，他就說這個是境外交易，我會跟他說明一下，這些消費確實是我本人作為，然後他就跟我確認我的人別資料。其實我覺得說，這就是林彥均主任以及林達檢察官所說的在過程當中的即時管控分析，我覺得這件事情是完全可行的情況。就以玉山銀行信用卡來說，就刷卡這件事情，他都可以中斷我刷卡，影響我刷卡的樂趣，請我打電話跟銀行說：對，不好意思，真的就是我。如果玩遊戲刷卡這個事情，他都可以中斷，就是因為這個就像是那種詐騙集團，它也是有頻繁的金錢往來。換句話說，銀行為什麼會通知我？其實就覺得說，第一個你可能刷卡的地點不太對，因為我先前在日本，因為我在日本頻繁刷卡後也會收到這種簡訊，臺灣的話可能這個交易習慣，可能短時間內有這個大筆的交易，他也覺得怪怪的，我就必須要去跟銀行這邊反應，然後跟銀行會核實我的資料以及核實交易的目的。我覺得就銀行這邊，在這個技術面上，他們有辦法做透過大數據的分析，分析出你這樣的狀況，暫停你的情形，然後請你本人打電話去跟他說明，如果我們用在這個人頭帳戶，或者用到這種帳戶這個使用上面的話，如果我們有辦法做暫時的，譬如說人家這個叫冷卻還是熔斷還是融資，就是暫時發現這個 2、3 筆或 3、4 筆不太對的情況，就自動停止這個金融帳戶的存匯功能的話，逼迫帳戶持有人要打電話去跟銀行這邊做一個說明的時候，銀行這邊他們再了解一下這個登記名義人他的使用狀況的時候，他也可以適時的介入告訴他說你這個部分可能是有受到詐騙，或者是你這個帳戶可能是有一些這個金融往來異常的這種情形，那也進而會影響到，就是這個帳戶後來譬如他可能就匯個 2～3 筆、3～4 筆，他就不能用，他不會等到好幾個小時過去已經有 N 筆，這個數萬元的來來回回進去，裡面已經有這個金流來回數十萬甚至數百萬的情形，我們才來得及這

個警示，那當然會太慢了。所以說我覺得就這個要求金融業者配合的部分，技術上是做得到，那我也希望主管機關能夠就是以這個信用卡的使用為發想，去針對這個金融機關，請他們在這個技術面上有這樣子的設計跟要求。

臺灣大學法律學院/林鈺雄教授

今天提出很多有關金融及電信管理方面的建議是不是把它整理成比較具體的一些建議事項。坦白講，看看臺灣這整個詐騙集團的現象，實在非常不可思議，可以看出來有 2 個最大的機關，一個是 NCC，另外一個是金管會，涉及的主要是電信業者跟金融業者，為什麼我覺得這件事情不可思議？如果是其他的行業，那你的管制密度、法源基礎都有問題。但是這 2 個剛好都是特許行業，剛才余檢察長所提到的這些，你碰到有這種情況的時候，至少要有一個警覺，你要先給他做一些限制，然後讓他了解。這個說實在需要法律的層次來授權嗎？這個就是特許行業，特許行業講白話一點，從行政監管的角度來看是最方便的，很少會發生有電信公司不理你的一些情況，說實在你們那邊辦案沒日沒夜，還不如金管會找金控喝一杯咖啡，我有很多朋友從事法務，我知道請他們喝咖啡的作用會有多大。是不是最後歸納一些具體的建議給這些單位做參考，因為他不見得是從打詐的角度來看，以賣門號的案例就能了解，那就是利潤，如果這樣做，你就不要想在臺灣賺電信的錢，我覺得這個是合理的訴求。

臺北地檢署/林達檢察官

金融跟電信的部分，尤其是銀行端，他們很多櫃檯人員其實不是不願意做，但有時候實務操作會遇到剛剛提到申訴的問題，其實洗防的辦法都有，但是如果沒有被明確列出來，就變成授權每一個銀行的協理、經理、襄理他們自己去處理，在個案判斷上，他就變成自己要一個人去面對這個客戶，現在客戶當然會申訴啊。我們有金融評議中心，有好多金融消費反應的單位，如何把一個抽象的法條落實到基層，我認為是很重要的。行政院打詐國家隊也許可以出面整合，在金管會這邊直接訂出很明確的哪一些風險在管理上就是列管、禁止開戶、限制開戶、停止交易，每一個動作都做得很清楚，可以想像行員一做這個動作，馬上可以提出一個依據，我就是依照什麼規定做的，如果不服就再去申訴，而不是把問題就丟給基層人員。我們基層檢察官很苦，相信銀行員也很苦，要讓基層人員好做，就不能談得那麼抽象，要讓執行面的人很好操作，這個是未來一定要去做到的

臺高檢署/戴東麗檢察官

其實最近一直在處理洗錢評鑑的事情，剛才大家提到一個很重要的關於犯罪所得的查扣，我們辦詐欺案件遇到很重大的問題是我們都查不到、扣不到錢。大家辦案時都會發現，錢都在短時間之內就出去，所以扣不到，其實我們有個官方的機構，我們一直沒有去討論它，那就是調查局的洗錢防制處，他們有分析人員在做金流分析。像這類詐騙案件，他會在短時間之內，在某一個特殊的帳戶有很多的錢一直進去，就像剛剛講的這些網銀，這些錢很快地進去以後又很快地出去，如果要在第一時間把這個錢扣住的話，要透過洗錢防制處。那麼各銀行為什麼不敢去扣？因為這涉及商業利益的問題，銀行很希望他們開戶的帳戶是很多的，他們在商業上可以得到一些利益，再來，他們沒有凍結的權利，只能用道德勸說，因為這涉及到個人帳戶使用的權利，而且法律也沒有賦予他們公權力，讓他們在認為有問題的情況下去凍結該帳戶的金流。可是現在官方其實有一個機構可以有這樣子的權利，但是還必須透過修法，修洗錢防制法，讓洗錢防制處

在第一時間做分析的時候，發現哪個帳戶是有問題，他就凍結了，凍結以後趕快通知那家銀行，請這個帳戶所有權人來做說明。從源頭凍結以後，後續我們的案件就會大量地減少。所以我認為可以在洗錢防制法做一個條文的修正就可以了，賦予調查局洗錢防制處一個凍結的權利，他們那裡面有十幾個分析師，而且非常多人都具有反洗錢師的資格，這個是比較快速而且有效的方法。

臺北地檢署/黃士元檢察官

戴東麗學姐剛才提到一個似乎可以很好解決問題的處理方式，可是這似乎會連結到另一個問題，就是說我們要把人家的財產凍結，是不是會等於刑事訴訟法上面的扣押？如果要進行刑事訴訟法上面的扣押，需要法院裁定，原則上是這樣子。再來，調查局洗防處裡面這些統計人員，當有可疑申報或大額申報的資料進來的時候，他們只能做內部的稽考、統計，他們沒有司法調查人員的權限去做這樣的事情，他們可能還是需要跟法院聲請，所以又是檢調或是警察透過檢察官向法院聲請，由於這個涉及到財產權上的變動，扣押聲請的前提檢察官要釋明它是犯罪所得或是其他東西，所以似乎不是那麼容易解決，如果有很好的解決方式，當然我們很希望能夠在法制面上去做這樣的操作，這是我個人目前的想法。

洗錢防制處/陳國進科長

有關洗錢防制處，因為每個國家設立的方式不一樣，形式上是不一樣的。有些 FIU（金融情報機構）是有扣押權，可是臺灣是屬於執法型，所以就如同黃檢察官剛剛講的，我們分析時覺得可疑就凍結，這可能在修法之前是做不到的。目前洗錢防制法第 13 條有禁止處分命令，檢察官在偵查中可以禁止處分。實務上有些銀行對於異常交易，認為它已經是屬於第二類帳戶的時候，尤其是外商，是有禁止處分權的，他直接可以要求關戶、清戶。臺灣的本土銀行在這方面比較保守，有時候會請教我們的意見，因為這屬於個別銀行的經營方式，我們會通知，如果你認為是屬於第二類帳戶，可以用銀行帳戶管理辦法來處理的話，我們支持他這樣處理。可是通常的結果就是他會被客訴，或是他覺得這樣做可能金管會或相關單位沒有那麼足夠的力量去支持他。基本上銀行做一些禁止處分或是禁止交易時，原則上他們會將可疑交易報告過來，我們這邊都會受理。

臺灣大學法律學院/林鈺雄教授

各國在設定法律這個事情上面的作用是不一樣，我們確實比較消極，但是對於因為法規就是這樣，所以銀行也不能去凍結，我覺得並不是這樣子，銀行如果覺得你的帳戶不管是開戶資料或是其他什麼有問題，你想立刻提領，他請你跟他說明一下，請問銀行違反了什麼法？重點是銀行要不要做啊！你去外商看看，這麼多的國際銀行，被美國釘了之後，很多情況都是要你親自來說明，我不知道為什麼我們臺灣在經歷過這麼多洗防相關修法以及這些事件教訓之後，還一直覺得愛怎麼開戶、要怎麼樣都是我的權利，不然就是妨礙我的人權。我剛才說，我那個德國朋友，明明爸爸已經在德國了，孩子只是在大學需要用錢，要開一個普通的銀行帳戶，沒有什麼特別的，因為爸媽兩個都是監護人，就需要爸媽 2 個一起出面，不能寫委託書傳真過去什麼的，不行，一定要親自來，所以媽媽也要從臺灣再飛一趟德國，就是為了那個開戶。這個是觀念的問題，不是國內銀行不能這樣子做，也還沒有到扣押階段，甚至還不用到行政的禁止命令，都還沒有到那些地步，而是慣例上的標準。這樣做客戶會比較不爽，而且比較大的客戶是銀行眼中的金羊肥羊，這是他生意上的考量，但是很多規範不能只有生意的考量，不然你進來才 2 萬多人，你光賣那些漫遊卡就

賣 100 萬是在做什麼？對不對，這簡直是荒謬啊！曾有立委很生氣，別人銀行開戶，一個小時、半個小時就好，他還要被約談，弄了半天還沒弄好，我就跟他說，這表示洗防法修得有成效對不對？就是有成效，所以它才辨識出你嘛，你就是這麼重要的，像我就一點都不重要，我去開戶，怎麼半個小時就全部都開完了。今天還是要呼籲，關於電信，就是 NCC 主管的部分，還有金融，金管會主管這部分，建議要歸納一些意見做為具體的參考。

電子支付亂象之策進 / 基隆地檢署陳照世主任檢察官

針對電子支付帳戶相關的亂象以及相關策進作為提出建議，向各位與會者進行引言報告。談到電子支付帳戶的議題，先引用一些數據來向大家做報告。首先，從金管會的相關資料，可以看到電子支付帳戶之使用，有逐年成長之趨勢。簡報上面有統計自 112 年 1 月底的相關數據資料，另有更新至 112 年 4 月之統計數據。我們可以從數據中看到電子支付帳戶的使用人數已經到達 2000 多萬人並逐步地在成長中，且每月的交易金額已經將近達 130 億元。若以相關電子支付帳戶業者觀察，業務量最多者，是「街口支付」跟「一卡通」這兩家業者。

列出這樣的統計數據是要跟各位與會者報告，既然電子支付帳戶的使用人數逐漸地增加，業務量也逐漸成長，我們不禁憂心，在執法機關打詐議題的處理上面，這些逐漸增加的電子支付帳戶是不是有可能被充作為詐欺、洗錢的工具？觀察 110 年及 111 年相關被列為警示帳戶的電子支付帳戶之數據，從刑事警察局提供之數據資料，110 年統計被列為警示之電子支付帳戶有 4 萬 8,526 戶，到 111 年，列為警示之電子支付帳戶者大幅、大量增加變成 7 萬 1,330 戶的情況。

試想，這些被列為警示帳戶的電子支付帳戶，如果對應到司法基層在處理的刑事司法案件，會產生什麼影響？首先，跟各位報告，如果今天有一個被害人被騙，他把款項匯入到電子支付帳戶，旋即被轉出去，就司法刑事案件來說，這是一個案件，可是一個警示帳戶，它僅僅只會有一個被害人嗎？依據司法實務經驗，其實大部分的警示帳戶所對應的並不僅僅只會存在一個被害人。假設遭警示的電子支付帳戶如果還有其他 5 位被害人匯款至該帳戶，而這幾位被害人都在不同時間點報案的話，就每個時間點，一個報案就是一個案件，以 5 位被害人來講，一個遭警示的電子支付帳戶所對應的就是產生了 5 倍的刑事司法案件。如果對照前述刑事警察局所統計之 111 年的遭警示之電子支付帳戶有 7 萬多戶的話，如乘以被害人數量計算，恐怕是膨脹成數十萬件的司法刑事案件，顯示這些遭警示之電子支付帳戶所對應生成的司法刑事案件數量其實是非常驚人，對基層執法人員產生相當的負荷。

針對司法刑事案件，如果真的存在必須處罰的犯罪行為，基層執法人員當然是責無旁貸，必須偵辦、處理。然而，我們可以再從另一個角度來觀察，會發現這些遭到警示的電子支付帳戶所對應之刑事司法案件，

在檢警偵辦之後的最後結果，為何絕大多數都是不起訴呢？到底原因在哪裡？於是我們再更進一步去做相關原因探究，發現絕大多數遭警示的電子支付帳戶都是遭到「冒名註冊」，既然這一個電子支付帳戶是被冒名註冊，針對被冒名、實際上不知情的這個警示電子支付帳戶的註冊人，執法機關當然沒辦法追訴他構成犯罪，於是遭冒名註冊之電子支付帳戶註冊者就得到一個不起訴的結果。

在我們分析出原因之後，就可以開始再進一步探討，為什麼有這麼多遭冒名註冊的電子支付帳戶，到底原因出在哪裡？既然是註冊被冒名，那是不是在電子支付帳戶註冊的過程有過於簡單的情況？或者說，它在真實身分的驗證上面有不夠嚴謹的情況？

以一卡通電子支付帳戶之註冊教學跟宣導為例，業者為吸引閱覽者註冊一卡通帳戶，一開始在網頁上強調註冊一卡通是十分簡單，只要準備好身分證跟銀行帳戶，就可以立刻註冊完成並且可以馬上做使用。一開始就告訴大家這個註冊很簡單，請大家多多來註冊。接著再細部來觀察一卡通電子支付帳戶的註冊流程，除了設定 ID 之外，後面還有幾個驗證的步驟，包含驗證手機、驗證身分、金融驗證，最後是設定密碼。看起來，註冊電子支付帳戶過程中似乎有 3 個層面的驗證，一是手機，二是身分，三是金融的驗證。然而，需要進一步觀察的是，如果有這些驗證存在做把關的話，那為什麼還有這麼多遭到冒名註冊的電子支付帳戶存在呢？所以接下來我們再更進一步去檢視，到底這些驗證，是用什麼樣的方式為之？以及密度足夠嗎？那我們現在來逐一做觀察。

首先，從「身分驗證」的部分來看，註冊者需要填載身分證字號、姓名、出生年月日，但也只需要填載姓名、出生年月日、身分證字號等的個人資料即可，並沒有要求要上傳身分證或其他可供驗證身分之證件照片。

接下來「金融驗證」的部分，金融驗證部分是輸入本人銀行帳戶或信用卡資料，此部分驗證所強調的是註冊者本人的銀行帳戶或信用卡，也就是驗證所輸入的銀行帳戶或信用卡之申請人，與現在要註冊電子支付帳戶之名義人相符合，只要形式上相符合，即可通過這邊的金融驗證，如此看來，似乎「金融驗證」結合前述的「身分驗證」，在驗證方面已經有所把關，但是在現代的真實世界裡，做一個簡單調查，請問在座各位或線上各位與會同仁，有任何人有把握從來沒有提供過自己姓名、出生年月日、身分證字號等個人資料或自己名下的銀行帳戶帳號給其他人過嗎？應該很少人有確信的把握，因為在真實世界裡，有時候在填載一些申報資料的時候，就會填載到這些個人的資料，那如果個資的防堵不夠嚴謹的話，其實這些資料極有可能就會洩漏出去，因此，你的姓名、身分證等相關資料或銀行帳號，就有可能落在別人手上。結果有一天你就會發現，詐騙集團利用你的身分證、相關姓名資料以及銀行帳戶號碼，幫你註冊一個電子支付帳戶，而你並不知道已經有被冒名註冊的情形。

我們也可以就實務上發生的情況來做觀察，為什麼最近幾年，冒名註冊電子支付帳戶的情況特別多，情況之一就是疫情期間，有很多假的失業補助網頁讓一般大眾去做填載，填載完之後相關個資及所填載的資料等就被拋轉出去，被有心人士拿走了。又或者是，有一些釣魚簡訊，你不知道點進去填完之後，你的個資帳號等資料也被拿走，所以詐騙集團，利用假網頁、釣魚網站、釣魚簡訊等等，是有辦法去取得個人身分證相關資料跟銀行帳戶資料。在這樣的情況下，雖然設計了前述的「身分驗證」、「金融驗證」，但是成效恐怕就有限。如此的話，那麼另外一個驗證或許就會變成是我們所期待的，即「手機驗證」。亦即，在註冊電子支付帳戶的時候，要求註冊人於註冊時要填入手機號碼，並且搭配驗證手機裡所收到的 OTP 簡訊之驗證機制，此部分若能確實落實，看似是能有期待效果的，但是我們可以看到，在偵辦這種案件，

一卡通公司會給執法機關做以下這樣的回覆，當承辦檢察官會問公司：請問一下，要填入這個手機號碼有沒有什麼樣的限制？一卡通公司給檢察官的回函會說：這個驗證通過的行動號碼，不一定要是本人身分證字號向電信公司所申辦的門號。換言之，註冊時要填入手機號碼沒錯，但並不限於是註冊人名下的手機號碼，這會產生什麼樣的結果呢？如果今天是一個有心的詐騙集團成員，他想要去冒名註冊一個電子支付帳戶的話，根據剛剛的說明，他已經透過各種管道，不管是假網頁或者是釣魚簡訊或者是其他蒐集個資的方式，去取得特定人的身分證、姓名、出生日以及帳戶號碼等資料，在這樣的情況底下，雖然手機驗證欄位要求要填入電話門號，但假設我就是那個有心人士，我就填入我個人使用的手機門號就好，而且這樣的填載是完全符合公司註冊的規定，因為並不限於一定要填載註冊人名下的門號，雖然公司搭配有 OTP 的簡訊認證碼機制，但是這樣的 OTP 簡訊，只會傳送到我這個有心人士所填載的、我所使用的手機門號裡，我看到之後，當然就可以輸入 OTP 驗證碼進行驗證，如此一來，即使有填載手機門號搭配 OTP 的簡訊認證，但這樣的驗證功能基本上還是失效的。

從實際刑事案件處理的過程來看，檢察官在偵辦此類案件的時候，面對一個因電子支付帳戶涉及到詐欺或者洗錢的被告時，可能的情況是，檢察官傳訊該被告，問被告：這個帳戶的註冊資料，這是你的身分證資料嗎？被告回答：完全符合，是啊。檢察官問：這是你的帳戶資料嗎？被告回答：也是。檢察官問：，你有沒有申辦這個電子支付帳戶？被告回答：檢察官，我沒有申辦。檢察官問：為什麼沒有申辦？註冊資料上面不是有電話號碼，不是有傳 OTP 簡訊給你嗎？你再看一下這是你的電話號碼嗎？被告回答：報告檢察官，不是，註冊資料上所填載的真的不是我的電話門號。而檢察官實際去調查，也發現該註冊資料上所填載的電話號碼還真的不是被告所申辦，這個電話號碼可能是來自一家境外公司所申辦，確實不是被告所申辦。檢察官再核對註冊當時的上網 IP 位置，發現竟然是用境外 IP 進行註冊，更可以見得，當時人在臺灣的這個被告確實有可能是被冒用身分進行電子支付帳戶的註冊。再來，細心的檢察官再做進一步的確認，麻煩被告把手機借檢察官看一下，檢視結果被告所使用的手機裡面也真的沒有這個涉案遭警示的電子支付帳戶，而且調閱綁定的銀行帳戶交易明細比對，被害人遭詐騙匯入涉案電子支付帳戶內的款項，並沒有轉存入遭綁定的被告本人名下銀行帳戶，而是從涉案的電子支付帳戶直接再轉出去，也就是被告實際上沒有拿到這筆遭詐騙款項，顯示被告可能真的遭到被冒名註冊電子支付帳戶，於是，檢察官經過前述種種的調查比對、花費力氣之後，最後對被告做出一個結論-不起訴處分，這就是目前實務上電子支付帳戶涉及詐欺案件之第一線執法人員看到及遇到的情況。

而這種情況並不是單一事件，在這麼多的電子支付帳戶成為涉案工具的案件裡面，絕大多數的案件是偵查結果是獲不起訴處分，且絕大多數皆是被遭冒名註冊電子支付帳戶的情況。檢察官花這麼多時間去做偵辦，得到這樣的不起訴處分結論。說真的，對詐欺的防堵，有助益嗎？如果沒有助益的話，那是不是要需要去思考要怎麼樣做一個改進。

如果從基層檢警要處理這種案件的時間勞力花費上觀察，首先，遇到這樣的案件，即使知道，絕大多數涉案之電子支付帳戶是遭冒名註冊，絕大多數最後的結果是不起訴，可是遇到這個案件有被害人提告，檢警難道可以說，大部分都是被冒名，所以檢警不偵辦嗎？不可能。那檢警如果要偵辦，檢警會做什麼事情？除了要傳喚通知被告到場說明外，通常至少就會做幾件事：第一，調註冊該涉案電子支付帳戶的註冊資料查證；第二，向電信公司調閱註冊資料上所填載之電話號碼之申登人資料，核對該電話門號申登人為何人、是否係被告，甚至去比對註冊時之上網 IP 位置，確認是否可能是被告註冊等等。在花費勞力時間經過一系列的種種調查之後，最後得到結論是不應該起訴。再加上不起訴處分的決定檢察官是要敘明為何不起訴

的理由，除了附加理由外，還要製作書類，寄給相關的人，之後還有可能會有告訴人不服的再議程序產生。整個過程下來，都是一些勞力、時間及成本的花費，而這些勞力、時間及成本的花費，其實耗損的就是第一線同仁、檢警的能量，而這些能量的耗損自然會排擠到其他處理真正有意義案件的能量跟效能，這是必須要好好審慎面對的。

依據先前的說明，電子支付帳戶屢遭冒名註冊，其實很大的問題是出在無法有效驗證把關，既然如此，在改進的方法上，是否就應該要強化驗證的機制、改善具體的做法，又如果如同先前所述，手機號碼的驗證出現驗證成果不彰的情況，那不是就應該在填載門號這邊要強化做驗證。針對這一點也很感謝金管會在 112 年 4 月 1 日提出一些要求，要求驗證號碼時要增加核驗申請人員原留存在銀行或發卡行的手機號碼，強化此部分的驗證機制。但有這樣的強化驗證機制及做法之後，我們還是要再去做一個觀察，問題徹底解決了嗎？從刑事警察局提供之統計數據觀察，看起來遭警示電子支付帳戶數量的統計數字上確實有些下降，如果統計 112 年 1 至 3 月是 1,714 戶的警示電子支付帳戶，平均一個月大概 500 戶，後來同年 4 月降成 150 戶，同年 5 月降成 120 戶警示電子支付帳戶，顯示似乎這樣的驗證方法是有效果的，確實警示電子支付帳戶數據有下降的趨勢。然而我們還是要去檢討，既然後來的強化驗證機制有效果，那為什麼後來還是會有這些警示帳戶的存在？即使變少，但還是有，顯示問題似乎沒有完全的解決。這部分或許是來自於執行面的問題，現在有要求要強化手機門號的驗證，但是執行面會不會所有業者都能有效的落實跟執行？這一點可能要打一個問號，那如果就執行面這一點而言，不能確認的話，我們是不是應該要建立一個持續觀察監督的機制，甚至在最後統計數據發現某個特定業者或某幾個特定業者在電子支付帳戶遭警示的數量相對比較多的時候，對該些業者做一些強力的檢查跟控管。

再來，就驗證的密度上來看，剛剛有提到，「身分驗證」部分，註冊時不需要上傳身分證或其他證件的，如果要強化驗證的話，是不是這個身分驗證部分也要做一些加強，要求更加強力有效的身分驗證，這個部分待會陳信郎主任檢察官會做更進一步的說明跟解釋，所以這邊就點到為止。

另外針對策進作為，簡單提出幾點供與者會做一些討論跟思考。首先，銀行帳戶與電子支付帳戶間若其一遭警示是否應連帶衍生管制至另一邊。試想如果今天是一般銀行帳戶的話，一個人名下的銀行帳戶遭受到警示，該特定人的其它銀行帳戶會連帶受到衍生的管制，但該人的電子支付帳戶會連帶受到管制嗎？答案是不會，換句話說，如果我是有心人士，我在賣完銀行帳戶後，即使名下的銀行帳戶遭到衍生管制，但我的電子支付帳戶還是可以正常使用，甚至再出售一次，等於讓我這個有心人士可以有再賣一次帳戶的機會，那麼這樣子在防堵上面是不是密度不夠全面呢？反之也是相同，如果有特定人的電子支付帳戶遭列為警示帳戶，在前述強化驗證、杜絕冒名註冊機制有效運作下，於未來理應可消除遭冒名註冊的情況，遭警示者僅剩下那些有意交付電子支付帳戶的情況，既然是有意交付電子支付帳戶的情形，那是否在電子支付帳戶遭警示時，也可以衍生管制其名下的銀行帳戶，以達到更強而有效的管制。第二，電子支付帳戶之匯款是否應該要搭配設計 OTP 簡訊驗證機制。對照網路銀行在匯款到非約定帳戶的時候，有些銀行會設計 OTP 的簡訊驗證機制，亦即，銀行網路轉帳要輸入 OTP 驗證碼驗證成功之後，這筆款項才能夠匯款出去，那麼對照到電子支付帳戶的情況，是不是也應該要有同樣的機制，若從保護被害人財物的角度來看，如果能夠設計 OTP 的簡訊驗證機制，在被害人要匯款的時候，讓被害人必須多做一個動作，或許可以讓被害人可以再次去思考說，是不是確實要把款項匯出去，某程度來說，可以降低被害人被詐騙成功的可能性。再者，進一步延伸，做這樣的 OTP 的簡訊驗證要求，如果今天是無意協助詐騙集團之電子支付帳戶的申登人，在看到自己的電子支付帳戶內有不明款項進來的時候，照理不應該協助將已進入自己電子支付帳戶

內的不明款項，再從自己的電子支付帳戶往下匯往他處，OTP 的簡訊驗證要求，某程度可以提醒該電子支付帳戶的申登人，不要成為詐騙集團的協助者，另一方面，如果該電子支付帳戶的申登人仍然執意輸入 OTP 簡訊驗證碼將款項匯往他處，就犯罪偵辦角度，該電子支付帳戶的申登人將難以抗辯不知道有不明款項進入自己的電子支付帳戶或難以抗辯說不知道自己的電子支付帳戶內有款項匯往他處，亦是有助於犯罪之偵辦。

最後，其實詐騙集團利用網路躲在後面的情況越來越多，包含利用網路銀行進行犯罪行為，如果針對網路銀行施以更加嚴格的管控而變成較不方便使用之工具時，是不是有可能詐騙集團就會轉向使用相對管制較鬆的電子支付帳戶做為工具？如果現在就意識到存在這樣的可能性，是不是在這個時間點就先做一些預防性的強化管控，而非等事態嚴重再行處理。

電子支付亂象之策進 / 臺中地檢署陳信郎主任檢察官

111 年中檢發現大量冒辦電子支付帳戶，當時提案至高檢署成立的打詐平台，並邀請電子支付業者及金管會相關業者開會研議改善方案。經過落實相關改善方案後，遭冒辦的電子支付帳戶確實減少，但並未完全斷絕，今日我提出更進一步的改善方案供大家參考。

方才照世學長已經就電子支付帳戶向與會同仁充分說明，利用電子支付帳戶犯罪的態樣跟一般的金融帳戶或者行動電話不太一樣，電子支付帳戶最大宗的犯罪態樣就是來自冒名註冊申辦。

檢察官辦理利用銀行帳戶犯罪的態樣，傳訊到庭說明的被告都說我是求職、我是貸款、我是怎麼樣.....，可是利用電子支付帳戶犯罪的當事人 (被告) 到庭都是說這不是我辦的，幾乎 90%案子都是如此，而且後來都獲得不起訴處分。

在這之前先跟大家說明，可能大家對電子支付帳戶這個名詞會覺得很陌生，可是其實它就存在各位生活週遭，大家手機裡面應該都有 line，line 裡面除了 line pay 還有一個叫做 line 一卡通，我自己就有申辦 line 一卡通，申辦 line 一卡通有什麼好處呢？如我們轉帳給同事不用錢，只要有同事的 line，我就可以直接轉帳給他，所以有時候有一些同事退休、同仁大家團購或者買紀念品的時候，事後就可以用 line pay 轉給參與分攤的同事，我不用知道他的銀行帳號，我只要用 line，我就可以直接轉給他。我們所熟悉的電子票證業者，比如一般大眾使用的悠遊卡，電子票證業者後來都被金管會輔導為電子支付業者，所以現在其實電子支付就是存在我們生活周遭。金管會有意並努力的推廣電子支付帳戶，為什麼呢？因為它的功能就是小型的銀行，而它跟第三方支付，或者是其他支付工具不太一樣的是第三方支付只能做代收代付，可是電子支付的功能比較強，可以轉帳、可以儲值，除了轉帳之外，未來金管會逐步推行到讓我們可以買外幣。好像昨天的新聞看到全聯的全支付已經推出可買基金，所以可以此為投資行為，就是一個小型銀行的帳戶，功能性相當強。

如同剛剛照世學長所提，我底下有配屬的檢察事務官同仁，在去年下半年核閱分流案件的時候，當時就發現很奇怪，事務官送來的案件很多都是電子支付的案件，且絕大部分被告或犯罪嫌疑人都抗辯被冒名的。而此類型的案件密集到什麼程度？當時我們每十幾個偵案就會有一件電子支付的案件，就可以知道當時地檢署開始收到多少數量的類似案件，而我剛剛所講的一卡通就是當時案件量最多的。

於是我們去研究一下為什麼有這個漏洞，怎麼讓那麼多民眾被冒辦？其實問題就是出在我們的法規密度不足，剛剛照世學長也點出這個問題。法規名稱叫做「電子支付機構身分確認機制及交易限額辦法」，是來自於電子支付機構管理條例裡面授權的法規命令，該辦法在第 9 條規定，身分驗證要落實設有 3 個關卡：第 1 個，就是要先做一個行動電話的認證；第 2 個，要做身分資料的驗證；第 3 個，要確認本人使用的支付工具。以上看起來條文內容很多，好像真是有密度的管制。可是仔細看一下我們發現：第 1 個，行動電話認證的部分，原來的規定是只要能利用該行動電話操作接收訊息就可以，換句話說，只要能夠收到發出來的 OTP 就可以，它並沒有要求要用使用者本人使用的電話，所以今天一個路人甲去申請電子支付帳戶時，他只要用它自己門號收到 OTP，第 1 關就過了，並未要求是否為本人所申辦持有的電話。第 2 個，就身分資料驗證的部分，僅要求提供資料讓它做驗證，並沒有要求上傳身分證的檔案，就像剛剛照世學長所說的，如果有心人士取得我們個資資料的時候，其實它就過第二關。第 3 個，要確認本人使用的金融支付工具部分，此部分的驗證方式完全沒有任何規定，付之闕如，完全一個字都沒有寫。

當時一卡通把金融帳戶分兩類，如果是第一類的話，是會傳 OTP 密碼來跟我們驗證；但如果是第二類，第二類裡面有一個很大宗大家都有的就是郵局，只要知道我的郵局帳號，可以完成金融帳戶的綁定，換句話說，我從頭到尾都沒有收到任何 OTP，對方只要知道我的郵局帳號，就會通過第三道驗證，所以非常非常的簡單，因此為什麼電子支付帳戶，可能看到很多當事人都是郵局的帳號，就是因為一卡通裡面郵局被歸類為第二類帳戶。

111 年 12 月 26 日我參與臺灣高等檢察署召集國內電子支付業者及金管會，召開的「電子支付遭詐騙集團不法利用策進作為研商會議」。當時我提出兩個議案，相關與會者並有做成決議。第一個就針對 OTP 密碼的部分，第二個部分就是針對阻詐面。當時就 3 個漏洞我都有出相關的對策、對案，可是當時業者及金管會的想法認為這些都是新創業者，他們人力還沒有完全可以負擔，意思是他們還在賠錢經營，如果我們一口氣把他們掐死的話，業者會受不了，所以當時各方與會者經過一段拉扯，當業者發現最大宗的案件是來自於行動電話，即是適才所講的第一層管制，用的是人頭的行動電話，就此部分我們做了一個決議，就行動電話的部分，我們要求至少要做一個驗證，確認它是原留存於金融機構的行動電話來傳送 OTP 密碼，而且不要分第一類帳戶、第二類帳戶，看能不能把案件量消除下來，但決議後面也留一個伏筆，如果身分驗證的部分後續成效不彰的話，將來還會再行研議如何管制。

後來就如剛剛照世學長所引言，112 年 4 月 1 日金管會已經要求各業者落實，就第一關行動電話驗證部分，要求以留存在銀行或發卡行的行動電話門號驗證，不要隨便拿一個企業門號或路人甲的門號就來做驗證。

我們看管制之後的成效，當時於 111 年 12 月開會後，可以看到 112 年 1 月時的案子確實有減少，依據最新取得的資料，112 年 3 至 5 月的案件量有持續減少，但仍存在冒辦的狀況，並沒有完全的消除，為什麼？就像我剛剛講的，我們只補了 3 個漏洞其中的 1 個漏洞，所以當然還是會有冒辦的情況。

根本解決冒辦的方法，就如同剛剛所說的，電子支付功能是比第三方支付或是其它支付工具的功能強大，它就像一個小型銀行，我們去辦一個銀行帳號，傳訊這種人頭帳戶的當事人，當事人都不會講說我是被冒辦的，他們一定會講其他理由，所以照理來講，金管會應該要去落實客戶審查的義務，而這也規定在洗錢防制法裡面。當時我有提出要根本解決的方法，最簡單的就是要本人拍照，比照虛擬貨幣帳戶開戶的驗證方法，是拿著證件，上面寫說僅限於什麼用途使用，確認是本人。所以傳訊開虛擬帳戶的當事人來說明，他們不會說這個帳戶不是我開的，他們只會說我這是求職或什麼理由交付，以這樣的方式就可以落實解決冒名註冊申辦的問題，而當初業者意思是如果要保管這個檔案，類似開銷太大等等，沒辦法負擔。

根本解決冒名的方法真的就是完全阻止冒名註冊申辦發生，為何會有這樣子的想法？其實是因為洗錢防制法第 7 條已明確規定金融機構有確認客戶身分程序的義務，如果違反需遭處罰。換句話說，金管會負責阻詐的業務，要落實防制人頭帳戶進行詐騙。

電子支付帳戶跟其他支付工具最大的不同點，是冒辦數量還是存在，而法規已經存在並施行，在 111 年 12 月開會之後，業者也大概知道目前情況，我們現在已經撲滅一大部分的冒辦，洗錢防制法已經有相關明文規定，今天主管機關金管會是不是應該加強監督這些業者，完全落實洗錢防制法第 7 條的規定，並依規定處罰，期能達到完全沒有冒辦的情事。

洗錢防制法新修正第 15 條之 2 的規定也很清楚，只要我們交付或提供個人帳戶給別人，就要進入裁罰警告或是刑法的問題，如果我們今天還是容許冒辦的情況存在，變成我們就沒辦法依洗錢防制法第 15 條之 2 處罰或管制。所以金融帳戶、電子支付屬特許行業，金管會應該要承擔起這個責任，既然是一個特許行業，這些業者也有義務把冒辦情形防堵起來，不能有冒辦的情況，只要你一冒辦，我們就沒有辦法依洗錢防制法第 15 條之 2 做處理。因此如果今天確認是本人，今天跟承辦檢察官講貸款或求職，檢察官都可以依照洗錢防制法第 15 條之 2 的規定來處理，至少警察機關可以裁處警告，綁他 5 年不能再交付給別人，如果再交付就可以處罰，以刑罰部分起訴，希望可以落實洗錢防制法第 7 條第 1 項的規定。

第三方支付亂象之策進 / 橋頭地檢署鄭子薇檢察官

今天非常榮幸來這邊分享，我們去年實際偵辦的案件，以及從去年的第三方支付的案件，我們看到的第三方支付的亂象。

第三方支付是目前為止我們覺得最棘手、也是最難以監控的，因為上午場我們談到的人頭帳戶，它的主管機關是金管會，是由銀行發動。剛才上一場兩位尊敬的主任所提到的電子支付是根據電子支付機構管理條例，也是屬於特許行業，它是屬於金管會監管的特許行業。現在在臺灣的電子支付機構，經過特許的電子支付機構，各位猜猜看有幾家？其實只有 10 家。可是第三方支付，跟電子支付機構有一個一模一樣的業務叫做代收代付，那第三方支付在經營代收代付所透過的管道，最主要是 3 種，第一種是虛擬帳號，也就是我們現在詐騙案件的大宗之一叫做虛擬帳號，它每一個帳號都是獨一無二的帳號，它不像人頭帳戶一樣，我一個帳戶收的每一筆錢都是匯到同一個帳戶。虛擬帳號，是同一個公司或同一個自然人去申請第三方支付的虛擬帳號，每一筆錢都是不一樣的帳號，所以變成每一筆錢都要重新去查，重新去查它的來源跟去向；第二種是信用卡支付，會牽涉到信用卡的使用；第三種是超商代碼繳費，這三種是目前代收代付最主要收款的渠道。

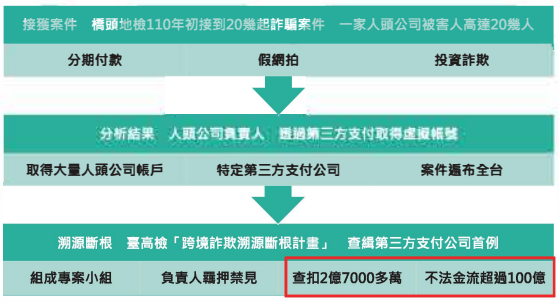
電子支付跟第三方支付，在這一塊的服務是一模一樣的，可以透過電子支付收虛擬帳號的錢，也就可以透過第三方支付來收虛擬帳號的錢，虛擬帳號也是一樣由銀行發出來的。可是跟各位報告，第三方支付不屬於特許行業，也不是金管會監管，而是由數位發展部監管。

各位猜猜看，現在第三方支付全國有多少家？答案是 1 萬多家，而且持續在增加中。所以一模一樣的服務，一模一樣的詐欺風險，可是監管力道是完完全全的南轅北轍，所以等一下就跟各位報告我們在第一線實務上看到的問題。

我只針對檢察機關的書類搜尋統計，從有史以來，我們能搜尋到「虛擬帳號」加「詐欺」作為關鍵字，數量是 1 萬 6 千多件。但光是 108 年到 112 年，最近這 4 年就佔了八成，108 年剛好就是第三方支付業蓬勃發展的時候。112 年 1 月 1 日有一件很重要的事情是「第三方支付服務業洗錢防制與打擊資恐辦法」通過，但是即使它正式上路了，第三方支付服務業正式要負洗錢防制的責任，還是一直在增加，這些案件並沒有減少。

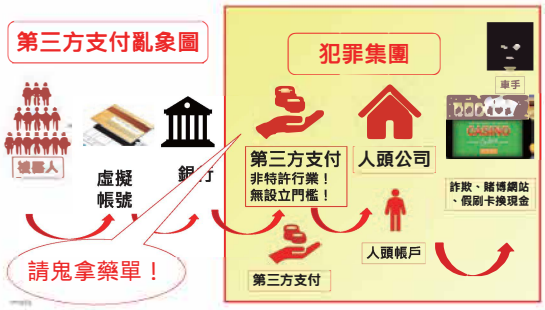
刑事局統計遭通報警示虛擬帳號及檢察署案件數，只有統計至 111 年 4 月，有跟刑事局確認，後來沒有再做新的統計，為什麼沒有統計？我猜原因之一是很難統計，因為不是特許行業，又太多家，到底要怎麼統計？不像銀行或電子支付那麼容易取得統計數據。所以其實有非常多是屬於黑數，或是我們沒有辦法經過統計的。但是，我們會看到有幾組虛擬帳號可能就有幾個被害人，光是到 111 年 4 月就有 6000 多件，仍一直持續增加中。

橋頭地檢署去年偵辦高雄的兩間老字號的第三方支付，當時有記者的標題為「擁有龐大金流的 xx 公司外觀十分不起眼」，其實從我們偵辦這兩間公司，其中一間甚至只有 3 個員工，可是這 3 個員工就可以掌握一年好幾 10 億的金流，可是還沒有到達金管會監管的門檻。



其實這種案件的被害人各式各樣的方式都有，有分期付款詐款、有假網拍詐騙、有投資詐欺，有在假博弈網站被騙、有在假投資網站被騙、也有三方詐騙，各式各樣詐騙都有。他們的手法就是會取得大量的人頭公司帳戶，找大量的人頭去設立人頭公司，用這些帳戶跟第三方支付公司簽約以後，再透過信用卡跟虛擬帳號的方式去進行詐騙。案件我們總共查扣了 2 億 7000 多萬元，可是跟各位報告，這些錢裡面，不只詐欺的錢，還包含了賭博網站的錢，也包含假刷卡換現金的這種債務協商的錢，也包含一般銀行不會收的八大行業、各式各樣、奇奇怪怪、灰色地帶違法的金流都在這裡面。實際統計，洗錢有經手的金額就超過 100 億。

這種案件對檢警查辦來說，增加了什麼樣的成本？這些被害人報案時會提供一個虛擬帳號，就是他們匯錢進去的帳號，一開始我們拿到這個帳號之後，必須要先跟銀行問說，請問一下這個帳號是發給誰？銀行就會告訴我們一家第三方支付公司，但是呢，這家第三方公司，我們就還要發函問它說，請問一下，你這組虛擬帳號到底是給哪一個客戶，就是所謂的賣方客戶。它可能會跟我們講說，是某家公司，第三方支付公司可能背後還會再接一家第三方支付公司，再往下接人頭公司。甚至還不只接人頭公司，可能還會接自然人的人頭帳戶。那麼銀行可不可以提供虛擬帳號給一般的自然人用？答案是不行。金管會明訂，銀行不可以收自然人申請虛擬帳號服務，可是第三方支付完全沒有規範，所以他們有的是收了一大堆人頭，接了一大堆的人頭帳戶，有的是接了一大堆的人頭公司，有的是又接第三方支付公司又接人頭公司又接人頭帳戶，所以它接了幾層我們就要發函調幾層，這中間可能就好幾個月過去了，可是真正背後使用這個服務的是誰？就是詐欺集團、賭博網站或是我剛才提到假刷卡換現金的這些人。



因為我們剛有提到第三方支付不是特許行業，沒有任何設立門檻，所以如果我今天是一個詐欺集團或賭博集團，我可不可以自己去設一家，開一家第三方支付公司？當今天這家第三方支付公司如果跟我是有共犯關係，或是它就是我自己開的時候，我去跟它調資料，根本就是請鬼拿藥單。為什麼是請鬼拿藥單，因為這些人頭公司的負責人就是跟第三方公司簽約的人頭公司的負責人通常就是被移送的對象。他們來到我們面前通常就講說，我就是每個月領 2 萬塊，開公司當人頭，公司在幹嘛我不知道，在哪裡賣什麼東西，我不知道，我什麼都不知道，可是這樣的人還是可以開公司。再來，有一些比較聰明的會講說，我們真的有在做生意，我們真的賣食品、真的有在賣遊戲點數等等，可是要他提出交易紀錄，完全沒辦法提出來，這樣子的，其實我們警方要去警示就會手軟，因為萬一他真的有在做生意呢？所以他們這些人頭公司，或者第三方支付公司，即使牽涉到詐騙也完全沒有辦法有效的去做警示帳戶，所以一家公司可以一直騙。光是一家人頭公司，我就收 22 件案子，因為有 22 個被害人報案就會收 22 個案件。而像這樣子的案件遍佈全台灣，我相信在場也有學長姊受害，光收到一家人頭公司的案件，就吸 20、30 個案件進來。

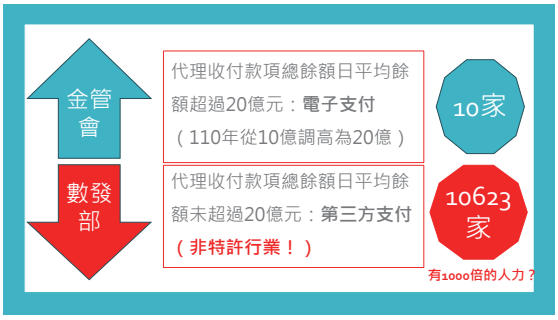
他是怎麼樣經營呢？其實一開始在申請的時候，有的這些人頭公司會說，我是在某個網站上面賣東西，這個網站看起來很正常，賣食品、賣 3C 用品，可是他是掛羊頭，實際上串接過去的是博弈網站或是假投資網站或是詐欺網站，所以是掛羊頭賣狗肉的情形。甚至還有博弈網站直接在它的網站上面廣告說，我們

可以用信用卡儲值，不用擔心被銀行發現你在玩現金版，因為我們有跟金流公司簽三方合約，所以銀行只會看到金流公司，就是第三方支付公司，可是看不到實際上是在博弈網站刷卡。

是誰允許信用卡串接賭博網站，讓這些賭客可透過信用卡的方式跟銀行借錢來賭博？是誰呢？就是某些不肖的第三方支付業者。我們看到的一些情況是什麼樣，我們剛提到請鬼拿藥單，為什麼會這樣講，因為第一個，第三方支付後面又去串第三方支付，再去串自然人的人頭帳戶，會一直長出很多的斷點，我們要不斷的去查，可是查到都是無效的資訊，在這個過程當中，他們會去洩密給背後的人頭公司，說警方盯上你們了，而這個犯罪集團、詐欺集團，就可以再去找新的人頭成立新的人頭公司，把原本那家停掉。

接著，回復我們的資料可能是假的，甚至有的第三方支付公司是接到警方來函，問說這筆錢到底是分配給哪家，他們才討論說，不然就分配給這家，就回復給警方說是這一家，去查其實也是個人頭。還有就是塗改，比方說第三方支付公司看到，糟糕這 20 家賣方客戶的公司都是同一個門號，這樣警方會不會起疑？乾脆把門號塗掉，就是會有這樣的情況。我們拿到的資料不見得是一個有用的或者是有可信的資料，再來，他們會把這些報案的被害人設成黑名單，再把他們的身分證字號跟個資都全部再洩漏給同業。哪些同業呢？就是這些賭博網站跟詐欺網站的同業，說你要注意這個人，他來註冊的話不要讓他加入，因為他會去報案。

再來，收到警方來函說沒問題，我已經把錢圈起來，所以不用擔心，可以發還給被害人，實際上錢早就已經撥給詐欺集團。他說他已經圈存，實際上已經撥款，但因為說已經圈存，我們就相信他已經圈存，所以就不需要做後續的警示。因此，從來沒有一家人頭公司，幾乎沒有一家人頭公司因為牽涉到詐欺案件而被警示，這是一個非常嚴重的問題，沒有辦法有效去做一個警示，是因為第三方公司扮演一個稱職的防火牆。



一樣是用虛擬帳號代收代付，可是監理的強度有非常大的落差，剛才有提到，它代理收付的款項，一樣做代收代付，可是要每年的平均，一天代收的總額，日平均餘額超過 20 億元，才是歸金管會管，但是沒有超過就是第三方支付。我們可以看到金管會管 10 家電子支付，可是 1 萬多家歸數發部管，數發部有沒有 1000 倍的人力去管這些？想必是沒有。再來，這個辦法說第三方支付業者要做 KYC，請你要去確認客戶身分、請你要留資料、請你要去了解他們在做什麼，了解業務目的的範圍跟性質。實際上我們真正聽到的，他們說，第一個，當然不是所有的，部分的第三方支付說我們不用做 KYC，只有銀行才需要做；第二個說，我們客戶要接到哪個網站去賣什麼東西，我也沒辦法知道，原本跟我講要接這個網站，之後去亂接別的網站我也不知道，請問如果是銀行，我發一個刷卡機給商家，他隨便拿去別的商家擺，你會允許嗎？一定不會，可是為什麼第三方支付可以允許這件事情？再來又說，我的客戶都是在線上申請，沒有留存任何客戶的資料，這是我們目前遇到的現況。

理想是什麼呢？如果今天主管機關真的有發揮功能的話，我們查到它沒有落實 KYC，他們讓這些人頭公司來簽約，最多可以裁罰多少錢？答案是 100 萬，因為它不是金融機構，所以最多只能罰 100 萬，可是我們會發現，即使是一家只有 3 個人的第三方支付公司，它每一年也可以賺到 1 億元的手續費，所以它會怕嗎？第一個，你罰他，他可能不會怕；第二個，他被罰就關掉，再重開一家就好了，反正又不是特許，又沒有門檻，甚至連營業項目要不要寫，第三方支付都沒有規定。所以現在銀行有的會來問我，請問一下，這一家說它的營業項目沒有第三方支付，可是它好像在做第三方支付怎麼辦？還會有人來問我說，它的營業項目有寫第三方支付，但是它好像不是在做第三方支付，好像在做虛擬貨幣，怎麼辦呢？這些都是問題。

其實我們在 111 年中就一直不斷的呼籲一些建議事項，包含從 111 年 7 月，我們跟臺高檢署提出 3 項建議：要求全面落實 KYC，同年 7 月份法務部跟經濟部、第三方支付業者開會，我親耳聽到有某個第三方支付業者說，我們為什麼要做 KYC，是銀行濫發虛擬帳號。可是實際上跟賣方客戶接觸的人是誰？不是銀行，是你第三方支付耶，那你為什麼不用做 KYC 呢？再來，最後在同年 9 月，新世代打擊詐欺策略行動研習會，台中舉辦場次，我們有當場向數發部的長官提出建議，建議查核後台是串接哪些網站，是不是要做查核？他們的回答是「數發部的職責是推動發展，而非監管」，再帶回去了解。數發部部長，我非常尊敬的唐鳳部長，也有在新聞中提到，數發部的態度就是推動發展，不是監管。可是我們這邊很想要詢問的是說，請問被害人應該是發展的犧牲品嗎？特別像是虛擬貨幣，虛擬貨幣已經是我們現在詐欺集團最主要的洗錢管道之一，我們為了要推動產業發展就可以讓這些被害人成為犧牲品嗎？那我們到底還要等多久，才能夠等到一個安全的金融環境？

我們想要請教的是，到底我們稽查幾家，裁罰幾家第三方支付業者？背後串接的網站我們有沒有徹底了解？我們要怎麼樣去解決沒有辦法調到有效資料的問題？我們想提的是，數發部好像只有兩個人在處理所有第三方支付業者的監管業務，幾乎等同是自由業，可以想像這個監管的強度。我們相信絕大部分是好的，也有規模大的第三方支付業者，並非所有的都這樣，只有少數的是壞的，我們不要讓少數老鼠屎壞一鍋粥。好的讓它特許，壞的撤照查辦，人民才有保障，唯有列為特許行業，我們才有可能有效的去監管第三方支付，這是我們向主管機關，還有向跟在場各位學長姐提出的報告跟呼籲。

第三方支付亂象之策進 / 臺北地檢署蕭永昌檢察官

今天不知道該用什麼樣的心情來與各位參與這場活動，其實詐欺的問題，近來非常慘烈，事實上我不是很在意分案數字的人，但是連我這個隨興之人，在今年以來就感覺到詐欺案件確實是每個月分案量三分之一那麼多。回到第三方支付的部分，其實也要呼應一下鄭子薇檢察官，鄭檢察官剛才介紹的非常清楚，同時也呼籲數發部，請數發部應該要負起自己應該要有的監督責任。該說是有點遺憾吧！主要是數發部的立場認為該機關的重點是在於推動發展而不是監督，如果從「數位發展部」這 5 個字聽起來，好像言之成理，但是我特別查一下「數位發展部組織法」，該組織法明明在第 2 條第 4 款就有明文規定「數位經濟相關產業政策、法規、重大計畫與資源分配等相關事項之擬訂、指導及監督」都算是數位發展部應該負責的職責，怎麼會變成只有推動發展而不監督的情形，這跟它的組織法不合。

因為第三方支付的部分確實有很多的問題，我簡要的跟各位說明一下，其實一般來說，我身為基層的檢察官，我接到類似案子的話，其實它類似電子支付的狀況，一樣是民眾被冒用身分，然後申請綁定之後產

生一個虛擬的帳戶，接著詐欺集團再用虛擬帳戶詐騙民眾，只是民眾把這個錢匯到虛擬帳戶，之後把虛擬帳戶的錢，直接移轉到其他的虛擬帳戶或者買虛擬貨幣或者遊戲點數，這是一般來說比較常見的類似電支帳戶的詐欺的手法。不過這個部分，我確實也開了眼界，因為它遇到狀況跟電支帳戶一樣，辦案之後才知道，原來開電支帳戶或者開第三方支付的帳戶這麼的簡單，完全沒有做一些很詳盡的身分查核，特別是手機門號的簡訊認證，隨便的一個人頭卡、王八卡，接受認證就可以啟動帳戶。這類型的案件最恐怖的點在於綁定帳戶這件事情，不要說當事人本人不知道，我覺得最可怕的是就連金融業者也不知道。舉例來說，我今天綁玉山銀行，我之前有發函過，玉山銀行會跟你說沒有任何的資訊顯示當事人的這個帳戶有被綁在電支帳戶下，更不要說當事人會知道這件事情。今天一個涉嫌提供電支帳戶的被告真的可能完全不知道嗎？他會完全不知道，因為舉例來說他可能綁了郵局的帳戶，這筆錢進了虛擬帳戶之後，事實上在郵局帳戶，也就是這個所謂綁定的帳戶不會有任何金流相關的資訊。現在郵局 APP，假設我有薪資匯進來，或是我定期匯款匯出去，APP 會跳通知或有簡訊通知，但如果是用虛擬帳戶的話，當事人是完全不會收到任何通知。在這種情況之下，等於沒有任何人知道自己被辦了帳戶，也沒有任何人有辦法事先的預防。

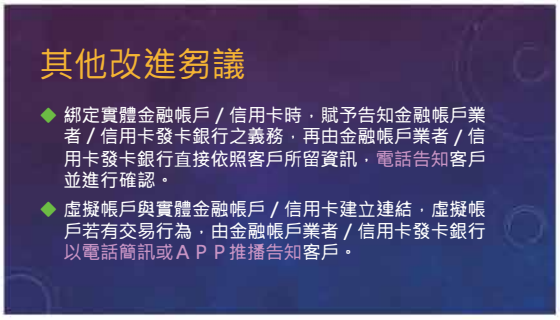
我後來想一想，最完美的預防方法是什麼？最完美的預防方法就是現在假設市面上有多少電支帳戶，全部我都去申請，我搶在詐欺集團之前，我把它請遍了，詐欺集團就拿不到手，當然這是一個方法，但這個方法就凸顯我們現在這個制度本身的荒謬，因為我們在偵辦案件的過程當中，很多時候虛擬帳戶進來的錢，會透過層層層轉，要不是個人幣商，要不是遊戲賣家，我們在偵辦案件的過程當中，我們會心存起疑，為什麼？有一些幣商、個人幣商或者遊戲點數賣家，一再地被移送進來。其實地檢署的分案是同一個被告會一直分在同一個檢察官那邊，所以我一直收到同一個被告、同一個幣商，同一個遊戲點數賣家的案件，他一直出庭但是他完全無所謂，事實上他為什麼無所謂，因為他知道我奈何不了他，為什麼？因為要說他有沒有遊戲點數的交易？有。他跟你說我也是三方詐欺的被騙者，我是無辜的，那到底是誰騙了他？是不是真的有所謂有第三隻腳的第三方？不知道，為什麼？因為不可查，為什麼不可查？因為詐欺集團是用假資料去申請的。

坦白說，他跟你說我們真的有做交易，可能進了虛擬帳戶或可能進了蝦皮帳戶，可能後來有做一些交易，我們有時候會試圖做追查。譬如可能進虛擬帳戶的錢去買一些東西，是不是真的有買？是不是真的有簽收？因為會牽涉到物流業者。像這部分先前有在偵辦的時候，我們請物流業者提供是誰簽收貨物的，把簽收貨物的資料給我，但往往都是石沉大海，要不然就是沒有資料，相關主管機關沒有要求一定要保留這些資料，所以到底後續衍伸的交易是真的是假的，也無法確定，所以在這類型案件當然會造成我們偵辦上跟追查上面很大的困難。

其實外界可能很難理解，會覺得說我們要努力的辦，努力地去溯源，這個想法是對的，但是很可怕的一點是，地檢署的工作或者法院的工作，事實上就類似俄羅斯方塊一樣。因為新收案件就很像從上方落下的方塊，會一直掉下來，要趕快消除下面的方塊，把方塊一排排給消掉，不消掉怎麼辦呢？不消掉就跟俄羅斯方塊一樣，疊到最後就爆掉，為什麼會講爆掉？假設我今天為了要追查這個，我覺得這個有鬼，我要查，可能我一再的發函，一再的去挖，這個案子結不掉，一個案子結不掉，兩個案子結不掉、10 個案子結不掉、20 個案子結不掉，接著我的未結案可能就不知不覺到 200、300、400，到最後我所有案子都動不了，就跟俄羅斯方塊一樣。我才說這類型案件，你如果期待司法機關、檢察機關在末端運用超高的手速，把俄羅斯方塊底部給消掉，這件事情是非常不切實際的，為什麼？因為很多時候，你前端可以做好的事情，後端就可以省掉很多事。

其實這類型狀況最大的還是在於人頭帳戶，人頭帳戶是財產犯罪的護身符，第三方支付的業者為什麼可以不要成為特許行業？不像一般的電支業者是特許行業，其實從剛才鄭子薇檢察官的介紹可以看出來差別在哪？差別在經手的金額沒那麼高，所以說它可能不需要特許。但是最可怕的是「量大會造成質變」，今天假設我經手金額很高，而第三方支付設立經營非常簡單沒有成本，我就直接多設定幾家第三方支付，用數量來補足，只用一家如果做不到，我就弄 3 家、5 家、10 家來做。事實上，這邊就會變成化外之地，法律上完全沒有辦法有效約束。

以結論來說，今天要正視量大造成質變的狀況，我們要重便利、要發展金融、要活絡，但它呈現的狀況是：你今天活絡經濟，活絡經濟是一個得，但是讓你失去很多東西，事實上就是有人被騙，被騙的金錢事實上是落入不法集團的手上，不過它是隱性的損失，一來一回的話，到底我們是得還是失？為了追求金融的活絡，而完全捨棄監督，造成地下經濟的囂張甚至犯罪的滋長，這個到底是正確投資的方向，還是是錯誤的方法？我想這部分應該是不證可明的。



最後有一些個人想法，第一部分，我會認為綁定的時候當事人會完全不知道，為什麼？因為它留的手機號碼根本是假的，不是我本人。我認為這時候就「告知」的部分，應該要由金融業者，也就是綁定的銀行，依照客戶留存在銀行、郵局的電話資訊告知客戶並且進行確認。其實我覺得這件事情應該還算有實現可能性，為什麼？我三不五時收到來電，接起來，就聽到「不好意思，你是我們優良客戶，接下來我們有個很好的貸款專案...」，它都有辦法常常電話行銷貸款資訊，藉由金融業者的電話告知與確認，有助於不會一而再、再而三頻繁的發生，所以賦予電話告知義務的部分，讓被綁定的金融機構來執行的話，可能會比較好，而且比較有辦法確定對話的對象是本人。

第二部分在於建立連結部分，我覺得說，金融交易的通知，一樣是從綁定的金融業者或信用卡的發卡銀行用電話簡訊、APP 推播方式來確保今天本人能夠完整收到資訊，而不是由其他莫名其妙的人。因為時間的關係，我做個補充，以結論來說，不能夠單純小看第三方支付所造成的影響，只因為他們經手的錢很少、我們要活絡經濟。我覺得今天的狀況就是一群螞蟻咬死大象。

臺北地檢署/林達檢察官

個人認為第三方支付目前的狀況，會成為國家未來最大的亂源。於偵辦虛擬帳號案件的過程中，函調相關人頭帳戶資料後，繼續溯源查察，溯源的結果竟是虛擬的第三方業者，找到第三方業者的登記者后，經傳喚到庭，發現該人年紀輕輕卻前科累累，想透過其協助追查背後主謀者，猶如請鬼拿藥單，其提供給我的物件資料完全是造假的。

依照「第三方支付服務業洗錢防制與打擊資恐辦法」，是有要求第三方支付業者對於它的委任人要進行檢查，並需留存與委任人簽訂的契約與相關委任人填載資料，經向第三方支付業者函調結果，委任人相關資料全部都是亂填，如此這般何人去檢查了？主管機關有落實檢查的工作嗎？且以主管機關數發部現有人員的配編置僅 2 至 4 人，如何確實執行檢查工作？

金管會所建門檻為 20 億元以上歸金管會管理，20 億元以下歸數發部管理。個人認為如此治理方式極為不妥。如此有心人士可以控制僅做到 19 億元的規模，或於即將跨越 20 億元門檻之際再開立另外一家公司等方式，來規避金管會監督管理，遊走於此灰色地帶。

對策面而言，個人認為第三方支付這一塊一定要監督管理，而且要立刻即時進行，最好是明天就全部改為「特許」，落實確實的監管才可以去蕪存菁，好的業者留之，壞的業者汰除。將第三方支付列為特許行業，規範要求業者想藉此營業獲利，則必需提出計畫與達成一定資本額，並完成所有必備程序與流程，方對該業者開放准予特許，並要求業者每個月提交報告予監管機關，由公務員被動審查，如發現有問題，即對業者施予裁罰、撤照等處分。

我們也不是怪數發部，因為現在的情況是對第三方支付業者不列特許行業來管理，數發部就需邊努力檢查，如果多給數發部 1000 人力，1 人管理 10 家，每個月追著業者跑，然後咧？發現有問題裁罰業者 100 萬，而業者又不理也不怕，它把公司收起來，個人是存疑罰款會有人繳嗎？如果因此再啟動行政執行，由行政執行署進行查封，如此更突顯對於此種公司之治理毫無效能可言。

所以個人認為需要立刻將第三方支付業變成特許行業，第三方支付的虛擬帳號，一天可以產生幾千個、幾萬個、幾十萬個、幾百萬個，如不對其進行管理、監管，這是十分嚴重的事情。於適才的研討場次，已得知電子支付帳戶部分已得到控制，而第三方支付這部分的監督管理機制真的不能再拖延。

政治大學法學院/李聖傑教授

我想電支都已經有管制，第三方支付形成的問題更大，對於詐騙集團來說，我們知道他們轉幾手之後，幾分鐘之內相關的不法所得就完全不見了，而且沒有辦法追蹤，這個讓犯罪集團成本非常低微，然後獲取不法利益非常龐大。我想第三方支付的管制是必要的，管制的方法如果以特許的方式呈現的話當然最好。

橋頭地檢署/鄭子薇檢察官

承接剛才林達學長所說，現在在查相關金流確實有發現一個現象，就是他們底下接的這些不管是人頭的自然人也好，或者是人頭公司也好，確實會有一個輪流的現象，這個月去接 A 第三方支付公司，下個月去接 B 第三方支付公司，再下個月接 C 第三方支付公司，為什麼？因為分散金流，可以避免靠近金管會立的門檻。

其實金管會的門檻本來是 10 億，後來提高到 20 億，那一年發生了一件事情，依照電支機構管理條例的規定，如果第三方支付的規模達到一定程度，必須在 6 個月內提出許可的申請。當時有一家快要逼近 10 億，就是樂購蝦皮，但是不知為何，就結論而言，金管會把這個門檻提高了，所以到現在我們非常熟知的第三方支付包含 line pay，包含蝦皮，其實樂購蝦皮就是蝦皮自己成立的第三方支付公司專門做代收代付，即使是這麼大規模的金流，還是沒有達到金管會所訂的門檻。

所以我們可以知道，它是一個洗錢防制很大的漏洞，當今天沒有一個有效的監管措施時，它就會變成犯罪集團可能會很喜歡使用的方式。

我有一點想要提出來討論，如果是非電支機構經營儲值業務，是一個刑事犯罪，我忘記刑期是幾年以上，有點類似銀行法的概念。上午場有聽到最後一組引言及與談有提到蝦皮，我們也可以把錢存在蝦皮裡面，那這樣到底算不算儲值？

另外觀察到第三方支付公司，例如我們查到的其中一家，幾乎有 9 成的業務都是接博弈網站，博弈網站其實是可以在上面儲值的。如果今天賭客在博弈網站刷卡儲值，或是透過虛擬帳號儲值，這到底算不算收受儲值業務？是不是一個刑事犯罪？我之前研究的時候發現這是一個可以解釋的空間，因為好像有一個法院判決，必須收受的是不特定多數大眾的沒有特定用途的儲值，才叫做儲值業務。如果我今天只是收受特定，比方說特定的娛樂城，或者是今天是特定的網站收受的儲值，這樣是不是就不屬於電支機構所講的儲值業務？可是為什麼儲值要特許？就是因為儲值的本質上是一個吸金，所以既然是吸金，就要特許，不然我們沒有辦法保障人民大眾的財產權。但是，難道我在一個單獨的網站，或是我經營一家第三方支付公司，雖然不是直接去保管這些儲值的錢，可是我是一個渠道，我讓這些賭客可以在賭博網站上面儲值，或者我讓這一些消費者可以在某個購物網站上儲值，這樣是不是也是一種儲值業務，如果沒有經過特許，沒有經過有效的監管，會不會沒有辦法保障我們社會大眾人民的財產權？這是我拋出來的疑問，請教在場的先進。

（待續）