第一節　前言

本章的主旨是介紹國際上常見的洗錢及資恐者使用的金融工具、管道及手法，並以案例闡釋多種態樣。

首先，在第二節介紹最常被用來洗錢的金融工具「電匯」。由於科技不斷進步，銀行間的支付系統使得不論是國內或國際電匯都變得更方便、更快速，而且可以輕易移動大筆資金到幾乎世界各個國家。尤其是 SWIFT 全球銀行代碼系統的建置，大大地提昇了銀行間支付系統的可靠性與效率。但是，新科技與新服務的出現，也同時帶來了新風險，尤其是透過電匯資恐的風險；對洗錢者及恐怖組織而言，先進的電子系統仍然有誘人之處及漏洞。

第二節也說明透過電匯的資恐交易很難只靠系統監控，還要依賴銀行的櫃檯人員與法令遵循人員的充分訓練、有效宣導與專業警覺性。另外，本節也詳述監控透過電匯的資恐交易，容易令人困惑的的幾個特點，與核准跨境電匯交易之前須確認的重點。本節附有四個國際洗錢案例，說明洗錢者與恐怖組織如何利用電匯移轉資金。

第三節討論非營利組織。由於非營利組織掌握龐大的財務資源，即使僅有極小部分被洗錢者利用於洗錢，仍可能造成很大影響，因此需要特別關注與防範。本節介紹洗錢者，尤其是恐怖份子及恐怖組織，利用非營利組織的原因，以及有效防堵洗錢者及恐怖組織利用非營利組織移動資金的關鍵監控措施。本節附有四個國際洗錢案例，說明洗錢者與恐怖組織如何利用非營利組織移

轉資金。

第四節介紹罪犯如何利用保險工具洗錢。保險是一個規模龐大的產業，每年收取的保險費相當驚人，總資產更是難以計數。人壽保險、產物保險及再保險，與其他金融商品一樣，都有被利用為洗錢工具的風險，因為其具有幾個特點。本節也例舉洗錢者利用保險洗錢的幾個常見態樣，及保險公司與經銷保險的金融機構應如何注意防範。第四節也分析了保險公司陳報的疑似洗錢交易報告不多的可能原因。本節附有四個國際洗錢案例，說明洗錢者與恐怖組織如何利用保險洗錢。

第五節討論「重要政治性職務人士」(Politically Exposed Persons，簡稱 PEPs) 的定義及為何這類人士屬於洗錢高風險族群，還研討金融機構應如何防範重要政治性職務人士洗錢。本節附有四個重要政治性職務人士洗錢的國際案例供參考。

最後，第六節談不肖的「守門員」(Gatekeepers)，亦即律師及會計師等專業人士，如何利用他們的專業知識與技術，為洗錢者或犯罪組織提供洗錢諮詢，甚至設計及執行洗錢計畫。本節說明要有效地防止與遏阻洗錢者利用理應扮演守門員角色的專業人士洗錢，專業人士及金融機構都應該認真執行驗明客戶身分、客戶審查、監控交易及陳報可疑交易等基本的防制洗錢內部控制程序。本節附有六個國際洗錢案例，舉出幾個非金融事業或人員協助洗錢者與恐怖組織移轉資金的態樣。

第二節　電匯

洗錢者，尤其是恐怖份子，經常使用電匯來移動資金。許多證據顯示，美國 911 事件的劫機者，主要是透過電匯途徑，取得計畫過程及最終實施恐怖攻擊所需的大部分資金。

一、洗錢者常用電匯移轉資金

所謂「電匯」(Wire Transfer 或 Funds Transfer) 是指個人或團體，透過一個金融機構，以電子傳輸方式，將資金移轉到另一個金融機構的個人或團體。電匯交易的匯款人與受款人有可能是同一個人。電匯可能是國內銀行間的境內交易，也可能是跨越國境的國際交易。由於電匯實際上無須移動實體貨幣，它是一個從甲地移轉資金到乙地最快速且安全的方法。

銀行間的支付系統的出現，使得不論是國內或國際電匯都變得更方便、更快速，而且可以輕易匯款到世界各個國家。尤其是 SWIFT 全球銀行代碼系統的建置，大大地提昇了銀行間支付系統的可靠性與效率，因此也提高每天的匯款交易件數及交易金額。隨著科技的發展，有些銀行更提供以電話或網路即可匯款的服務；但是這種非面對面的新服務，也同時帶來了新風險。

二、銀行間支付系統功能強大

日新月異的科技發展，使銀行間的支付系統越來越強而有

力。然而，這種發展趨勢對於洗錢防制的影響而言，卻是利弊互見。從正面角度看，先進的電子支付系統：

(一) 可以預設交易監控參數，自動產生可疑交易警示；

(二) 可以透過電子交易紀錄，輕易地追蹤個別交易；

(三) 可以自動產生與儲存交易紀錄。

但是，對精明的洗錢者而言，先進的電子系統仍然有誘人之處及漏洞：

(一) 可以快速且大量地匯款；

(二) 每家銀行對於匯款資料的要求並不一致，要求較鬆者，可能可以提供極佳的洗錢機會；

(三) 每家銀行對於交易資料的保存規定未盡相同；

(四) 每家銀行對可疑交易的定義不同，對陳報「疑似洗錢交易報告」(Suspicious Transaction Report，簡稱 STR) 的標準也不同；

(五) 每家銀行的經營策略不同、風險胃納也不同、獲利目標有高有低、管理哲學互異、內部控制鬆緊有別、對法令遵循的重視程度有差異；

(六) 每家銀行的薪酬制度不同、獎金紅利制度不同、業績壓力也不同；

(七) 每家銀行都由人經營，而每個人的價值觀及道德感不同。

總而言之，電匯是洗錢者快速且大量移轉資金的有效工具。如果洗錢者發現某家銀行的洗錢防制內部控制或法令遵循有漏

洞，即會利用該銀行進行洗錢。

為了躲避交易監控，有些洗錢者會將一筆資金進行多次電匯，企圖使金流複雜化，不容易讓人輕易看出資金來源及去處。洗錢者也常常使用「白手套」(編注：英文稱為 Straw Men，意思是「稻草人」或「假人」)，找一個可以提供無不良紀錄與真實身份證明的第三者充當匯款人或受款人，目的也是規避監控。另一個手法是透過多家銀行的多個白手套，將非法資金化整為零，以小額匯款方式匯到洗錢者指定的帳戶。

三、資恐交易的特點

值得注意的是，資恐資金的來源大都是合法的、小額的電匯，例如 25 至 500 美元之間，一般的交易監控系統不一定會視之為可疑交易，因此不會自動產生警示報告。經過恐怖份子的小心設計，資恐資金為了躲避監控，也為了降低被扣押與沒收的風險，以及減少發生風險的損失，通常較少出現大額交易，使得資恐交易監控難以只靠系統監控，還要依賴銀行的櫃檯人員與法令遵循人員的充分訓練、有效宣導與專業警覺性。

利用電匯資助恐怖組織的罪行，很難完全依靠自動化交易監控系統去偵測，必須加上人員輔助，確實會增加監控的難度。但是根據打擊資恐的實務經驗，銀行如果建置有效的洗錢防制內部控制政策與程序，而且有效地執行與監督，還是可以有效地偵測出可疑交易，甚至經過審慎地調查後，可能可以阻止資恐交易的發生。

打擊資恐要特別注意以下幾個容易令人困惑的特點：

(一) 資恐交易的金額並無固定規則，可大可小；

(二) 資恐交易的匯款人不一定是罪犯或犯罪組織，許多是有正當職業與合法收入的個人或法人團體；

(三) 資恐交易的受款人不一定是罪犯或犯罪組織，而可能是普通上班族或合法登記的法人團體；

(四) 匯款人與受款人所在國家不一定是高敏感國家、高風險國家或被制裁國家。

要有效的打擊資恐，須在核准跨境 (Cross-Border) 電匯交易之前，確認以下幾個要點：

(一) 匯款人的姓名、身分與所在國家；

(二) 受款人的姓名、身分與所在國家；

(三) 如果受款人不是最終受益人 (Ultimate Beneficiary)，須查明最終受益人的姓名、身分與所在國家；

(四) 匯款人與受款人的關係；

(五) 匯款目的。

【國際案例 2-1：恐怖份子自 A 國取得資金以支持 B 國的恐怖組織】

A 國某恐怖組織透過其支持者，向移民至富裕的敵國 (B 國) 的族人強制徵收「救助故鄉慈善獻金」。這些獻金都被合法地存入在 B 國登記有案的財團法人慈善基金會，再光明正大地以電匯方式從 B 國移轉至 A 國鄰近國家的慈善或宗教團體；那些團體都

是 A 國恐怖組織控制的外圍組織。

這些 A 國鄰近國家不是 B 國的直接敵對國家，因此比較容易購買到武器與物資，然後自邊境走私到 A 國，供 A 國的恐怖組織進行訓練及最終發動對 B 國的恐怖攻擊行動。

【國際案例 2-2：恐怖組織利用電匯跨國轉移資金至恐怖行動目標國】

在 X 國的恐怖組織利用電匯來轉移資金到恐怖行動的目標國 Y 國，用於支付恐怖份子在 Y 國住處之租金、購買車輛與電子零件，以製造炸彈。恐怖組織在 X 與 Y 國都使用白手套帳戶移動資金。這些帳戶使用與恐怖組織無明顯關聯的自然人或法人組織來開設，但是自然人之間有親屬關係，而法人組織之間則有隸屬關係，因此他們之間的轉帳既合情、合理，而且合法。

這些資金的來源是恐怖組織在 X 國帳戶的現金存款，再從 X 國電匯到 Y 國銀行帳戶。一旦金錢到達目的地 Y 國，帳戶持有人將資金放在儲蓄帳戶中或是投資共同基金，以保持隱密，並可隨時供恐怖組織需要時使用。資金也可能會被轉到恐怖組織聘用的財務經理人之帳戶，再從那裡支付購買設備與物資或恐怖組織秘密行動所需的費用。

【國際案例 2-3：恐怖份子使用電匯方式接受捐款】

在一個對 C 國的 D 公司的調查行動中發現，D 公司涉嫌以郵購名義募款，以快遞方式發送低價貨品，以電匯方式收取高額貨款，並以非法所得資助 E 國的恐怖組織。

調查發現，D 公司的員工寄出大量的可背書轉讓支票到 E 國

的一個恐怖組織外圍團體。另外的證據顯示，D 公司的收入大部分是 C 國境內的小額匯款，大部分客戶是來自 E 國的新移民，交易的商品是成本低廉但售價高昂的成衣或日用品。

根據以上資訊，執法單位自法院取得對 D 公司的搜索令。分析文件與銀行紀錄之結果，顯示嫌犯利用電匯募資，以資助 E 國恐怖組織。

【國際案例 2-4：有計畫性的匯款以躲避監控】

AZ 先生與他的叔叔在 A 國經營一家專門替客戶匯款的 SS 公司已經四年。SS 公司是一家大型匯款公司 SXS 的加盟店，而 SXS 一直被執法單位懷疑涉及資恐交易。SS 公司後來因為涉及一件可疑交易，也遭到監理單位調查。

調查顯示在過去 4 年期間，SS 公司從不同客戶收到超過 4 百萬美元的現金，並替他們匯到不同的國家，其中包括 B 國。為了避免被 B 國的銀行申報大額外匯交易，AZ 先生參考同業作法，建議客戶將匯款拆成多筆低於一萬美元(B 國的大額外匯申報門檻)的小額匯款，再匯至受款人在 B 國多家銀行的不同帳戶。如果受款人只有一個帳戶，AZ 先生會建議客戶將匯款拆成多筆低於一萬美元的小額匯款，於短期間內陸續匯入該帳戶。

AZ 先生最後被控共謀有計畫性地匯款，以規避 B 國外匯交易申報規定。AZ 先生後來同意認罪，以換取較輕的刑罰。

第三節　非營利組織

非營利組織 (Non-Profit Organizations，簡稱 NPO) 在全世界各國都扮演重要的社會服務或慈善公益角色，重要性與必要性無庸置疑。但是，由於非營利組織掌握龐大的財務資源，即使僅有極小部分被洗錢者利用於洗錢，仍可能造成很大影響，因此需要特別關注與防範。

一、恐怖組織利用非營利組織的原因

恐怖組織為達成不同目的，可能以多種方式利用非營利組織洗錢，洗錢態樣與案例不勝枚舉。恐怖組織利用非營利組織的原因很多，例如：

(一) 非營利組織容易獲得民眾信任，可以被恐怖份子或恐怖組織利用，作為公開募款管道；

(二) 有些非營利組織是跨國性或世界性組織，提供極佳的國際作業及資金移轉平台；

(三) 各國法令雖有不同，但是通常對非營利組織的成立條件與營運監理要求比較寬鬆；

(四) 許多非營利組織享有賦稅優惠，更是一大誘因；

(五) 非營利組織可依設立宗旨，公開地在特定族群或宗教社區中活動；

(六) 有些人基於宗教或慈善目的捐獻現金，不會堅持非營利組

織必須開立收據；

(七) 有些非營利組織設有匿名現金捐款箱，可以不開收據；

(八) 許多金融機構或其員工，對非營利組織極為友善，於作業上會給予方便或協助；

(九) 非營利組織之間的跨國資金移轉通常不會特別引人注目；

(十) 恐怖組織甚至可以掛羊頭賣狗肉，以合法的非營利組織掩飾非法的恐怖活動，跨國公開營運。

二、關鍵監控措施

要有效防堵洗錢者及恐怖組織利用非營利組織移動資金，以下是關鍵監控措施：

(一) 注意非營利組織與其他有問題的非營利組織之間的關聯性，例如營運或財務有無往來，有無相同的管理者或董事；

(二) 留意非營利組織的管理者或董事有無不良紀錄；

(三) 非營利組織的董事有無外籍人士；

(四) 查核非營利組織與聯合國制裁名單上的個人或團體有無任何往來或關聯；

(五) 媒體有沒有對非營利組織的負面報導；

(六) 非營利組織有沒有被檢舉過有不法行為；

(七) 執法單位有沒有查詢過非營利組織的交易紀錄；

(八) 非營利組織的主管機關或稅務單位是否曾查詢過該組織的交易紀錄；