銀行公會
The Bankers Association of the Republic of China
會訊 第一〇三期
中華民國 107 年 1 月
發 行 人　呂桔誠
發 行 所　中華民國銀行公會
地　　址　104 台北市德惠街 9 號 3 樓
電　　話　(02)8596-2229
傳　　真　(02)8596-2230
創　　刊　中華民國 90 年 1 月
設計美編　文匯印刷資訊處理有限公司

銀行應瞭解的資恐案例及最新趨勢

孫欣 *、沈柏君 **、謝丹瑜 ***
* 安侯法律事務所執行顧問
** 安侯法律事務所律師
*** 安侯法律事務所律師

壹、前言

我國將於 2018 年第四季接受亞太洗錢防制組織（APG）相互評鑑，如果評鑑結果不佳，可能導致跨國交易的成本提高，甚至他國可能拒絕與我國從事貿易活動，因此主管機關如火如荼的進行修法，於 2016 年訂定「資恐防制法」，要求金融機構如知悉自己持有或管理指定制裁對象的財物財產上利益及其所在地時，應即凍結並通報法務部調查局。如有違反，可能會被處以新臺幣二十萬元以上一百萬元以下罰鍰。

由於資恐與洗錢手段多有類似，我們必須多加瞭解洗錢及資恐的手段，瞭解不法的錢是如何透過金融機構洗白，以及資恐的錢如何透過金融機構轉移到恐怖分子手上，銀行在偵測疑似洗錢及資恐交易時才能更有意識，避免無形中成為資恐的幫手。因此，我們整理一些國際上常見的洗錢及資恐案例，以及資恐趨勢，俾對資恐的手段及風險更加瞭解。

貳、洗錢案例

移轉資金常見的考量包含了每筆交易中能夠移轉資金的數量、資金移轉被發現的風險、資金移轉的便利性、成本及速度。一般來說，「匿名」的程度影響了資金移轉被發現的風險高低，因此匿名性高的管道，例如在國家邊境攜帶現鈔，或地下外幣匯兌，都容易成為洗錢及資恐的管道。但如果考量資金移轉的數量和效率，銀行仍對不法及恐怖分子具有高度吸引力。以下介紹幾個常見透過銀行洗錢的案例：

一、外匯存款

不法資金常會在國際間流動，以隱匿其資金的真實來源。銀行在發現客戶的身分與其所擁有的外幣不符，或客戶的帳戶常有不明的匯款人匯入外幣時，就要注意是否有疑似洗錢的疑慮。

南歐的某間銀行曾發現其客戶 A 在該銀行的分

行帳戶多次存入大筆北歐貨幣，另有不明人士亦從國外匯入同類的貨幣到該帳戶。該銀行研判，A 為南歐國民，從來沒有去過北歐或出過國，且雖然某 A 本身是一間飯店的負責人，但也不應該有鉅額的現金提存款，因此不應該擁有鉅額的北歐貨幣。據此，該銀行向當地金融情報中心申報疑似洗錢交易。事後調查發現，不明的匯款人是北歐境內活躍的毒梟，這也坐實了 A 的洗錢罪名。

二、信用狀交易

在貿易融資的業務中，銀行常為客戶開立信用狀擔保提貨。如果客戶在信用狀中載明的商品金額明顯與該商品的市場公平價值不符，或運送的物品與客戶所屬產業別、營運項目不符或與本身營業性質無關，就可能有洗錢的疑慮。

例如某毒販 B，為了將在印度買賣毒品所得支付給印度相關人員，便透過銀行開立一紙受益人是在印度的出口商信用狀，並以買賣藥品掩人耳目。因為價差過於明顯，其他公司購買類似的產品與數量可能僅需 1 千萬元，B 卻以 2 千萬元購買，信用狀金額遠高於交易商品的價值，因此引起承辦人員的懷疑，加上 B 成立的公司為鋼鐵產業，卻進口不相關的化學藥品，因此承辦人員便申報疑似洗錢交易，B 的罪行也因此曝光。

三、開立假發票

開立假發票為隱藏不法所得的一種常見方式，實際上不存在的交易因為有發票憑證而使其他人信以為真。銀行雖然無法核實每一筆交易，但銀行或許可從觀察到的大額交易及異常交易發現蛛絲馬跡；大額現金交易、現金存入後立即轉匯國外、或交易規模與客戶收入或身分不相當的情形，雖然無法立即判定為洗錢交易，但已屬於疑似洗錢的徵兆。

例如外國國會議員某 C，由於自己負責規劃財政部的一項企劃案，該案對特定部門的公共政策預算案擁有提案及同意權，藉由掌握計畫核准與否，C 向廠商收取賄賂。D 是 C 的朋友，擁有一家貨幣兌換及旅遊公司，也願意協助 C 清洗所收受的賄賂。D 先是利用其職員充當人頭，在許多銀行開設帳戶以利洗錢，經由這些帳戶洗錢的金額超過美金 4 百萬元。不過現金交易及立刻轉匯至海外的行為容易引人起疑，因此 C 開始利用 D 的配偶所擁有的水果遞運公司開立假發票。C 利用製作假發票的手法，3 個月就清洗了美金 270 萬元。此一方式，既使 C 可以切斷與行賄者間的直接關聯，也使得與其有業務往來的商人有發票可辯解。水果遞運公司則可將匯往國外的款項，解釋為結清支付進口水果的款項。

該案例也說明了重要政治性職務之人因其職務關係，洗錢的風險較一般人高，因此對於特定政治人物，銀行的開戶作業及交易監控必須更加嚴格。

參、資恐案例

所有金融機構只要牽涉資金移轉都有潛在的資恐風險，因為恐怖分子有可能會利用這些金融機構來移轉資金。一般而言，在地的小型恐怖組織常仰賴國際恐怖組織資助來進行恐怖活動，因此跨國資金移轉對恐怖組織的活動而言至關重要；但伊斯蘭國（ISIS）卻是例外，觀察發現他的資金主要來自於組織活動當地，只有少部份是來自於外來的籌資管道。

在現今金融體系中，銀行仍為移轉資金最可靠和有效率的方式，有鑒於此，銀行所面臨的資恐風險居高不下，2014 年阿富汗毒品走私報告就指出，塔利班組織利用正規銀行體系來轉移走私毒品的不法獲利，FATF 也多次在報告中指出一些非政府組織利用銀行帳戶將資金移轉給恐怖組織。以下將介紹數起利用銀行移轉資金的常見態樣與案例：

一、多筆小額匯款

銀行因為其角色便利性，能快速地在國際金融體系中轉移資金，也因為國際金流的龐大規模，使得恐怖組織與其資助者能輕易隱藏在正常交易後不被察覺。通常，恐怖組織多以多筆小額交易的方式移轉資金，隱藏在銀行每日數萬筆交易中難以與合法交易相區辨，再加上合法設立的境外公司作為幌子，資金常因此輕易地被匯往國外。

二、金融卡提款

雖然各國紛紛祭出監管辦法強化對資恐風險的管制，但資恐的風險仍不容小覷，不只新興的金融交易模式容易被濫用，傳統的銀行商品也容易被利用成為資助恐怖分子的方式，例如，資助者可以開立一個存款帳戶並申請金融卡，再將金融卡交給恐怖分子帶到海外，如此一來恐怖組織就可以在海外

提取現金取得資金。

三、停止償付個人貸款

某 E 申請 2 筆個人款項，之後停止償還分期付款，銀行無法聯繫上 E，轉而聯繫 E 的雇主，卻從雇主處得知 E 已經離職了一段期間。經調查 E 經由第三地前往土耳其，主管機關認為此案可能涉及資恐並展開調查，同時凍結 E 及其家人的資產。

四、在社群網路上以預付卡方式募資

某一與恐怖組織 ISIS 相關的人員在 Twitter 上發起募捐活動，並要求捐贈人利用 Skype 與其聯繫。該名人員在 Skype 上要求捐贈人購買國際預付卡，然後經由 Skype 傳送國際預付卡的序號給他們。之後，該名人員將國際預付卡序號交給位於敘利亞鄰近國家的同夥，由同夥將低價轉賣預付卡所得之現金交給 ISIS。

肆、資恐籌資的新發展

一、非營利組織

恐怖組織有時會利用非營利組織作為籌資的手段，例如，法國慈善機構「Pearl of Hope 希望珍珠」，曾以救助敘利亞及巴勒斯坦貧困傷病兒童的生活與教育為名，拍攝了無數賺人熱淚的影片，發表在社群媒體與影音平台上，使許多人紛紛掏腰包捐款，最後卻發現慈善機構暗地裡把善款拿來資助敘利亞的聖戰士組織。

恐怖組織利用非營利組織慈善的外表降低大眾戒心，不僅能利用非營利組織獲取資金，更能利用非營利組織以建立人脈吸收成員或達到其不法目的，對於非營利組織的濫用已經嚴重侵害公益部門的正常運作，FATF 報告指出，恐怖組織常以下列方式利用非營利組織：

- ❑ 藉由非營利組織作為中介角色將關係人的資金投入恐怖組織之中
- ❑ 藉由非營利組織協助恐怖組織進行活動
- ❑ 藉由非營利組織作為掩護，運送資金或物資到恐怖組織手中
- ❑ 利用非營利組織暗中支持恐怖組織吸納成員
- ❑ 成立空殼非營利組織進行詐騙或掩護

FATF 報告指出，非營利組織若是在恐怖活動活躍地區或鄰近地區進行慈善活動，最容易被恐怖組織利用成為運輸資金的障眼法。曾有一家非營利組織勸募善款用來對巴勒斯坦與敘利亞地區進行人道救援活動，2013 年，該非營利組織帶著兩台救護車與醫療物資前往敘利亞地區建設醫院，活動與建設現場的照片都被貼在臉書上證明慈善活動的真實性。大約一個月之後，該非營利組織在社群媒體上發起新的募款活動，聲稱在土耳其需要資金，但一家法國機場海關通報，三名非營利組織人員各攜帶 9,900 歐元，規避海關的申報規定，但只有 6,000 歐元是被用來進行人道救援，其餘資金則都交給潛藏在當地的恐怖分子。

但這並不表示所有在恐怖活動活躍地區進行活動的非營利組織都有恐怖組織在背後操控，許多非營利組織確實單純在從事人道救援活動，並無其他不法目的摻雜其中，銀行若要辨別真假非常困難，除非銀行能對非營利組織的每一個交易對手都一一核實，並仔細瞭解捐款的流向，否則即使完成洗錢防制規定的重重程序，通常也無法發現可疑徵兆。因此，面對新成立或欠缺監管的非營利組織進行慈善活動的捐款時，銀行需要特別留意該筆交易。

二、網路平台

因為網路的普及化以及匿名性，加上社群媒體的蓬勃發展，除了傳統的募資渠道外，恐怖組織也開始利用網路平台作為籌資的管道。恐怖組織如今利用社群媒體作為宣揚恐怖主義以及招納支持者的平台，甚至在衝突地區利用網路進行直播。在 2013 年有人在臉書社團上發文籌募資金，宣稱一名在敘利亞的聖戰士急需裝備、食物與藥品，並要求捐款人把款項匯到德國銀行的帳戶中，調查發現帳戶持有人是恐怖組織的皈依者，懷疑是帳戶持有人發起這次募款。

另一個常被利用的網路平台就是群眾募資（簡稱群募）平台，群募讓企業、組織或個人可以在平台上募集資金，資金來源則來自群眾的小額借貸或捐款，因為有群募平台的出現，企業或個人有資金缺口可以不用透過銀行取得資金，但因為群募平台的審查機制不若銀行嚴謹，籌資的真實目的也很難被核實，潛藏有不小的資恐風險。

有時恐怖組織也會同時利用不同的網路平台與複雜的交易進行募資，例如曾有恐怖組織通過社交

媒體與網路進行籌資計畫，計畫成員都申請有數個電子錢包、信用卡以及手機號碼。打著為難民提供救助與建設設施的名義募款，實際上是用來救助恐怖分子及其家人，資金是先匯進電子錢包或信用卡帳戶之中，再通過層層的轉帳以及現金提領，最後交給恐怖分子。

三、結語

近年來，因為區域不穩定以及極端主義作祟，恐怖攻擊時有所聞，打擊恐怖組織最好的方式就是切斷其資金來源，為了能達成目的，需要政府機關與金融機構通力合作，揪出潛藏的恐怖分子與其資助者。隨著交易型態不斷進化以及非營利組織的被濫用，打擊資恐的難度越來越高；且由於銀行面對的是網路平台業者，難以對平台上每筆交易進行核對；或是因為披著非營利組織的外衣難以區辨出資恐活動，銀行很多時候是在恐怖攻擊事件發生之後才知悉特定人士是恐怖分子或為恐怖組織服務，所以反應速度是打擊資恐的關鍵點。

因此，在面對資恐防制要求時，金融機構應進行定期的教育訓練，培養員工對恐怖主義、資恐風險的認識；建立迅捷的反應機制，因應突如其來的恐怖攻擊事件；建立情報分享機制與其他金融機構、主管機關有效率地進行聯繫；並建立完整恐怖分子、恐怖組織名單，確實調查客戶資料，如此一來才能真正達到打擊資恐的目標。

生物辨識技術與我國金融機構之運用

黃世欽
臺灣銀行電子金融部科長

壹、前言

生物辨識（Biometrics）機制是存在生物界相當久遠且普遍的身分認證機制，每個生物均有其生物體本身獨一無二的生物特徵，足以提供其他生物辨識。老虎辨認對方氣味、企鵝辨識呼叫聲、人類透過證件的影像、電話的聲音或是契約的簽名來認識彼此。而生物辨識技術最早由 19 世紀法國巴黎的人類學者 Alphonse Bertillion 測量罪犯之頭圍、中指長度等資料，並加以建檔，以辨識罪犯。現代生物辨識技術由美國國防部於 1990 年代初期投入大筆資金，研究使用演算法辨識人類臉孔的可能性。隨著電腦科技的發展，當代生物辨識技術則專指基於人類獨特的生理特徵（Physiological）和行為表現（Behavioural），利用自動化設備，透過演算法轉變為模組（Template），用以辨識身分的電腦技術。

指紋用在犯罪現場辨識嫌犯已經有 100 多年的時間，雖然指紋辨識至今仍是生物辨識的主流，但仍有技術、成本、法律以及民眾心理的使用門檻，可以應用的場景仍有侷限性。2013 年 Apple 的 iPhone 5 採用指紋掃描，搭配 Touch ID 安全協定，使手機解鎖畫面不需再輸入密碼，其他智慧型手機業者亦紛紛跟進，落實指紋辨識技術在智慧型手機的應用。2017 年 4 月 Samsung 推出 Galaxy S8，整合指紋、臉部及虹膜等技術，同年 iPhone 問世 10 周年紀念旗艦機種 X 以臉部辨識 Face ID 取代 Touch ID，使生物辨識技術成為顯學，相關應用風起雲湧，逐步擴大生物辨識的實務運用。

智慧型手機已成為民眾每日生活中食衣住行不可或缺的重度使用配備，進而衍生出行動應用服務的龐大市場。銀行利用智慧型手機所提供的服務也有極大的進展，無論是轉帳、繳費及消費等行動支付的服務，或存匯、外匯、放款及理財等行動銀行的服務，都可以「隨時」、「隨地」進行。當自身擁有的生物特徵、隨手可得的智慧型手機與隨身攜帶的生物辨識技術結合，搭配便捷生物辨識技術的銀行行動化服務不再遙不可及，例如 Apple pay 即以指紋辨識驅動行動支付服務。我國金融監督管理委員會於 2016 年提出的「金融科技發展策略白皮書」亦將生物辨識列為金融科技的重大基礎建設之一，銀行應瞭解相關技術如何運作並與相關服務整合，以掌握未來金流的新趨勢，提供客戶更好的服務。

貳、生物辨識技術的內涵

隨著網路（Internet）及行動（Mobile）提供的服務日趨多元，加上安全等級與設定要求的不同，記憶多組使用者帳號與密碼作為身分認證的機制，已是資訊時代使用者的一大困擾，加上使用者帳號與密碼容易遭盜取或破解，不但無法滿足身分認證的需求，也無法達到交易安全的需求。因此隨著科技的進步，利用人體獨有的生理特徵或行為表現的生物辨識技術取代使用者帳號與密碼的需求日漸升高，逐漸吸引不同產業投入相關應用。有人甚至認為生物辨識技術是數位安全的未來，但也有人認為使用者帳號與密碼雖有缺點，但生物辨識會比較好嗎？至於認為生物辨識技術將伴隨著更嚴重的安全議題，也不乏論者！以下謹就前述議題分析生物辨識的相關內容與發展。

一、生物辨識技術的定義與特性

美國知名密碼學專家 Bruce Schneier 表示：「生物辨識技術簡單、方便，如果使用得當，非常安全。生物辨識不是萬能的，瞭解如何運作和失敗，對於瞭解何時改善安全，至關重要。」

生物辨識技術是基於生物獨特的生理特徵和行為表現，透過自動化裝置結合光學、聲學、生物感測器及生物統計學運算等高科技技術，經過感測、擷取、註冊、儲存、比對及決策等程序進行生物辨識的電腦技術。生理的特徵包括：人臉（Face）、指紋（Fingerprint）、靜脈（Vein）、虹膜（Iris）、心電圖（Electrocardiography, ECG）、腦波圖（Electroencephalography, EEG）及去氧核醣核酸（Deoxyribonucleic Acid, DNA）等；行為表現包括：步伐（Gait）、敲鍵（Keystroke）及簽字（Signature）等；以及兩者混和（Behaviometrics）的聲音（Voice）辨識技術。生物特徵之安全性與唯一性，均優於行為表現。可作為生物辨識技術之生物特徵的獨特性包括：

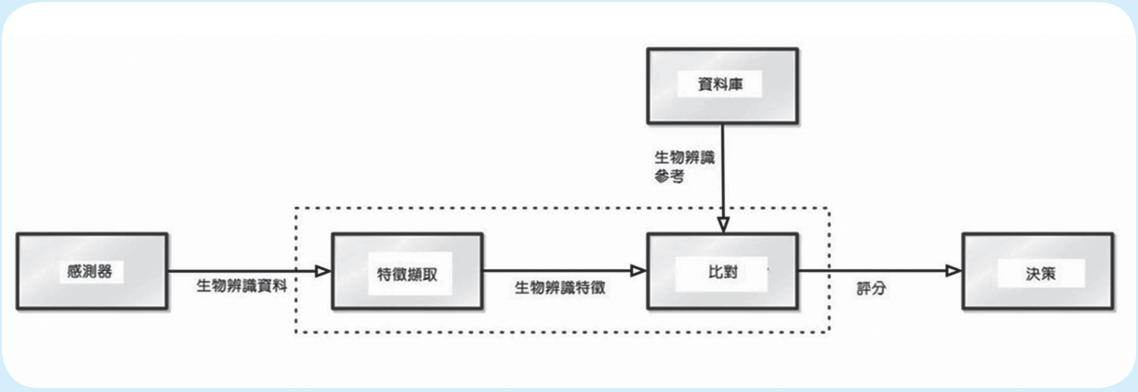
㈠普遍性（Universality）：每個人均擁有這些生物特徵；

㈡差異性（Distinctiveness）：任意兩人的生物特徵都會呈現相當程度的差異性；

㈢永久性（Permanence）：每個人的生物特徵在足夠長的時間中不會發生變化；

㈣可測性（Collectability）：可以定量方式去測量這些生物特徵。

圖一　生物辨識的程序：感測、擷取、註冊、儲存、比對及決策



運用生物辨識技術，身體或行為就是密碼，不怕遺失、不易複製、更不用擔心遭人盜用。生物辨識技術的作業流程如下：

㈠註冊（Enrollment）

1. 透過感測器（Sensor）取得選定的生物特徵；
2. 擷取生物特徵（Feature Extract）並註冊生物特徵統計模組；
3. 將模組儲存於資料庫（Database），包括本地資料庫、中央資料庫或可攜式的智慧卡。

㈡辨識（Recognition）

1. 即時掃描並擷取選定的生物特徵；
2. 提取生物特徵模組；
3. 將掃描的生物特徵與儲存的模組進行比對（Comparator）；
4. 為應用的業務程序提供比對評分（Score）；
5. 進行決策（Decision）。

二、生物辨識技術的準確率

生物辨識技術用以辨識個人身分的方式大致可以分為身分辨認（Identification 或 Recognition）與身分驗證（Verification）的能力，即從所有目標物中選擇出正確的身分，並且能夠合理無誤的確認該目標的身分為真實。由於沒有 100% 一致的確認機制，因此對於生物辨識系統的精確度來說，必然容許誤差值的存在：其中一種為拒絕誤差率（False Rejected Rate, FRR 或 False Negative），即合法的使用者卻無法正常通過身分辨識的比率（真實的使用者卻被拒絕）。另一種為接受誤差率（False Acceptance Rate, FAR 或 False Positive），即非法的使用者卻通過身分辨識的比率（假冒的使用者卻被接受）。FRR 太高會影響使用者對辨識系統的信任度及使用的便利性，FAR 太高則會明顯影響安全性，因此採取兩者交集最小值為目前實務上的作法，亦即交叉誤差率（Crossover Error Rate, CER）作為平衡點。各種技術要求不太一樣，若以最普遍的指紋辨識為例，會控制 FRR 約小於 3%，FAR 約小於 0.001%。生物辨識雖有此誤差率，但其安全性仍遠比使用者帳號與密碼的辨識安全度高。

三、不同生物特徵的生物辨識技術

指紋辨識利用資訊技術、光學技術及快速的統計演算技術獲得前所未有的進步，依據 2016 年國際生物辨識集團統計，指紋辨識在市場上的應用占比約 28.4%。不過指紋辨識的發展雖然相對成熟，卻仍有不少局限性，進而給其他生物辨識技術發展的契機，如臉部（11.4%）、虹膜（5.1%）、聲紋（3.0%）、靜脈（2.4%）及掌紋（1.8%）等生物辨識特徵，也陸續開發出許多實際應用的生物辨識系統。以下介紹常見的 4 種生物辨識技術：

㈠指紋辨識

生物辨識技術將傳統以油墨複印當事人指紋的指紋辨識方式，改變為以光學、半導體或超音波的方式對指紋進行掃瞄，其中光學技術為目前最常用的掃瞄方式，而超音波技術則是 3 種當中最準確的掃瞄方式。指紋辨識的原理是每個人的指紋都有其紋路之特徵，如指紋中紋脊及紋谷之分布型態，紋脊端點（ridges end）、分叉點（split）、分叉又接合點（split and join）或一個點狀等細微特徵（minutiae），作為指紋辨識比對系統之主要根據。

雖然指紋辨識可能因手指長繭、受傷、污垢或者、環境的過度乾燥或潮濕之影響而辨識失敗，年長者、戴手套者在登入指紋辨識系統也可能面臨困難。但是指紋仍有其獨特性，即使遇強酸腐蝕指紋，手指復原後所新長出的指紋仍會和過去相同。

指紋辨識使用之掃描器體積小，目前新款智慧型手機廣泛搭載此一功能。在智慧型手機高度普及化的趨勢下，使用者也在潛移默化中接受指紋辨識是一種方便、簡易又值得信任的生物辨識技術，進而使這項技術易於被接受且廣為流行。

㈡臉部辨識

攝影鏡頭影像畫質的提升、影像處理晶片效能的提高、辨識演算法的進展以及智慧型手機的整合，讓臉部辨識技術得以突飛猛進，能迅速將正確的辨識資料傳回前端裝置，藉此提升人臉辨識技術的精確性。

攝影機照相後，經過演算法從複雜背景中判斷出特定人物的五官和特徵，再進而比對以辨識身分。臉部辨識系統有以嘴巴、鼻子、眼窩及顴骨等特徵彼此之間的距離進行辨識，亦有些臉部辨識系統以臉部特徵的分布作為辨識的方法。

由於監視系統的廣泛設置與應用，使用者可能在未察覺的情況下進行辨識，侵入性較低，因此一般咸認為臉部辨識是較舒適之生物辨識方式。臉部辨識系統可能因為表情、年齡、化妝等些微的改變，以及久遠的資料、環境燈光或受辨識者的偽裝而影響辨識。人臉辨識除了基本的人臉定位、雙眼偵測、傾斜人臉校正、光線補償外，也同時採用觀察或記錄使用者眨眼或眼球轉動等特別的技術，以增強辨識成功率。

㈢虹膜辨識

虹膜位於眼球表面，虹膜的中心便是瞳孔，每個人的虹膜結構皆不相同，左右兩眼的虹膜也有明顯的不同。虹膜組織包含的資訊比人體任何部位還

要多。虹膜約有 240 個可供辨識的獨特處，臉部則約有 80 個、指紋只有 20 至 40 個。一般人自兩歲之後，虹膜就已經發展完成，永遠不會改變，且全世界幾乎找不到第 2 個虹膜相同的人，就連雙胞胎的虹膜也不相同。

虹膜辨識是內生物特徵，因此很難偽造。其辨識方式是使用者靜止於設備前，利用光線或紅外線打在眼球上，擷取虹膜上分布之斑點與線條，再藉由這些斑點與線條分布的位置作為辨識特徵。虹膜辨識過程中使用者不需要跟設備直接接觸，雖然並不會侵入人體，但是在辨識的過程中，利用光線或紅外線打在眼球，使用者的排斥性會比較強。但目前並沒有數據指出，在頻繁使用的情況下，是否會對眼球造成傷害。

虹膜可能受到糖尿病或青光眼等眼部病變而改變，且其設備的成本較高，雖有優異的 FRR 與 FAR，但目前的普及率尚待努力。

㈣聲紋辨識

聲紋辨識是以每個人聲音之不同作為辨識身分的方式，每個人的發音器官都不盡相同，因此聲紋特徵既有相對穩定性，又有變異性，不是絕對、一成不變的。聲紋辨識的優勢在於聲紋提取方便、自然，且獲取語音的識別成本低廉，只需要透過收音器將聲音傳輸至辨識端，不需要專屬設備，即可進行辨識。因此不論是電話或者電腦之麥克風均可以作為辨識之工具，但是由於收音器的收音品質不同，亦可能會影響聲紋辨識之準確度。

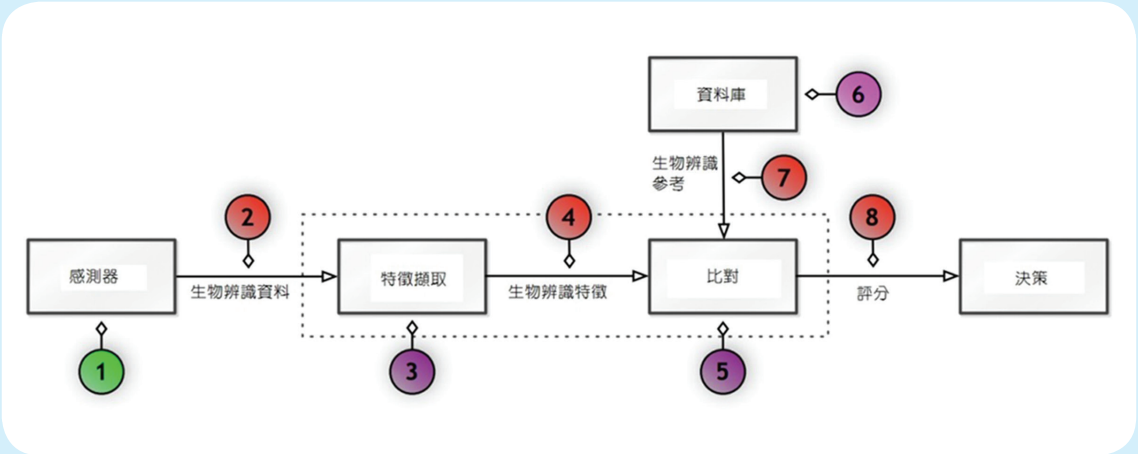
由於聲紋辨識使用方便，因此使用者對聲紋辨識技術的接受度頗高。雖然聲音可以被模仿或錄音假冒，但因機器辨識聲紋，其注重之處與人類聽覺注意之處並不相同，故而對於模仿之聲音亦可成功辨識。但是聲紋辨識並不適合作為主要的生物辨識方式，因為聲紋辨識會受到收音麥克風品質、背景噪音的音量或者受辨識者喉嚨不適等身體狀況的影響。

四、生物辨識技術的攻擊與挑戰

㈠直接攻擊（Direct attacks）與間接攻擊（Indirect-attacks）

圖二的程序 1 係直接攻擊，也被稱為展示或欺

圖二　生物辨識技術的直接攻擊與間接攻擊



騙攻擊（Presentation or Spoofing attacks），如透過特殊的工具蒐集指紋並進而欺騙指紋感測器，亦或者利用錄音重播、語音合成和語音轉換的方式欺騙聲紋感測器，即資料擷取階段的感測器 / 攝影機 / 相機並不一定是完全安全的裝置。

生物辨識技術有一個很大的問題：密碼外洩時可重新設定，生物辨識的唯一性卻可能因為事故（圖二的程序 2-8 的間接攻擊）而改變，驗證即永久失

敗。透過前述設備擷取的任何指紋或圖像都需要與原存取的參考資料進行比對，而此參考資料也必須是在安全環境中防護 / 儲存。是以生物特徵資訊的失竊無疑是所能想像的最具破壞性的身份資訊失竊形式之一。為避免遭竊用，對於生物特徵之儲存資料庫及讀取設備，應有高度安全性之保護措施。

㈡隱私權的挑戰

欲使用生物辨識技術進行個人身分辨識，不可避免地必須先就個人之生理特徵及行為表現進行蒐集，但生物辨識技術之資訊蒐集本身便可能存在法律上之爭議。由於個人之生理及行為特徵不僅可以作為辨識身分之用，同時亦可能涉及其他個人隱私的範圍，蒐集個人之生理特徵及行為表現便可能引發重大爭議。

參、生物辨識技術在我國金融機構之運用

隨著電腦技術的快速發展，利用資訊系統辨識使用者身分，已經行之有年並不斷精進，而如何透過電腦技術預防身分的偽冒，取得安全與便利之間的平衡，係資訊安全發展之重點。目前身分認證有以下 3 項技術：

一、你知（What you know）

與使用者所約定之資訊，且無第三人知悉（如密碼、圖形鎖、手勢等）。此即前述的使用者帳號與密碼，為目前資訊系統使用最普遍的基本認證方式。使用者輸入所知的使用者帳號與密碼，經核對使用者資料庫後，就能夠確認其合法身分。其缺點是過於簡單的密碼，或經常使用同一組密碼，極易遭到有心人士的破解。

二、你有（What you have）

使用者所持有之設備，並經確認該設備為雙方所約定持有之實體設備（如密碼產生器、密碼卡、晶片卡、電腦、行動裝置、憑證載具等）。此即透過使用者所持有獨一無二的設備，作為確認使用者合法身分的憑證。

三、你是（What you are）

使用者提供本身所擁有的生物特徵（如指紋、臉部、虹膜、聲音、掌紋、靜脈、簽名等），以辨識其真實身分。其優點是不用擔心會忘記「你知」的使用者帳號及密碼，或是忘記攜帶「你有」的特定設備，導致無法證明使用者的合法身分。

前述任何一項技術雖都可以當作身分認證之用，但是如果同時採用了「兩項以上技術」，其安全強度都會比使用單獨一項技術來得更強，此即所謂的雙因素驗證（two-factor authentication）方式。

中華民國銀行公會「金融機構辦理電子銀行業務安全控管作業基準」（以下稱安控基準）第七條交易面之介面安全設計規定，使用憑證簽章得應用於高風險交易，而高風險交易之安全設計可應用於低風險交易；應用於低風險交易之安全設計可應用於身分確認（如簽入作業）。使用晶片金融卡及使用一次性密碼（One Time Password, OTP）則僅限應用於低風險交易；至於使用前述三項之任「兩項以上技術」，也僅限應用於低風險交易，明確闡述了生物辨識技術在金融機構的使用，即在適當的「兩項以上技術」搭配下，生物辨識技術可以運用在低風險交易及身分確認（簽入作業）上。

2017 年 5 月公告之安控基準更將生物辨識技術增訂「間接」驗證機制，使金融機構可選擇「直接」或「間接」驗證生物特徵。依據安控基準規定：「間接驗證」係指由客戶端設備（如行動裝置）驗證或委由第三方驗證，金融機構僅讀取驗證結果，必要時應增加驗證來源辨識。此為我國已經開放金融機構可透過一定的安控機制而信任類似 Apple iPhone 手機指紋、臉部辨識或 Samsung Galaxy S8 虹膜辨識的驗證結果，進而進行低風險交易或簽入作業。反之，「直接驗證」即指自行驗證生物特徵，因此金融機構辦理生物特徵「直接驗證」需從事前述生物辨識技術的感測、擷取、註冊、儲存、比對及決策等程序。

生物辨識技術被使用的原因除了使用者或企業對於資訊安全的重視外，在使用時無須複雜的程序，以及具備較高的防護效果，都是關鍵因素。「間接驗證」生物辨識技術，金融機構不用去感測、擷取、註冊、儲存、比對及決策等涉及繁複申請程序及使用者隱私權的問題，也不用考慮使用者設備的類型或設備上所使用的生物辨識技術。「間接驗證」相較於「直接驗證」具備執行流程簡單、操作簡易及快速完成等特性，因此目前我國金融業主要是利用「間接驗證」生物辨識技術，搭配第 2 項身分認證

技術於行動銀行簽入的服務。

肆、結語

隨著科技的進步，生物辨識技術蓬勃發展，國際市場研究報告指出，2015 年運用行動生物辨識技術之交易認證超過 1.2 億次，預估 2020 年運用行動生物辨識技術的支付交易將超過 160 億次，而適合應用在行動金融服務之生物辨識科技，包括本文所介紹的生物辨識技術等。生物辨識技術再加上如密碼的第 2 個身分認證技術，的確能解決資訊安全和身分詐欺問題。

然而科技的發展也引發了重要的隱私權問題，究竟這些生物特徵資料屬於誰的？政府、司法機關、警察機關是否有權取用生物特徵資料？倘若指紋資料流出，遭有心人士利用會如何？生物特徵資料的安全性議題很重要，而生物辨識技術更牽涉複雜人權問題。我國 2005 年曾因為戶籍法第 8 條建立全民指紋資料庫有所爭議，並由大法官以釋字第 603 號解釋關於該條強制按捺指紋一案，認定戶籍法第 8 條之規定違反憲法第 22 條、第 23 條以及比例原則。2017 年又有立法委員提出戶籍法修正草案，主張國家應蒐集國民自出生至死亡都不會改變的生物資料如「虹膜」，供辨識身分之用，取代隨身攜帶身分證，引起軒然大波，遭質疑人權倒退並有「違憲」之虞。

其次，生物辨識特徵資料如何管理？由各機關自行管理或統一管理？以金融機構而言，生物辨識技術的過程中使用「直接驗證」需自行建置生物特徵資料管理平台，用來管理使用者的指紋、臉部、虹膜等生物特徵資訊，讓使用者依照不同服務的特性（例如登入帳戶、大額轉帳等），提供一個或多個生物特徵來進行驗證。而「間接驗證」機制除由金融機構所信任讀取的客戶端設備外，也包括委由第三方驗證的方式，即由一個統一的生物特徵管理平台，整合多種生物辨識特徵的認證技術以提供服務。但該第三方的驗證由誰建置？如何管理？值得討論。

隨著生物辨識技術日趨成熟，世界各國對於自動化身分認證之需求也日益增加。生物辨識技術之使用不僅可以減少各種身分盜用，亦可用於日常生活，使大眾生活更為便利與安全，因此可預見未來生物辨識技術將更廣泛與更普遍。創新的智慧型手機搭載生物辨識技術，為我國生物辨識技術的普及開啟了一扇門，金融機構也搭乘此一浪潮提供創新金融服務。然金融機構亦不應輕忽建立使用生物辨識技術之隱私權保障的重要性，以避免未來各種生物辨識技術應用可能引發對個人隱私之衝擊。

參考資料：

1. 王郁琦，「生物辨識技術之運用對隱私權的影響」，科技法學評論，2006.08。
2. 經濟日報，「生物辨識進化帶動 BANK3.0 應用」，2016.02.13
3. 金融監督管理委員會，「金融科技發展策略白皮書」，2016.05。
4. Digitimes，「生物辨識技術各分類研究與發展分析」，https://www.digitimes.com.tw/iot/article.asp?cat=130&id=0000173793_P278NER583OOLF4QEUQ10，2010.03。
5. 中華民國銀行商業同業公會，「金融機構辦理電子銀行業務安全控管作業基準」，2017.05。
6. 聯合報，「台權會痛批虹膜建檔侵隱私 已有綠委撤簽提案」，2017.11.15。
7. ERIK BOWMAN, EVERYTHING YOU NEED TO KNOW ABOUT BIOMETRICS 1, http://www.ibia.org/EverythingAboutBiometrics.PDF（last visited on Sept. 8, 2005）.
8. Alexander T. Nguyen, Here's Looking at You, Kid: Has Face-Recognition Technology Completely Outflanked the Fourth Amendment?, 7 VA. J.L. & TECH. 2（2002）.
9. Julia Scheeres, Smile, You' re on Scan Camera, http://www.wired.com/news/print/0,1294, 42317,00.html（last visited on Sept. 8, 2005）.
10. BOWMAN, supra note 1, at 2-3.
11. Bruce Schneier, The Guardian, Tigers use scent, birds use calls – biometrics are just animal instinct,（2009）.
12. 50 Years of Biometric Research: Accomplishments, Challenges, and Opportunities", Anil K. Jain, Karthik Nandakumar, Arun Ross, Pattern.
13. Sebastien Marcel, Trustech 2017 , "Challenges and Research Directions in Biometrics", 2017.11.

業務報導

1. 106 年 6 月 9 日至 12 月 8 日委託台灣金融研訓院承辦「2017 國際化金融人才培育計畫」，以育成海外業務開拓管理人才為目標，課程主題涵蓋「市場經營」、「策略運籌」、「管理思維」、「業務開發」及「跨國溝通」等五大領域，協助參訓人員建立國際視野、市場開發經營與產品服務之創新實力，訓練全球化競爭環境下銀行業亟需之整合型人才。
2. 106 年 6 月 9 日至 12 月 8 日與台灣金融研訓院共同主辦「2017 金融高階主管儲訓計畫」，以探究金融業經營模式「變革」與「創新」為主軸，架構「策略創新」、「領導發展」、「跨域整合」、「變革執行」四大培訓面向，協助金融機構培養具前瞻思維與決策能力之金融高階主管人才。
3. 106 年 12 月 5 日委託台灣金融研訓院承辦「兩岸金融研討會 - 兩岸銀行業轉型發展趨勢」，邀請兩岸產官學界資深專家從銀行轉型創新、行動支付業務及風險控管等觀點，探討台灣銀行業務未來轉型發展之方向與挑戰。
4. 106 年 12 月 6 日委託台灣金融研訓院承辦「國際科技金融論壇—智能理財與社群金融應用發展」，會中邀請新加坡、香港代表，針對金融業務創新趨勢提供精闢見解，探討智能理財與社群金融應用發展創新之機會與挑戰。

法規專區

法規新訊

1. 金融監督管理委員會於 106 年 11 月 16 日以金管銀法字第 10610005770 號令修正發布「銀行自有資本與風險性資產之計算方法說明及表格」第二部分信用風險標準法及內部評等法、第五部分市場風險及第七部分銀行自有資本與風險性資產計算表格。
2. 中央銀行於 106 年 12 月 21 日以台央業字第 1060050095 號令修正發布「金融機構流動性查核要點」，併修正規定第 7 點、第 10 點有關之「流動準備比率未達最低標準」通報單、新臺幣到期日期限結構分析表及「未來零至 30 天期距缺口比率未達最低標準」通報單表格。
3. 金融監督管理委員會於 106 年 12 月 25 日以金管銀法字第 10610006570 號令訂定發布「商業銀行申請轉投資創業投資事業及管理顧問事業規定」。
4. 金融監督管理委員會於 106 年 12 月 25 日以金管銀法字第 10610006575 號函停止適用財政部中華民國 87 年 8 月 31 日台財融字第 87807892 號函。

函釋命令新訊

1. 金融監督管理委員會於 106 年 11 月 17 日以金管銀法字第 10610005800 號令發布銀行法第 74 條規定解釋，商業銀行投資於綠能科技、亞洲矽谷、生技醫藥、國防產業、智慧機械、新農業及循環經濟等新創重點產業，核屬銀行法第七十四條第二項所稱之「配合政府經濟發展計畫」。
2. 金融監督管理委員會於 106 年 11 月 24 日以金管銀外字第 10600139780 號函釋示「銀行辦理衍生性金融商品業務內部作業制度及程序管理辦法」第 3 條第 1 項第 2 款第 3 目「持有有價證券」之範圍及認定標準疑義。

3. 金融監督管理委員會於 106 年 11 月 29 日以金管證發字第 1060042459 號函新修正「公開發行公司取得或處分資產處理準則問答集」第三十六題，銀行業、保險業、期貨商及槓桿交易商、證券商等金融特許事業辦理衍生性商品交易業務或從事衍生性商品交易，應依其業別適用「銀行辦理衍生性金融商品業務內部作業制度及程序管理辦法」、「保險業從事衍生性金融商品交易管理辦法」、「期貨商管理規則」、「槓桿交易商管理規則」、「證券商管理規則」，以及該會 105 年 10 月 18 日金管證券字第 1050030118 號（外國衍生性商品）及第 10500301181 號（國內衍生性商品）令等規定，爰得依本準則第 2 條但書排除適用本準則第 18 條至第 21 條規定。
4. 金融監督管理委員會銀行局於 106 年 12 月 6 日以銀局（外）字第 10650004410 號函釋示該會 106 年 6 月 20 日金管銀外字第 10600064741 號令第三點所稱集團企業提供「其他信用增強」適用疑義。