出國報告（出國類別：其他）

參加「APEC 金融監理人員訓練倡議—銀行詐欺偵測研討會」(APEC Financial Regulators Training Initiative: Regional Seminar on Bank Fraud Detection)

服務機關：金融監督管理委員會銀行局

姓名職稱：林家賢專員

出國地點：菲律賓馬尼拉

出國期間：106 年 5 月 15 日至 19 日

報告日期：106 年 6 月

目　　錄

出席 APEC 相關會議簡要報告 2

壹、研討會目的 4

貳、研討會過程 6

參、研討會重點摘要 8

一、舞弊行為的成因 8

二、傳統的銀行詐欺型態 9

三、新興的銀行詐欺型態 12

四、銀行詐欺事件的偵測 16

肆、心得與建議事項 21

伍、附件 24

出席 APEC 相關會議簡要報告

會議名稱（含英文縮寫）	APEC 金融監理人員訓練倡議—銀行詐欺偵測研討會 (APEC Financial Regulators Training Initiative: Regional Seminar on Bank Fraud Detection)
會議時間	106 年 5 月 15 日至 19 日
所屬工作小組或次級論壇	財長會議流程（FMP）
出席會議者姓名、單位、職銜	林家賢、金融監督管理委員會銀行局、專員
聯絡電話、e-mail	(02) 8968-9636 alianlin@banking.gov.tw
會議討論要點及重要結論(含主要會員體及我方發言要點)	一、 本次研討會討論各種銀行詐欺之態樣及偵測，包括信用卡詐欺、身分盜用、貸款詐欺、房貸詐欺、網路釣魚、ATM 詐欺及行動銀行詐欺等。除了講師授課外，尚有分組討論、經驗分享及意見交流，採互動方式進行。 二、 我方於本次研討會積極參與分組報告之討論，與各國金融監理人員就各項銀行詐欺議題進行意見交流，同時，也利用研討會的休息時間及空檔，主動宣傳我國金融市場與監理制度，並瞭解他國金融制度與監理情形，深化與各國金融監理機關的互動。 三、 由於我國正規劃將菲律賓列為免簽證試辦國，菲籍與會者對於免簽議題的詢問度頗高，我方已藉本次研討會向菲律賓朋友宣導免簽相關訊息，並邀請其來臺觀光交流。
後續辦理事項	
建議資深官員發言要點（★請務必依會議最新情形提建議，並	（無建議可免填）

提供簡要中英文說詞，以 1 頁為限）	
檢討與建議	本次研討會的建議事項計 3 項，分述如下： 一、 鑑於惡意軟體及駭客攻擊的威脅加劇，建議政府部門除強化資訊安全的措施之外，並持續關注對金融消費者帶來之影響。 二、 因應金融科技帶來的巨大變革，建議我國思考運用科技來強化金融監理。 三、 建議我方持續參加 APEC 研討會相關活動，且本會檢查局日後亦可視議題共同派員參與銀行詐欺有關之研討會。

1. 參加**資深官員會議暨相關會議**，請**於會議當日填列**此表，以 e-mail 寄至外交部 APEC 小組電子信箱：apecct@mofa.gov.tw, apecct@mofa.gov.tw。
2. 出席其他各項會議人員，請將本表附於與會報告首頁。
3. 14 號字標楷體，行距行高 20pt，請自行調整表格大小。

壹、研討會目的

1998 年 5 月，在 APEC（Asia-Pacific Economic Cooperation）各國財政首長的支持下，通過了 APEC 金融監理人員訓練倡議（APEC Financial Regulators Training Initiative, 簡稱 APEC FRTI），希望藉由對於各國銀行業與證券業監理人員的訓練課程，增進其對於各項新興監理議題及趨勢的瞭解，並強化亞太區域對於金融監理工作的協調與合作。

為了執行 APEC FRTI，亞洲開發銀行（Asian Development Bank, 簡稱 ADB）成立秘書單位，負責訓練課程規劃、講師遴選及相關訓練的執行，並設置兩個顧問小組（Advisory Group, 簡稱 AG）作為決策單位並督導 APEC FRTI 的執行工作。截至目前為止，已辦理 146 場次的 APEC FRTI 訓練活動，計有 6,180 人次的金融監理人員參訓。

本次研討會在位於菲律賓馬尼拉的 ADB 總部舉辦，由 ADB、菲律賓中央銀行（BSP）及菲律賓存款保險公司（PDIC）共同舉辦，計有來自斐濟（Fiji）、印度、印尼、南韓、馬來西亞、密克羅尼西亞聯邦（Federated States of Micronesia）、菲律賓、泰國及我國等 9 國共 45 位金融監理人員參加。

銀行詐欺（bank fraud）是指歹徒利用各種不法方式從金融機構或消費者身上取得財物之犯罪行為，近年來，不法之徒乘著網路及新興科技之便利，犯罪手法不斷翻新，詐欺事件層出不窮，使金融機構及客戶蒙受巨大的損失，目前各國金融監理機關的防制措施是否已跟上腳步調整，值得進一步探討。

本次研討會的目的是提供各國金融監理人員有關銀行詐欺事件的最新資訊、銀行詐欺事件的態樣、各種辨識及防制的工具等，預期目標包括：評估並瞭解銀行詐欺的現況、新興趨勢及面臨之挑戰；辨識不同類型的銀行詐欺，利用有效工具及技術發現問題並採取有效防範措施；從銀行詐欺的案例中學習如何應用工具及所學技術。

貳、研討會過程

課程安排及講師簡介

日期	議題	講師簡介
106 年 5 月 15 日	銀行詐欺簡介	Thomas Fu 任職於資誠聯合會計師事務所，具 CPA 及 CFE 等證照，已有 18 年在金融諮詢服務的經驗。
	銀行詐欺偵測	
	防制銀行詐欺計畫	
106 年 5 月 16 日	ATM、網路及行動銀行詐欺—案例	Dhanasite Suphachotiwatana 任職於泰國中央銀行(Bank of Thailand)，具 CISA 證照，在資訊系統檢查，以及銀行、特殊金融機構、非銀行支付業者監理之經歷超過 28 年。
	社群網路詐欺—案例	Mhel Plabasan 任職於菲律賓中央銀行(BSP)，具 CPA 及 CISA 證照，負責銀行資訊安全及支付系統之監理與檢查。
	身分盜用—案例	Dhanasite Suphachotiwatana 介紹同上。
	洗錢犯罪—案例	Dhanasite Suphachotiwatana 介紹同上。
106 年 5 月 17 日	小型企業詐欺—案例	Raymond A. San Pedro 任職於註冊舞弊檢查師協會菲律賓分會(ACFE Philippines Chapter)，具 CPA 及 CICA 證照，在內部稽核方面有超過 25 年的經驗。
	舞弊管理	Dante T. Fuentes 註冊舞弊檢查師協會菲律賓分會(ACFE Philippines Chapter)之主席，具 CPA、CFE 及 CAMS 證照。

106 年 5 月 17 日（續）	減少風險的對策	Mario B. Demarillas 國際電腦稽核協會馬尼拉分會(ISACA Manila Chapter)之主席，具 CPA、CFE 及 CISA 等證照，在資訊系統、內部稽核、資訊安全及資訊系統管理顧問的經歷超過 16 年。
	未來金融犯罪威脅的因應	Steve Cutler 曾任職於美國 FBI，有 5 年的時間領導 FBI 在菲律賓的調查及計畫工作，現已退休。目前任職於菲律賓一家從事資訊及數據收集應用的科技公司。
106 年 5 月 18 日	分組討論—辨識銀行詐欺個案研究	1.Reli Gueco 任職於資誠聯合會計師事務所，具有 CFE 證照，在內部稽核、特殊公司調查、企業資訊安全及風險管理等有超過 15 年的經歷。 2.Reiland Gumabao 任職於資誠聯合會計師事務所，具有 CPA 證照，在稽核、風險管理及法遵等有超過 10 年的經驗。 3.Adrian Festejo 長年擔任銀行法遵主管及顧問，並曾擔任菲律賓 Rural Bank of Bagabag 獨立董事。
106 年 5 月 19 日	分組討論—辨識銀行詐欺個案研究	Mario B. Demarillas 介紹同上。

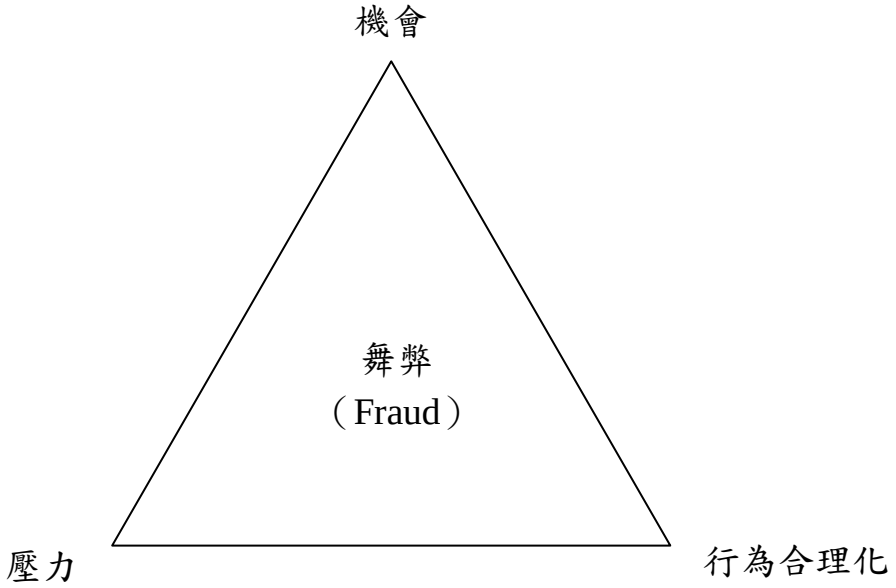
本次研討會分為 5 天進行，10 名講師分別來自監理機關、金融機構及金融產業部門，課程採互動方式進行，前 3 天主要是由講師介紹各項與銀行詐欺偵測有關的主題，並適時請各國金融監理人員分享監理經驗；最後 2 天則是由講師引導個案討論及分組報告，讓學員相互交流意見，表達監理上之觀點與看法。

參、研討會重點摘要

一、舞弊行為的成因

美國犯罪學家 Donald R. Cressey 提出的「舞弊的三角論」（Fraud Triangle），如圖 1 所示，以機會（Opportunity）、壓力（Pressure）及行為合理化（Rationalization）等三要素來解釋企業舞弊事件的發生原因。茲分別就各要素內容，說明如下：

圖 1　舞弊的三角論



1. 機會：(1)未建立有效的內部控制制度（internal control），或內控制度不完善；(2)制度或系統上的漏洞，遭人發現破解的方式；(3)對於員工過度的信任。
2. 壓力：(1)為滿足財務或物質上的慾望；(2)貪心或對於權力的渴望；(3)對於收入更高的期望。壓力可能來自於內部或外部的壓力，例如財務上的資金缺口或親朋好友的期待等，壓力是導致舞弊行為的動機。

3. 行為合理化：人們容易合理化自己不對的行為，同樣的，舞弊者在實行犯罪前，常會找到某個理由，以自己的道德觀念及準則說服自己，例如：「老闆平常對大家苛刻又小氣，拿一點回來剛好」、「不會因此有人受到傷害」、「這是自己原本應得的」、「自己的行為不是犯罪」等等。

二、傳統的銀行詐欺型態

(一) 信用卡詐欺（credit card fraud）

傳統的方式是不肖廠商利用側錄機（skimmer）在消費者刷卡時側錄信用卡上面的資料，然後將盜取的資料賣給不法集團，再經由這些信用卡資料製作偽卡，在消費者不知情的情況下，在實體店面購物消費。時至今日，線上購物消費變得十分普及，不法集團只要取得消費者信用卡的相關資料（例如持卡人姓名、卡號、有效年月及檢查碼等），就可能直接用於網路上的購物消費。

(二) 身分盜用（identity theft）

身分盜用是指不法之徒竊取個人資料，目的是為了利用被盜用者的身分獲取自己的好處及利益。個人的身分資料相當重要，不論是到銀行開戶或是線上購物等，都需要認證身分。個人身分資料洩漏的方式可能包括：線上購物、訂票、電話詐騙（telephone scams）、網絡釣魚（phishing）、駭客攻擊、信件或電腦遺失、未將資料清除乾淨的二手電腦等。

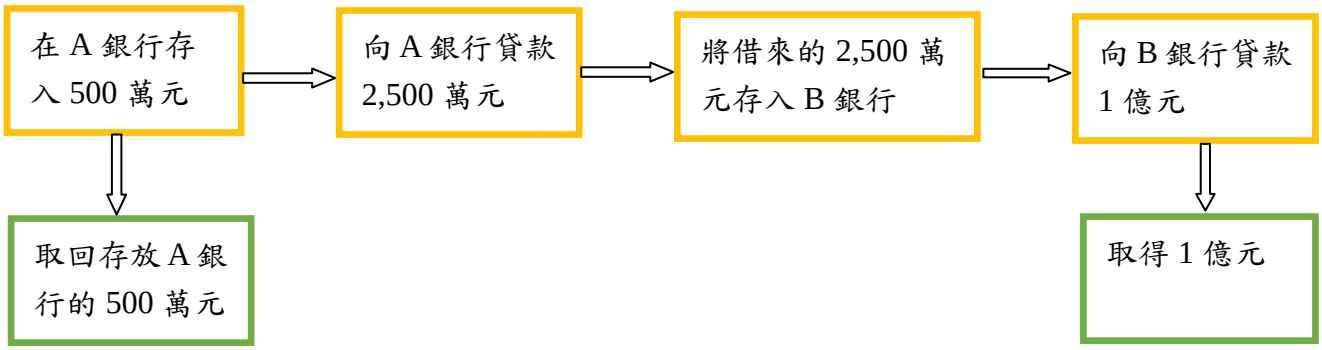
據美國政府統計，美國 2012 年曾經遭到身分盜用的受害者為 1,658 萬人，到了 2014 年已增為 1,758 萬人，可見身分盜用的問題益加嚴重。

歹徒可能利用這些盜用的身分進行銀行開戶、申辦信用卡或貸款、購物消費，甚至盜取受害者銀行帳戶內的餘額。此外，一些不肖銀行員工為了達成年度的績效，也可能會利用客戶的資料開立假帳戶進行交易，2011 年至 2016 年，美國計有 150 萬個假帳戶及 50 萬張未經授權申辦的信用卡，從事未授權的交易，雖然為銀行帶來了 260 萬美元的手續費收入，但銀行也因為這些詐欺事件付出 1.85 億美元的罰鍰，同時有 5,300 位銀行員工因此遭到解雇。

遭身分盜用的受害者除遭受財物損失外，信用及名譽也會同時受到影響，即便受害者是無辜的，但後續的清理及證明也將耗費相當多時間與功夫。

(三) 貸款詐欺（loan fraud）

圖 2　貸款詐欺的流程圖



常見的方式是借款人以無實際營運的空殼公司向銀行貸款，不久後就宣布破產或逃之夭夭，藉此將銀行的現金搬到自己的口袋之中。以圖 2 為例，不法份子設立一家空殼公司，利用一段時間建立起自己良好的信用紀錄，取得良好的信用評

等，以便向金融機構借款。之後，先向 A 銀行借入 2,500 萬元的貸款，並且利用 A 銀行的 2,500 萬元貸款再向 B 銀行借入 1 億元的貸款，接著宣布破產或直接捲款潛逃，從中獲取不法利益。

(四) 房貸詐欺（mortgage fraud）

房貸詐欺通常是該產業的內部人（包括銀行員工、鑑價公司、房屋經紀商、律師及其他專業人士）利用他們的專業知識及權力從事的不法行為。最近的報告顯示，大部分的房貸詐欺都涉及內部人士的勾結共謀（collusion）。

1. 用同一間房屋分別向不同的銀行申請房屋貸款。
2. 申請房屋貸款時，提供錯誤的房屋資產訊息，或慫恿鑑價公司高估房屋的價值，以便取得較高的房屋貸款（property flipping）。
3. 空氣房貸（air loan），是指不肖的房屋經紀商以虛假的借款人（可能是某位身分遭盜用的受害者）及不存在的房產作為抵押，虛設借款人的地址、工作、信用紀錄、房屋交易紀錄及鑑定價值，向銀行詐貸，當銀行發現時，沒有任何有價值的抵押品可以彌補損失。

(五) 支票詐欺（cheque fraud）

1. 未經授權更改支票上面的受款人或金額。
2. 盜取、複製或偽造支票。
3. 使用假發票騙取合法的支票。
4. 未經授權將支票存入第三人的帳戶。
5. 明知支票存款餘額不足，仍簽發支票付款（空頭支票）。

鑑於銀行目前對於支票詐欺已有一套辨識的程序，且實體支票多已被線上支付及電子支票（e-cheque）取代，爰筆者不多贅述。

三、新興的銀行詐欺型態

在數位科技的新時代，除了前述傳統的銀行詐欺型態，不法集團的犯罪手法也與科技結合，利用人性的弱點及系統的漏洞來詐取財物，且不斷地推陳出新，以下介紹幾種常見的新興詐欺型態。

(一) 假網站（fake website）

不法集團設計幾可亂真的銀行或信用卡公司的假網站，在沒仔細注意之下，人們不容易發現網址的不同，且介面幾乎和真實的一模一樣，常讓人誤信是真實的網站，進而被歹徒竊取帳號及密碼等資料。

(二) 網絡釣魚（phishing email fraud）

與假網站類似，但網路釣魚是經由不法份子寄送電子郵件給消費者，並偽稱是往來銀行或是信用卡公司，提供假的連結或惡意軟體（malware），或以資安警告為名要求消費者變更密碼，這些連結有銀行或信用卡公司的標誌，看上去幾可亂真，因此很容易受騙上當。

歹徒取得銀行帳戶、密碼及信用卡等資料後，會迅速地將帳戶內所剩的餘額取走，或利用信用卡資料進行線上購物消費。

(三) ATM 詐欺（ATM fraud）

ATM 為民眾的金融服務提供了便利性，然而，也因為 ATM 的普及、24 小時營運與無人看管的特性，加上程式或系統的安全漏洞，使 ATM 成為犯罪集團覬覦的目標。

傳統的 ATM 詐欺方式主要是 ATM 機體盜竊、在 ATM 卡片輸入處裝設側錄機盜取卡片資訊等手法，不過近年來在 ATM 植入惡意程式盜領現金的案件漸多，已成為新興的犯罪手法。

表 1　歐盟 2012-2016 年 ATM 犯罪統計

單位：件、百萬美元

	2012	2013	2014	2015	2016
一、ATM 相關犯罪					
發生件數	22,450	21,346	15,702	18,738	23,588
損失金額	283	265	299	349	355
二、ATM 機體攻擊事件					
發生件數	1,920	2,102	1,980	2,657	2,974
損失金額	20	25	29	52	52
三、ATM 惡意程式及系統攻擊事件					
發生件數	0	0	51	15	58
損失金額	0	0	1.28	0.79	0.48

資料來源：https://www.atmmarketplace.com/

表 2　近期亞太地區發生之 ATM 詐欺案例

國家	時間	事件摘要
日本	2016 年 5 月	日本 17 個都府縣超商的 1,400 臺 ATM，在 2.5 小時內遭到約百名嫌犯以偽造信用卡盜領超過 14 億日圓，由於銀行察覺有異狀，而通報警方追查。初步發現，疑似是南非銀行發行之上千張信用卡資料被側錄盜用。
我國	2016 年 7 月	第一金控旗下第一銀行的 41 臺 ATM 被國際犯罪集團植入惡意程式，短短 10 分鐘內被盜領超過新台幣 8,000 萬元現金，歹徒在未操作 ATM 的情形下，直接讓 ATM 大量吐鈔後提領。
泰國	2016 年 7-8 月	泰國國營的政府儲蓄銀行（GSB）21 臺 ATM 被植入惡意程式，被盜領約 1,229 萬泰銖，由於與臺灣第一銀行被盜領案手法類似，泰國警方懷疑為同一跨國犯罪集團所為。
俄羅斯	2016 年（時間不詳）	俄羅斯某銀行 8 部 ATM 遭到駭客攻擊，盜取約 80 萬美元，然而，警方調查時卻沒有發現任何惡意程式，ATM 日誌檔留下的兩句話成為僅有的線索。
日本	2016 年 4 月至 2017 年 3 月	日本 10 道府縣的 3 大銀行 ATM，在一年間遭嫌犯分次透過偽造大陸銀聯公司發行的銀聯卡盜領，金額達 32 億日圓。

資料來源：本報告自行整理。

從表 1 可知，歐盟 2016 年發生之 ATM 相關犯罪的件數超過 2 萬件，損失金額達 3.55 億美元，均較前幾年增加；值

得注意的是，2014 年開始出現 ATM 惡意程式及系統攻擊事件，截至 2016 年累計已發生 124 件。表 2 則整理了近期亞太地區發生的 ATM 詐欺案例，不論是以偽卡在 ATM 盜領現金或在 ATM 植入惡意程式盜領現金，兩種手法均造成各國金融機構嚴重的損失。

(四) 行動銀行詐欺（mobile banking fraud）

金融科技（FinTech）的快速發展，為消費者帶來許多快速又便利的金融服務，其中一項即是行動銀行，只要下載銀行的 app，就可以利用手機進行轉帳、收付款等交易，然而，在此同時手機卻也成為貪婪駭客攻擊的目標。

表 3　行動銀行詐欺的風險來源

風險因子	風險的來源
使用者	1. 手機遺失 2. 帳號及密碼被盜竊 3. 網路釣魚 4. 使用者不具風險意識或對風險不夠瞭解
裝置（手機）	1. 作業系統的漏洞 2. 瀏覽器及 app 的漏洞 3. 病毒、木馬及惡意程式
手機營運商/提供服務廠商	1. 設備的安全性不足 2. 監督的漏洞
金融機構	1. 設備的安全性不足 2. 詐欺偵測計畫的缺乏 3. 銀行員工的教育訓練及風險意識不足

四、銀行詐欺事件的偵測

(一) 信用卡詐欺的偵測

在消費者完成信用卡交易後，銀行通常會發送簡訊（Short Message Service, 簡稱 SMS）到消費者登記的手機號碼，確認是否為持卡人，當持卡人對於簡訊所載的消費有疑義時，便可向發卡銀行瞭解原因並立即通知止付。儘管如此，當持卡人沒注意到或遺漏簡訊通知的時候，不法的交易還是可能發生。

為了加強防範信用卡詐欺，銀行可以採用以下其他方式來確認是否為消費者授權的交易行為：

1. 對於持卡人過去消費行為（消費金額、商店、消費地點等）的大數據（big data）分析，有助於辨識可能的詐欺行為。
2. 拜科技進步所賜，銀行也可以利用生物特徵的辨識技術來保護持卡人免於信用卡被盜刷，利用指紋、聲音、臉部特徵來確認持卡人的交易行為。
3. 現代人手機不離身，加上金融科技的興起，消費者使用行動支付工具（如 Apple Pay、Samsung Pay）來付款變得相當普遍，消費者使用手機 app 進行行動支付的同時，app 也會利用手機的 GPS 定位交易發生的位置，銀行可以利用手機 GPS 的資訊來進一步確認交易的合法性。
4. 與前者類似，銀行也可以利用消費者在購物網站的 IP 位址，來辨識可能的詐欺行為。例如某甲在 5 月 15 日下午有一筆在美國的信用卡消費，經銀行比對資料，發現某甲在同日上午也有一筆在購物網站消費的紀錄，IP 位置在臺灣，由此合理懷疑其中一筆交易有可能涉及詐欺。

除了銀行方面的防範措施外，就持卡人而言，也要牢記以下的安全措施：

1. 勿隨意將信用卡號、生日或其他重要的個人資訊提供他人（例如電話行銷公司），因為銀行會利用這些資訊來驗證消費者的線上購物交易。
2. 如果帳單上出現可疑或不明的交易，立即通知發卡銀行。
3. 不要在不明的網站或商店購物消費。
4. 如果每個月的帳單是以紙本寄送的，須定期注意每月是否按時收到信用卡帳單，確認只有自己可以開啟郵箱，防範他人竊取帳單，取得信用卡資料。
5. 在海外旅遊時，也要將手機調整成可以接收簡訊的模式，以免出國期間信用卡被盜刷，遺漏銀行發送的交易訊息。

(二) 貸款詐欺的偵測

1. 案例：A 利用盜用來的身分，向同一間銀行的不同分行，分別申請多筆貸款，每筆貸款的金額都不高，且這些貸款的經手人都是銀行內部的一位作業主管 B。A 不斷利用借來的新款來償還舊的貸款，建立自己良好的信用紀錄，因 A 的信用紀錄良好，因此銀行給某 A 的利率下降，貸款的額度也逐漸提高，最後 A 在取得大筆貸款後便消失無蹤。
2. 詐欺的偵測：
   (1) 辨識同一人利用借新還舊的方式，建立自己良好信用紀錄的手法。
   (2) 注意貸款人是否只支付貸款利息，卻不償還本金。
   (3) 注意貸款人過去是否曾涉及其他銀行詐欺的事件。
   (4) 留意銀行作業主管核貸的情形。

(5)注意給予客戶不正常的低貸款利率。

(三) 貸款詐欺的進一步偵測

如果銀行可以從貸款人的人際關係或社群網路（例如 Facebook, Linkedin, Line, WhatsApp, Wechat）取得更多的資訊，將可用於分析貸款人在網路上的行為，並從社群網站給予的信用分數，進一步瞭解貸款人的信用狀況。

1. 分析貸款人的網路活動情形，包括他們常去的網站及他們在網路上的評論。
2. 分析貸款人在社群網站的交友狀況，他的朋友是否大部分都是信用狀況不良或曾經涉入詐欺事件？
3. 一些社群網站會根據使用者在線上消費交易的狀況，給予個人信用評比的分數，這些資訊有助於進一步瞭解其信用狀況。

(四) 房貸詐欺的偵測—使用大數據分析辨識可能的詐欺行為。

1. 從銀行的資料庫，找到客戶申請房貸的房屋地址。
2. 使用 Google 地圖找到該筆房屋的位置，確認地址的真實性，同時利用 Google 提供的街景服務，查看房屋的外貌，初步瞭解房屋的狀況（例如申請的房屋座落於住宅區，但實際上卻是位於工業區的鐵皮屋工廠，明顯與事實不符）。
3. 目前政府已實施「不動產實價登錄」制度，因此可經由政府的不動產交易實價查詢網站，查詢該筆房屋附近區域的交易價格，經過對交易價格的分析，鑑估該筆房屋可能的價值，進一步辨識客戶申請的房屋貸款是否有過高之情形。

(五) ATM 詐欺的解決方案

1. 確保 ATM 開機的安全性，由於 BIOS（Basic Input Output System, 基本輸入輸出系統）可以讓使用者選擇從哪個裝置啟動系統，因此應有密碼保護。
2. 在 ATM 系統建立防火牆（firewall）。
3. 移除系統內未使用的程式。
4. 建立有效的防毒機制。
5. 定期修補 ATM 作業系統及所有內建的軟體程式。
6. 不同的 ATM 系統使用者，應有不同的帳號及權限。
7. 每年定期對於 ATM 進行脆弱性和滲透測試（vulnerability and penetration test）
8. 考慮 ATM 硬體環境的安全性是否足夠。

(六) 行動銀行詐欺的解決方案

1. 行動銀行 app 的提供者
   (1) 加強對偽冒 app 的偵測。
   (2) 對於消費者資料的加密保護機制。
   (3) app 安全性的自我評估。
   (4) 每年至少做一次道德入侵（ethical hacking）報告。道德入侵簡單來說就是在不破壞受駭者的資料下，成功的入侵系統並發現漏洞，同時告知受駭者進行修補。
   (5) 實施提升客戶風險意識的計畫。
   (6) 利用簡單易懂的文字，持續利用手機 app 或社群網站，讓客戶瞭解最新的網路攻擊方式及威脅的來源，並教導客戶如何防範。
2. 行動銀行的備援系統

(1) 硬體及系統邏輯的評估。

(2) 防範惡意軟體的入侵。

(3) 系統脆弱性的自我評估。

(4) 軟體的更新與修補。

(5) 資料外洩的預防。

(6) 工作日誌。

3. 行動銀行的登入

(1) 使用者須輸入帳戶及密碼登入。

(2) 限制登入失敗次數的上限。

(3) 使用時間的限制（使用者在一定時間無任何操作，即自動登出）。

(4) 有可疑情形發生時，利用簡訊或電子郵件向使用者示警。

4. 行動銀行的交易

(1) 使用雙重身分認證（two factor authentication），亦即只有帳號和密碼的認證還是不夠的，還需要透過第二種認證方式進行身分的驗證，例如簡訊、一次性密碼（One Time Password, 簡稱 OTP）及代碼（token）等。

(2) 有可疑情形發生時，利用簡訊或電子郵件向使用者示警。

(3) 建立每日交易的工作日誌。

5. 消費者方面

(1) 不要連結不安全的網站或下載可疑的 app。

(2) 安裝防毒軟體及安全更新。

(3) 不要設定容易讓人猜中的密碼。

(4) 定期檢視行動銀行的交易紀錄。

肆、心得與建議事項

一、 參與研討會之心得

乘著網路及新興科技之便，不法份子從銀行或銀行客戶取得財物的手法日益翻新，詐欺事件常難以被發現。因此，如何偵測詐欺舞弊的事件，發現問題並進一步採取防制措施，成為金融監理的一個重要課題。

本次研討會除了從 10 名專家精闢的解說中，汲取其寶貴的實務經驗外，筆者更經由分組報告的腦力激盪中，對於各種銀行詐欺的型態及偵測方式，有更深層的認識，獲益良多。此外，筆者也利用研討會的休息時間及空檔，與各國金融監理人員進行意見交流，主動宣傳我國金融市場與監理制度，並瞭解其金融制度與監理情形，深化與各國金融監理機關的互動。

在研討會課程之外，與菲律賓央行及菲律賓存保公司的監理人員建立良好的友誼關係是此行的另一收穫，由於我國正規劃將菲律賓列為免簽證試辦國，菲籍與會者對於免簽議題的詢問度頗高，筆者已藉此機會向菲律賓朋友宣導免簽相關訊息，並邀請其來臺觀光，深化民間的交流。

二、 本次研討會之建議事項

(一) 鑑於惡意軟體及駭客攻擊的威脅加劇，建議政府部門除強化資訊安全的措施之外，並持續關注對金融消費者帶來之影響

從銀行詐欺手法的演變來看，近年來惡意程式及駭客攻擊的威脅，有日益嚴重的趨勢，2016 年已有多國金融機構的 ATM 遭到駭客盜領；不僅如此，受害者也從金融機構及消費者，擴及政府部門，近期最著名的案例，便是孟加拉央行的海外帳戶在 2016 年初遭到駭客盜領的事件。

駭客係以惡意程式駭入孟加拉央行負責國際轉帳電匯的電腦與印表機，假冒該行向紐約聯邦儲蓄銀行提出轉帳請求，巧妙地利用孟加拉央行休假日的空檔，企圖從該行於紐約聯邦儲蓄銀行的存款轉走 10 億美元，最後成功得手 8,100 萬美元（部分轉帳因為駭客將帳戶名稱拼錯而遭擋下，使整起事件曝光），部分贓款已流到菲律賓的賭場進行洗錢。事件爆發後，引起全球高度關注，孟加拉央行總裁因此引咎辭職。

目前政府多數業務都已從人工及紙本改為電子化作業，自動化雖帶來了快速及便利，但電腦系統的潛在漏洞，也容易讓駭客有機可乘，一旦發生問題，影響範圍廣大且深遠。面對惡意軟體及駭客攻擊的威脅，建議政府部門提高警覺，強化資訊安全的措施。

在另一方面，近期行動支付在全球各地掀起一股熱潮，Apple Pay、Samsung Pay、Android Pay 等國際行動支付相繼來臺布局，並與銀行業者合作推出諸多優惠措施吸引消費者使用，可預見行動支付將日漸普及，在此同時，如何確保消費者使用手機進行安全及便捷的交易，也就更形重要。政府已於 2015 年提出「電子化支付比率五年倍增計畫」，希望到 2020 年，國內電子支付比率從 26%提高到 52%，建議政府在推動計畫的同時，持續關注資訊安全與消費者保護的相關議題。

(二) 因應金融科技帶來的巨大變革，建議我國思考運用科技來強化金融監理

近年來金融科技的發展如火如荼，為金融服務及消費模式帶來重大的改變。然而，科技帶動金融科技的同時，也遭不法份子利用，出現新的犯罪手法與模式，使詐欺偵測的難度提

高，如何因應新興的舞弊模式，形成金融監理的一大挑戰。

為因應此一趨勢，金融監理也須與時俱進，跳脫傳統的思維，重新審視既有的監理模式，並思索在有限的人力及資源下，如何運用監理科技（RegTech, 即 Regulation 與 Technology 之重組字）提升監理的效率與效度，節省時間及作業成本。

(三) 建議我方持續參加 APEC 研討會相關活動，且本會檢查局日後亦可視議題共同派員參與銀行詐欺有關之研討會

本次研討會課程內容及討論之案例，涉及偵測銀行詐欺事件之實務及執行面，部分國家之與會代表為金融監理機關之檢查人員，或同時由監理人員及檢查人員參加。依據本會檢查局組織法第 2 條規定，檢查局掌理金融控股公司、銀行業、證券業、期貨業及保險業金融檢查制度之建立及檢查等事項，對於金融機構的檢查經驗豐富，爰日後如有類此議題之研討會，除我方可持續派員參加，並建議本會檢查局亦可視議題共同派員出席，分享在偵測舞弊事件上的檢查實務經驗與看法。

伍、附件

一、 研討會議程。

二、 研討會參與者聯絡方式。