

出席“2016年萬事達卡 亞太風險管理年會”



2016年8月1日至4日，本局委派資訊罪案調查處二等刑事偵查員彭倩祺前往印尼峇里參加由萬事達國際組織舉辦的“2016年萬事達卡亞太風險管理年會”，與會者有來自馬來西亞、菲律賓、新加坡、越南，以及中國台灣、香港和澳門等地的代表，會議主要由各國從事相關業務的專家進行專題演講，內容圍繞欺詐、風險管理、資料安全、資料洩漏，支付模式之改變及趨勢帶來之機遇與挑戰等。

隨着科技進步及數位金融的成熟，利用創新數位科技產生之支付方式大大改變了人類的消費及生活模式，並提高了商務及個人交易的效率。人們交易方式由從前使用現金轉變至使用銀行卡和各種支付卡，再逐漸轉變為使用固定互聯網網絡及移動設備進行支付，均體現人類對便捷支付之需求。然而，各種便捷支付方式出現之同時，各種危害支付環境及客戶帳戶及個人資料安全之欺詐行為亦相繼產生。

為提升整個支付系統的安全性和可靠性，萬事達國際組織針對支付安全問題作出應對，致力研發創新科技。鑑於與支付卡相關之網上交易欺詐日益嚴峻，萬事達國際組織採取如下對策：

1. 於2001年推出EMV技術，EMV的核心技術是在每筆交易中加入動態數字信息，引入唯一的權杖，令複製資訊幾乎不可能，提高了交易的安全性，降低了客戶被欺詐的風險。當消費者在支援EMV技術的終端設備付款時，動態驗證可以立即識別該筆交易是否真實、是否經過核准、是否由真實持卡人發起。在使用PIN碼（個人識別碼）時，EMV晶片還可驗證使用者是否為真正的持卡人。

2. 推行SecureCode，購物者須在一個由發卡機構提供的頁面視窗中輸入SecureCode，其線上交易才可獲得授權。僅需幾秒鐘，發卡機構即可確認進行交易者是否持卡人本人。

3. CVC2保安碼。每年有越來越多的商戶與線上客戶進行“無卡”交易，電子商務日益頻繁，新的欺詐形式亦隨之產生，將這個只有發卡銀行及持卡人才知道的CVC2保安碼印製於支付卡的背面，大大提高了支付卡的安全性。

4. NFC技術，是一種近距離的資訊無線傳輸技術，通過讀卡器產生磁場，磁場產生電流驅動連接之晶片進行計算，計算結果透過電磁波傳給讀卡器，完成資訊傳遞。此技術兼容手機，比接觸式晶片更為方便。

5. HCE行動支付服務。任何Android手

機使用者不必更換 SIM 卡，就能將手機當作信用卡直接進行支付，實現了手機信用卡化。

6. Tokenization，即令牌化。自九十年代初起，世界各地有大量磁帶卡資料被盜並用以複製假卡進行交易，時至今日，被盜取的信用卡資料多被用於網上交易，這情勢促使晶片及各類安全支付軟件的誕生，儘管晶片卡及安全軟件絕少被破解，但一旦發生就必須廢除有關支付卡帳號及所有被綁定之信息，手續十分繁複。因此，令牌化可解決支付卡資料被盜或遺失手機的問題，令盜用者無法使用相關之支付帳戶資料。令牌化的核心就是讓 16 碼的支付卡卡號轉化成代碼（代替帳戶號碼及密碼），手機送出代碼至銀行，銀行會翻譯成對應之帳戶號碼並進行操作，整個支付過程除銀行以外的其他環節無法獲知真實的帳戶號碼及資料，大大降低支付帳戶資料洩漏的風險。

此外，萬事達卡創新實驗室亦致力研究利用生物技術進行支付認證，包括臉部認證及指紋認證技術，為邁向先進而安全的交易新世代做好準備，實現“萬物可支付”的目標。

最後，各國及地區執法部門代表進行閉門

會議，分別講述了當前各地銀行卡犯罪的概況與趨勢，以及在偵查銀行卡犯罪時所面對的挑戰和難處，其中，各國警方均表示面對越趨嚴重的盜用支付卡資料進行網上交易的案件，因着各國的法制差異及限制，在案件協查、情報互通等方面均有待加強，並須完善相關的合作機制。此外，基於先進科技及加密技術之發展，各國警方在調查相關犯罪時均面臨取證困難，因此必須貫徹落實科技強警的理念，貼近時下之科技發展趨勢，瞭解當前的犯罪模式及變化。

本局人員透過是次會議更深入瞭解主辦組織在管理資料安全及控制風險方面所實施之措施、商務卡及銀行卡交易與相關服務提供者之關係、資料在保存及傳送期間的洩漏風險等問題；同時也知悉世界各地有關銀行卡的犯罪模式及趨勢、執法部門打擊相關犯罪所面對的挑戰和困難，以及一系列具建設性和創新的應對建議。本局人員透過會議與各國及地區警方加深了互動及聯繫，對日後的刑偵實務工作有莫大的裨益。

