第五章

美麗交易：重新省思電子商務安全

Ed Bellis

資訊安全一直是執行電子商務的最大障礙，我們這群人在清醒時刻，無時不在想新的與不同的方式來確保這些系統和應用程式的安全性，這些系統和資料一起啟動。畢竟，這些都是我們想保護的資料。

電子商務安全中一個主要的挑戰，在於以實際的方法確保支付交易資料。這意味著在各個不同的應用中有很多不同的安全議題待執行，本章的重點將專注於信用卡資料，如帳戶號碼、安全和 CV2 碼、PIN 碼、磁條資料、到期和發卡日期。另外也將包括我們認為有必要的額外資料，使這個程序更安全，如一筆交易的驗證和授權。

讓我們來看看信用卡資料可能的故障點。當消費者使用他的信用卡或借記帳號（沒有卡）進行購物，無論是在線上或離線，譬如電話購物的情況下，把資料提供給商家，以證明他有足夠的資源或信用來支付商品。這些資料經由支付閘道器、後台辦公應用軟體、銀行網路和系統、發卡銀行和卡相關網路等，穿透商家內部與外部的環境。

其中一些商家（分支機構）可能代表其他商家轉售商品，另有其他商家（包裝）幫助各供應商和轉售商包裝商品和提供各項服務。這意味著，目前的資料必須通過所有提供服務的商家和輔助商務系統，耗用了許多時間在不同的地方，敏感的資料駐在其中（見圖 5.1）。最後，安全等級降低，因為許多這些網路和系統包含老舊應用程序和操作系統，難以保護支付資料。

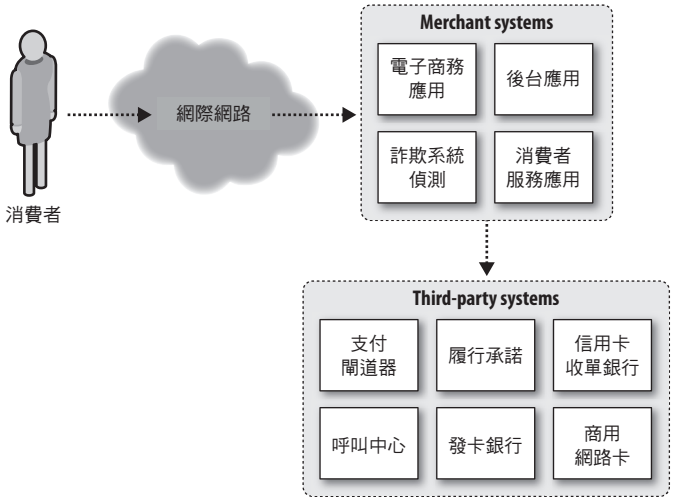

圖 5.1 信用卡資料激增

但是，如果我們採取另一種方法？推翻當下在電子支付和電子商務的一些假設，並假定商家不儲存任何資料，這時會發生什麼事呢？如果我們從來沒有把敏感資料送給商家列在第一順位的話，會發生什麼事呢？正如我們所看到的，要保護這些資料的安全性，其中一個主要的困難是在驗證每個資料會流經的地方。但是，如果這驗證不再要緊？或者至少不是那麼要緊的話呢？

5.1 解構商務

為了重新思考電子商務的安全性，首先我們必須檢視當下電子商務的安全性是如何運行的。目前的資安模型有其根本上的缺陷，並陷入過於廣泛和沒必要的假設中。一系列的補丁和急救包被標榜為最佳做法，並成了深入安全策略的一部分。雖然這些安全做法在一般意義上有助於保護資料，但並未著重在支付系統實際會遭遇的問題上。

作為一個行業，我們花了大量時間和金錢追蹤資料，經過加密改造資料，在儲存和傳輸時保護其安全，在在都只是彌補這不安全模型。

電子商務業界已對商家和服務提供商建立其營運需求，此需求之建立是基於支付卡行業的資料安全標準。但是，為什麼？這些資料已經成為很多在電子商務和零售行業安全專業人員（和與他們敵對的人）皇冠上的寶石。

5.1.1 分析安全性內容

根本的問題是，持卡人的資料變成**共享的秘密**。正如我們所看到的，這個秘密通常需要和許多群體共享，即使只是一筆交易。由於安全性依賴當事人之間對安全控制的共識，帳戶資料被洩漏幾乎是無可避免的事。

Visa 公司指出，在 2008 年第三季財報，Visa 品牌包括 Visa、Interlink、Plus 和 Electron，交易總額由 86.5 億美元增加到 95.9 億美元，這使得我們對資料侵害產生了一些看法。Visa 是卡的最大品牌，但也只是眾多品牌之一。而且每一筆交易可能要通過多個商戶系統、支付閘道、服務提供商、執行系統、銀行網路和卡網路。這麼多的共享秘密令人不寒而慄！

要混成這些議題再加上共享秘密的複雜性，商家或服務提供商總有理由儲存敏感資訊，如在帳號最初交易完成後，要處理下列程序：

經常性費用

許多商家提供服務，每週、每月、每季或年度需要做定期支付。為了對同一帳戶作定期商務處理，只要消費者是商家顧客，商家就必須要儲存敏感支付資訊。

退款

要發出退款，商家必須儲存帳戶號碼以提供服務或收費。為防止詐騙，許多收到款項的銀行會要求商家或服務提供商退款給之前已付款的帳戶，並確認帳號是絕對正確的。

便利消費者

消費者往往選擇將自己的帳戶資料存到經常往來的商家。這與我們後續要討論的消費誘因得出結果類似，便利超過風險。

5.2 微弱的改善意願

為了解決這一大群共享秘密的人，卡協會想出了一個安全的概念代碼（CV2），把三或四位數字印在卡片上。這是作為一個另類二級驗證元素，試圖證明買方真的擁有這張卡片。

在這個補救系統有兩個缺點。首先，安全碼變成了另一個共享秘密。對商家或服務供應商而言，引入安全碼等於又引入一些和安全碼相關的規則。但商業體質未變，仍要依靠購買路徑中的薄弱連結。其次，目前並非所有銀行都支援安全碼，就算支援也不是在所有情況都需要。這意味要讓商家因安全碼的原因拒絕買賣，商家幾乎無此意願執行此規則。因此，安全代碼對反詐騙系統而言只有一點點作用。

雖然 CV2 嘗試驗證消費者，但卻缺乏對商家的驗證。購買者怎麼知道商家是合法的？用什麼方法來防止消費者從社交工程或釣出其支付資料？

該卡協會和第三方付款服務供應商建立了額外的安全計劃，在無卡場合執行驗證和授權。讓我們來分析目前幾個比較常見的程序，評估這些程序是怎麼運作的，有什麼缺點。

5.2.1 3-D 安全

3-D 安全是由 Visa 基於 XML 協定制定的，目的在驗證消費者的卡。VISA、萬事達和 JCB International 都採用此協定，使用的名稱分別是 Verified by Visa、MasterCard SecureCode 和 J/Secure。

3-D 安全交易

3-D 這個名詞意指涉及安全模型的三個領域。第一個領域是**收購者**，實質上是電子商務的商家或收單銀行。商家使用相容的軟體，呼叫發卡銀行（第二個領域，發卡銀行人），以確認該帳戶持有人（第三個領域）已在 3-D 安全卡方案註冊。如果持卡人已註冊，發卡銀行則從商家的網頁收集帳戶持有人的 PIN 碼或密碼。此驗證協定以 XML 格式在 SSL（Secure Socket Layer）上傳輸。在 SSL 確保帳戶持有人的 PIN 碼或密碼的機密性和主機與客戶端的真實性。與此同時，PIN 碼或密碼不用提供給商家或收單銀行，保持此資料的機密性，只有持卡人和發卡銀行知道。這個過程雖複雜不易描述，但卻是個大家熟悉的第三方信任的情景：

1. 購物者連接到商家的網站，進行購買選擇，並輸入信用卡資料。
2. 商家伺服器插件（MPI）發送主帳戶號碼（PAN）到目錄服務伺服器。
3. 該目錄伺服器查詢相對應的存取控制伺服器（ACS），以確定主帳號認證的有效性（或證明一個認證嘗試）。

如果沒有適當的存取控制伺服器可用，目錄伺服器會建立一個 MPI 回應，接著從步驟 5 繼續處理下去。

4. 存取控制伺服器回應給目錄伺服器。
5. 該目錄伺服器轉發存取控制伺服器回應（或自己）到 MPI。

   如果沒有認證，也沒可用的企圖驗證證明，3-D 安全處理結束。如果需要的話，商家、收購方或付款處理器可提交一個傳統的授權要求。
6. MPI 發送付款人的認證請求（PAR）給存取控制伺服器。
7. 存取控制伺服器收到付款人身份驗證請求。
8. 存取控制伺服器進行身份驗證，使用適用於主帳號（PAN）的購物流程，這可能涉及到一個密碼、晶片或 PIN 等，另外，存取控制伺服器可能會產生一個嘗試認證的證明。
9. 存取控制伺服器，將付款人認證響應資訊格式化成適當的值，並執行簽署動作。
10. 存取控制伺服器將付款人的認證回應資訊傳送回 MPI，以便將資料存於快取，進行進一步的交易。存取控制伺服器可以選擇將資料發送給認證歷史伺服器（AHS）。
11. 付款人收到的 MPI 認證響應。
12. MPI 驗證付款人認證響應的簽章（自己執行驗證或將訊息傳送到獨立的驗證伺服器）。
13. 商家與收單銀行交換授權資料。

繼續步驟 13，收單銀行經由授權系統如 VisaNet 與發卡銀行共同處理授權，然後將結果傳回給商家。

評價 3-D 安全

3-D 安全有一些不錯的功能可用於驗證用戶與帳戶對應匹配，在商家部份盡了很大責任，以確保已向信用卡品牌註冊；使用標準支付軟體，並對收單銀行保有一個有用且合法的商家帳戶。但在實用上已證明其不便使用。

釣魚在 3-D 安全一直是個持續的問題。一方面，一些釣魚者模仿 3-D 行為；另一方面，一些用戶把 3-D 安全交易誤認企圖釣魚而加以拒絕。這跟 PIN 驗證與本身具有的不同調有關，因為請求是來自不同領域而不只是商家，且事實上，消費者可能無法識別發卡銀行和 DNS 名稱。

在 3-D 安全上一個更基本的安全問題是：就像在上一節所描述的 CV2 號碼一樣，並沒有硬性規定所有交易都要使用它。因此，客戶的帳號仍然是一個有價值的共享秘密。由於主帳號在交易流程需跨越商家、支付系統和供應商系統，這些參與交易個體都必須執行同等級的預防措施以保護主帳號資訊。

事先認證帶來了一些額外的負擔，因為必須在商家、銀行和消費者之間的協定做些設定。雖然其負擔遠低於我們即將要討論的 SET 協定，但它仍不是很理想。

3-D 安全除了要面對其消費者常面臨的釣魚抱怨這個不力局面之外，另有些其他難處。支持 3-D 的信用卡公司都表示，若詐欺交易貫穿 3-D 安全，他們不會承擔對商家應負的責任。但這卻是要求商家執行 3-D 安全的一個很大的激勵措施，若把責任轉嫁給消費者，但這一區塊通常消費者又不用負什麼責任。因此 3-D 安全並非萬無一失，持卡人無法據此安步當車。本質上它是將成功的釣魚攻擊歸咎給受害者。

5.2.2 安全電子交易

安全電子交易（SET）是在 1996 年由 Visa 和 MasteCard 共同開發的協定，以便在不安全的網際網路執行安全的信用卡交易。SET 採用 X.509 及其擴展版本的憑證格式，並使用公共密鑰加密，以確保參與電子交易各方的傳輸數據，同時保有機密性。SET 獨有的具有約束力的演算法，以臨時憑證取代消費者的帳號資訊，讓網路商家永遠不需要取得顧客敏感資訊。參與交易每一方都需預先向憑證授權機構（CA）註冊，使得發卡銀行在允許商家進行電子商務交易之前，先盡職調查，然後對交易各方進行認證。

在消費者端，SET 為訂單資訊連同付款資訊建立雜湊值。然後付款資訊連同已簽署的訂單雜湊資訊傳送給銀行，消費端的軟體同時也將訂單資訊連同簽署過的付款資訊雜湊值發送到商家。持卡人和商家兩者都對訂單建立雜湊值，銀行或支付閘道器收到資料後會比對兩個雜湊值是否相等。

此協定為交易提供了幾個保護措施：

- 在交易之初，驗證各方已在 CA 註冊。
- 藉由在消費者、商家和支付閘道器交換憑證，在執行交易時進行附加認證。
- 敏感資料如帳戶號碼，只有在消費者與銀行之間共享，並只共享必要資料，無任何冗餘，商家不必儲存或傳輸這些敏感資料。

SET 交易

一筆交易的序列事件順序如下：

1. 客戶取得銀行核發信用卡帳號，該銀行支持電子支付和 SET。
2. 客戶收到由銀行簽署的 X.509 V3 數位憑證。
3. 客戶下單。
4. 每個商家都有自己的憑證，並將此憑證發送給客戶，以便客戶驗證它是一個有效的商店。
5. 送出該訂單及付款。
6. 商家要求發卡銀行授權支付。
7. 商家確認訂單。
8. 該商家提供服務，遞送貨物給客戶。
9. 商家要求發卡銀行付款。

評估 SET

不幸的是，由於公共密鑰基礎設施（PKI）所需的龐大支出和 SET 所需的註冊程序，SET 很難被廣泛採用。管理上的複雜性使得 SET 難以在電子商務市場佔有一席之地。

5.2.3 單用途和多用途虛擬卡

最近的一個趨勢是使用虛擬卡以確保持卡人安全。一些公司如 PayPal、MBNA 和 Citi 集團，在此應用領域，彼此互相成為強烈的競爭對手。

虛擬卡就像一個普通的信用卡一樣，但用在無卡交易場合，商家處理方式和普通信用完全相同。有鑑於此，商家甚至不用知道這卡是虛擬的，商家系統處理虛擬卡和處理其他信用卡帳戶號碼程序是相同的。

虛擬卡如何工作？

每個供應商執行虛擬卡的方式略有不同 ，但基本上有兩種型號：一次性使用和多次使用虛擬卡。這兩種類型可透過持卡人的要求快速產生。現有信用卡帳戶持有人從虛擬卡供應

商處申請一個虛擬卡，在特定的電子商務網站使用。虛擬卡供應商將虛擬卡號、到期日期和 CV2 安全碼提供給申請者。

單一用途卡可用於有限付款的單筆交易。這些卡通常在幾個禮拜或甚至更短的時間內就到期，只能用於持卡人指定的商家。因此，即使相關資訊遺失或被偷，很快就變得無效，對攻擊者形同無用。

有很多虛擬卡供應商提供多用途虛擬卡。這些卡可適用於經常性收費，如每月支付賬單。多用途卡和單一用途卡一樣，具有很多安全功能，例如只能用在指定的商家，有消費金額上限等。如果多用途卡遺失或被盜，攻擊者只可在特定商家使用，也只能用在指定授權的經常性費用。這大大減輕了詐騙行為。

5.2.4 殘破的激勵機制

經濟領域中的資訊安全部分一直存在一個破碎獎勵的問題。激勵機制在一個需多方協調執行的任何系統，都是一個關鍵因素，特別是依賴人做“正確的事”，但又不能保證他一定會照規定做。如果沒有適當的激勵機制，通常就會發生問題。要調整這個導致故障（市場失靈）的外部壓力，金融系統會採用兩種方法：

規定

政府或行業協會制定規定，以解決市場失靈問題，如壟斷、污染、缺乏“真的很好”的定位或在此所提的資訊安全。在這方面的規定形式包括健康保險攜帶和責任法（HIPAA，Health Insurance Portability and Accountability Act）、金融服務現代化法案（GLBA，Gramm-Leach-Bliley Financial Services Modernization Act）和沙賓法案（SOX，Sarbanes-Oxley Act）等。

責任

這是一個法律機制，對被判定造成損害的一方，強制執行賠償（通常是金融）責任。在資訊安全的情況下，一個人或公司可能會發現，如果他們不採取合理的預防措施來保護資料，將承擔法律責任。

現在我們來看看信用卡在“安全市場”失敗的經驗。經過我們的財務模型，我們必須深入研究當前的主要參與者：消費者、商家、服務供應商、收單銀行、發卡銀行和卡組織等，其動機為何。

消費者

人們常常認為，消費者得小心保護自己的信用卡資料，因為他們最常被濫用，但由於一些現有的法規控制這些外部因素，實際上不是這樣的。在美國，消費者對任何詐騙行為，只需承擔 50 美元的責任。在一般情況下，發卡銀行會撤消這 50 元罰款，讓消費者愉快消費。

因此，雖然大多數消費者都希望能保護他們的帳戶號碼、安全碼和截止日期等，但在購買的慾望下，消費者少有動機去保護資料。這動機即使存在也不是財務上的，大多是為了省時間或避免卡被侵害所帶來的麻煩。

要做比較的話，消費者對借記卡倒有更大的保護動機，因為消費者並未受到與信用卡相同的法規保護。而且借記卡往往直接與消費者的支票和儲蓄帳戶有關，若借記卡遭到侵害，對消費者便會造成直接的損失。

商家和服務供應商

在現有模式下，若有侵害事件發生，通常都會造成商家損失。若持卡人資訊遭侵害，可能導致雙方得釐清有關規定和應負責任的後果。商家會受到支付卡行業中卡協會的規範，其中規定了安全標準，當商家在處理和傳送資料時，必須遵守相關規定。違反標準的商家在財務和經營上都會遭受處罰。經濟處罰往往是由收單銀行進行評估，然後再將罰款通知遞交給商家。商家也可能被判定負有責任且被發卡銀行起訴，並賠償違規事件造成的任何費用損失，包括補發卡的成本等。

商家也要承擔接受詐騙卡消費的財務責任（除非使用 3-D 安全）。一個商人必須把數個詐欺檢測系統放到適當位置，以確保該正在使用的卡是有效的，並真的是由持卡人所擁有。若商家最終還是接受了信用卡詐欺行為，發卡銀行將發出退款單，將錢退還給消費者。如果商家已經處理這筆交易，並已送出這些產品或服務，它必須自行吸收交易損失。

儘管商家有很多的動機來保護這些資訊，但他們並沒有在採購過程實施有效的控制。如前所述，這個資料必須通過多個系統，包括商家直接控制外的系統。我們還看到，交易後商家還長期持有相關資訊，進一步增加了許多風險。

服務提供商也必須遵循 PCI 資料安全標準（DSS）的規範。根據 PCI 安全委員會的定義，服務提供者意為：

> ... 企業實體，不是品牌支付卡的成員，或不是直接涉及處理、儲存、傳輸和交換交易資料及持卡人資訊的商人，或以上兩者都不是。這也包括提供服務給商家的公司、服務供應商或可控制及影響持卡人資料安全的機構會員。例如，提供防火牆管理的管理服務供應商、IDS、其他服務、主機服務商和其他實體。一些實體如電信公司，只提供通信聯繫，不觸及到應用層者，不在服務提供者定義內。

許多同樣的規則適用於商家也適用於服務提供者，其負有相同的罰責和刑事責任。他們的動機不盡相同，也沒有與消費者直接互動。這也就是說，在企業對業務這個領域，品牌的損害仍是一個重要因素。

收單和發卡銀行

收單（商家）銀行和發卡銀行是受到嚴格監管的實體，其所要求對資訊的保護遠遠超出了支付卡行業。發卡銀行有一個附加的獎勵，獎勵消費者在此交易。這意味著它不僅只是保護這些資料，也要對客戶扮演安全擁護者的角色。商家銀行，受到許多金融法律和金融交換的規範，通常充當中間人或經手人，因此與商家和服務提供商共擔刑罰。當商家或服務供應商之一被認為是違規，收單銀行將透過與這些群體相關的卡協會被處以罰款，因為他們直接管理與商家的關係。

卡協會

卡協會的主要動機，在於防止詐騙行為以保障品牌。簡單地說，卡遭嚴重侵害有損品牌形象，降低商務網路使用率。信用卡遭侵害對信用卡協會的財務影響不一定是有形的。信用卡協會主要是希望消費者在使用他們的卡購物時能感到安全。支付卡行業資料安全標準（Payment Card Industry Data Security Standard，PCI DSS）由幾個卡品牌所組成，結合他們的安全計劃，期望做到自律和保護自己的品牌。

誰控制了香料？

整體而言，參與每個交易的成員都帶有些保護資料的動機（諷刺的是，消費者動機最低）。但很明顯，有控制權的卻不一定有保護資料動機。也就是說，沒有任何單一成員可以完全控制資料的保護；且當共享秘密穿越各種環境時，當事人保護資料的動機可能根本不及其握有控制保護權的程度。

目前的系統有太多的成員需要了解共同秘密相關知識，但他們卻沒有足夠的動機來激勵他們確保資料在其整個生命週期的安全性。將圖 5.1 中單筆交易圖乘上一張卡在整個生命週期的交易數量，你會看到成千上萬的資料處理程序只交由一個共享秘密掌控。

5.3 改造電子商務：新的安全模型

透過審查電子商務交易的安全模型，我們能深入了解它的優點和弱點。現在我想提出一個更優雅的方式來看待電子商務的安全性，使得卡帳戶資訊對攻擊者沒有價值，為消費者帶來保險。

使用信用卡或借記卡交易而卡卻不在現場的情況下，有七個基本要求以確保交易的安全性，同時可持續讓系統為消費者和商家所用。

5.3.1 要求 1：消費者必須通過驗證

第一個要求是，對消費者驗證，以確認他們對自己身分的說詞是無誤的。例如，消費者 John 的信用卡帳戶名稱是 John123，我們必須先確認消費者真的是 John。那麼，該由誰來執行認證以及使用什麼認證方法才是最好的呢？

最適合執行認證的人是持卡帳戶的管理者，大多數情況下是發卡銀行。這是有幾個原因：首先，發卡銀行已有帳戶相關資訊，因此在資料的儲存部分不會因此而添加系統故障點；同時他們也有最多資源投注在專業知識和流程上以執行適當的身分驗證；最後，發卡者的數量也是遠少於其他個體的。

這種驗證可以透過下列三個古典身分驗證要素的任意組合完成：

- 消費者**知道的東西**，如密碼。
- 消費者**有的東西**，如令牌或證書。
- 消費者**與生具有的唯一特徵**，如生物識別資料。

正如我們將在後面看到，後兩者可能會在資料的大量散佈和管理上增加複雜性。

5.3.2 要求 2：商家必須通過驗證

第二個要求是驗證商家。這為消費者保證商家是合法的，是提供消費者訂購的商品和服務。和上一個要求類似，最佳的驗證機構是商家帳戶的管理者，大多數情況下是收單銀行。

OK，所以我們必須驗證消費者和商家，但現在我們遇到了一個挑戰。就算發卡銀行和收單銀行已分別對消費者和商家進行驗證，但交易正在消費者和商家之間進行。我們要如何分享這個身分驗證資訊，好讓交易程序中的消費者和商家得以查核對方的真偽呢？這時需要發卡銀行和收單銀行進行保密通訊交換驗證資訊。上述過程，在我提供建議的流程時會再詳細說明。

5.3.3 要求 3：交易必須經過授權

第三個要求：交易本身必須被授權。到目前為止，我們已經驗證了消費者真的是 John，且他的帳戶資訊也是正確的。同時也已經證實了商家 Vencer 公司是一個合法的商家，在收單銀行的帳戶資訊無誤。現在，我們需要知道，消費者 John 被授權可以進行這次消費。

第三個要求幸運的是，還沒在電子商務上出現過什麼問題，消費者都經過正確的身分驗證。收單銀行可根據所有現存系統中有關消費者的帳戶狀態，信貸限額等評斷是否允許交易。因此，如果要求 1 做得好的話（說起來容易做起來難），舞弊入侵者（通常稱為“敵對欺詐”）是可以預防的。

誠然，電子商務系統可能遭受所謂（一個矛盾的術語）“友好欺詐”，詐欺來自於商家最喜歡與之交易的對象。友好欺詐是發生在消費後改變心意或乾脆拒絕合法收費。要對每筆交易檢測友好欺詐比檢測敵對欺詐更難。有可能透過數位簽章將友好欺詐量降到一個較可以接受的量，但是這超出了本章的範圍。

5.3.4 要求 4：驗證資料不應該被驗證方和被驗證方以外的實體共享

對電子商務交易安全的第四個要求，是驗證資料不應該被驗證方和被驗證方以外的實體共享（在本例中，只能由消費者或商家共享）。在一個典型卡不在場的交易，這四種不同的實體參與其中。（1）消費者：由發卡銀行驗證。（2）發卡銀行：驗證消費者。（3）商家：由收單銀行驗證。（4）收單銀行：驗證商家。真正的奧妙在於將驗證成功或不成功的資訊分享給所有參與交易的實體，但卻不必分享實際的憑據。

不像今天的模型有自己廣為共享的秘密，我們的新模式能夠共享消費者和商家的身分驗證狀態，但不用憑據。如果我們能做到這一點，則商家對消費者的身分驗證狀態資訊遭到侵害的話，不會影響消費者的信用帳戶。消費者可以依賴發卡銀行系統的安全，而不用依賴曾經消費的每一個商家的安全性。

商家通常是由這類單一提供者執行驗證，提供者是收單銀行。由於收單銀行驗證商家，我的模型是在完成交易前先將驗證狀態分享給消費者。正如我們將看到的，我建議的交易流程應由發卡銀行與收單銀行之間的卡網路控管。

5.3.5 要求 5：過程必須完全依賴共享的秘密

第五個要求簡單地重複本章的中心思維。若商家或服務提供商的系統受損，新模式不能被破壞。先前提到的虛擬卡帳戶號碼，是一個滿足這個要求很好的辦法，但是它必須具有普遍性。當提供的只是一次性或有限使用的帳戶，單一商家或服務提供者的損害將不會破壞整體電子商務的認證模式。

5.3.6 要求 6:認證應該是可以移植（不受硬體或協定的限制）

可攜性是必須的，因為根本上就太多太多的基礎設施和系統需要大規模重新部署或全面檢查。我們必須建立一個模型，讓消費者和商家在現有的支付架構和網路上執行認證。

雖然 SET 提供了一套強大的安全控制，且到目前為止符合所提到的大部分要求，在目前這個領域它還是有所不足的。增加 PKI 基礎結構和流程額外負擔，已證實了對目前付款的流程而言是多餘的。

5.3.7 要求 7：資料和交易的機密性與完整性必須保持

第七個也是最後的要求，保持資料和交易的機密性和完整性，想都不用想，這注定是我們新模型必須嚴謹遵循的要求。它包括所有的資料認證、交易資料、訂單資料和所有維持這些狀態的資料。這一個要求必須嚴格遵守，尤其是資料必須經由這些系統跨越網路傳輸和儲存，機密性和完整性的重要不言可喻。

5.4 新模型

貫通前面七項要求，接著我提出一個無卡交易的支付模式。我以一個使用新模式的電子交易來做說明：

1. 消費者將訂單資訊以一般格式傳送給商家和發卡銀行。
2. 當商家收到來自消費者的訂單資訊，商家透過收單銀行進行驗證，並將訂單資訊以單向雜湊運算後傳送給銀行。
3. 驗證成功後，收單銀行簽署訂單資訊的雜湊值後，將此資訊透過信用卡網路傳送給發卡銀行。
4. 發卡銀行驗證收單銀行的簽章，並根據步驟 1 收到的訂單資訊重建雜湊值，然後將此值和收單銀行傳送過來的雜湊值相比對，這兩個值應相等，代表正確無誤。
5. 如果發卡銀行成功地驗證了收單銀行和消費者的訂單資訊，發開銀行發出一個虛擬卡號給消費者，額度和訂單消費金額相等。
6. 消費者將虛擬信用卡交付給商家。

以上步驟展現於圖 5.2。

這相當簡單的六個步驟，正符合我們所有的要求，並可防止單筆交易遭侵害而影響整個帳號權益。雖然在資訊安全領域，這些不是什麼新的安全觀念，但它們一直都未被有效結合並應用在當今電子商務領域。我想這個簡單的特性就是它之所以為美的原因，並擴展到今天的環境。透過融合了一系列現有的安全功能和流程，我們可以從根本上改變整體模型，形成混合、簡單，安全和美麗的新交易模式。

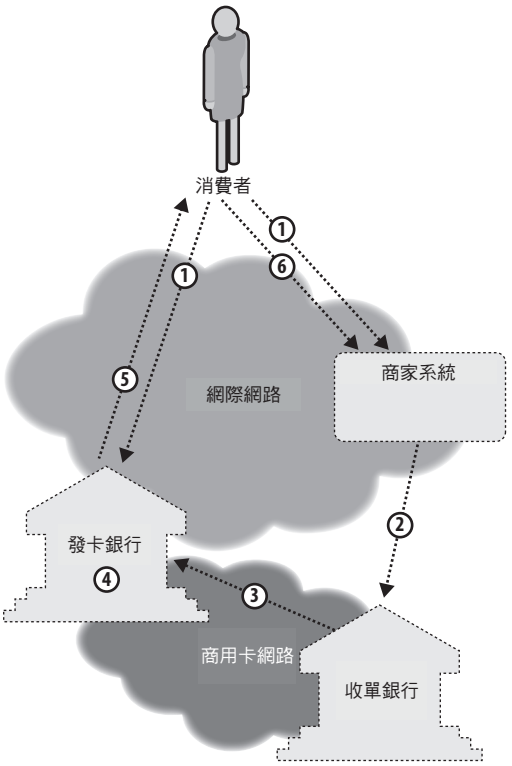

圖 5.2 信用卡交易新模型