AMERICAN EXPRESS

Data Security Operating Policy (DSOP)

變更欄

變更摘要表中列出了重要變更，並在 DSOP 中用變更欄表示。變更欄是左側邊距中的垂直線，用於標識修改、添加或刪除的文本。DSOP 中的所有變更透過變更欄表示，如此處所示。

變更摘要表

下表列出了重要的變更，並在 *DSOP* 中使用變更表示。

款 / 分款	變更描述
此發布版本沒有任何變更。	

如果發生資安事件怎麼辦？

如果貴寶號的營業場所發生了資安事件，請遵循以下步驟。

第 1 步：

在發現資安事件後的 72 小時之內填寫特約商資安事件初次通知表並透過電子郵件發送至 EIRP@aexp.com。

第 2 步：

進行徹底調查；這可能需要貴寶號僱用支付卡行業 (PCI) 鑑識調查員。

第 3 步：

立即向本公司提供所有洩露的美國運通® 卡號。

第 4 步：

與本公司合作以幫助解決因資安事件出現的任何問題。

查看款 3「資安事件管理責任」了解關於資安事件管理責任的詳細資訊。

是否有其他疑問？

美國：(888) 732-3750 （免費電話）

國際：+1 (602) 537-3021

EIRP@aexp.com

美國運通是消費者保護方面的領導者，長期致力於保護美國運通卡持卡人資料和敏感認證資料的安全性。

資料外洩會對消費者、特約商、服務供應商和發卡機構產生負面影響。一次事件便足以嚴重損害公司的聲譽，削弱其有效開展業務的能力。透過實施安全操作政策來應對該威脅，幫助提高客戶的信任度，提升盈利能力，並加強營造公司的聲譽。

美國運通深知我們的特約商和服務供應商（以下統稱貴賓號）與我們有同樣的顧慮，並要求**貴賓號**（作為貴賓號責任的一部分）遵守**協議**中的資料安全條款，以接受（就特約商而言）或處理（就服務供應商而言）美國運通®卡（分別稱為**協議**）及本「Data Security Operating Policy」（我們可能會不時修訂）。該等要求適用於儲存、處理或傳輸加密金鑰、美國運通卡持卡人資料或敏感認證資料（或以上組合）的所有設備、系統和網路（及其組件）。

本文所用但並無作出界定的術語具有本政策末尾詞彙表所賦予該等術語的涵義。

款 1 有針對性的分析計畫 (TAP)

美國運通卡持卡人資料外洩可能由貴寶號的美國運通卡持卡人資料環境 (CDE) 之安全性漏洞引起。

美國運通卡持卡人資料外洩示例包括但不限於：

- **共同 POS (CPP)：**美國運通卡會員報告其卡帳戶中的欺詐性交易，隨後被識別和確定為與在貴寶號特約商店進行的購買有關
- **找到卡帳戶資料：**在萬維網上找到美國運通卡和美國運通卡持卡人帳戶資料，並且這些資料與在貴寶號特約商店進行的交易相有關。
- **疑似惡意程式：**美國運通懷疑貴寶號正在使用感染了惡意程式碼或容易受到惡意程式碼攻擊的軟體。

TAP 旨在識別可能的美國運通卡持卡人資料外洩。

在收到美國運通對可能的美國運通卡持卡人資料外洩之通知時，貴寶號應而且必須讓貴寶號之所屬政策適用人員遵循以下要求。

- 貴寶號必須立即檢視貴寶號的 CDE 是否存在帳戶資料安全性漏洞，並糾正所有發現的問題。
  - 若外包，貴寶號必須使貴寶號的第三方供應商對貴寶號的 CDE 進行徹底的調查。
- 貴寶號必須在收到美國運通的通知後，提供針對貴寶號審查、評估和／或補救措施的已採取或計劃採取之措施的摘要。
- 貴寶號必須按照款 5「重要事項：貴寶號系統的週期性驗證」提供更新的 PCI DSS 驗證文件。
- 若適用，在貴寶號或所屬政策適用人員出現以下情況時，貴寶號之貴寶號應委請合格的 PCI 鑑識調查員 (PFI) 來檢查貴寶號的 CDE：
  - 無法在美國運通確定的合理時間內解決美國運通卡持卡人資料外洩；或者
  - 確認已發生資安事件並符合款 3「資安事件管理責任」規定的要求。

表 A-1：TAP 違規罰金

說明	一級特約商或一級服務供應商	一級特約商或二級服務供應商	三級或四級特約商
如果未於第一截止日前履行 TAP 責任，則可能收取違規罰金。	USD $25,000	USD $5,000	USD $1,000
如果未於第二截止日前履行 TAP 責任，則可能收取違規罰金。	USD $35,000	USD $10,000	USD $2,500
如果未於第三截止日前履行 TAP 責任，則可能收取違規罰金。 **註：***違規罰金可能會繼續收取，直到履行責任或 TAP 得以解決。*	USD $45,000	USD $15,000	USD $5,000

若貴寶號未履行 TAP 責任，則美國運通有權累積收取違規罰金、扣留款項和 / 或終止協議。

款 2 加密金鑰、美國運通卡持卡人資料及敏感認證資料之保護的標準

貴寶號以及貴寶號所涵蓋之所屬政策適用人員必須：

- 根據協議之規定與要求，僅可出於促成美國運通卡交易的目的儲存美國運通卡持卡人資料。
- 符合現行的適用於貴賓號處理、存儲或傳送美國運通卡持卡人資料或敏感認證資料的 PCI DSS 和其他 PCI SSC 要求，時間不可遲於實施該適用要求之版本的生效日期。
- 部署新的或替代的 PIN 碼輸入裝置或付款應用程式（或兩者）時，只能使用經 PCI 核准的裝置或應用程式。

貴寶號必須保護所有美國運通消費記錄，以及在符合這些資料安全規定的情況下，依據此協議所取得的信用額度記錄；貴寶號僅能依此協議之目的使用這些記錄，並且依協議維護之。貴寶號需承擔財務之一切責任，以向美國運通確保貴寶號所屬政策適用人員遵守這些資料安全規定（為了示範貴寶號所屬政策適用人員遵循本政策款 5「重要事項：貴寶號系統的週期性驗證」之合規性除外，除非本款另有規定）。

款 3 資安事件管理責任

貴寶號必須於發現資安事件後立即通知美國運通，並且無論原因，不得遲於七十二 (72) 小時進行通知。

如果貴寶號要通知美國運通，請聯絡「美國運通企業事故應急計畫」(EIRP)，電話號碼為 +1 (602) 537-3021（+ 號代表國際直撥電話「IDD」前綴，適用於國際長途電話費率），或傳送電子郵件至 EIRP@aexp.com。貴寶號必須為此資安事件指定一名人員來作為貴寶號聯絡人。此外：

- 貴寶號必須對每個資安事件進行徹底的取證調查。
- 針對涉及 10,000 組或以上獨特帳戶號碼的資安事件，貴寶號必須在發現資安事件之後的五 (5) 天內，委請 PCI 取證調查機構 (PFI) 進行此調查。
- 自未編輯的鑑識報告完成日起十 (10) 個工作天內，必須向美國運通提供此報告。
- 貴寶號必須訊速地向美國運通提供所有資料外洩卡片的號碼。美國運通有權自行實施內部分析，以確認資安事件所涉及的信用卡帳號。

鑑識報告須使用可向 PCI 取得的最新「取證事故最終報名範本」填寫。鑑識報告須包含取證評論、合規性報告，以及其他所有和資安事件相關的資訊；找出資安事件發生的原因；確認貴寶號在資安事件發生時是否符合 PCI DSS；並透過 (i) 提供一份說明如何改善所有 PCI DSS 現有不足的計畫以及 (ii) 參與美國運通合規計畫（如下所述），以確認貴寶號在未來有能力避免資安事件的發生。當美國運通有所要求時，貴寶號應提供由合格安全審查機構 (QSA) 完成的認證，以證明所有不足之處皆已被改善。

儘管款 3 「資安事件管理責任」：

- 美國運通可全權判斷要求貴寶號委請 PFI 對涉及少於 10,000 組獨特帳戶號碼的資安事件進行取證調查。任何此類調查必須符合本款 3 「資安事件管理責任」之上述規定，並且必須在美國運通要求的期限內完成。
- 美國運通可全權判斷單獨委請 PFI 對任何資安事件進行取證調查，並要求貴寶號承擔調查成本。

貴寶號同意與美國運通合作以針對因資安事件所引起的所有問題進行補救，包含向美國運通諮詢如何與受到資安事件影響的美國運通卡會員溝通，並向美國運通提供 （和取得任何必須提供的棄權書）所有能夠證明貴寶號在未來將能夠遵循協議方針，避免資安事件發生的所有相關資訊。

無論本協議中的任何相反之保密義務，美國運通根據適當的法律要求，有權向美國運通卡會員、發卡機構、其他美國運通網路參與者，以及社會大眾披露資安事件的相關資訊；依司法、行政或監管命令、法令、傳票、要求，或旨在減少詐欺及其他傷害之風險的其他程序，或適合於在美國運通網路內運作的其他程序。

款 4 資安事件的損害賠償責任

貴寶號肇因於資安事件而對美國運通所產生之損害賠償責任，應在保留美國運通的任何其他權利和補救措施的情況下，根據此款 4 「資安事件的損害賠償責任」。除損害賠償責任 （若有）之外，貴寶號還可能需要支付本款 4 「資安事件的損害賠償責任」中所列之資安事件違規罰金。

對於涉及

- 10,000 組或以上美國運通卡帳號的資安事件，且具有以下任一情況：
  - 敏感認證資料，或
  - 到期日

  貴寶號應按每個帳號 5 美元的費率向美國運通賠償。

但是，美國運通將不會於下列狀況下，因資安事件向貴寶號要求損害賠償：

- 該事件所包含之美國運通卡帳號少於 10,000 組，或
- 包含 10,000 組或以上美國運通卡帳號，並且貴寶號須滿足以下條件：
  - 貴寶號已依本款 3 「資安事件管理責任」規定，通知美國運通有關資安事件之情事，
  - 貴寶號於資安事件發生時遵循 PCI DSS 之規範（取決於 PFI 對於資安事件所進行之調查）且
  - 該資安事件並非肇因於貴寶號或貴寶號所屬政策適用人員的不法行為。

儘管有款 4 「資安事件的損害賠償責任」之上述規定，對於任何資安事件，無論所涉及之美國運通卡帳號數量為多少，若貴寶號未遵循款 3 「資安事件管理責任」所列之任何責任，則貴寶號應為每次資安事件向美國運通支付不超過 10 萬美元之罰金 (由美國運通全權判斷)。為了避免疑慮，針對任何單獨資安事件評估之總違規罰金不得超過 10 萬美元。

美國運通將不計算在通知日期前十二 (12) 個月內提出的先前資安事件賠償申索中包括的任何美國運通卡帳號。美國運通根據此方式所做的所有計算皆為最終結果。

依據協議，美國運通可能會向貴寶號收取資安事件違規罰金總額，或從美國運通支付給貴寶號之款項中扣除（或從貴寶號的銀行帳戶中相應地扣款）。

貴寶號對於資安事件所承擔的下文中的賠償責任，不得根據協議被視為偶然、間接、投機性、後果性、特殊、懲罰性或懲戒性的損害賠償；但此類義務不包括與利潤或收入損失、商譽損失或商業機會損失相關或同性質的損害。

美國運通得依其全權判斷在符合以下條件的資安事件中，特約商可減免的賠償責任：

- 在資安事件之前已使用適用的風險緩解技術，並且在整個資安事件事件窗口期間使用該技術，
- 已經根據 PFI 計畫完成徹底調查 （除非事前另有其他書面協議），
- 取證報告明確陳述已使用風險緩解技術在資安事件發生時處理、儲存和 / 或傳輸資料，以及
- 貴寶號不會儲存（亦不會在整個資安事件事件窗口期間儲存）可讀取的敏感認證資料或任何美國運通卡持卡人資料。

如果提供賠償減免，對於賠償責任（不包括任何應付的違規罰金）的減免將依如下方式認定：

表 A-2：賠償責任減免必要條件

賠償責任減免	必要條件
標準減免： 50%	晶片裝置所處理的總交易大於 75%[1] 或
	風險緩解技術使用於 75% 以上的特約商地點 [2]
增強減免： 75% 到 100%	所有交易中，超過 75% 的交易是在晶片裝置上處理 [1] 以及超過 75% 的特約商地點使用其他風險緩解技術 [2]

[1] 由美國運通內部分析決定

[2] 由 PFI 調查決定

- 增強減免（75% 到 100%）的認定應取決於使用晶片裝置的交易和使用其他風險緩解技術的特約商店地點的百分比（視何者較少）。下面的例子說明賠償責任減免的計算方法。
- 貴寶號必須依據產品的設計及目的有效運用科技，才能認定該技術為合格的風險緩解技術。舉例來說，將晶片裝置與處理晶片卡部署為磁條或按鍵輸入交易並不屬於該技術的有效用途。
- 使用「風險緩解技術」的地點之百分比由 PFI 調查所決定。
- 賠償責任的減免不適用於與資安事件有關的應付款項的任何違規罰金。

表 A-3：增強賠償責任減免條件

範例	使用中的風險緩解技術	合格	減免
1	80% 的晶片裝置交易	否	50%：標準減免 （使用風險緩解技術比例不到 75% 者不符合增強減免的資格）[1]
	0% 的地點使用其他風險緩解技術		
2	80% 的晶片裝置交易	是	77%：增強減免 （根據有 77% 的地點使用風險緩解技術的情況）
	77% 的地點使用其他風險緩解技術		
3	93% 的晶片裝置交易	是	93%：增強減免 （根據 93% 的晶片裝置交易）
	100% 的地點使用其他風險緩解技術		
4	40% 的晶片裝置交易	否	50%：標準減免 （不到 75% 的晶片裝置交易不符合增強減免資格）
	90% 的地點使用其他風險緩解技術		

1 涉及 10,000 組美國運通卡帳戶的資安事件，以每個帳號 5 美元費用的條件 (10,000 x $5 = $50,000) 得符合減免 50% 的資格，將賠償責任從 $50,000 減至 $25,000（不包括任何違規罰金）。

款 5

重要事項：貴寶號系統的週期性驗證

貴寶號必須依照下述行動，對於貴寶號及加盟貴寶號者用以儲存、處理或傳輸美國運通卡持卡人資料或敏感認證資料的設備、系統和 / 或網路（以及其組件）的狀態，進行每年度和每 90 天的 PCI DSS 驗證。

貴寶號需要進行四個行動以完成此驗證：

行動 1：參與本政策中的美國運通 PCI 合規計畫（以下簡稱「計畫」）。

行動 2：確定貴寶號特約商等級和驗證要求。

行動 3：完成貴寶號必須傳送給美國運通的驗證文件。

行動 4：在規定的時限內將驗證文件傳送給美國運通。

行動 1：參與本政策中的美國運通合規計畫

一級特約商、二級特約商與下述的所有服務供應商必須參與本政策中的計畫。美國運通得依其全權判斷，指定具體三級和四級特約商根據本政策參與計畫。

要求參加計畫的特約商和服務供應商須在規定的時間內加入美國運通選擇的計畫管理機構提供的入口網站。

- 貴寶號應接受與使用入口網站相關的所有合理條款與條件。
- 貴寶號應在入口網站內至少指定一個資料安全聯絡人並提供準確資訊。必要的資料元素包括：
  - 全名
  - 電子郵件地址
  - 電話號碼
  - 實體郵寄地址
- 貴寶號應在資訊變更時在入口網站內更新指定資料安全聯絡人的資訊或提供新資訊。
- 貴寶號應確保更新貴寶號之系統，以允許來自入口網站指定域的服務通訊。

貴寶號未能提供或維護最新資料安全聯絡人的資訊或未能啟用電子郵件通訊並不會影響我們評估費用的權利。

行動 2：確定貴寶號特約商等級和驗證要求

根據美國運通卡交易情況，特約商共有四個等級，而服務供應商有兩個等級。

- 對於特約商來說，此數量是由其商店所請款，隨著數量增加，可達到最高的美國運通特約商帳戶等級。*
- 對服務供應商來說，此數量是貴寶號為之提供服務的服務供應商和實體服務提供商所請款的總和。

在用於判定特約商等級與驗證要求的美國運通卡交易數量中，並不包括購買者發起付款 (Buyer Initiated Payments, BIP) 交易。貴寶號可以在下列的特約商與服務供應商表中找到貴寶號所屬的等級。

* 如為加盟授權者 (Franchisor)，這時會包括其加盟者 (Franchisee) 商店交易筆數的數量。負責委任加盟者使用 POS 系統或服務供應商的加盟授權者，也必須為受影響的加盟者提供驗證文件。

特約商驗證文件要求

特約商（非服務供應商）共有四個特約商等級類別。在下表中確認特約商等級後，貴寶號可查閱特約商表 A-4：特約商驗證文件表來確定驗證文件要求。

- **一級特約商** —— 美國運通卡交易數量達到每年 250 萬筆以上；或任何其他由美國運通全權判斷其為一級的特約商。
- **二級特約商** —— 美國運通卡交易數量達到每年 5 萬至 250 萬筆。
- **三級特約商** —— 美國運通卡交易數量達到每年 1 萬至 5 萬筆。
- **四級特約商** —— 美國運通卡交易數量每年少於 1 萬筆。

表 A-4：特約商驗證文件

特約商等級 / 每年美國運通交易情況	符合性報告合規聲明書 (ROC AOC)	問卷合規聲明書 (SAQ AOC) 和季度外部網路漏洞掃描 （掃描）	合格特約商的 STEP 聲明書
一級 / 250 萬或更多	必要	不適用	美國運通核准情況下的選項 (取代 ROC)
二級 / 5 萬到 250 萬	選項	SAQ AOC 必要 (除非提交 ROC AOC)；特定 SAQ 類型必須進行掃描	選項 (取代 SAQ 與網路掃描或 ROC)
三級 / 1 萬至 5 萬	選項	SAQ AOC 選項 (如果美國運通要求則為必要項)；特定 SAQ 類型必須進行掃描	選項 (取代 SAQ 與網路掃描或 ROC)
四級 / 1 萬或以下	選項	SAQ AOC 選項 (如果美國運通要求則為必要項)；特定 SAQ 類型必須進行掃描	選項 (取代 SAQ 與網路掃描或 ROC)

* 為了避免疑慮，除非美國運通自行提出要求，否則三級與四級特約商將不需要請款驗證文件，但儘管如此，仍需遵守此 「Data Security Operating Policy」所有其他條款的責任並且受其約束。

美國運通保留驗證貴寶號 PCI 驗證文件之完整性、準確性和適宜性的權利。美國運通可能會出於此目的要求貴寶號提供其他證明文件以進行評估。此外，美國運通有權要求貴寶號委請經 PCI 安全標準委員會核准之 QSA 或 PFI。

安全性技術改良計畫 (STEP)

符合 PCI DSS 的特約商若在其卡片處理環境中另外部署特定的安全性技術，可在美國運通決定下符合加入美國運通的安全性技術改良計畫 (Security Technology Enhancement Programme, STEP) 的資格。STEP 僅適用於在最近十二個月內未發生資安事件，且所有特約商卡交易中有 75% 是結合下列改良安全選項執行的特約商：

- **EMV、EMV 感應或電子錢包** —— 位於有效的晶片裝置上，其擁有有效且現行的 EMVCo (www.emvco.com) 核准 / 認證，並能夠處理相容於 AEIPS 的晶片卡交易。（美國特約商必須包括感應式卡片）
- **點對點加密 (Point-to-Point Encryption, P2PE)** —— 如果貴係使用經 PCI-SSC 核准或經 QSA 核准的點對點加密系統，與特約商的處理代理機構進行通訊
- **Token 化** —— 實施的 Token 化解決方案應：
  - 符合 EMVCo 規範；
  - 由遵守 PCI 的第三方服務供應商保衛、處理、儲存、傳輸以及完全控制；而且
  - 不能對 Token 進行逆向工程以向特約商揭示未掩碼的主帳號 (PAN)。

STEP 合格特約以降低 PCI 驗證文件的要求，詳見下面的行動 3：「完成貴寶號必須傳送給美國運通的驗證文件」。

服務供應商要求

服務供應商（非特約商）共有兩個等級類別。在下表中確認服務供應商等級後，貴寶號可查閱表 A-5：服務供應商文件表來確定驗證文件要求。

一級服務供應商 —— 美國運通卡交易數量達到每年 250 萬筆 以上；或任何其他由美國運通認定為一級的服務供應商。

二級服務供應商 —— 美國運通卡交易數量為每年 250 萬筆以下；或任何其他未由美國運通認定為一級的服務供應商。

服務供應商不符合 STEP 資格。

表 A-5：服務供應商文件

級別	驗證文件	要求
1	年度符合性報告合規聲明書 (ROC AOC)	必要
2	年度 SAQ D（服務供應商）和季度網絡掃描或年度符合性報告合規聲明書 (ROC AOC)（若首選）	必要

建議服務供應商同時遵守 PCI 特定機構補充驗證要求。

行動 3：完成貴寶號必須傳送給美國運通的驗證文件

以下為上述特約商表與服務供應商表中所列出的不同等級特約商和服務供應商所需之文件。

貴寶號應提供適用查核類型的合規聲明書 (AOC)。AOC 是由貴寶號對於合規性狀態所作的聲明，因此，應由貴寶號組織內適當級別的領導層簽名並註明日期。

除了 AOC 之外，美國運通可能會要求貴寶號提供完整查核的副本，以及由本公司決定，提供證明貴寶號符合 PCI DSS 要求的其他證明文件。驗證 文件由貴寶號承擔費用完成。

符合性報告合規聲明書 (ROC AOC) ——（年度要求）—— 符合性報告記錄對貴寶號用以儲存、處理或傳輸美國運通卡持卡人資料或敏感認證資料的設備、系統和網路的詳細現場檢驗的結果。共有兩種版本：特約商版本和服務供應商版本。符合性報告必須由以下人員執行：

- 一位 QSA 或是
- 貴寶號來執行，並由貴寶號執行長、財務長、資訊安全長或法定代理人進行聲明

AOC 應由 QSA 或內部安全審查員以及貴寶號組織內授權級別的領導層簽名並註明日期，每年至少向美國運通提供一次。

自我評估問卷合規聲明書 (SAQ AOC) ——（年度要求）—— 自我評估問卷允許貴寶號對於貴寶號用以儲存、處理或傳輸美國運通卡持卡人資料或敏感認證資料（或兩者）的設備、系統和網路（以及其組件）進行自我檢驗。SAQ 有多種版本。貴寶號可以根據貴寶號美國運通卡持卡人資料環境選擇一個或多個版本。

SAQ 可以由貴寶號公司內有資質準確、認真仔細回答問題的人員完成，或者，貴寶號可以委請 QSA 提供協助。AOC 應由貴寶號組織內授權級別的領導層簽名並註明日期，每年至少向美國運通提供一次。

核准之掃描供應商外部網路漏洞掃描摘要（ASV 掃描）——（90 天要求）—— 外部漏洞掃描是一項遠端測試，以幫助識別貴寶號美國運通卡持卡人資料環境（例如，網站、應用程式、Web 伺服器、郵件伺服器、面向公眾的域或主機）中的潛在弱點、漏洞以及網際網路面向組件的配置錯誤。

ASV 掃描必須由核准之掃瞄供應商 (ASV) 執行。

如果 SAQ 要求，貴寶號必須每 90 天至少向美國運通提交一次 ASV 掃描報告掃描合規聲明書 (AOSC) 或執行摘要，包括掃描到的目標計數、證明結果滿足 PCI DSS 掃描程序的認證以及 ASV 完成的合規狀態。

除非有具體要求，否則 ROC AOC 或 STEP 無須提供 AOSC 或 ASV 掃描執行摘要。為了避免疑慮，如果適用的 SAQ 有此規定，必須進行掃描。

為了避免疑慮，如果適用的 SAQ 有此規定，必須有 ASV。

STEP 聲明書驗證文件 (STEP) ——（年度要求）—— STEP 僅提供給符合上文行動 2：「確定貴寶號特約商等級和驗證要求」中所列標準的特約商。如果貴寶號公司符合條件，貴寶號必須每年完成一次 STEP 聲明書表格並提交給美國運通。年度 STEP 聲明書表格可於入口網站下載。

不符合 PCI DSS ——（年度、90 天和 / 或臨時要求）—— 如果貴寶號不符合 PCI DSS，則貴寶號必須提交下列其中一份文件：

- 包括「第 4 部分：違規範狀態之行動計畫」的合規聲明書 (AOC)（可於 PCI 安全標準委員會網站下載）
- PCI 優先方法工具摘要（可於 PCI 安全標準委員會網站下載）
- 專案計畫範本（可於入口網站下載）專案計畫可以代替年度聲明書 (SAQ/ROC) 和 / 或掃描要求提交。

上述每個文件必須指定改善日期，不得超過文件完成日期後的十二 (12) 個月，以便符合規範要求。貴寶號應將貴寶號依「違規範狀態」所進行的改善進度的定期更新提供給美國運通（一級、二級、三級和四級特約商；所有服務供應商）。為符合 PCI DSS 所需之改善行動由貴寶號承擔費用完成。

為符合 PCI DSS 所需之改善行動由貴寶號承擔費用完成。

美國運通不得因在改善日期之前所發生的違規情況，向貴寶號收取未驗證罰金（以下詳述），但貴寶號仍然需要對美國運通承擔資安事件的所有損害賠償責任，並受本政策的所有其他規定制約。

為排除所有疑慮，不符合 PCI DSS 規定的特約商一律不能加入 STEP。

行動 4：將驗證文件傳送給美國運通

所有要求參加計畫的特約商與服務供應商須在適用期限前向美國運通提交行動 2：「確定貴寶號特約商等級和驗證要求」的表格中標為「必要」的驗證文件。

貴寶號應使用美國運通選擇的計畫管理機構提供的入口網站向美國運通提交貴寶號的驗證文件。透過提交驗證文件，貴寶號即向美國運通聲明並保證以下內容真實 （盡貴寶號所能）：

- 貴寶號的評估完整、徹底；
- 無論符合或是不符合，在完成之時已準確聲明 PCI DSS 狀態；
- 貴寶號有權披露其中的資訊，而貴寶號向美國運通提供之驗證文件將不會侵害他方之權利。

未驗證罰金與協議終止

若貴寶號無法滿足這些要求或無法於適用期限前向美國運通提供必要之驗證文件，美國運通有權向貴寶號收取未驗證罰金，並且終止本協議。美國運通將針對各個年度和季度報告週期，單獨對貴寶號發出有關適用期限的通知。

表 A-6：未驗證罰金

說明 *	一級特約商或一級服務供應商	一級特約商或二級服務供應商	三級或四級特約商
如果未於第一截止日前收到驗證文件，我方將收取未驗證罰金。	USD $25,000	USD $5,000	USD $50
如果未於第一截止日前收到驗證文件，我方將另外收取未驗證罰金。	USD $35,000	USD $10,000	USD $100
如果未於第二截止日前收到驗證文件，我方將另外收取未驗證罰金。 註：未驗證罰金可能會繼續收取，直到提交驗證文件。	USD $45,000	USD $15,000	USD $250

* 未驗證罰金將以當地貨幣等價收取。

* 不適用於阿根廷。

若貴寶號未履行 PCI DSS 驗證文件責任，則美國運通有權累積收取未驗證罰金、扣留款項和 / 或終止協議。

款 6 保密

美國運通應採取合理措施來保持（並促使其代理人和外包商（包括入口網站提供者保持）貴寶號報告之合規性，其中包括驗證文件之機密性，以及未披露驗證文件給任何第三方（美國運通的相關企業、代理、代表、服務供應商和外包商除外），且保密期限為收到文件後的三年內，除非此保密義務不適用於以下驗證文件：

a. 美國運通已在其披露前瞭解的驗證文件；
b. 藉由不違反美國運通的本條款之途徑而提供給公眾的驗證文件；
c. 美國運通以正當途徑由第三方所取得且無需承擔保密責任的驗證文件；
d. 美國運通單獨完成的驗證文件；或
e. 依據法院、行政機構或政府當局的命令必須予以披露的驗證文件；依據任何法律、規則或法規；傳票、調查要求、傳喚或其他行政或司法程序必須予以披露的驗證文件；或由任何政府機構或當局（包括任何監管機構、勘驗人或執法機構）透過任何正式或非正式的詢問或調查必須予以披露的驗證文件。

款 7 免責聲明

美國運通特此聲明，對於本「DATA SECURITY OPERATING POLICY」、PCI DSS、EMV 規範，以及 QSA、ASV 或 PFI（或以上任何一者）之指派與表現，美國運通公司不以明示、暗示、法令規定或其他方式做任何聲明或保證（其中包括用於特定用途之可銷售性或適當性保證），亦不承擔任何相關責任。根據本政策，美國運通卡發卡機構並非第三方受益人。

實用網站

美國運通資料安全：www.americanexpress.com/datasecurity

PCI 安全標準委員會：www.pcisecuritystandards.org

詞彙表

僅出於本 Data Security Operating Policy (DSOP) 之目的，當與*特約商法規*中之條款相違背之時，以下定義適用且管制：

美國運通卡或卡片係指標示美國運通或美國運通關係企業的名稱、標識、商標、服務標章、商業名稱或其他稱號並由發卡機構或卡片帳戶號碼發行的卡片、帳號存取設備、付款裝置或業務或卡片帳戶號碼。

合規聲明書 (AOC) 係指以支付卡產業安全標準委員會所提供之形式，由貴寶號對於 PCI DSS 的合規性狀態所作的聲明。

核可的點對點加密 (P2PE) 解決方案，包含於經驗證解決方案的 PCI SSC 清單裡，或已通過 PCI SSC 合格安全審查機構 (QSA) P2PE 公司驗證。

核准之掃描供應商 (ASV) 係指已由支付卡產業安全標準委員會核可之實體，可對網際網路面向的環境執行弱點掃描，以驗證其是否符合特定 PCI DSS 要求。

掃描合規聲明書 (AOSC) 係指以支付卡產業安全標準委員會所提供之形式，由貴寶號基於網路掃描，對於 PCI DSS 的合規性狀態所作的聲明。

購買者發起付款 (BIP) 交易係指由透過 BIP 處理之付款指令文件支援的付款交易。

美國運通卡持卡人資料將在 PCI DSS 條款的現有詞彙表中進行定義。

美國運通卡持卡人資料環境 (CDE) 係指儲存、處理或傳輸美國運通卡持卡人資料或敏感證資料的個人、流程和技術。

美國運通卡會員係指 (i) 已與發卡機構達成協議建立卡片帳戶，或 (ii) 美國運通卡上載有其姓名或名稱之自然人或機構。

美國運通卡會員資訊係指有關美國運通卡會員及美國運通卡交易之任何資料，包括其姓名、地址、卡帳戶號碼及美國運通卡識別號碼 (CID)。

卡片號碼係指發卡機構在發卡時分配給卡片的唯一標識號。

消費係指以美國運通卡所作之付款或購買行為。

晶片係指整合式微晶片，其內建於卡片之中，包含美國運通卡會員及帳戶資訊。

晶片卡係指嵌有 IC 晶片之美國運通卡，並得設定密碼以進行持卡會員及 / 或晶片所含資訊之驗證，或以上兩者 （又可稱為 「智慧卡」、「EMV 卡」，或簡稱 「ICC」，或在本公司的資料中稱為 「整合電路卡」）。

晶片裝置係指一種 POS 系統裝置，其擁有有效且現行的 EMVCo (www.emvco.com) 核准 / 認證，並能夠處理相容於 AEIPS 的晶片卡交易。

資料外洩卡帳號係指與資安事件有關的美國運通卡片帳戶號碼。

涵蓋當事人係指貴寶號任何或全部員工、代理、代表、外包商、處理代理機構、服務供應商、貴寶號 POS 設備或系統，或付款處理解決方案的供應者、與貴寶號美國運通特約商帳戶相關聯的實體，以及貴寶號依據協議提供美國運通卡會員資料或敏感認證資料 （或兩者）存取的任何他方。

退款係指就以美國運通卡所為之購買或付款，貴寶號退還予美國運通卡會員之消費金額。

資安事件係指涉及美國運通加密金鑰外洩或疑似外洩的事故，或至少涉及一筆美國運通卡帳戶號碼的事故，在事故中：

- 對使用貴寶號設備、系統和/或網路（或其組件）或貴寶號要求使用或提供的設備進行儲存、處理或傳輸作業的資料，包括加密金鑰、美國運通卡持卡人資料或敏感認證資料（或每項俱存）進行未經授權的存取或使用；
- 以不符合協議規範的方式使用前述加密金鑰、美國運通卡持卡人資料或敏感認證資料（或每項俱存）；和/或
- 被懷疑或確認已透過任何媒體、素材、記錄或含有前述加密金鑰、美國運通卡持卡人資料或者敏感認證資料（或每項俱存）之資訊等任何手段，而使資料遺失、被盜用或挪用。

資料事故事件窗口是指最終取證報告 （如 PFI 報告）中規定的入侵窗口 （或類似確定的時間段），如果未知，則在向我們報告的資料洩露中涉及的潛在事故卡號的最後通知日期前 365 天。

EMV 規範係指由 EMVCo 所發布的規範，貴寶號可於以下網站查閱詳細內容： www.emvco.com。

EMV 交易係指一筆在可使用 IC 卡且採用有效且現行的 EMC 類型認證的 POS 系統 (POS) 終端所進行的整合電路卡（又可稱為 「IC 卡」、「晶片卡」、「智慧卡」、「EMV 卡」或 「ICC」）交易。有關 EMV 類型認證的詳細內容，請造訪 www.emvco.com。

加密金鑰 （「美國運通加密金鑰」）係指處理、產生、加載和 / 或保護帳戶資料時所使用的所有金鑰。其中包含（但不限於）下列項目：

- 主要加密金鑰： 區域主金鑰 (ZMK) 及區域 Pin 碼金鑰 (ZPK)
- 用於安全加密裝置的主金鑰：本地主金鑰 (LMK)
- 卡片安全碼金鑰 (CSCK)
- PIN 碼金鑰：基礎導出金鑰 (BDK) 、PIN 碼加密金鑰 (PEK) 及 ZPK

取證事故最終報名範本係指 PCI 安全標準委員會提供的範本，可在 www.pcisecuritystandards.org 上找到。

加盟者係指獨立擁有和經營的第三方 （包括加盟者、經授權服務者或是分支），但不可為由加盟授權人授權經營加盟店以及與加盟授權人締結書面協議的加盟成員，加盟者始終以明顯方式顯示外部標識，透過加盟授權人標記或是向大眾宣傳，表明自己為加盟授權人公司集團成員。

加盟授權者係指公司業者，該業者授予人員或實體 （加盟者）權利，使加盟者可依據或使用授權者之 「標誌」從事商品及 / 或服務的散佈；在商務營運上為加盟者提供協助，或影響加盟者的營運方式；以及要求加盟者支付使用費。

發卡機構係指經美國運通或美國運通的相關企業許可發行美國運通卡並從事卡發行業務的任何實體 （包括美國運通及美國運通的相關企業）。

一級特約商係指美國運通卡交易數量達到每年 250 萬筆以上；或任何其他由美國運通認定為一級的特約商。

二級特約商 —— 美國運通卡交易數量達到每年 5 萬至 250 萬筆。

三級特約商 —— 美國運通卡交易數量達到每年 1 萬至 5 萬筆。

四級特約商 —— 美國運通卡交易數量少於每年 1 萬筆。

一級服務供應商 —— 美國運通卡交易數量達到每年 250 萬筆以上；或任何其他由美國運通認定為一級的服務供應商。

二級服務供應商 —— 美國運通卡交易數量為每年 250 萬筆以下；或任何其他未由美國運通認定為一級的服務供應商。

特約商 —— 係指依照與美國運通或其關係企業之間的協議，接受美國運通卡的特約商與其關係企業。

特約商級別係指本公司相對於特約商的 PCI DSS 合規驗證義務分配給特約商的稱號，如款 5 「重要事項：貴寶號系統的週期性驗證」所述 .

通知日期係指美國運通給發卡機構提供資安事件最終通知的日期。此日期可以依據美國運通收到最終取證報告或內部分析的日期，視具體情況而定，且美國運通得依其全權判斷。

付款應用程式將在安全軟件標準和安全軟件生命週期標準的現行詞彙表中進行定義，可在 www.pcisecuritystandards.org 上找到。

支付卡產業資料安全標準 (PCI DSS) 係指支付卡產業資料安全標準，可在 www.pcisecuritystandards.org 上找到。

支付卡產業資料安全標準委員會 (PCI SSC) 要求係指與維護和保護支付卡資料有關的一組標準和要求 （包括 PCI DSS 和 PA DSS），可在 www.pcisecuritystandards.org 上找到。

PCI 認證係指由 PCI 標準委員會所維護的已核可的認證公司與供應商列表時所配置出現的 PIN 碼輸入裝置或付款應用程式 （或兩者），可在 www.pcisecuritystandards.org 上找到。

PCI DSS 係指支付卡產業資料安全標準，可在 www.pcisecuritystandards.org 上找到。

PCI 取證調查機構 (PFI) 係指已由支付卡產業安全標準委員會核可，可針對支付卡片資料的漏洞或外洩進行取證調查機構的實體。

PCI PIN 碼安全要求係指支付卡產業 PIN 碼安全標準要求，可在 www.pcisecuritystandards.org 上找到。

PIN 碼輸入裝置其定義與當時現行詞彙表中的支付卡產業 PIN 碼交易安全 (PTS) 互動點 (POI)、模組安全要求，對此定義的說明一致，可在 www.pcisecuritystandards.org 上找到。

POS 系統係指處理資料的系統或設備，包含一台終端、個人電腦、電子收銀機、感應式讀卡機或付款引擎或程序，由特約商使用，以取得授權或收集交易資料 （或兩者）。

點對點加密 (P2PE) 係指會透過加密方式，保護從商家接受支付卡片的端點到加密安全點之間帳戶資料的解決方案。

入口網站係指由美國運通選擇的美國運通 PCI 計畫管理機構提供的報告系統。特約商與服務供應商必須使用入口網站向美國運通提交 PCI 驗證文件。

主帳號 (PAN) 的定義與當時現行詞彙表中的 PCI DSS 對此定義的說明一致。

處理代理機構係指幫助特約商促進美國運通網路的授權和提交處理的服務供應商。

計畫係指美國運通 PCI 合規計畫。

合格安全審查機構 (QSA) 係指已由支付卡產業安全標準委員會核可之實體，可驗證是否符合 PCI DSS。

風險緩解技術 —— 由美國運通判定，可提升美國運通美國運通卡持卡人資料和敏感認證資料安全性的技術解決方案。若要符合風險緩解技術的資格，貴寶號必須以符合其設計與預期用途的方式展現能夠有效利用該技術的能力。範例包括但可能不限於：EMV、點對點加密和 Token 化。

自我評估問卷 (SAQ) 係指已由支付卡產業安全標準委員會所建立的自我評估工具，可用於評估和證明是否符合 PCI DSS。

敏感認證資料其定義與當時現行詞彙表中的 PCI DSS 對此定義的說明一致。

服務供應商係指已取得授權的處理者、第三方處理代理機構、閘道供應者、POS 系統整合業者，以及 POS 系統特約商之任何其他供應商，或是其他付款處理解決方案或服務的任何其他供應商。

安全性技術改良計畫 (STEP) 係指由美國運通主導，鼓勵特約商運用可加強資料安全性之技術的一項計畫。

有針對性的分析計畫係指盡早識別貴寶號的持卡人資料環境 (CDE) 中可能的美國運通卡持卡人資料外洩的計畫。參見款 1「有針對性的分析計畫 (TAP)」。

Token 係指根據給出的不可預測值索引取代 PAN 的加密 Token。

交易係指透過卡片完成的消費或信用額度。

驗證文件係指與年度實地查核或 SAQ 共同呈送的 AOC、與季度網路掃描共同呈送的 AOSC 及執行摘要，或年度安全性技術改良計畫聲明書。