

## 沃爾夫斯堡有關信用卡／簽賬卡發卡及商戶收單活動的防止清洗黑錢指引

1. 序言
2. 範圍
3. 背景
4. 卡種類
5. 發卡
6. 商戶收單
7. 總結

### 1. 序言

沃爾夫斯堡國際金融機構組織（「沃爾夫斯堡組織」[1]）已發表全球防止清洗黑錢指引、聲明及原則，涉及多個相關主題，包括私人銀行、代理銀行、制止資助恐怖主義活動、交易監察、匯集工具及風險為本的原則<sup>A</sup>。沃爾夫斯堡組織認為，持守這些原則有助於促進有效的風險管理，使金融機構能夠在商業交易方面作出良好的商業判斷，同時進一步體現沃爾夫斯堡組織成員努力防止其機構被利用從事犯罪活動的目標。

### 2. 範圍

2.1 本文件旨在探討信用卡／簽賬卡「發卡」活動在清洗黑錢方面所受威脅及相關薄弱環節，並提供管理此等風險的指引，作為全面的防止清洗黑錢合規管理的一部分。此外，本文件也討論商戶收單（「收單」），即批核商戶、提供及維護銷售點客戶關係等活動。收單活動及與之相關的防止清洗黑錢措施，可能與卡的相關風險和監控緊密相關，而很多大型金融機構同時為持卡人及商戶提供服務。

因此，本指引應與沃爾夫斯堡組織的其他文件（如適用）一併考慮，並應尤其注意該組織有關風險為本的原則[2]。

2.2 本文件不討論扣賬卡<sup>B</sup>（包括僅與存款戶口連結的「自動櫃員機」專用產品或儲值卡／預付卡）。

2.3 雖然本文件不具體討論此類產品中與欺詐相關的傳統威脅（而有關這方面的證據多不勝數），但是，許多與實際或潛在欺詐，尤其是身份盜竊相關的風險指標，皆與防止清洗黑錢息息相關。儘管如此，我們同時亦要明白，欺詐與清洗黑錢的方法不盡相同，有關詳情將於下文作更詳細討論（請參閱第 5.6 節「交易／客戶監察」），而在制訂及執行有效的交易監察架構時，應加以考慮。

---

<sup>A</sup> 在 2009 年以前上載沃爾夫斯堡網頁的多個文件中譯本內，“Risk based approach”譯為“以風險為基礎的審查方法”，現改譯為“風險為本的原則”。

<sup>B</sup> 簽賬卡即 Charge Card；扣賬卡即 Debit Card。

2.4 雖然本指引並無特別處理資助恐怖主義活動問題，但是，適當地執行客戶身份識別（包括參照主管機關提供的適用制裁名單進行審查）、客戶申請受理、初步及持續的盡職審查程序，均有助防止恐怖份子或恐怖組織利用各種金融服務，包括那些與提供信用卡／簽賬卡<sup>B</sup>發卡及商戶收單相關的服務。

### 3. 背景

金融機構一直面對被利用進行清洗黑錢活動的威脅，而最有效的管理方法，是通過瞭解與客戶、產品、服務、地域及交易相關的潛在清洗黑錢風險，將其納入有效的全面防止清洗黑錢合規程序。金融機構亦應採用這個程序，確定相關員工所需接受的培訓水平及種類。

銀行業、銀行監管機構及執法人員以往一直認為，信用卡發卡及收單相比其他金融產品及服務，所伴隨的清洗黑錢風險較低。對於信用卡產品及服務，銀行使用精密系統以審查有關申請及監察欺詐，並對現金付款、現金提取及貸方餘額施加限制，使信用卡產品及服務不容易成為有效清洗黑錢的工具。

基於卡產品本身的性質，清洗黑錢活動在將黑錢存置入銀行系統，以及與合法來源資金融合的階段，受到若干「結構性」的監控／限制（例如：(i)持卡人可提取的金額一般受到信用額限制；(ii)持卡人向金融系統注入現金的能力亦受到類似限制；及(iii)持卡人一般須以當地貨幣還款，因此，用作結清卡賬的資金在到達發卡機構之前，應已存放於當地受規管銀行系統內）。

雖然如此，除非使用有效措施盡量減低風險，否則，信用卡與其他金融服務產品一樣容易被濫用。例如，信用卡可被用作轉移犯罪活動產生的資金。整個電子銀行業的科技一日千里，以及因應消費者需求而推出的若干新產品特點（請參閱第 5.1 節「產品設計」），亦可能容易招致清洗黑錢。發卡機構應進行定期檢討，以識別新浮現的風險及確定如何加強現行防止清洗黑錢措施，以應對這些風險。

一直以來，發卡及收單活動均訂有針對欺詐威脅的嚴厲措施及監督，並且不斷改良。所有金融犯罪，包括清洗黑錢，都是利用虛假或盜竊身份來增加犯罪的成功機會，而發卡機構及收單機構均注重維持有效的客戶身份識別程序。此等措施亦可有效管理與發卡及收單活動相關的清洗黑錢風險。

### 4. 卡種類

銀行及其他金融機構可以某組織／全球信用卡網絡成員的身份，發行本身的牌卡。在此商業模式下運作的組織，通稱為信用卡系統下的卡計劃營運機構。大型國際組織如威士(Visa)、萬事達(MasterCard)、美國運通(American Express)及發現(Discover)，均以營運機構身份與第三方發卡機構合作，由這些第三方機構發行「雙品牌」卡。本指引適用於所有就下列類別信用卡及簽賬卡而建立及提供服務的發卡機構夥伴關係：

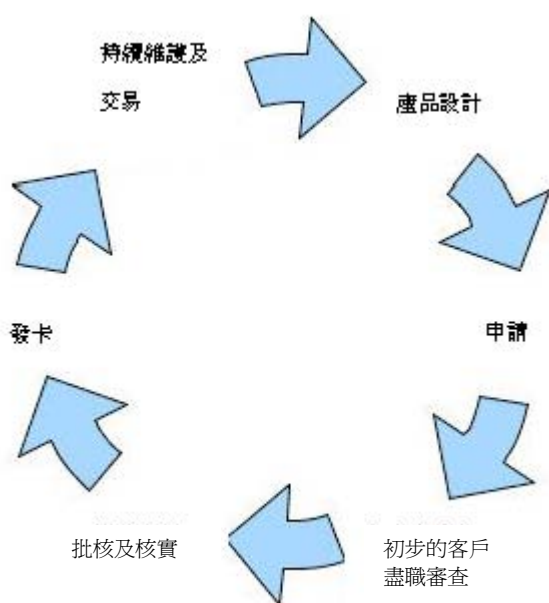
- 非專用卡。這類卡一般由國際組織發行，可用於多家零售商，例如：
  - 一般用途卡；
  - 聯營卡（如會籍卡）；
  - 夥伴商戶卡；
  - 公司卡（發行予企業及公司供其本身僱員使用）。
- 專用卡。這類卡一般僅可用於發卡的特定零售商，而該零售商通常並非任何組織／全球信用卡網絡的成員。

金融發卡機構負責維持防止清洗黑錢合規程序，但營運機構除承擔發卡機構的責任外，亦須各自負責維持風險為本的防止清洗黑錢合規程序。此等程序考慮到由第三方發卡涉及的一些額外風險，以及在不同國家／地區可能須予遵守的不同地方法律／監管規定。

## 5. 發卡

### 一般卡類的壽命周期

沃爾夫斯堡組織認為，在評估與發卡相關的整體風險（有別於下文所討論與商戶收單相關的風險）時，應當考慮在卡的開發、交付及使用周期中，與各個不同階段相關的特定威脅及薄弱環節。這些階段（包括持續的交易監察）可劃分如下：



### 5.1 產品設計

在產品壽命周期中，個別卡產品的市場區域、整體產品規格及功能均在產品設計階段確定。金融犯罪、合規、業務發展、信貸風險及市場推廣等專責小組在此程序中發揮多方合作。

就新產品及服務或對現有產品及服務的重大修改而言，評估及審批程序必須考慮相關的清洗黑錢風險因素及所需的適當措施。必須從防止清洗黑錢的角度考慮產品的所有方面，亦要同時考慮用以減輕及管理此等風險的措施。例如，可應對產品或服務的某些特點設定限額，如現金信用額。

具備下列特點的產品可能容易被利用進行清洗黑錢活動，因此可能需要採取措施減輕風險：

- 開出便利支票；
- 以多種貨幣提取現金的能力（特別是在海外）；
- 多方授權使用者（或附屬卡持有人）；
- 卡戶口結算，特別是利用貨幣及現金等值工具或由第三方進行結算；
- 即時批核信用卡（一般與第三方供應商（如零售店）聯營）。

產品的某些特點亦可降低產品被用作清洗黑錢的可能。對現金提取、授權使用者、其他較高風險特性施加限制，加上對超額付款及貸方餘額返還採取適當措施，再輔以對欺詐及不尋常交易採取嚴謹的交易監察，將可減低或消除按客戶種類進行風險評級的需要。

## 5.2 申請／身份識別及核實

發卡機構用以識別及核實申請人身份的工具，會視乎司法管轄地區而有所不同，以及可能受到有關發卡活動的時間影響。有些司法管轄地區設有完善的徵信機構／系統，有些地區則欠奉。同樣地，有些司法管轄地區可能要求發卡機構向卡申請人索取由政府發出的身份證號碼，而有些地區則可能基於私隱理由或其他考慮而禁止發卡機構索取這類號碼。但無論如何，開戶程序必須足夠地嚴謹，以確保發卡機構能夠合理相信其所知悉的客戶真正身份。在那些設有完善的徵信機構／系統的司法管轄地區，非面對面的開戶程序是常見的信用卡發卡業務模式，而這種開戶程序可使用來自徵信機構／系統的資料進行身份核實。例如，在預先審查[3]過程中從客戶信用記錄報告取得的資料，或從其他可靠來源取得的資料，均可用以核實身份，以及確證申請表格內所提供的其他資料。

如果相關司法管轄地區已制訂法律或法規，規定發卡機構必須識別客戶身份，則發卡機構奉行該等法律或法規，一般可被視為已作出足夠的盡職審查。不過，視乎與產品及客戶關係有關的風險程度，發卡機構可能適宜採取更嚴格的措施。例如，發卡機構可能會向商業用途信用卡產品的申請人，索取更多適當資料（如註冊成立記錄及商業執照），而個人及家庭用途的信用卡產品申請人，所需提交的資料可能較少。

## 5.3 初步的客戶盡職審查

發卡機構在考慮將要進行的盡職審查水平時，應使用風險為本的原則。如屬附屬卡或多方持卡人，則應同時考慮需對個人作出的適當身份核實，以及附屬卡持卡人可使用的產品特點所需設置的限制及監控（例如禁止對戶口作出合約條款變更）。這項考慮應在產品設計階段確定。

向上市、受規管或具透明度的公司的僱員發行公司卡所產生的風險，亦與向小企業及非市市公司發卡的風險不同，因為後者設有適當措施的可能性相對較低。

在此階段，發卡機構亦應引入識別潛在高風險客戶的程序，並加以管理。除非當地法律及／或法規有所指定，否則應使用適當的風險為本的原則。有關進一步指引，可參閱沃爾夫斯堡的風險為本[2]原則。

為符合全球制裁機制、當地法律／法規或計劃規則，發卡機構可能需要根據適用的制裁名單，對個人及機構進行審查。某些針對特定國家的制裁計劃並沒有（或基於法律理由而不可能）在所有司法管轄地區內統一採用，這是可以理解。但發卡機構應在開戶程序內結合適當的監控措施，確保符合針對個人及機構的當地及全球制裁。

除主要申請人外，作為風險為本原則的一部分，發卡機構亦應對照適用名單對附屬卡持卡人進行審查。

## 5.4 申請途徑

很多信用卡發卡機構都提供多種申請途徑，包括：親身、網上、電話、直接郵寄、推廣活動，以及經中介人推薦。發卡機構應就每種途徑的防止清洗黑錢風險進行獨立評估。事實上，申

請階段通常並非面對面進行的程序，但並不表示此階段屬於「高風險」。相反，這意味着發卡機構應全面評估可使用的措施（尤其是其他並無文件支持的身份核實方法），以應付此等風險。值得注意的是，規定的監管方法可能會削弱發卡機構對在此階段識別的風險靈活運用動態監控措施的能力。

#### **5.4.1 互聯網／電話；直接郵寄**

發卡機構須確保設有足夠措施來核實客戶身份。發卡機構可使用風險為本的原則，採用適當的、並無文件支持的客戶身份識別程序，如信用機構、公眾檔案資料或第三方服務等。發卡機構及處理申請手續的第三方服務供應商應接受適當培訓（例如，申請表格被明顯竄改、來自同一互聯網 IP 地址的重複申請等），以便能夠察覺申請中的「警示」或其他不尋常情況。

#### **5.4.2 第三方**

發卡機構須確保由第三方代其收取的申請，符合與經由直接服務途徑收取的申請類似的客戶身份標準。最重要是，發卡機構及第三方均維持有效的防止清洗黑錢合規程序，包括定期進行風險為本的檢查及檢討。

#### **5.4.3 商戶優惠卡（如百貨公司優惠卡）**

不同用途的商戶優惠卡涉及不同的風險。例如，僅可用於一家商戶或少數指定商戶的「專用」商戶優惠卡，相比由商戶發行可作一般用途的「非專用」商戶優惠卡，風險顯著較少。這些商戶應與其他第三方一樣，接受適當的培訓及商戶監督，發卡機構更可制訂交易監察境況，用以查找在這些商戶出現的不尋常消費模式。

#### **5.4.4 即時批核信用卡**

發卡機構應考慮即時批核信用卡的審批程序所涉及的額外風險。在這種安排中，發卡機構可能僅對申請人進行有限的初步審核，以便特定商戶向客戶提供即時作單次使用的信貸產品（客戶一般會在幾日內收到信用卡）。除欺詐監察措施外，發卡機構應特別注意這種發卡程序所引發的防止清洗黑錢考慮事項。

### **5.5 批核及核實**

發卡機構必須在批准客戶使用信用額前，取得有關客戶資料，並須採用風險為本的原則，及時核實客戶身份。

### **5.6 交易／客戶監察**

5.6.1 在發卡後，發卡機構必須即時建立有效的交易監察架構，進行持續的盡職審查。發卡機構應把握機會制訂防止清洗黑錢的監察境況，並在適當情況下將之與其他系統整合，例如那些欺詐監察措施。如上文所述，身份盜竊或濫用可能是金融犯罪的其中一環，這與防止欺詐及清洗黑錢同樣重要。因此，有效的防止欺詐與防止清洗黑錢合規程序兩者之間，可能包含多項重疊的元素。但在其他方面，如限制大額付款、現金付款及電匯，此等程序的目標並不一致，甚至可能顯得互相衝突。總括而言，在設計用以識別不尋常清洗黑錢活動的監察工具時，必須同時考慮這些風險之間的異同。

5.6.2 在開始設計有效的欺詐監察境況時，通常會參考早期導致已識別虧損的連串客觀事件；而清洗黑錢的境況，則從犯罪情報／類型的角度出發。換句話說，清洗黑錢者會設法維持表面良好的戶口操作（例如準時支付賬單），使發卡機構對他們採用較少「警示」的「標準」監察方法。發卡機構必須瞭解不同境況之間的差異，以便設計有用的監察工具及定期評估此等工具的有效性。

5.6.3 有效的交易監察架構必須至少包括下列程序：(i)在內部上報潛在可疑活動，(ii)向政府金融情報單位或其他機關提交可疑活動報告，(iii)考慮是否終止與持卡人的客戶關係，及(iv)記錄相關程序及編製文件。監察程序應包括適當運用技術解決方案，並須確保所有負責評估及調查交易的人員已接受足夠的相關培訓。

## 5.7 「警示」指標

如上文所述，某些產品的特點、功能或活動可能會構成產品被不正當用作清洗黑錢的風險。以下列出數個與防止清洗黑錢相關的「警示」，這清單並不完備，而且必須謹記，風險識別是一個動態及不斷演變的過程。另外，雖則明白到發卡機構可能會遇到重大限制（例如是否有可用數據），以致削弱其監察所有此等指標的能力，但是，在調查不尋常及潛在可疑交易時，發卡機構適宜考慮此等指標。

有關不尋常及潛在可疑活動指標的監察和培訓，仍然是嚴謹的防止清洗黑錢程序中重要的元素。

### 5.7.1 申請、身份識別及批核：

- 申請表格資料不符；
- 申請表格內的資料／地址／客戶與預先審查的申請人不同；
- 無法核實持卡人的身份資料；
- 無法提供由政府發出的身份識別資料；
- 主卡／附屬卡使用者名列於適用的政府監察／制裁名單內；
- 於發卡或增加信用額後不久，持卡人將地址更改至高欺詐風險地區或有問題的司法管轄地區。

### 5.7.2 交易監察

- 於自動櫃員機用卡進行次數頻密及不尋常的現金提款；
- 有組織地進行付款／超額付款：如持卡人超額付款或如商戶向戶口存入信用額，卡結餘可能會轉撥為一般賬戶結餘。而貸方餘額返還可能被用作從事清洗黑錢活動；
- 不尋常的現金透支活動及大額現金付款：現金入賬必須受到監察，因為過度的現金付款經常是清洗黑錢的一種技倆。由於通過累積貸方餘額產生退款（貸方餘額返還）可能是清洗資金計劃的一種手段，發卡機構必須加以監察；
- 跨境：在另一個司法管轄地區用卡提取現金，便可在有限的審查追蹤下輕易地（並可能涉及巨大金額）跨境轉移資金；
- 在一些被某機構視為涉及較高的清洗黑錢風險的國家或地區，不尋常地購買貨品或服務；
- 利用商戶禮物卡超額支付同一商戶的優惠卡賬項；
- 以個人優惠卡在商戶內購物，而消費模式顯然與過往消費行為不符；
- 商戶的貸項並未與商戶交易對銷；

### 5.7.3 客戶監察

- 過度使用客戶電話服務；
- 客戶不尋常地處理聯絡資料（例如經常更改地址）。

### 5.7.4 卡戶口結算：

- 多次頻密的現金付款或開立匯票；大額的跨境電匯付款；
- 來自無關聯第三方的結算／部分結算（如發行機構取得該項資料）；
- 由無關聯的支票／往來戶口支付多個信用卡戶口的賬項（如發卡機構取得該項資料）；
- 過度／持續的大額貸方餘額返還。

## 5.8 結束卡戶口

根據可疑活動的嚴重性及頻密程度，在法律許可的情況下，發卡機構適宜終止卡戶關係。如上文所述，發卡機構應定出準則，在發現和舉報可疑活動，或在識別負面的客戶資料之後，終止卡戶的關係。這些標準應闡明發卡機構會否及在何種情況下主動通知執法機關，並應訂明相關程序，以防持卡人獲「通風報信」。

## 6. 商戶收單

商戶收單業務的清洗黑錢風險與發卡業務不同，而且風險可能較高。這是因為商戶執行的金融交易基本上與持卡人所執行者並不相同（包括交易量及價值的差異；商戶辦理退款的能力，而這可增加串謀舞弊的風險；對不存在貨品收費；收費單據的可轉讓性等）。

在建立商戶收單安排前，收單機構應進行風險為本的評估，當中應考慮商戶的業務類型，以適當釐定應進行的盡職審查水平。被識別為高風險的商戶應接受更嚴格的盡職審查（包括在可能及適當情況下進行現場查訪），並且在維持業務關係期間應接受更頻密的審核。

### 6.1 減輕風險措施

部分監管機構期望商戶收單機構瞭解收單程序涉及的風險，並相應實施適當的戶口及交易監察。很多關於商戶收單的營運規則，如萬事達及 Visa 頒布的規則，均在這方面提供與欺詐相關的指引。

收單機構應通過瞭解本身商戶提供的貨品種類，以及就該業務而言，哪些活動／交易能夠顯示清洗黑錢活動，從而減輕一家或多家商戶涉及清洗黑錢的風險（及提防商戶串謀舞弊的風險）。

如果收單機構使用第三方（如獨立銷售組織（ISO））代表收單機構批核及／或提供設備或其他服務，則應確保訂有適當的合約，明確規定第三方供應商應符合的服務要求及水平。

### 6.2 初步及持續的盡職審查

收單機構應從商戶申請表格獲取足夠資料，以便評估風險。申請表格所載相關資料可以適當的電子形式或合適的文件加以確證。這可包括（如有及適用）商業信用機構報告及商戶負責人的個人信用記錄報告。收單機構應通過分析收單前及收單後的資料，以瞭解商戶的一般收費種類及金額，並應不時驗證有關活動。

初步的盡職審查應通過交易監察，以協助識別可能顯示清洗黑錢及其他非法活動的收單活動（如交易量、資金流速等）。

### 6.3 風險／警示指標

正如發卡活動一樣，商戶收單業務可構成一系列獨有的風險威脅，這些威脅可能與欺詐或清洗黑錢有關。以下「警示」清單列出其中一些威脅。無可否認，收單機構可能會遇到重大限制（例如是否有可用數據），以致影響其監察所有此等指標的能力，但是，在調查不尋常及潛在可疑交易時，收單機構適宜考慮此等指標。

#### 6.3.1 開立戶口：

- 商戶負責人似乎對業務並不熟悉或缺乏清楚瞭解；
- 較高風險的商戶／產品類別；
- 缺乏由第三方及／或政府發出的可靠業務核證；
- 所顯示（或確證）的地址被識別為郵箱或其他高風險地址，而非確實街道地址；
- 預期交易額／退款／簽賬退款與現場查訪或同類商戶／同業集團不符；
- 業務相對較新，幾乎沒有過往營運記錄可供評估；
- 業務負責人／擁有人並無政府發出的身份識別文件或政府機關核證（如適用）；
- 商戶／負責人／擁有人名列於適用的監察／制裁名單內。

#### 6.3.2 交易及商戶監察：

- 與開戶時預估的情況相比，處理交易量（資金流速）及金額（例如平均交易金額、銷售量、簽賬退款及退款率等）出現不尋常的變化或趨勢轉變；
- 偏離慣常模式或過度的現金透支額或貸方餘額返還；
- 缺乏收費活動（即監察不活躍戶口是否可能被利用作不法的資金轉移）；
- 加強監察被某機構評估為較高風險的商戶的交易活動；
- 簽賬退款與交易種類／交易量不符；
- 在開立戶口後隨即出現不尋常交易量、更改戶口地址或進行其他活動；
- 有證據顯示商戶的設施由第三方使用；
- 商戶／負責人／擁有人可能名列於政府監察／恐怖份子名單內。

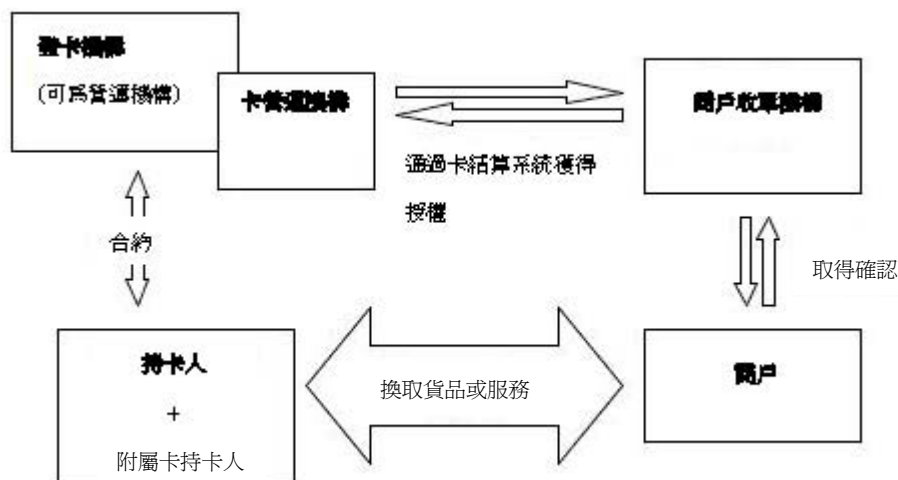
## 7. 總結

與發卡及收單活動有關的清洗黑錢風險，過往一直被認為較許多其他金融產品及服務的風險為低。然而，除非使用適當措施以識別及管理此等風險，發卡及收單活動均容易受到威脅及被濫用。最有效的監察方法，是將此等措施納入風險為本的全面防止清洗黑錢合規程序內，此程序包括嚴謹的客戶盡職審查、有效的交易監察，以及適當的員工培訓，並充分利用現有欺詐偵測及戶口管理設施的優點。



## 附錄一

### 卡交易的各方



## 附錄二

### 詞彙表

#### 收單機構 (商戶收單機構)

與商戶、零售商及其他服務供應商維持業務關係，為其處理卡交易的銀行或其他金融機構。收單機構處理已收單的扣賬卡及信用卡交易，向商戶償付銷售金額，並就服務徵收服務費／佣金。

#### 授權

商戶要求批准使用卡進行特定金額交易的程序。

#### 自動櫃員機

亦稱為現金自動提款機、現金提存機或櫃員機，為電腦化的自助服務器材，允許持有適當的卡和私人密碼的人士從本身戶口提取現金，以及使用其他銀行服務。

#### 發卡機構

向其客戶發行付款卡、自動櫃員機卡或支票擔保卡的金融機構。就付款卡及自動櫃員機專用卡而言，發卡機構承擔有關卡交易的結算責任，惟某些存在欺詐的情況除外。

#### 持卡人

持卡人是指以其名義獲得發卡機構發卡的用戶或客戶。持卡人亦包括由持卡人為其提出要求而發卡機構同意向其發出附屬卡的任何附屬卡使用者。

## 卡營運機構

營運機構處理卡的生產及管理，包括負責償還信用卡的任何未償還結欠或確保扣賬卡交易結欠不超過相關戶口的可用結餘。營運機構及發卡機構可以是同一機構，或營運機構可訂約承辦發卡機構的卡營運業務。

## 卡計劃

卡計劃訂立營業規則，監管附有卡計劃標誌的付款卡的發卡事宜。一般來說，此等規則適用於世界各地，確保各種卡能夠共同運作。許多國家或地區亦經營本地的卡計劃。這些計劃負責營運付款卡交易的結算及交收。在英國，銀行及房屋建築協會必須屬於適當計劃的成員，才可發卡及從事卡交易收單業務。國際卡組織包括 Visa、萬事達、美國運通、Discover 及大來等。

## 簽賬卡(Charge Card)

一種付款卡，持卡人可用以購物及提取現金，一般已預設上限，其條款包括在指定期限結束前悉數結賬的責任。持卡人一般需要繳交年費。

## 簽賬退款

發行機構因持卡人提出爭議及／或發卡機構發現交易不當，而向收單機構退回交易賬單。

## 便利支票

一種由信用卡發卡機構向消費者提供的支票，使持卡人可從信用卡戶口提款。便利支票的用途與個人支票相同。

## 信用卡

一種付款卡，持卡人可用以購物及提取現金，一般已預設上限。已授出的信用額可於指定期限結束前悉數或部分結賬，若部分還款，則會收取利息。如屬現金提款，利息一般由交易日開始計算。持卡人或要繳交年費。

## 電子銷售點

可於銷售點（如商店、銀行等）使用的終端機或類似器材。

## 發卡機構

向其客戶發行付款卡、自動櫃員機／現金自動提款機卡或支票擔保卡的銀行或房屋建築協會。就付款卡而言，發卡機構承擔有關卡交易的結算責任，惟某些存在欺詐的情況除外。

## 商戶

已訂約由收單機構承辦交易處理的任何人士、商號或法團。

## 綜合付款服務機構

付款服務供應商，專門將同一商戶（或信用卡戶口）的多宗小額交易合併至一個綜合主戶口，以便由此戶口作出較大額而較少次數的付款。

## 私人密碼

持卡人於銷售點或利用客戶服務啟動器（如現金自動提款機）用以核實身份的一組數字符號，一般為四位數序列。該組數字在首次發卡時由發卡機構產生，隨後可由持卡人更改。

## 預先審查

編製客戶郵寄名單及將客戶的回應視作一項申請處理，包括審核客戶的信用記錄報告。

---

<sup>1</sup> 沃爾夫斯堡組織由下列具領先地位的國際金融機構組成：西班牙國家銀行（**Banco Santander**）、三菱東京 **UFJ** 銀行、栢克萊銀行、花旗集團、瑞信集團、德意志銀行、高盛、滙豐、摩根大通、法國興業銀行及瑞士銀行。

另外，下列機構亦參與編製本文件：美國運通公司、勞埃德 **TSB**。

<sup>2</sup> 請於 <http://www.wolfsberg-principles.com/standards.html> 參閱已發表的沃爾夫斯堡文件。

<sup>3</sup> 預先審查是為卡產品識別潛在客戶的程序，包括那些「預先批核」產品。

---

© 沃爾夫斯堡組織 – 2009 年 5 月 4 日