

渣打銀行信用卡網路服務暨行動銀行約定條款

本約定條款適用之對象僅限定為渣打國際商業銀行(以下簡稱貴行)之所有信用卡正卡持卡人(以下簡稱立約人)，立約人使用本行信用卡網路服務暨行動銀行與交易時，視同接受本約定條款。

一、契約之適用範圍

本約定係信用卡網路服務暨行動銀行之一般性共通約定，除個別契約或本行另有規定外，悉依本約定辦理。本契約未約定事項，悉依一般約定事項及相關銀行規定辦理，但個別契約對立約人之保護更有利者，從其約定。本契約條款如有疑義時，應為有利於立約人之解釋。

二、名詞定義

1. 「信用卡網路服務暨行動銀行」係指立約人端電腦或智慧型手機經由網際網路與 貴行電腦連線，無須親赴 貴行櫃台，即可直接取得 貴行所提供之各項金融服務。「行動銀行」係指以智慧型手機使用 貴行行動銀行 APP 中網路理財內之信用卡網路服務。
2. 「電子文件」：係指 貴行或立約人經由網路連線傳遞之文字、聲音、圖片、影像、符號或其他資料，以電子或其他以人之知覺無法直接認識之方式，所製成足以表示其用意之紀錄，而供電子處理之用者。
3. 「SSL 安全機制」SSL (Secure Socket Layer)是一種網際網路上最普遍使用的安全通訊協定，保障網站伺服器及瀏覽器之間的數據資料傳輸的安全性。透過使用這個協定，網路上的數據傳輸會採 128 位元(含以上) 對稱性加密演算法進行加密，更會檢查資料的完整性。除此以外，透過所謂『金鑰』的加密技術及嚴謹的 SSL 認證註冊的程序，SSL 可以驗證伺服器的身分而達到網站瀏覽者向網站身分作出檢查的目的。
4. 「使用者名稱」係由立約人自行設定一組 6~12 位英文字母、數字，至少須有一英文字母，英文字母區分大小寫，且不得為立約人身分證字號或連續相同英文字母、數字，作為立約人透過電腦或智慧型手機登入信用卡網路服務時，身分驗證的資料之一。
5. 「使用者密碼」：係由立約人自行設定一組 6~12 位英文字母、數字，至少須有一英文字母，英文字母區分大小寫，不得為立約人身分證字號或連續相同英文字母、數字，且不得與使用者名稱相同，作為立約人透過電腦或智慧型手機登入信用卡網路服務身分驗證的資料之一。
6. 「簡訊密碼 (SMS OTP, Short Message Service One Time Password)」：指立約人進行線上立即申請或忘記使用者名稱及密碼時，系統將自動發送一組「簡訊密碼」(內含 OTP 密碼及申請內容)至立約人所約定之一組行動電話號碼，確保網路交易之安全性(每次傳送 OTP 密碼皆為亂數產生，且僅當次有效)，有關 OTP 之交易機制，以 貴行網站所載規定為準。簡訊密碼此項服務之提供與發送，以 貴行簡訊廠商與各電信業者簽定的服務範圍(如國際漫遊協議等)為限。

三、銀行資訊

1. 銀行名稱：渣打國際商業銀行
2. 申訴及客服專線：客服專線:全省市話請撥：4058-0088/行動電話請撥：02-4058-0088；本行免付費申訴專線 0800-051234
3. 網址：<https://www.sc.com/tw>
4. 地址：新竹市中央路 106 號
5. 傳真號碼：03-5722107
6. 銀行電子信箱：Callcenter.tw@sc.com

四、網頁之確認

立約人使用信用卡網路服務暨行動銀行前，請先確認信用卡網路服務正確之網址並透過本行官方網站使用信用卡網路服務，行動銀行請至 AppStore (iPhone) 或 Google Play (Android) 下載安裝行動銀行 APP，請勿自其他網站下載；

如有疑問，請致電 貴行客服專線(24 小時客服市話請撥：4058-0088/行動電話請撥：02-4058-0088)詢問。貴行須以一般民眾得認知之方式，告知立約人信用卡網路服務暨行動銀行業務應用環境之風險。貴行應盡善良管理人之義務，隨時維護網站的正確性與安全性，並隨時注意有無偽造之網頁，以避免立約人之權益受損。

五、服務項目

當立約人申請核准後，貴行提供之信用卡網路服務及行動銀行內容以貴行網站與信用卡網路服務及行動銀行公告揭露為主，貴行應確保該網站訊息之正確性，對立約人所負之義務不得低於網站之內容。

未來貴行若有新種業務開辦或信用卡網路服務或行動銀行內容有變動(含新增、調整、變更或取消)，貴行僅須於貴行網站與信用卡網路服務及行動銀行公告揭露，即可提供相關服務。

六、連線所使用之網路

貴行及立約人同意使用網路進行電子文件傳送及接收。

使用雙方各自約定之相關網路業者，雙方應分別就各項權利義務關係與網路業者簽訂網路服務契約，並各自負擔網路使用之費用。

七、電子文件之接收與回應

貴行接收經貴行及立約人同意用以辨識身分之電子文件後，除查詢之事項外，貴行須提供該交易電子文件中重要資訊之網頁供立約人再次確認後，即時進行檢核及處理，並將檢核及處理結果，以網頁即時呈現或電子郵件或其他雙方約定之方式通知立約人。

貴行接收立約人或立約人接收貴行之任何電子文件，若無法辨識其身分或內容時，視為自始未傳送，但貴行可確定立約人身分時，應立即將內容無法辨識之事實，以網頁即時呈現或電子郵件或其他雙方約定之方式通知立約人。立約人所發送之電子訊息，若為非發送日所須立即處理者，立約人同意以發送時與貴行所約定之情況為準。

八、電子文件之不執行

如有下列情形之一，貴行將不執行任何接收之電子文件：

- 1.有具體理由懷疑電子文件之真實性或所指定事項之正確性者。
2. 貴行依據電子文件處理，將違反相關法令之規定者。

貴行不執行前項電子文件者，應同時將不執行之理由及情形，以網頁即時呈現或電子郵件或其他雙方約定之方式通知立約人，立約人受通知後得透過客服電話或親臨分行或以其他雙方約定方式向貴行確認。

九、電子文件交換作業時限

信用卡網路服務及行動銀行電子文件係由貴行資訊系統自動處理，立約人發出電子文件，經立約人依第七條第一項貴行提供之再確認機制確定其內容正確性後，傳送至貴行後即不得撤回。

本服務為 24 小時服務機制，貴行如因特定因素(如資訊系統例行維護等)無法提供服務時，貴行需提前於貴行網頁及行動銀行明顯處公告之；惟若遇突發狀況，為保障立約人權益，貴行得隨時暫停服務，進行狀況排除，但須於貴行網頁及行動銀行明顯處公告之。

十、費用

立約人自使用本契約服務之日起，願依約定收費標準繳納服務費、手續費及郵電費，並授權貴行自立約人之帳戶內自動扣繳；如未記載者，貴行不得收取。

前項收費標準於訂約後如有調整，貴行應於貴行網站上明顯處公告其內容，並以電子郵件或其他雙方約定之方式使立約人得知調整之內容。若配合貴行優惠活動，得依較優惠之價格收取費用，並於活動開始後公告即可。

第二項之調整如係調高者，貴行應於網頁上提供立約人表達是否同意費用調高之選項。立約人未於調整生效日前表示同意者，貴行將於調整生效日起暫停立約人使用信用卡網路服務及行動銀行一部或全部之服務。立約人於調整生效日後，同意費用調整者，貴行應立即恢復信用卡網路服務及行動銀行契約相關服務。

前項貴行之公告及通知應於調整生效六十日前為之，且調高之生效日不得早於公告及通知後次一年度之起日。

十一、立約人軟硬體安裝與風險

立約人申請使用本契約之服務項目，應自行安裝所需之電腦/智慧型手機之軟體、硬體，以及其他與安全相關之設備。安裝所需之費用及風險，由立約人自行負擔。

第一項軟硬體設備及相關文件如係由 貴行所提供， 貴行僅同意立約人於約定服務範圍內使用，不得將之轉讓、轉借或以任何方式交付第三人。 貴行並應於網站及所提供軟硬體之包裝上載明進行本服務之最低軟硬體需求，且負擔所提供軟硬體之風險。

立約人於契約終止時，如 貴行要求返還前項之相關設備，應以契約特別約定者為限。

十二、立約人連線準備及其責任

1.若 貴行與立約人有特別約定者，立約人必須與 貴行為必要之測試後，始得連線。

2.立約人對 貴行所提供或授權使用之使用者名稱、使用者密碼或簡訊密碼、約定接收簡訊密碼之行動電話及其行動電話號碼之 SIM 卡之軟硬體及相關文件，應負保管之責，未妥善保管而發生遺失、毀損、滅失所致之損失，由立約人自行負責， 貴行不負任何賠償責任。

第一項軟硬體設備及相關文件如係由 貴行所提供， 貴行僅同意立約人於約定服務之範圍內使用，不得將之轉讓、轉借或以任何方式交付第三人。倘因立約人之行為致侵害 貴行或第三人之智慧財產權或其他權利，或因不當之操作使用導致損害時，應自負其責任。

立約人輸入前項密碼(使用者名稱或使用者密碼或簡訊密碼)連續錯誤達三次時， 貴行電腦及行動銀行即自動停止立約人使用本契約之服務。立約人如擬恢復使用，應依約定辦理相關手續。

十三、交易核對

貴行於每筆交易指示處理完畢後，以電子文件或 貴行及立約人約定之方式通知立約人，立約人應核對其結果有無錯誤，如有不符，應於交易完成日起四十五日內，以透過客服電話或親臨分行或其他雙方約定之方式通知 貴行查明。 貴行應於每月對立約人以平信或其它雙方約定方式寄送上月之交易月結單（該月無交易時不寄）。立約人核對後如認為交易月結單所載事項有錯誤時，應於收受之日起四十五日內，以透過客服電話或親臨分行或其他雙方約定之方式通知 貴行查明。

貴行對於立約人之通知，應即進行調查，並於通知到達 貴行之日起三十日內，將調查之情形或結果以書面方式覆知立約人。

十四、電子文件錯誤之處理

立約人利用本契約之服務，如其電子文件因不可歸責於立約人之事由而發生錯誤時， 貴行應協助立約人更正，並提供其他必要之協助。

前項服務因可歸責於 貴行之事由而發生錯誤時， 貴行應於知悉時，立即更正，並同時以電子文件或 貴行及立約人約定之方式通知立約人。

十五、電子文件之合法授權與責任

雙方同意應確保所傳送至對方之電子文件均經合法授權。

雙方同意於發現有第三人冒用或盜用經合法授權之使用者名稱及密碼，或其他任何未經合法授權之情形，應立即以電話或其他雙方約定方式通知他方停止使用該服務並採取防範之措施。

貴行接受前項通知前，對第三人使用該服務已發生之效力，由 貴行負責。但有下列任一情形者，不在此限：

1. 貴行能證明立約人有故意或過失。
2. 貴行依雙方約定方式通知交易核對資料或帳單後超過四十五日。惟立約人有特殊事由(如長途旅行、住院等) 致無法通知者，以該特殊事由結束日起算四十五日，但 貴行有故意或過失者，不在此限。

針對第二項冒用、盜用事實調查所生之鑑識費用由 貴行負擔。

十六、資訊系統安全

雙方應各自確保所使用資訊系統之安全，防止非法入侵、取得、竄改或毀損業務記錄及立約人個人資料。

第三人破解 貴行資訊系統之保護措施或利用資訊系統之漏洞爭議，由 貴行就該事實不存在負舉證責任。因第三人入侵 貴行資訊系統所造成之損害，由 貴行負擔。

十七、保密義務

除其他法律規定外， 貴行應確保所交換之電子文件因使用或執行本契約服務而取得立約人之資料，不洩漏予第三人，亦不可使用於與本契約無關目的，且於經立約人同意告知第三人時，應使第三人負本條之保密義務。

前項第三人如不遵守此保密義務者，視為本人義務之違反。

十八、損害賠償責任

雙方同意依本契約傳送或接收電子文件，因可歸責於當事人一方之事由，致有遲延、遺漏或錯誤之情事，而致他方當事人受有損害時，該當事人應就他方所生之損害負賠償責任。

十九、紀錄保存

1. 雙方應保存所有經由本服務所提供之相關電子文件紀錄，並應確保紀錄之真實性及完整性。

2. 貴行對前項紀錄之保存，應盡善良管理人之注意義務。保存期限至少為五年以上，但其他法令有較長規定者，依其規定。

3. 本服務提供之各項信用卡交易資料，僅供立約人作為參考之用，正確之資料仍應以 貴行提供之月結單為準。

4. 若本服務因電腦系統暫停服務而無法辦理或查詢資料時，請來電 貴行 24 小時客戶服務中心。

二十、電子文件之效力

雙方同意以電子文件作為表示方法，依本契約交換之電子文件，其效力與書面文件相同。但法令另有排除適用者，不在此限。

二十一、客戶終止契約

立約人本人得隨時來電本行 24 小時客戶服務中心，經由服務人員核對身份與資料無誤後，終止本約定條款。

二十二、 貴行終止契約

貴行得於發生下列行為時立即終止提供本約定之服務：

1. 立約人如企圖利用信用卡網路服務及行動銀行搜集他人資料或有不良之使用記錄或有任何破壞及不當行為時，貴行得不經通知立即取消立約人之使用資格。
2. 得依本約定條款於網站揭示後停止提供此項服務，惟應於三十日前公告於本行網站。
3. 立約人違反本約定條款之規定或擅自將使用本服務之權利或義務轉讓第三人使用者。
4. 立約人依破產法聲請宣告破產或消費者債務清理條例聲請更生、清算程序者。
5. 立約人違反本契約第十五條至第十七條之規定者。
6. 立約人違反本契約之其他約定，經催告改善或限期請求履行未果者。

二十三、契約修訂

本契約約款如有修改或增刪時，於修改日十日前將修改內容公告於本行網站，立約人於十日內不為異議者，視同承認該修改或增刪約款。但下列事項如有變更，應於變更前六十日以雙方約定方式通知立約人，並於雙方約定方式以顯著明確文字載明其變更事項、新舊約款內容，暨告知立約人得於變更事項生效前表示異議，及立約人未於該期間內異議者，視同承認該修改或增刪約款；並告知立約人如有異議，應於前項得異議時間內通知銀行終止契約：

1. 第三人冒用或盜用使用者代號、密碼，或其他任何未經合法授權之情形， 貴行或立約人通知他方之方式。
2. 其他經主管機關規定之事項。

二十四、文書送達

立約人同意以契約中載明之地址或立約人依信用卡合約書留存之地址為相關文書之送達處所，倘立約人之地址變更，應即以書面或其他約定方式通知 貴行，並同意改依變更後之地址為送達處所；如立約人未以書面或依約定方式通知變更地址時， 貴行仍以契約中立約人載明之地址或最後通知 貴行之地址為送達處所。

二十五、法令適用

關於本約定條款，除雙方有特別約定者外，適用中華民國法律。

二十六、法院管轄

因本契約而涉訟者， 貴行及立約人同意以台灣台北地方法院為第一審管轄法院。但不得排除消費者保護法第四十七條或民事訴訟法第四百三十六條之九規定小額訴訟管轄法院之適用。

二十七、標題

本契約各條標題，僅為查閱方便而設，不影響契約有關條款之解釋、說明及瞭解。

二十八、契約分存

立約人可於 貴行官方網站直接列印本約定書予以留存，但最終版本須以 貴行網站上列示為準。

二十九、信用卡網路服務及行動銀行使用

1. 使用方式：立約人須經由連結網際網路之電腦或智慧型手機，連結至貴行提供之「信用卡網路服務網頁」，申請使用之。
 - A. 信用卡網路服務線上申請流程：立約人需登入貴行官方網站，並以貴行連結網址進入信用卡網路服務頁面，點選網頁上之「線上立即申請」後，閱讀並同意本條款，再經 貴行身分驗證後，以立約人留存於本行之行動電話號碼接收簡訊密碼，再由立約人自行設定使用者名稱及使用者密碼後，即可登入使用信用卡網路服務，如立約人於貴本行未留存行動電話號碼，則於線上申請完成後須致電客服中心進行啟用，始可登入使用信用卡網路服務。
 - B. 立約人於使用時需輸入正確的身分證字號、使用者名稱及使用者密碼，經貴行驗證立約人身分無誤後，方得登入使用本服務。
 - C. 行動銀行開通及停用：本服務功能須由立約人登入信用卡網路服務且詳閱並同意「渣打行動銀行注意事項」，輸入使用者密碼後進行行動銀行開通及行動裝置認證程序，本行將提供一組 4 位數行動裝置認證密碼，立約人須登出信用卡網路服務後，由立約人自行於智慧型手機下載渣打銀行行動銀程式並完成安裝，且於智慧型手機開啟程式並輸入與信用卡網路服務相同之使用者名稱及使用者密碼後，再輸入行動裝置認證密碼，經本行驗證後，始開始使用相關服務。立約人須於取得認證密碼時起 24 小時內依 貴行指定之行動銀行服務系統認證方式完成個人智慧型手機認證。倘立約人逾前述密碼認證時效尚未進行認證作業，系統將自動取消該組認證密碼，立約人日後若仍擬使用行動銀行，應於信用卡網路服務依下述行動裝置認證程序重新辦理認證手續。停用時亦須由立約人登入信用卡網路服務且詳閱並同意「渣打行動銀行注意事項」後完成行動銀行停用設定，停用後所有已認證之行動裝置將同步取消。
 - D. 行動裝置認證：立約人如需於未經 貴行認證之智慧型手機進行 貴行行動銀行服務，立約人須登入信用卡網路服務且輸入「使用者密碼」，以進行行動裝置認證。 貴行將顯示一組 4 位數行動裝置認證密碼於網頁上，立約人須先登出信用卡網路服務，再以智慧型手機登入行動銀行，並輸入該 4 位數行動裝置認證密碼，始得完成行動裝置認證程序並使用行動銀行相關服務。立約人須於取得認證密碼時起 24 小時內依 貴行指定之行動銀行服務系統認證方式完成個人智慧型手機認證。倘立約人逾前述密碼認證時效尚未進行認證作業，系統將自動取消該組認證密碼，立約人日後若仍擬使用行動銀行，應於信用卡網路服務重新辦理認證手續。行動裝置認證最多以三組智慧型手機為限。立約人如需刪除行動裝置認證，須登入信用卡網路服務刪除該組行動裝置認證，並輸入「使用者密碼」後，即完成刪除程序。

E.同一客戶(同一身分證字號)於同一時間僅可擇一透過連結網際網路之電腦或智慧型手機,登入使用本行提供之「信用卡網路服務」。

2.使用限制

A.初次或重新申請信用卡網路服務時,立約人需輸入個人及信用卡重要資料供系統驗證,若所輸入資料經驗證錯誤達三次,系統將自動鎖定暫時停止其信用卡網路服務之申請;立約人需親自來電客服辦理「解除申請鎖定」方可重新註冊。

B.為保護立約人權益,登入時如「使用者名稱」或「使用者密碼」累計輸入錯誤達三次(分開計算),貴行電腦即自動停止使用本契約之服務。立約人如需恢復使用,應重新辦理註冊申請手續。(即於網頁登入頁面上點選「線上立即申請」)

C.貴行對立約人輸入身分證字號、使用者名稱與使用者密碼使用之各項信用卡網路服務及行動銀行,均認定係立約人所為之有效指示,故同一時間內,系統只允許一人透過電腦或智慧型手機登入信用卡網路服務。基於風險考量,若同一時間有二人以上以同一身分證字號登入使用網路服務,貴行除將自動拒絕受理第一位以外使用者使用網路服務系統外,亦會將第一位使用者強制登出,並於五分鐘內暫停此使用者登入之權利。

D.立約人透過電腦或智慧型手機登入使用信用卡網路服務及行動銀行,若忘記登出離開貴行系統或超過五分鐘未執行任何指令時,貴行會自動將立約人自系統登出,以避免為他人所使用。立約人必須重新透過電腦或智慧型手機登入,始可繼續執行交易。

E.如超過一年未成功登入,貴行將終止信用卡網路服務及行動銀行,如擬恢復使用,立約人需重新申請。

F.立約人對其身分證字號、使用者名稱及使用者密碼及其自身相關資料應負保密之責。

3.責任及義務

A.貴行認定憑正確身分驗證資料申請貴行信用卡網路服務及行動銀行之立約人均為立約人本人。

B.除因貴行之故意或重大過失所致者外,貴行對因電腦系統、電信線路故障或第三人之行為或疏漏所致之錯誤或延誤,或對任何服務行為所生之直接、間接或其他損失均不負任何責任。

C.若因電腦系統暫停而無法辦理或查詢資料時,立約人可由其他方式如:24小時電話客戶服務人員、電腦語音查詢等辦理所需之服務。

D.立約人應利用其私人電腦、智慧型手機使用本服務。立約人若因使用位於公共場所的電腦設備而造成資料外洩,以及因該項資料外洩而造成之損失,貴行不負任何責任。惟貴行同意提供必要之協助。

E.除另有約定外,所有對立約人之通知,貴行得以書面或貴行同意之其他方式為之,以立約人留存之最後申請異動或最後通知之通訊資料為送達之最後處所。且貴行依該資料寄送後,經通常郵遞期間,即視已依約對立約人送達。

4.不可抗力

A.貴行於發生不可抗力情事時,對於本約定所生義務之不履行或遲延履行均不視為違約,亦無須負任何賠償責任。

B.前項所稱之不可抗力,指因天災、罷工、停工、政府法令限制、或其他任何貴行所不能控制之情事。

5.資料之提供及保密約定

貴行信用卡網路服務及行動銀行查詢網站上之所有相關業務資料包括文字圖片等,專利權、商標、營業秘密、其他智慧財產權、所有權或其他權利,均為貴行所有。除事先經過貴行之合法授權外,均不得擅自重製、傳輸、改作、編輯、登載或以其他任何形式基於任何目的加以使用,否則應負所有法律責任。

Credit Card Online Service and Mobile Banking Agreement

The terms and conditions are applicable to all principal cardholders of the credit cards (hereinafter referred to as the "Customers") issued by Standard Chartered Bank (hereinafter referred to as the "Bank") only. By using the Credit Card Online Service and Mobile Banking, the Customers agree to the terms and conditions herein.

1. Scope of application of contract

This agreement generally applies to Credit Card Online Services and Mobile Banking. Unless otherwise provided under individual contract, this agreement shall always govern. For matters not provided under this agreement, the general terms and conditions and relevant bank policies shall apply; provided, however, that an individual contract that provides you with better protection shall prevail. Where the terms and conditions of the contract are ambiguous, interpretations shall be made favorable to you.

2. Definition

- (1) "Credit Card Online Service and Mobile Banking" means the financial services directly available by the Bank to you through the network connection of your computer and smart phone with the Bank's computer without going to a bank teller. "Mobile banking" means the Credit Card Online Service directly available by the Bank's APP to you through the network connection of your smart phone
- (2) "Electronic document" means any records of communication made up of words, voices, pictures, videos, signs or other materials transmitted via network connection between you and the Bank for electronic process in electronic or any manner which human cannot directly perceive.
- (3) "SSL" or "Secure Socket Layer" is the most common security communication protocol used on the Internet that protects the security of transmission of data and information between website server and browser. Through the use of the protocol, data transmitted on the Internet will be encrypted according to various security level based on the type of certification (128 bit). The protocol examines integrity of information. In addition, through an encryption technology called "key" and strict procedure for SSL certification, SSL verifies the server identity in order for a website browser to validate the identity of a website.
- (4) "User name" means a name made up of 6~12 English letters and Arabic numerals created by you. User name is used as part of the identification verification information when you log in to access your Credit Card Online Service and Mobile Banking.
- (5) "Password" means a password made up of 6~12 English letters and Arabic numerals which is different from the user name created by you. Fixed Password is used as part of the identification verification information when you log in to access your Credit Card Online Service and Mobile Banking, and used as the password for low risk transactions.
- (6) "SMS OTP" or "Short Message Service One Time Password" means the "SMS password" containing transaction ID code, OTP and transaction message automatically generated by the system and sent to the mobile phone number designated by you when you perform a non-designated account's transaction, trust investment, or personal information setup, to ensure the security of online transaction. (Each and every transaction code and OTP transmitted is randomly generated and is valid only for one time use.) The OTP Transaction method shall be governed by the rules contained on the Bank's website. The provision and sending of the SMS OTP is limited to the scope of service entered into between the SMS Company engaged of the Bank and the carriers.

3. Bank information

- (1) Name of the Bank: Standard Chartered Bank (Taiwan) Limited
- (2) Complaint and Customer service: 4058-0088 if calling from a fixed line or 02-4058-0088 if calling from a mobile phone; the Bank's toll free complaint line: 0800-051234.
- (3) Website: <https://www.sc.com/tw>
- (4) Address: No.106, Zhongyang Rd., Hsinchu City
- (5) Fax number: 03-5722107
- (6) Email address: Callcenter.tw@sc.com

4. Verification of website

Prior to your use of Credit Card Online Service and Mobile Banking, make sure you use the correct website address for Credit Card Online Service and use Credit Card Online Service by accessing our official website. Please download the Bank's APP from either AppStore (iPhone) or Google Play (Android) but not from any other application downloading platform. If you have any question, please call the Bank's customer service number (24-hour customer service number is 4058-0088 if calling from a fixed line or 02-4058-0088 if calling from mobile phone). The Bank shall notify you of the risks involved in online banking application environment in a way normal people can understand. The Bank shall always exercise the duty of care of a good faith manager in maintain the accuracy and safety of the website and making sure there is no phony webpage to prevent any damage to you.

5. Services

After approval of your application, the Credit Card Online Service and Mobile Banking available from the Bank shall be based on the notices post on the Bank's website and Credit Card Online Service and Mobile Banking. The Bank shall ensure the accuracy of the information on the website, and the Bank's obligations to you shall not be less than what is stated on the website.

If new types of business are available from the Bank or there is a change to the Credit Card Online Service and Mobile Banking (including addition, adjustment, change or cancellation) in the future, except for account's transactions for which a separate contract in the electronic or written form shall be signed, the Bank may disclose the information by posting a notice on the Bank's website and Credit Card Online Service and Mobile Banking before relevant services may be available.

6. Network used for online services

The Bank and you agree to use the Internet for transmission and reception of electronic documents.

For use of the Internet service provider as agreed to by either party, the parties shall enter into an Internet service contract with respect to their rights and obligations respectively with their own service provider and be responsible for the cost of use of the Internet.

7. Receipt and reply of electronic documents

Upon receipt of the an electronic document used for identity verification agreed to by you and the Bank, and after providing a webpage which displays the important information in such electronic document of transaction for your re-verification unless it is a matter of inquiry, the Bank will promptly perform verification or handle the matter and notify you of the result of verification or outcome of the matter by immediate webpage display, an email or in any manner agreed to by the parties.

If the Bank receives an electronic document from you (and vice versa) and the contents of the document is illegible, the message shall be deemed to have been never sent by the sender. However, if the Bank receives an illegible message but the identity of the sender can be verified, the Bank shall immediately notify you of the fact that you have sent an illegible message to the Bank by immediate webpage display, an email or in any manner agreed to by the parties.

If you send an electronic document for a matter not required to be immediately handled on the same day, you agree the matter may be handled in a manner as agreed to by you and the Bank at the time of the message.

8. Invalid electronic document

In any of the following circumstances, the Bank will not perform a request contained in the electronic document received:

- (1) The Bank has a concern over authenticity of an electronic document or accuracy of the request stated therein for a specific reason;
- (2) The Bank will violate applicable laws and regulations if performing a request contained in the electronic document;

If the Bank decides not to perform a request contained in an electronic document as described in the preceding paragraph, it shall at the same time notify you of the reason why it will not perform the request and status of the matter by immediate webpage display, an email or in any manner agreed to by the parties. Upon notification, you may call the Bank's customer service number, come to any of the Bank's branches personally or in a manner agreed to by the parties to confirm the matter.

9. Electronic document exchange timeframe

Credit Card Online Service and Mobile Banking electronic documents are processed automatically by the Bank's information system. Once you have sent an electronic document to the Bank and verified its accuracy in accordance with the re-verification system provided by the Bank under paragraph 1 of Article 7, you may not withdraw, cancel or revise your document.

Credit Card Online Service is 24 hours service. If the Bank is unable to provide services in certain circumstance (e.g. regular maintenance of information system), the Bank shall post an advance notice in a conspicuous manner on the Bank's webpage. However, in the event of an unexpected situation, the Bank may suspend services at any time in order to protect your rights and benefits and remove the situation; provided, however, that the Bank shall post a notice in a conspicuous manner on the Bank's webpage.

10. Expenses

You agree to pay the service fee, handling fee, and postage and telecommunication fees according to the fee schedule as agreed from the first day of your use of services under the contract, and authorize the Bank to automatically deduct such fees from your account; the Bank may not charge a fee which is not stated in the contract.

In the event of an adjustment to the fee schedule as mentioned above after the contract is entered into, the Bank shall post the details of the change in a conspicuously manner on the Bank's website and issue a notice by email or in a manner agreed to by the parties to inform you of the adjusted fees. If you agree to participate in

promotional activities offered by the Bank to be eligible for discount price, a notice may be posted after the activities start.

If the adjustment in the second paragraph is to increase the fees, the Bank shall provide an option on the website for you to express if you agree to the increase of fees. If you have not agreed prior the effective date of the adjustment, the Bank will suspend your use of part or all of the Credit Card Online Service and Mobile Banking from the effective date of the adjustment. If you agree to the adjustment of fees after the effective date of the adjustment, the Bank shall immediately resume the Credit Card Online Service and Mobile Banking. The Bank's post and notice in the preceding paragraph shall be made sixty (60) days prior to the effective date of adjustment, and the effective date of an increase may not be earlier than the first day of the year after such post and notice.

11. Software/hardware installation and risks

When you apply for use of services under the contract, you shall be responsible for installing computer/ smart phone software, hardware and other related security device as required. You shall be solely liable for the costs and risks involved in the installation.

In case the software, hardware and related documents in the preceding paragraph are provided by the Bank, the Bank only agrees you may use them to the extent they are required to enable the agreed services and you shall not assign, lease or deliver any of the above to third party. The Bank shall specify the minimum hardware/software requirements for using the services on the website or on the package of the hardware/software provided by the Bank and shall bear the risks involved in the hardware/software provided by the Bank.

The Bank may not ask you to return the related device in the preceding paragraph upon termination of contract unless otherwise specially provided in the contract.

12. Your responsibility for connection

(1) In case that the Bank has a special agreement with you, you are required to perform necessary tests with the Bank before the connection may be enabled.

(2) You shall be responsible for keeping the user name, Password or SMS OTP, hardware and software of mobile phone or the SIM card for such phone used for receipt of SMS OTP, and related documents provided or authorized for use by the Bank. You shall be solely liable for any and all losses caused by loss, damage or destruction of the above due to your negligence and the Bank shall not be liable for any such damage.

In case the software, hardware and related documents in the preceding paragraph are provided by the Bank, the Bank only agrees you may use them to the extent they are required to enable the agreed services and you shall not assign, lease or deliver any of the above to third party. If your act infringes the Bank's or a third party's intellectual property rights or other rights, or damage is caused due to improper operation, you shall take the full responsibility.

If you have entered an incorrect password in the preceding paragraph (user name, Password or SMS OTP) for three (3) consecutive times, the Bank's computer will immediately suspend your use of Credit Card Online Service. If you wish to continue your use, you need to follow the relevant procedures as agreed.

13. Transaction verification

Upon completed performance of service requested in a transaction instruction, the Bank will send an electronic document to you or otherwise notify you in a manner agreed to by you and the Bank. You shall verify the accuracy of outcome of the transaction. If the event of any discrepancy, you shall give a notice to the Bank by calling the Bank's customer service number, coming to any of the Bank's branches personally or in a manner agreed to by both parties within forty-five (45) days after completion of the transaction.

The Bank shall send a monthly statement to you for previous month (no statement will be sent if no transaction during the statement cycle) by regular mail or in the manner agreed to by the parties on a monthly basis. Upon verification, if you believe there is an error in the monthly statement, you shall give a notice to the Bank by calling the Bank's customer service number, coming to any of the Bank's branches personally or in a manner agreed to by the parties within forty-five (45) days after receipt of the statement.

With regard to your notice, the Bank shall promptly conduct an investigation and notify you in writing of the status or outcome of investigation within thirty (30) days after receipt of your notice.

14. Handling of errors in electronic documents

When you use the services under the contract, if there is an error in electronic document due to a circumstance for which you are not liable, the Bank shall assist you in making the correction and furnish other necessary assistance.

If an error occurs to the above services due to a circumstance for which the Bank is liable, the Bank shall immediately make the correction upon discovery of the error and at the same send an electronic document to you or otherwise notify you in a manner agreed to by you and the Bank.

15. Legal authorization and responsibility of electronic documents

The parties agree to ensure that electronic documents sent to the other party are all legally authorized.

The parties agree that in the event of discovery of unauthorized use or theft of legally authorized user name and password by third party, or any other circumstances where legal authorization is not obtained, the party discovering the violation shall immediately call or notify the other party in a manner agreed to by both parties to stop using the service and take precautionary measures.

The Bank shall remain liable for use of the services by third party that has taken effect prior to the Bank's receipt of notice, except for any of the following circumstances:

- (1) The Bank is able to prove you had such an intention or committed negligence
- (2) It has been more than forty-five (45) days after the Bank notifies you to verify the transaction or bill in a manner agreed to by the parties. If there is any special circumstance (e.g. long distance travel or hospitalization) which impedes you from being notified, The forty-five (45) days shall begin from the end of the special circumstance. Provided, however, that the Bank shall remain liable if the Bank had such an intention or committed negligence.

The Bank shall be liable for the forensics fees incurred for investigation of the unauthorized use or theft in the preceding paragraph.

16. Information system security

The parties shall ensure security of its information system respectively and prevent illegal access to the system, acquisition, unauthorized modification or damage or destruction of business records and customer's personal information.

In the event of a dispute over third party's removal of protection measure for the Bank's information system or use of a loophole in information system, the Bank shall bear the burden of proof with regard to non-existence of such event. The Bank shall be liable for the damage arising from third party's unauthorized access to the Bank's information system.

17. Confidentiality obligation

Unless otherwise provided by law, the Bank shall ensure not to disclose to third party any electronic documents exchanged between the parties or any information of you received by the Bank in the use or performance of services under the contract and not to use such documents and information for purposes unrelated to the contract. If a third party is to be informed of such documents and information, subject to your consent, the Bank shall cause the third party to be bound by the confidentiality obligation hereunder.

In the event of a violation of the confidentiality obligation hereunder by third party in the preceding paragraph, the disclosing party shall be deemed in breach of its obligation.

18. Damage liability

The parties agree that in the event of damage to either party caused by delay, omission or mistake in sending or receiving electronic documents under the contract due to a circumstance for which the other party is liable, the party shall be liable for damage sustained by the other party and interest accrued thereon.

19. Recordkeeping

(1) The parties shall keep all records related to electronic documents sent through the services and shall ensure the truthfulness and integrity of the records.

(2) The Bank shall exercise the duty of care of a good faith manager in keeping the records in the preceding paragraph for at least five (5) years; provided, however, that if there are longer periods specified in laws, such longer periods shall prevail.

(3) The credit card transaction information provided by the Service is provided to the Customers for their reference only. The correct information shall be based on that identified in the monthly statements provided by the Bank.

(4) If the Customers cannot process or search for any information via the Service due to interruption in the computer system, please call the Bank's 24-hour Customer Service Centre.

20. Validity of electronic documents

The parties agree to communicate by electronic documents, and the electronic documents exchanged under the contract shall be as valid as written documents, unless such validity is prohibited by laws.

21. Termination of contract by customer

The Customers may call the Bank's 24-hour Customer Service Centre in person at any time to terminate the terms and conditions herein after their identity and information have been verified by the service representatives.

22. Termination of contract by the Bank

The Bank may terminate the Service immediately upon the occurrence of any of the following circumstances:

- (1) If the Customers attempt to collect another person's information via the Credit Card Online Service, are proven to have accessed the service improperly, or have been engaged in destruction and misconduct, the Bank may cancel the customers' access authority immediately without prior notice.

- (2) The Bank may suspend the Service after disclosing the suspension on the website pursuant to the terms and conditions herein, provided that it shall disclose the suspension on the website thirty days prior to the suspension.
- (3) You assign your rights or obligations under the contract to third party without consent or authorization of the Bank;
- (4) You have filed for bankruptcy in accordance with the Bankruptcy Act or filed for rehabilitation or liquidity in accordance with the Consumer Debt Clearance Act;
- (5) You breach the provisions under Articles 15 to 17 of the contract; and
- (6) You breach any other provisions under the contract and fail to make a correction upon request or fail to perform your obligation within a specified period of time.

23. Modifications

Where there is any modification or amendment to any provision under the contract and shall post the content of the amendments on the Bank's website 10 days prior to the amendments, you will be deemed to have agreed to such modification or amendment to the provision unless you send a notice to the Bank within ten (10) days, indicating your dissent. However, where there is a change to the following items, the Bank shall notify you in writing or in a manner agreed to by both parties sixty (60) days prior to such change stating the changed items and the new and old provisions in a conspicuous and clear manner, and that you will be deemed to have agreed to such modification or amendment to the provision unless you send a notice to the Bank before the effective date of the changed items indicating your dissent, and that you shall notify the Bank to terminate the contract within the dissenting period above if you have any dissent:

- (1) The manner in which you or the Bank notifies each other where there is any unauthorized use or theft of legally authorized user name and password by third party, or any other circumstances where legal authorization is not obtained.
- (2) Other items prescribed by competent authorities.

24. Notices

You agree that all notices from the Bank to you will be sent to the address left by you in the contract or to the address left by you in the credit card agreement. Where there is any change to your address, you should immediately notify the Bank in writing or in a manner agreed, and you agree that all notices from the Bank to you will be sent to the changed address. If you do not notify the Bank of the change to your address in writing or in a manner agreed, all notices from the Bank to you will still be sent to the address left by you in the contract or the last notified address left by you.

25. Governing Law

Unless otherwise agreed by both parties, the terms and conditions herein shall be governed by the laws of the Republic of China (Taiwan).

26. Jurisdiction

The Bank and you agree that all disputes, controversies, differences or claims arising out of, relating to or in connection with the contract, or the breach, termination or invalidity thereof shall be subject to the jurisdiction of ROC Taipei District Court. However, this does not exclude the application of Article 47 of the Consumer Protection Act or Article 436-9 of Civil Procedure Code for the small-claim proceeding.

27. Headings

All headings and titles used in the contract are for the convenience only and shall in no circumstances affect interpretation, explanation and understanding of the provisions of the contract.

28. Counterparts

You could print out the contract for your reference from our public website. However, the final version is based on the one on our public website.

29. Use of Credit Card Online Service and Mobile Banking

1. Use: The Customers shall login to the "Credit Card Online Service" provided by the Bank to register for the Service.
 - A. Registration for Credit Card Online Service: You need to go to our public website and redirect to the page of registration for Credit Card Online Service. By clicking "How to register" and reading/checking the contract, the Bank will verify your identification via the mobile number you left with SMS password. Then you will set up the username and password by yourself before you could log in. If you don't left mobile number, you will need to contact our contact center for further actions.
 - B. The Customers shall correctly enter the National ID number, username and the user's password to use the Service, and may log in and access the Service after the Bank verifies their identity.
 - C. Mobile Banking Service- Activation and Suspension: To access the Services, you should log in the Credit Card Online Service and review carefully and agree to the "Standard Chartered Bank (Taiwan) Limited - Terms and Conditions for Mobile Banking Services". Then you should enter the password to activate the Mobile Banking Services and then complete the following mobile device verification

procedure. The Bank will issue a 4-digit mobile device verification code. You should log off the Credit Card Online Service and download and install the application to your smart phone. After activating the application on your smart phone and enter the same username and password for your Credit Card Online Service, you should enter the mobile device verification code for the Bank's verification. Upon completion of the process, you may start to use the Services. You are required to complete verification of your personal smart phone by following the verification method for Mobile Banking Services system designated by the Bank within 24 hours of receipt of your verification code. A delay of your verification beyond the above time period will result in automatic cancellation of the issued verification code by the system. If you wish to use the Mobile Banking Services in the future, you should repeat the same verification procedure at the Credit Card Online Service. To suspend the Services, you should log in the Credit Card Online Service and review carefully and agree to the "Standard Chartered Bank (Taiwan) Limited - Terms and Conditions for Mobile Banking Services" and then enter password to complete the procedure to suspend your Mobile Banking Services. The Mobile Device Verification will be cancel at the same time.

- D. Mobile Banking Service- Mobile Device Verification: You should log in the Credit Card Online Service and then enter your fixed password to began the mobile device verification process if the smart phone have not been verified yet. A 4-digit mobile device verification code will appear on the Bank's webpage. You need to log off the Credit Card Online Service and use your smart phone to log in the Mobile Banking Services and enter the 4-digit mobile device verification code to complete the mobile device verification procedure and begin to use the Mobile Banking Services. You are required to complete verification of your personal smart phone by following the verification method for Mobile Banking Services system designated by the Bank within 24 hours of receipt of your verification code. A delay of your verification beyond the above time period will result in automatic cancellation of the issued verification code by the system. If you wish to use the Mobile Banking Services in the future, you should repeat the same verification procedure at the Credit Card Online Service. For mobile device verification, the maximum number of accepted smart phones is three. You could log in the Credit Card Online Service and then enter your fixed password to cancel the mobile device verification.
- E. You (base on the same national ID) could log in Credit Card Online Service or Mobile Banking Service at the same time.

(2) Limitation on use

- A. When applying for the Credit Card Online Services for the first time or reapplying, the Customer is required to enter important personal and credit card information for verification purposes. If the Customer enters incorrect information three times, the system will automatically lock the Customer out and suspend the application for the Credit Card Online Services. The applicant will then be required to telephone the customer service to remove the lockout status before he is able to reapply.
- B. To protect the rights of our customers, three failed login attempts using an incorrect "username" or "password" (counted separately) will result in the Bank's computer automatically terminating the services specified herein. If the Customer wishes to restore the access, the Customer will be required to reapply for the services. (i.e. By clicking on "online application" on the webpage.)
- C. The Bank will always identify the Customers' input of their Username, National ID numbers and the user's password to use the Service as the Customers' valid instruction. Therefore, the online service system and Mobile Banking will be available to only one user at a time. In consideration of the risk, if more than two users use the Service under the same account at the same time, the Bank will automatically reject access to the online service system by any users other than the first user, and will also make the first user log out compulsorily and suspend this user's access to the system for the following five minutes.
- D. When using the Bank's Credit Card Online Service and Mobile Banking, if the Customers forget to log out from the Bank's system or fail to execute any command for more than five minutes, the Bank will have the customers log out from the system automatically to prevent other users from using. The Customers must re-login to the Bank's Credit Card Online Service system first and then may continue accessing the Service.
- E. If there has not been a successful login for more than a year, the Bank will terminate the access to the Credit Card Online Services and Mobile Banking. The Customer will be required to reapply to restore access.
- F. The Customers shall keep confidential their Username, National ID number, user's password and personal information.

(3) Responsibilities and Obligations

- A. The Bank identifies the Customers who request the Bank's Credit Card Online Service and Mobile Banking based on the correct identification information as the Customers per se.

- B. The Bank will not be liable for any error or delay caused by the computer system, failure in telecommunication lines or any third party's activity, or direct, indirect or other loss arising from any service, unless the error, delay or loss is caused due to the Bank's intentional act or gross negligence.
 - C. If the Customers cannot process or search for any information due to interruption in the computer system, the Customers may request for the Services they need in other manners, e.g. 24-hour customer phone service representatives and interactive voice response systems.
 - D. The Customers shall utilize their PCs and smart phone to access the Service. If the Customers utilize the computer equipment in any public place and thereby disclose their information, the Bank will not be liable for the disclosure and the loss incurred thereby, provided that the Bank agrees to provide necessary assistance.
 - E. Unless otherwise agreed, all of the notices to the Customers hereunder shall be made in writing or in any other manners agreed by the Bank and shall be served to the latest address updated or notified by the Customers. Upon the Bank's service of the information to said address, the information shall be deemed served to the Customers as agreed after the normal mailing period has passed.
- (4) Force majeure
- A. In the event of force majeure, the Bank's failure to perform or delay in performing with respect to the obligations set out herein shall not constitute its breach of the Agreement, nor shall the Bank be liable for the damages incurred there from.
 - B. The force majeure referred to in the preceding paragraph includes natural calamity, strike, lockout, government act and legal restrictions and prohibitions or any other incidents beyond the Bank's control.
- (5) Supply of information and confidentiality agreement
- The business information in relation to the Bank's Credit Card Online Service and Mobile Banking, including words, graphics, patents, trademarks, trade secrets, other intellectual property rights, titles or other rights, shall be vested in the Bank. Without the Bank's prior legitimate authorization, no person shall reproduce, transmit, adapt, compile, publish, or use such business information in any forms for any purposes. Violation of the foregoing will result in legal liability.