

客戶重要通知

Important Notice to Customers



更新「網上企業銀行服務的特別條款及細則」通知

為配合本行即將於「建行(亞洲)企業銀行」手機應用程式推出「流動保安編碼」，本行將於 **2025 年 5 月 24 日 (星期六) (「生效日」)** 更新本行的網上企業銀行服務的特別條款及細則 (「條款」)。本行將於條款內新增有關「流動保安編碼」的條款和條件。具體變動於本通知下的表格中展示。

客戶可自生效日起於此網頁下載條款最新的 PDF 版本：
https://www.asia.ccb.com/hongkong_tc/aboutus/terms_fees/index.html，客戶亦可聯絡客戶經理索取完整之修訂本。客戶除可經客戶經理查詢詳情，亦可致電客戶服務熱線 +852 2903 8366 了解更多。此外，客戶可於生效日前於上述網頁下載現有條款。請注意，條款的更新在生效後，客戶未必能夠查閱或下載過去的條款。

若客戶於生效日或之後繼續使用網上企業銀行服務，上述更新將對客戶具有約束力。倘客戶不接受有關修訂，客戶有權於生效日前根據相關條款和條件中列明的方法終止網上企業銀行服務，請致電客戶經理或前往分行以作安排。

請注意，在生效日或之後，當客戶再次使用網上企業銀行服務時，客戶必須閱讀及接受條款的有關更新。

本通知之中英文文本如有歧異，概以英文文本為準。

中國建設銀行（亞洲）股份有限公司 / 中國建設銀行股份有限公司香港分行(中國建設銀行股份有限公司是於中華人民共和國註冊成立的股份有限公司)

謹啟 2025 年 4 月

客戶重要通知

Important Notice to Customers



Notice of Amendments to "Specific Terms and Conditions for Online Enterprise Banking Services (OEBS)"

With effect from **May 24, 2025 (Saturday) ("Effective Date")**, to cope with our introduction of 'Mobile Token' on the "CCB(Asia) Business" Mobile App, we will update our Specific Terms and Conditions for Online Enterprise Banking Services (OEBS) (the "**Terms**"). New terms and conditions relating to 'Mobile Token' will be added to the Terms by the Bank. Specific amendments can be found under the table in this notice below.

Customers may download the latest PDF version of the Terms here https://www.asia.ccb.com/hongkong/aboutus/terms_fees/index.html starting from the Effective Date. Customers may contact our relationship manager for a copy of the full version of the Terms. For enquiry, please contact any of our relationship managers, or call customer service hotline at +852 2903 8366. Also, customers may download the existing version of the Terms (prior to the updates) before the Effective Date from the link above. Customers are reminded that (the former version of) the Terms may not be available for access or download after the amendments have taken effect.

The amendments shall be binding on customers if customers continue to use our Online Enterprise Banking Services ("**OEBS**") on or after the Effective Date. If customers decline to accept the above amendments, customers have the right to terminate the use of the OEBS in accordance with the respective terms and conditions before the Effective Date. Should customers wish to terminate OEBS, please notify us through our relationship manager or visit our branch.

Please note that customers will be required to, after the Effective Date, read and accept the amendments to the Terms in order to continue using the OEBS.

The English version of this notice shall prevail if there is any discrepancy between the English and Chinese versions.

China Construction Bank (Asia) Corporation Limited / China Construction Bank Corporation Hong Kong Branch (China Construction Bank Corporation is a company incorporated in the People's Republic of China with limited liability)

April, 2025

客戶重要通知

Important Notice to Customers



表格

	現有條款	新條款
		本主條款B部第12章所載的附加條款（「本條款」）適用於要求提供網上銀行服務的客戶。
	重要提示： 在閣下登記使用網上企業銀行服務（定義見下文）前，請仔細閱讀本條款及細則（「本條款」）。當閣下登記使用或使用手機銀行應用程式（定義見下文）、網站（定義見下文）及網上企業銀行服務，閣下將被視為已接納本條款、本行之 私隱政策 及 個人私隱條例通告 ，並受其約束。	重要提示： 在閣下登記使用網上企業銀行服務（定義見下文）前，請仔細閱讀本條款及細則（「本條款」）。當閣下登記使用或使用手機銀行應用程式（定義見下文）、網站（定義見下文）及網上企業銀行服務（ 定義見下文 ），閣下將被視為已接納本條款、本行之 私隱政策 及 個人私隱條例通告 ，並受其約束。

定義及詮釋

	現有條款	新條款
12.4	「 授權代表 」指： (a) 獲客戶不時透過網上企業銀行服務申請/更改表格授權經網站或手機銀行應用程式使用網上企業銀行服務的個人（於下文第 21 條詳述）；及	「 授權代表 」指： (a) 獲客戶不時透過網上企業銀行服務申請/更改表格授權經網站或手機銀行應用程式使用網上企業銀行服務的個人（於下文第 12.21 條詳述）；及
12.4	「 審核員 」指由主用戶或客戶透過網上企業銀行服務申請/更改表格（及/或本行不時要求的任何其他表格及/或資料）及/或網上企業銀行服務所直接委任並經本行批准執行下文第 21(b)條所述的所有事項（該條文可能會不時修訂）的個人。	「 審核員 」指由主用戶或客戶透過網上企業銀行服務申請/更改表格（及/或本行不時要求的任何其他表格及/或資料）及/或網上企業銀行服務所直接委任並經本行批准執行下文第 12.21(b) 條所述的所有事項（該條文可能會不時修訂）的個人。
12.4	「 生物憑據認證服務 」與本條款附件 1(生物憑據認證服務條款及細則) 第 3 條所界定者具有相同涵義。	「 生物憑據認證服務 」與本條款附件 1 (流動保安編碼 及生物憑據認證服務條款及細則) 第 3 條中界定的具有相同涵義。

客戶重要通知

Important Notice to Customers



12.4	「 生物憑據 」與本條款附件 1(生物憑據認證服務條款及細則) 第 5 條所界定者具有相同涵義。	「 生物憑據 」與本條款附件 1(<u>流動保安編碼及生物憑據認證服務條款及細則</u>) 第 5 條中 所界定者具有相同涵義。
12.4	「 現有條款 」指 (其中包括) 「 戶口及有關服務的條款和條件 (企業客戶) 」、「 賬戶及服務主要條款和細則(商業客戶) 」、「 有關快速支付系統的銀行服務的條款和條件 」、「 投資服務之條款和條件 」、「 WhatsApp 智慧助理使用條款及細則 」, 及客戶與本行簽訂的任何其他適用協議或條款及細則 (每項可能會不時修訂)。	「 現有條款 」指 (其中包括) 「 戶口及有關服務的條款和條件 (企業客戶) 」、「 賬戶及服務主要條款和細則(商業客戶) 」、「 有關快速支付系統的銀行服務的條款和條件 」、「 投資服務之條款和條件 」、「 WhatsApp 智慧助理使用條款及細則 」、 <u>「流動保安編碼及生物憑據認證服務條款及細則」</u> , 及客戶與本行簽訂的任何其他適用協議或條款及細則 (每項可能會不時修訂)。
12.4	「 制單員 」指由客戶或主用戶透過網上企業銀行服務申請/更改表格 (及/或本行不時要求的任何其他表格及/或資料) 及/或網上企業銀行服務所直接委任並經本行批准執行下文第 21(c)條所述的所有事項 (該條文可能會不時修訂) 的個人。	「 制單員 」指由客戶或主用戶透過網上企業銀行服務申請/更改表格 (及/或本行不時要求的任何其他表格及/或資料) 及/或網上企業銀行服務所直接委任並經本行批准執行下文第 <u>12.21(c)</u> 條所述的所有事項 (該條文可能會不時修訂) 的個人。
12.4	「 主用戶 」指由客戶透過網上企業銀行服務申請/更改表格 (及/或本行不時要求的任何其他表格及/或資料) 及/或網上企業銀行服務所直接委任並經本行批准執行下文第 21(a)條所述的所有事項 (該條文可能會不時修訂) 的個人。	「 主用戶 」指由客戶透過網上企業銀行服務申請/更改表格 (及/或本行不時要求的任何其他表格及/或資料) 及/或網上企業銀行服務所直接委任並經本行批准執行下文第 <u>12.21(a)</u> 條所述的所有事項 (該條文可能會不時修訂) 的個人。
12.4		<u>「流動保安編碼」</u> 俱有其在 “ <u>流動保安編碼及生物憑據認證服務條款及細則</u> ” 中的意義。
12.4		<u>「流動保安編碼密碼」</u> 俱有其在 “ <u>流動保安編碼及生物憑據認證服務條款及細則</u> ” 中的意義。
12.4	「 網上企業銀行服務 」指本行允許客戶透過手機銀行應用程式或網站獲取	「 網上企業銀行服務 」指本行允許客戶透過手機銀行應用程式或網站獲取

客戶重要通知

Important Notice to Customers



	的銀行產品或服務（可能會不時修訂）。	的銀行產品或服務， <u>以及其中相關的內置功能（包括流動保安編碼及/或生物憑據認證服務）</u> （可能會不時修訂）。
12.4	「密碼」指本行向客戶發出或客戶自行採用的任何機密密碼、短語、代碼或數字或任何其他驗證方法（包括任何安全碼），用以登入網上企業銀行服務。	「密碼」指本行向客戶發出或客戶自行採用的任何機密密碼、短語、代碼或數字或任何其他驗證方法（包括任何安全碼 <u>或（如適用）任何流動保安編碼密碼</u> ），用以登入網上企業銀行服務。
12.4	「安全碼」指授權代表登入網上企業銀行服務時，由保安裝置所產生的一次性密碼。	「安全碼」指授權代表登入網上企業銀行服務時 <u>所使用的</u> ，由保安裝置所產生的 <u>或顯示的</u> 一次性密碼 <u>或（如適用）流動保安編碼</u> 。
12.4	「保安裝置」指本行指定及提供予各個授權代表使用的電子裝置，以便各個授權代表使用該電子裝置所產生的安全碼登入網上企業銀行服務。	「保安裝置」指本行 <u>（應要求）</u> 指定及提供予各個授權代表使用的 <u>實體</u> 電子裝置，以便各個授權代表使用該電子裝置所產生的安全碼登入網上企業銀行服務。

使用及更新

	現有條款	新條款
12.7	網上企業銀行服務（本行的許可人或第三方服務供應商提供的資訊除外，例如市場資訊及物業估價）由本行開發並完全擁有。本行可未經事先通知隨時撤銷、修改、暫停或終止任何網上企業銀行服務。本行可全權酌情，在未經事先通知的情況下，決定客戶或其任何授權代表是否合資格使用任何網上企業銀行服務，並暫停其使用網上企業銀行服務、網站及/或手機銀行應用程式（或其中任何部分），或而中止其登入網上企業銀行服務、網站及/或手機銀行應用程式。本行在這	網上企業銀行服務（本行的許可人或第三方服務供應商提供的資訊除外，例如市場資訊及物業估價）由本行開發並完全擁有。本行可未經事先通知隨時撤銷、修改、暫停或終止任何網上企業銀行服務。本行可全權酌情，在未經事先通知的情況下，決定客戶或其任何授權代表是否合資格使用任何網上企業銀行服務，並暫停其使用網上企業銀行服務、網站及/或手機銀行應用程式（或其中任何部分），或而中止其登入網上企業銀行服務、網站及/或手機銀行應用程式 <u>（包括透過</u>

客戶重要通知

Important Notice to Customers



	方面有最終決定權。本行將不對客戶因該等決定而遭受的任何損失或損害承擔責任。	流動保安編碼及/或生物憑據認證服務 。本行在這方面有最終決定權。本行將不對客戶因該等決定而遭受的任何損失或損害承擔責任。
12.9	受第 65 條所限，本行不會就客戶使用手機銀行應用程式或網站收取任何費用。然而，客戶將負責支付在其流動裝置或任何其他電子設備上使用數據服務的相關費用。客戶應向其網路營運商查詢使用費的詳細資訊。	受第 12.65 條所限，本行不會就客戶使用手機銀行應用程式或網站收取任何費用。然而，客戶將負責支付在其流動裝置或任何其他電子設備上使用數據服務的相關費用。客戶應向其網路營運商查詢使用費的詳細資訊。

手機銀行應用程式

	現有條款	新條款
12.11	手機銀行應用程式只能在本行不時指定的相容設備上使用。本行不保證任何特定設備或型號與手機銀行應用程式相容。客戶確認其全權負責確保其流動裝置符合最低要求，否則可能會導致手機銀行應用程式故障。	手機銀行應用程式只能在本行不時指定的相容設備上使用。本行不保證任何特定設備或型號與手機銀行應用程式相容。客戶確認其全權負責確保其流動裝置符合最低要求， 並且僅從官方應用程式商店下載手機銀行應用程式及其更新 ，否則可能會導致手機銀行應用程式故障。

網上企業銀行服務

	現有條款	新條款
12.13	在不影響及附加於下文第 58 條的前提下，本行有絕對酌情權自行決定並不時更新或修改客戶可隨時獲得的網上企業銀行服務的範圍及類型，包括但不限於，隨時：	在不影響及附加於下文第 12.58 條的前提下，本行有絕對酌情權自行決定並不時更新或修改客戶可隨時獲得的網上企業銀行服務的範圍及類型，包括但不限於，隨時：
12.17	本行的政策是保持網上企業銀行服務隨時可用。然而，網上企業銀行服務的某些功能可能在正常服務時間之外無法使用，客戶將在手機銀行應用程式或網站（視情況而定）上收到有關這些服務中斷的通知。本行也可能暫	本行的政策是保持網上企業銀行服務隨時可用。然而，網上企業銀行服務的某些功能可能在正常服務時間之外無法使用，客戶將在手機銀行應用程式或網站（視情況而定）上收到有關這些服務中斷的通知。本行也可能暫

客戶重要通知

Important Notice to Customers



<p>停企業網上銀行服務，包括但不限於當本行懷疑存在任何安全性漏洞、進行例行或緊急維護檢查或本行根據監管規定而需要這樣做的情況。本行將盡力在任何此類服務中斷或暫停之前透過手機銀行應用程式或網站（視情況而定）通知客戶，除非提供此類事先通知不切實際或非法。</p>	<p>停網上企業銀行服務（包括流動保安編碼或生物憑據認證服務），包括但不限於當本行懷疑存在任何安全性漏洞、進行例行或緊急維護檢查或本行根據監管規定而需要這樣做的情況。本行將盡力在任何此類服務中斷或暫停之前透過手機銀行應用程式或網站（視情況而定）通知客戶，除非提供此類事先通知不切實際或非法。</p>
--	---

手機銀行應用程式上的營銷功能

	現有條款	新條款
12.19	<p>在不限第 18 條的情況下，本行將透過手機銀行應用程式向客戶發送有關一般市場資訊、促銷優惠或銀行其他通訊的推送通知。客戶可以隨時透過關閉其流動裝置上的推送通知服務以關閉該項功能。在向客戶發送推送通知之前，本行將徵求客戶的同意。客戶可以隨時透過關閉其流動裝置上的推送通知服務以撤回該項同意。</p>	<p>在不限第 12.18 條的情況下，本行將透過手機銀行應用程式向客戶發送有關一般市場資訊、促銷優惠或銀行其他通訊的推送通知。客戶可以隨時透過關閉其流動裝置上的推送通知服務以關閉該項功能。在向客戶發送推送通知之前，本行將徵求客戶的同意。客戶可以隨時透過關閉其流動裝置上的推送通知服務以撤回該項同意。</p>
12.20	<p>[手機銀行應用程式中的社交媒體分享功能將使客戶能夠在各種社交媒體平台（由銀行不時指定）的客戶賬戶上分享及轉發從手機銀行應用程式獲得的某些資訊。在客戶不點擊其流動裝置上任何或所有允許的社交媒體賬戶的「分享」按鈕的情況下，此功能將保持停用狀態。由於不同的流動裝置及社交媒體平台可能提供不同的方式來停用社交媒體分享功能，客戶應檢查其流動裝置及其不同的社交媒體帳號的設定以取得更多資訊。當客戶使用社交媒體分享功能，客戶承認並接受，客戶對其透過其社交媒體賬戶分享及轉發的任何內容及客戶就此發表</p>	<p>[手機銀行應用程式中的社交媒體分享功能將使客戶能夠在各種社交媒體平台（由銀行不時指定）的客戶賬戶上分享及轉發從手機銀行應用程式獲得的某些資訊。在客戶不點擊其流動裝置上任何或所有允許的社交媒體賬戶的「分享」按鈕的情況下，此功能將保持停用狀態。由於不同的流動裝置及社交媒體平台可能提供不同的方式來停用社交媒體分享功能，客戶應檢查其流動裝置及其不同的社交媒體帳號的設定以取得更多資訊。當客戶使用社交媒體分享功能，客戶承認並接受，客戶對其透過其社交媒體賬戶分享及轉發的任何內容及客戶就此發表</p>

客戶重要通知

Important Notice to Customers



<p>的評論和言論承擔全部責任。在不限制下文第 61 至 64 條的情況下，本行將不對客戶因使用社交媒體分享功能而遭受的任何損失負責。客戶進一步同意並承諾，應本行要求，立即刪除透過使用手機銀行應用程式中的社交媒體分享功能在其社交媒體賬戶傳播的任何本行合理判斷為非法的、不準確的、誤導性的、不適當的或在任何方面損害銀行的利益的內容、評論及/或言論。手機銀行應用程式中的社交媒體分享功能目前僅以有限度形式推出，並僅支援指定的流動裝置，但本行會逐步擴大其推出範圍。]</p>	<p>的評論和言論承擔全部責任。在不限制下文第 12.61 至 12.64 條的情況下，本行將不對客戶因使用社交媒體分享功能而遭受的任何損失負責。客戶進一步同意並承諾，應本行要求，立即刪除透過使用手機銀行應用程式中的社交媒體分享功能在其社交媒體賬戶傳播的任何本行合理判斷為非法的、不準確的、誤導性的、不適當的或在任何方面損害銀行的利益的內容、評論及/或言論。手機銀行應用程式中的社交媒體分享功能目前僅以有限度形式推出，並僅支援指定的流動裝置，但本行會逐步擴大其推出範圍。}</p>
--	--

授權代表的任命

	現有條款	新條款
12.22	如客戶委任多於一名授權代表，則每位授權代表各自將會獲得獨有的用戶名稱、客戶號碼、密碼及保安裝置。本行將向主用戶發出有關的用戶名稱、客戶號碼、初始密碼及保安裝置，主用戶須負責將相應的用戶名稱、客戶號碼、初始密碼及保安裝置轉交各審核員及/或制單員。	如客戶委任多於一名授權代表，則每位授權代表各自將 <u>被分配</u> 會獲得獨有的用戶名稱 <u>及</u> 、客戶號碼、密碼及保安裝置。本行將向 <u>客戶</u> 主用戶發出有關的用戶名稱 <u>及</u> 、客戶號碼、初始密碼及保安裝置，主用戶 <u>客戶</u> 須負責將 <u>其</u> 相應的用戶名稱 <u>及</u> 、客戶號碼、初始密碼及保安裝置轉交各 <u>主用戶</u> 、審核員及/或制單員。

向本行作出指示

	現有條款	新條款
12.24	本行將接收並依照有關客戶賬戶或與本行的其他關係或事項的指示行事，但始終受限於以下規定： (a) 本行應確保在執行任何指示之前，本行透過檢查客戶的用戶名稱、客戶號碼、密碼、安全碼及（如適	本行將接收並依照有關客戶賬戶或與本行的其他關係或事項的指示行事，但始終受限於以下規定： (a) 本行應確保在執行任何指示之前，本行透過檢查客戶的用戶名稱、客戶號碼、密碼、安全碼、 <u>（如適</u>

客戶重要通知

Important Notice to Customers



<p>用) 生物憑據認證服務下的生物識別憑據 (統稱「身份驗證資訊」) 中任何一項或多項來驗證該指示的真實性, 但沒有義務對提交指示的人士的權限進行任何進一步的查詢、認證或其他步驟;</p>	<p><u>用) 流動保安編碼下的流動保安編碼密碼及 (如適用) 生物憑據認證服務下的生物識別憑據 (統稱「身份驗證資訊」) 中任何一項或多項來驗證該指示的真實性, 但沒有義務對提交指示的人士的權限進行任何進一步的查詢、認證或其他步驟;</u></p>
---	--

保安措施

	現有條款	新條款
12.29	<p>(a) 定期更改其密碼, 並避免將其密碼透露給任何無權獲取該密碼的人士, 包括本行的任何成員或人員;</p> <p>(b) 避免選擇任何先前使用過的密碼, 或任何試圖登入網上企業銀行服務的人士可能猜到的密碼。例如, 授權代表不應選擇生日或電話號碼作為密碼;</p> <p>(c) 盡快銷毀本行發出的有關密碼的任何信件;</p> <p>(d) 如客戶或任何授權代表知悉或懷疑任何人士可獲取其密碼、安全碼或保安裝置, 應立即通知本行。網上企業銀行服務將被立即暫停, 直到客戶設定新密碼;</p> <p>(e) 一旦客戶登入網上企業銀行服務, 切勿讓設備或流動裝置處於無人看管的狀態, 並且在客戶退出網上企業銀行服務之前, 不允許其他人使用流動裝置及/或任何其他電子設備;</p> <p>(f) 避免在裝置或流動裝置連接至區域網路或公共終端且無法確保沒有第三方能夠觀察或複製客戶的登入時登入網上企業銀行服務。這包括透</p>	<p>(a) 定期更改其密碼<u>或流動保安編碼密碼 (如適用)</u>, 並避免將其密碼<u>或流動保安編碼密碼 (如適用)</u> 透露給任何無權獲取該密碼<u>或流動保安編碼密碼 (如適用)</u> 的人士, 包括本行的任何成員或人員;</p> <p>(b) 避免選擇任何先前使用過的密碼<u>或流動保安編碼密碼 (如適用)</u>, 或任何試圖登入網上企業銀行服務的人士可能猜到的密碼。例如, 授權代表不應選擇生日或電話號碼作為密碼<u>或流動保安編碼密碼 (如適用)</u>;</p> <p>(c) 盡快銷毀本行發出的有關密碼的任何信件;</p> <p>(d) 如客戶或任何授權代表知悉或懷疑任何人士可獲取其密碼、<u>流動保安編碼密碼 (如適用)</u>、安全碼、<u>流動保安編碼</u>或保安裝置, 應立即通知本行。網上企業銀行服務將被立即暫停, 直到客戶設定新密碼<u>或新流動保安編碼密碼 (如適用)</u>;</p> <p>(e) <u>如客戶懷疑自己受到任何欺詐性網站、流動電話應用程式、電子郵件或短訊/無綫應用協議 (WAP) 推</u></p>

客戶重要通知

Important Notice to Customers



<p>過流動裝置及/或本行任何分行或任何其他公共區域提供的任何其他電子設備登入網上企業銀行服務時保持警惕；</p> <p>(g) 如任何授權代表離職，需通知本行，並撤銷其代表客戶行事的授權。客戶必須確保該等人士無法登入網上企業銀行服務；</p> <p>(h) 確保用於登入網上企業銀行服務的電腦系統、流動裝置及/或任何其他電子設備具有最新的安全修補程式，並採取所有合理可行的措施以確保用於登入網上企業銀行服務的任何裝置不存在任何電腦病毒或其他惡意軟件；</p> <p>(i) 如保安裝置無法運作或登入網上企業銀行服務出現任何問題，需立即通知本行；及</p> <p>(j) 遵守網站、手機銀行應用程式及用戶指引中規定及不時更新的所有其他安全保障措施。</p>	<p><u>送訊息的欺騙（例如，客戶在使用正確的生物識別憑據後無法登入手機銀行應用程式，無論是否有任何警告提示），應立即更改密碼和流動保安編碼密碼（如適用）；</u></p> <p>(f) 一旦客戶登入網上企業銀行服務，切勿讓設備或流動裝置處於無人看管的狀態，並且在客戶退出網上企業銀行服務之前，不允許其他人使用流動裝置及/或任何其他電子設備；</p> <p>(g) 避免在裝置或流動裝置連接至區域網路或公共終端且無法確保沒有第三方能夠觀察或複製客戶的登入時登入網上企業銀行服務。這包括透過流動裝置及/或本行任何分行或任何其他公共區域提供的任何其他電子設備登入網上企業銀行服務時保持警惕；</p> <p>(h) 如任何授權代表離職，需通知本行，並撤銷其代表客戶行事的授權。客戶必須確保該等人士無法登入網上企業銀行服務；</p> <p>(i) 確保用於登入網上企業銀行服務的電腦系統、流動裝置及/或任何其他電子設備具有最新的安全修補程式，並採取所有合理可行的措施以確保用於登入網上企業銀行服務的任何裝置不存在任何電腦病毒或其他惡意軟件；</p> <p>(j) 如保安裝置或流動保安編碼無法運作或登入網上企業銀行服務出現任何問題，需立即通知本行；及</p> <p>(k) 遵守網站、手機銀行應用程式及用戶指引中規定及不時更新的所有其他安全保障措施。</p>
--	--

客戶重要通知

Important Notice to Customers



		<u>若客戶未能遵守上述措施，客戶可能需要負上由此引起的損失的責任。</u>
12.30	如客戶以外的任何人士獲取或知悉客戶的身份驗證資訊，客戶同意就所有損失、損害、成本及費用（包括專業及法律費用）全額彌償本行、其聯屬公司及/或其被許可人（如適用）。除第 61 條規定的任何原因外，本行不會對任何未經授權的交易所造成的任何損失負責。	如客戶以外的任何人士獲取或知悉客戶的身份驗證資訊，客戶同意就所有損失、損害、成本及費用（包括專業及法律費用）全額彌償本行、其聯屬公司及/或其被許可人（如適用）。除第 12.61 條規定的任何原因外，本行不會對任何未經授權的交易所造成的任何損失負責。
12.31	本行可自行決定要求客戶使用安全碼登入網上企業銀行服務或發出某些類型的指示。客戶須自行負責提出索取保安裝置的要求。	本行可自行決定要求客戶使用安全碼登入網上企業銀行服務或發出某些類型的指示。客戶須自行負責提出索取保安裝置的要求 <u>或自行設定流動保安編碼。</u>
12.32	任何保安裝置屬於本行的財產，並應在網上企業銀行服務終止時歸還本行或按照本行的指示進行處置。	任何保安裝置 <u>或流動保安編碼（如適用）</u> 均屬於本行的財產，並應在網上企業銀行服務終止時， <u>客戶應（在適用保安裝置的情況下）立即將保安裝置歸還本行或（在適用流動保安編碼的情況下）立即將流動保安編碼註銷或以其他方式停用</u> 或按照本行的指示進行處置。
12.33	客戶應妥善使用保安裝置，未經本行事先書面同意，不得更改、竄改或修改保安裝置，或造成保安裝置的任何遺失或損壞。客戶在發現保安裝置有任何遺失、損壞、破壞、外洩或故障後，應在合理可行的情況下盡快通知本行。對於客戶因保安裝置的任何遺失、損壞、破壞、外洩、故障、缺陷、失靈或損壞而遭受的任何損失，本行概不負責。	客戶應妥善使用保安裝置 <u>或流動保安編碼（如適用）</u> ，未經本行事先書面同意，不得更改、竄改或修改保安裝置， <u>不得干擾、操縱、損害、破壞或逆向工程流動保安編碼（如適用）</u> 或造成保安裝置 <u>和流動保安編碼（如適用）</u> 的任何遺失或損壞。客戶在發現保安裝置 <u>及/或流動保安編碼</u> 有任何遺失、損壞、破壞、外洩、 <u>未經授權的使用</u> 或故障後，應在合理可行的情況下盡快通知本行。對於客戶因保安裝置、 <u>流動裝置或流動保安編碼</u> 的任何

客戶重要通知

Important Notice to Customers



	遺失、損壞、破壞、外洩、故障、缺陷、失靈或損壞而遭受的任何損失，本行概不負責。
--	---

生物憑據認證服務

流動保安編碼及生物憑據認證服務

	現有條款	新條款
12.34	與登入手機銀行應用程式的生物憑據認證相關的更多服務條款及細則載於本條款附件 1 (生物憑據認證服務條款及細則)。	與登入手機銀行應用程式的 流動保安編碼及/或生物憑據認證服務 相關的更多服務條款及細則載於 流動保安編碼及生物憑據認證服務條款及細則 。

資料收集

	現有條款	新條款
12.36	當客戶使用手機銀行應用程式、網站及/或任何一項網上企業銀行服務，即表示客戶同意本行、其聯屬公司及/或其被許可人收集及使用客戶的流動裝置及/或任何其他電子設備裝置的位置及技術信息，包括 IP 地址、廣告 ID、唯一設備識別碼及設備類型的技術信息、有關其流動裝置及/或任何其他電子設備上使用的操作系統及應用程式軟件信息，及手機銀行應用程式或網站中基於互聯網或無線的網上企業銀行服務的有關軟件、硬件及周邊設備的其他非個人信息，以改進本行、其聯屬公司及/或其被許可人向客戶提供的產品及服務。	當客戶使用手機銀行應用程式、網站、 流動保安編碼 及/或任何一項網上企業銀行服務，即表示客戶同意本行、其聯屬公司及/或其被許可人收集及使用客戶的流動裝置及/或任何其他電子設備裝置的位置及技術信息，包括 IP 地址、廣告 ID、唯一設備識別碼及設備類型的技術信息、有關其流動裝置及/或任何其他電子設備上使用的操作系統及應用程式軟件信息，及 流動保安編碼 、手機銀行應用程式或網站中基於互聯網或無線的網上企業銀行服務的有關軟件、硬件及周邊設備的其他非個人信息，以改進本行、其聯屬公司及/或其被許可人向客戶提供的產品及服務。
12.42	客戶進一步確認並同意，其個人資料及資訊將為了第 41 條所述的目的而被收集、儲存、存取、使用及處理。客	客戶進一步確認並同意，其個人資料及資訊將為了第 12.41 條所述的目的而被收集、儲存、存取、使用及處理。

客戶重要通知

Important Notice to Customers



<p>戶進一步確認，如其決定撤回對此類個人資料或資訊收集的同意，客戶可變更其流動裝置及/或任何其他電子設備上的設定。客戶理解，如客戶撤回其同意，客戶可能無法使用手機銀行應用程式及/或網站的某些功能。</p>	<p>客戶進一步確認，如其決定撤回對此類個人資料或資訊收集的同意，客戶可變更其流動裝置及/或任何其他電子設備上的設定。客戶理解，如客戶撤回其同意，客戶可能無法使用手機銀行應用程式及/或網站的某些功能。</p>
---	--

客戶的義務

	現有條款	新條款
12.47	(a) 不會以任何違反任何適用監管規定的方式使用手機銀行應用程式、網站及網上企業銀行服務，包括適用於手機銀行應用程式、網站或任何網上企業銀行服務使用或為其提供支援的技術的所有技術控制或出口法律及法規（「有關技術」）；	(a) 不會以任何違反任何適用監管規定的方式使用手機銀行應用程式、網站及網上企業銀行服務（ <u>包括透過流動保安編碼及/或生物憑據認證服務進行的存取</u> ），包括適用於手機銀行應用程式、網站、 <u>流動保安編碼、生物憑據認證服務</u> 或任何網上企業銀行服務使用或為其提供支援的技術的所有技術控制或出口法律及法規（「有關技術」）；
12.47	(h) 不會以任何非法方式、為任何非法目的或以與本條款不符的任何方式使用手機銀行應用程式、網站或網上企業銀行服務，或採取欺詐或惡意行動，例如非法侵入手機銀行應用程式、網站或任何作業系統；	(h) 不會以任何非法方式、為任何非法目的或以與本條款不符的任何方式使用手機銀行應用程式、網站、 <u>流動保安編碼、生物憑據認證服務</u> 或網上企業銀行服務，或採取欺詐或惡意行動，例如非法侵入手機銀行應用程式、網站或任何作業系統；
12.47	(i) 在使用手機銀行應用程式、網站或網上企業銀行服務時，不會在本條款許可的使用範圍外侵犯本行的知識產權或任何第三方的知識產權；	(i) 在使用手機銀行應用程式、網站、 <u>流動保安編碼、生物憑據認證服務</u> 或網上企業銀行服務時，不會在本條款許可的使用範圍外侵犯本行的知識產權或任何第三方的知識產權；
12.47	(k) 不會傳送、發送或上傳包含病毒、木馬病毒、蠕蟲、定時炸彈病毒、鍵盤記錄工具、間諜軟件、廣告軟	(k) 不會傳送、發送或上傳包含病毒、木馬病毒、蠕蟲、定時炸彈病毒、鍵盤記錄工具、間諜軟件、廣告軟

客戶重要通知

Important Notice to Customers



	件或者對手機銀行應用程式、網站、任何網上企業銀行服務或任何操作系統的運作造成不利影響的任何其他有害程式或類似的電腦代碼的任何數據或資料；	件或者對手機銀行應用程式、網站、 <u>流動保安編碼</u> 、 <u>生物憑據認證服務</u> 、任何網上企業銀行服務或任何操作系統的運作造成不利影響的任何其他有害程式或類似的電腦代碼的任何數據或資料；
12.47	(l) 不會以可能對本行的系統或安全造成破壞、導致其無法正常運作、使其負荷過重、使其受損或導致其被入侵或者幹擾其他用戶的方式使用手機銀行應用程式、網站、任何網上企業銀行服務；	(l) 不會以可能對本行的系統或安全造成破壞、導致其無法正常運作、使其負荷過重、使其受損或導致其被入侵或者幹擾其他用戶的方式使用手機銀行應用程式、網站、 <u>流動保安編碼</u> 、 <u>生物憑據認證服務</u> 、任何網上企業銀行服務；
12.47	(n) 不會在未經授權的情況下存取、幹擾、操控、損壞或破壞： (i) 手機銀行應用程式或網站的任何部分； (ii) 存儲手機銀行應用程式或網站的任何裝置、流動裝置或網絡； (iii) 提供手機銀行應用程式或網站的任何軟件；或 (iv) 任何第三方擁有或使用的任何裝置、流動裝置或網絡。	(n) 不會在未經授權的情況下存取、幹擾、操控、損壞或破壞： (i) 手機銀行應用程式或網站的任何部分； (ii) 存儲手機銀行應用程式或網站的任何裝置、流動裝置或網絡； (iii) <u>流動保安編碼</u> 或提供手機銀行應用程式或網站的任何軟件；或 (iv) 任何第三方擁有或使用的任何裝置、流動裝置或網絡。
12.48	(c) 客戶意識到任何人士正在實施或試圖實施第 47 條中提到的任何行為；	(c) 客戶意識到任何人士正在實施或試圖實施第 <u>12.47</u> 條中提到的任何行為；
12.48		<u>若客戶未能在合理可行情況下儘快通知本行該等事情，或存在欺詐或嚴重疏忽行為，客戶可能需對所有該等交易及所引致的直接損失負責。</u>
12.49	客戶確認網上企業銀行服務、網站、手機銀行應用程式及其所包含的軟件均為本行所有。如本行有合理理由懷疑客戶違反本條款（包括第 47 條）中	客戶確認網上企業銀行服務、網站、手機銀行應用程式、 <u>流動保安編碼</u> 及其所包含的軟件均為本行所有。如本行有合理理由懷疑客戶違反本條款

客戶重要通知

Important Notice to Customers



	<p>的任何保證及承諾，客戶同意本行無需通知客戶有權立即關閉其於本行開立的任何或全部賬戶並對客戶採取法律行動。如果客戶發現任何其他人士正在作出第 47 條中所述的任何行為，客戶承諾立即通知本行。</p>	<p>(包括第 12.47 條) 中的任何保證及承諾，客戶同意本行無需通知客戶有權立即關閉其於本行開立的任何或全部賬戶並對客戶採取法律行動。如果客戶發現任何其他人士正在作出第 12.47 條中所述的任何行為，客戶承諾立即通知本行。</p>
12.50	<p>客戶確認本行為透過網上企業銀行服務、網站及手機銀行應用程式傳輸或傳達指示或任何資訊而採用的通訊設施(包括網路)可能隨時不可靠或不可用，透過此類通訊設施傳輸資料時，可能導致發生中斷、延遲、資料損壞或遺失、資料傳輸機密性喪失或傳輸惡意軟件的情況。此外，客戶與本行之間透過網上企業銀行服務、網站及手機銀行應用程式傳輸或傳達指示或任何資訊可能會因一系列因素而延遲，包括但不限於時區差異、香港特別行政區或海外公眾假期或其他本行無法控制的原因，本行不會就該等延誤或由此產生的任何利息(如有)承擔責任。客戶接受因其接受本行提供的任何網上企業銀行服務而產生的所有風險，包括但不限於客戶與本行之間通過網上企業銀行服務傳輸或傳達指示或任何資訊的任何延誤、錯誤或遺漏或任何其他原因而遭受的任何損失。</p>	<p>客戶確認本行為透過網上企業銀行服務(包括透過流動保安編碼及/或生物憑據認證服務進行的存取)、網站及手機銀行應用程式傳輸或傳達指示或任何資訊而採用的通訊設施(包括網路)可能隨時不可靠或不可用，透過此類通訊設施傳輸資料時，可能導致發生中斷、延遲、資料損壞或遺失、資料傳輸機密性喪失或傳輸惡意軟件的情況。此外，客戶與本行之間透過網上企業銀行服務、網站及手機銀行應用程式傳輸或傳達指示或任何資訊可能會因一系列因素而延遲，包括但不限於時區差異、香港特別行政區或海外公眾假期或其他本行無法控制的原因，本行不會就該等延誤或由此產生的任何利息(如有)承擔責任。客戶接受因其接受本行提供的任何網上企業銀行服務(包括透過流動保安編碼及/或生物憑據認證服務進行的存取)而產生的所有風險，包括但不限於客戶與本行之間通過網上企業銀行服務傳輸或傳達指示或任何資訊的任何延誤、錯誤或遺漏或任何其他原因而遭受的任何損失。</p>
12.52	<p>客戶自行承擔使用手機銀行應用程式、網站及網上企業銀行服務的風險。手機銀行應用程式、網站及網上企業銀行服務均按「現狀」提供。在</p>	<p>客戶自行承擔使用手機銀行應用程式、網站、<u>流動保安編碼</u>及網上企業銀行服務的風險。手機銀行應用程式、網站、<u>流動保安編碼</u>及網上企業</p>

客戶重要通知

Important Notice to Customers



<p>監管規定允許的最大範圍內，本行排除所有可能適用於手機銀行應用程式、網站及網上企業銀行服務的明示或暗示的條件、保證（包括但不限於有關適銷性、適用於任何特定用途、準確性和不侵犯第三方權利的任何保證）、陳述或其他條款。</p>	<p>銀行服務均按「現狀」提供。在監管規定允許的最大範圍內，本行排除所有可能適用於手機銀行應用程式、網站、流動保安編碼及網上企業銀行服務的明示或暗示的條件、保證（包括但不限於有關適銷性、適用於任何特定用途、準確性和不侵犯第三方權利的任何保證）、陳述或其他條款。</p>
---	--

知識產權及資料擁有權

	現有條款	新條款
12.57	(a) 手機銀行應用程式、網站、網上企業銀行服務及有關技術在全球任何地方的所有知識產權（包括但不限於商標、標識和服務商標）均屬於本行或其許可人；	(a) 手機銀行應用程式、網站、 流動保安編碼 、網上企業銀行服務及有關技術在全球任何地方的所有知識產權（包括但不限於商標、標識和服務商標）均屬於本行或其許可人；
	(b) 手機銀行應用程式及網站僅以許可方式授與（而非出售）給客戶使用，因此客戶對手機銀行應用程式、網站、網上企業銀行服務或有關技術除根據本條款使用的權利外並無其他權利；	(b) 手機銀行應用程式及網站僅以許可方式授與（而非出售）給客戶使用，因此客戶對手機銀行應用程式、網站、 流動保安編碼 、網上企業銀行服務或有關技術除根據本條款使用的權利外並無其他權利；

服務可用性及終止

	現有條款	新條款
12.58	受限於監管規定，本行可隨時不經事先通知或提供任何理由的情形下而暫停、終止、撤銷或修改網上企業銀行服務。受限於適用於本行的監管規定，本行沒有義務持續提供網上企業銀行服務。本行有絕對酌情權，在本行認為適當的情況下，暫停客戶對網上企業銀行服務或其中任何部分的使用，或者不經事先通知而中止客戶對網上企業銀行服務的使用權限。本行	受限於監管規定，本行可隨時不經事先通知或提供任何理由的情形下而暫停、終止、撤銷或修改網上企業銀行服務（包括透過 流動保安編碼及/或生物憑據認證服務進行的存取 ）。受限於適用於本行的監管規定，本行沒有義務持續提供網上企業銀行服務（包括透過 流動保安編碼及/或生物憑據認證服務進行的存取 ）。本行有絕對酌情權，在本行認為適當的情況下，暫

客戶重要通知

Important Notice to Customers



	在這方面所作的決定是最終的並對客戶具有約束力。本行將不對客戶因該等決定而遭受的任何損失或損害承擔責任。	停客戶對網上企業銀行服務或其中任何部分的使用，或者不經事先通知而中止客戶對網上企業銀行服務的使用權限。本行在這方面所作的決定是最終的並對客戶具有約束力。本行將不對客戶因該等決定而遭受的任何損失或損害承擔責任。
12.59	(a) 客戶在從本行收到保安裝置後 60 天或本行規定的其他期限內未啟動網上企業銀行服務；	(a) 客戶在從本行收到保安裝置通知後 60 天或本行規定的其他期限內未啟動網上企業銀行服務；
12.60	在不限制第 7 條的情況下，客戶可透過以本行不時指定的形式和方式向本行發出事先通知終止本條款。客戶同意由客戶發出的任何終止通知僅在本行確認後方才生效。網上企業銀行服務的任何暫停或終止不會影響在暫停或終止之日或之前可能產生的任何權利或義務，並且本條款中與客戶仍需履行或解除的任何義務或責任相關的條款將在本條款終止後繼續對客戶具有約束力。	在不限制第 12.7 條的情況下，客戶可透過以本行不時指定的形式和方式向本行發出事先通知終止本條款。客戶同意由客戶發出的任何終止通知僅在本行確認後方才生效。網上企業銀行服務的任何暫停或終止不會影響在暫停或終止之日或之前可能產生的任何權利或義務，並且本條款中與客戶仍需履行或解除的任何義務或責任相關的條款將在本條款終止後繼續對客戶具有約束力。

本行的權利及責任限制

	現有條款	新條款
12.61	受限於下文第 62 條及第 63 條，本行僅在客戶因使用網上企業銀行服務而遭受直接損失且該等損失是由於本行的重大過失、欺詐或故意不當行為而造成的情況下才承擔責任。	受限於下文第 12.62 條及第 12.63 條，本行僅在客戶因使用網上企業銀行服務而遭受直接損失且該等損失是由於本行的重大過失、欺詐或故意不當行為而造成的情況下才承擔責任。
12.62	在不影響上述第 58 條的情況下，本行保留更改、取消、終止或暫停全部或部分網上企業銀行服務的權利，而無需給予通知或理由。客戶同意在適用於本行的監管規定允許的最大範圍內，在沒有重大過失、欺詐或故意不	在不影響上述第 12.58 條的情況下，本行保留更改、取消、終止或暫停全部或部分網上企業銀行服務的權利，而無需給予通知或理由。客戶同意在適用於本行的監管規定允許的最大範圍內，在沒有重大過失、欺詐或故意不

客戶重要通知

Important Notice to Customers



	當行為的情況下，本行或其任何人員或僱員均不對客戶或任何其他人士因本行行使上述權利而可能產生或遭受的任何種類的任何損失、損害成本、費用或開支承擔責任。	當行為的情況下，本行或其任何人員或僱員均不對客戶或任何其他人士因本行行使上述權利而可能產生或遭受的任何種類的任何損失、損害成本、費用或開支承擔責任。
12.63	除上述第 62 條外，本行不對客戶因使用網上企業銀行服務而造成的任何損失或損害承擔責任，包括但不限於：	除上述第 12.62 條外，本行不對客戶因使用網上企業銀行服務而造成的任何損失或損害承擔責任，包括但不限於：
12.63	(a) 本行提供網上企業銀行服務、透過網上企業銀行服務傳輸任何指示或資訊時發生的任何中斷、延遲、暫停、攔截、遺失或其他故障，而該等情況超出本行的合理控制範圍，包括（但不限於）通訊網路或系統故障、第三方提供者的任何作為或不作為、設備故障或任何政府命令；	(a) 本行提供網上企業銀行服務、透過網上企業銀行服務（ 包括透過流動保安編碼及/或生物憑據認證服務進行的存取 ）傳輸任何指示或資訊時發生的任何中斷、延遲、暫停、攔截、遺失或其他故障，而該等情況超出本行的合理控制範圍，包括（但不限於）通訊網路或系統故障、第三方提供者的任何作為或不作為、設備故障或任何政府命令；

客戶重要通知

Important Notice to Customers



附件 1- [流動保安編碼及生物憑據認證服務條款及細則](#) (「附件 1」)

現有條款	新條款
	本附件1是網上企業銀行服務的特別條款及細則第12.34條下所提及之流動保安編碼及生物憑據認證服務之條款及細則，且可不時作出修訂。

一般條款

現有條款	新條款
1 本附件 1 適用於使用本行提供的生物憑據認證服務（定義見本附件第 3 條）的客戶。	1 本附件 1 適用於使用本行提供的(1) 流動保安編碼及/或(2)生物憑據認證服務 （各定義見本附件 1 第 3 條）的客戶。
2 本附件 1 附加於並補充本條款。為免生疑，如本附件 1 的規定與本條款其他部分載列的條文不一致，就生物憑據認證服務而言，概以本附件 1 為準。	2 本附件 1 附加於並補充 網上企業銀行服務的特別條款及細則本 (「 網上企業銀行條款 」)。為免生疑，如本附件 1 的規定與本條款其他部分載列的條文不一致，就 流動保安編碼及生物憑據認證服務 而言，概以本附件 1 為準。

定義及詮釋

現有條款	新條款
4 本條款中界定的詞語或短語具有與本附件 1 中相同的涵義（除非本附件中另有明確說明）。	4 網上企業銀行條款 本條款中界定的詞語或短語具有與本附件 1 中相同的涵義（除非本附件中另有明確說明）。
5 「認可流動裝置」指本行不時允許使用生物憑據認證服務的任何流動裝置，包括但不限於操作流動裝置該等所用的操作系統或軟件。	5 「認可流動裝置」指本行不時允許使用 流動保安編碼及/或生物憑據認證服務 的任何流動裝置，包括但

客戶重要通知

Important Notice to Customers



			不限於操作流動裝置該等所用的操作系統或軟件。
5		5	<p><u>「流動保安編碼」指手機銀行應用程式內建並連接手機銀行應用程式的功能，用於計算保安編碼或以其他方式認證客戶及允許客戶進入及/或使用任何網上企業銀行服務。</u></p> <p><u>「流動保安編碼密碼」指客戶為使用客戶的流動保安編碼而自選及指定的個人識別號碼。</u></p>
5	請於「設定及其他」>「管理生物憑據認證」>「生物憑據認證服務常見問題」內查閱該等認可流動裝置的最新清單。	6	<p>請於</p> <p>https://www.asia.ccb.com/hongkong_tc/doc/commercial/faq_oeps_mb.pdf「設定及其他」>「管理生物憑據認證」>「生物憑據認證服務常見問題」內查閱該等認可流動裝置的最新清單。</p>

生物憑據認證服務的提供資格

現有條款		新條款	
7	為使用生物憑據認證服務，客戶必須：	7	為使用 <u>流動保安編碼及/或生物憑據認證服務（如適用）</u> ，客戶必須：
7	(d) 持有已啟用生物憑據認證功能的認可流動裝置；	7	(d) <u>（僅適用於生物憑據認證服務）</u> 持有已啟用生物憑據認證功能的認可流動裝置；
7	(e) 至少已錄入客戶的一種生物識別憑據以用於控制對認可流動裝置的使用；及	7	(e) <u>（僅適用於生物憑據認證服務）</u> 至少已錄入客戶的一種生物識別憑據以用於控制對認可流動裝置的使用；及
7	(f) 已根據本行的啟動指示，使用客戶的身份驗證訊息以及本行將向客戶發送的一次性密碼啟動生物憑據認證服務。	7	(f) 已根據本行的啟動指示，使用客戶的身份驗證訊息以及本行將向客戶發送的一次性密碼 <u>設置並</u> 啟動生物憑據認證服務 <u>（如適用）</u> 。

客戶重要通知

Important Notice to Customers



		9	<p>客戶確認本行可不時規定必須安裝的手機銀行應用程式, 本行網站及其內置功能更新, 以使手機銀行應用程式, 流動保安編碼及/或生物憑據認證服務正常運行。客戶確認, 客戶須獨自負責更新其手機銀行應用程式及/或進入本行網站的最新更新版本以使用流動保安編碼及/或生物憑據認證服務進入網上企業銀行服務。如果客戶 (A) 未有安裝手機銀行應用程式的任何要求安裝的更新, 或(B)未進入本行網站的最新版本, 對於客戶因不能進入任何網上企業銀行服務而招致之任何損失或損害, 本行概不對客戶承擔任何責任。雖有前述規定, 但本行並不對流動保安編碼及/或生物憑據認證服務的隨時可用, 或與任何特定設備或型號、軟件或本行不時提供的其他網上銀行服務相容, 作出陳述或保證。客戶應負責確保其流動裝置是足以滿足任何相容要求的認可流動裝置。如未能滿足這要求, 或會導致流動保安編碼及生物憑據認證服務發生故障。</p>
--	--	---	--

流動保安編碼

現有條款		新條款	
		10	<p>流動保安編碼是由本行向已經下載及註冊手機銀行應用程式的客戶提供的數碼保安編碼, 作為客戶認證其身份以進入及/或使用網上企業銀行服務的其中一個方式。客戶可透過以下方式在銀行接受的任何認可流動裝置上設置其流動保安編碼:</p>

客戶重要通知

Important Notice to Customers



		<p>(a) <u>登入手機銀行應用程式及接受為設置和使用流動保安編碼所有適用的條款及條件；</u></p> <p>(b) <u>輸入發送至客戶指定及已在銀行登記之流動電話號碼的安全碼；</u></p> <p>(c) <u>指定流動保安編碼密碼；</u></p> <p>(d) <u>（僅適用於生物憑據認證服務）將客戶的生物識別憑據用於認證；及</u></p> <p>(e) <u>（僅適用於生物憑據認證服務）在客戶的流動裝置具備生物認證功能且如果客戶已同意本附件1下的條款及條件的情況下，允許客戶透過生物憑據認證服務進入並使用流動保安編碼，</u> <u>或遵循銀行不時規定的任何其他步驟或指示。</u></p>
	11	<p><u>設置和啟動流動保安編碼時，認可流動裝置上將創建並保存一個數碼保安編碼。客戶確認每個流動保安編碼每次僅可在一個認可流動裝置上進行綁定並啟動。一旦綁定流動保安編碼，客戶被綁定的認可流動裝置將被銀行持續用作識別及認證客戶在進入和使用任何網上企業銀行服務身份的目的。銀行對透過使用流動保安編碼登入網上企業銀行服務的任何人士，均無義務亦無責任查詢或核實其身份或權限。如果客戶希望停止使用流動保安編碼或希望將認可流動裝置與流動保安編碼解綁，客戶可在網上企業銀行服務中為相關的認可流動裝置和流動保安編碼解綁，或致電銀行不時於</u></p>

客戶重要通知

Important Notice to Customers



			銀行網站或手機銀行應用程式中發佈之客戶熱線與銀行聯繫，以獲取進一步協助。
		12	客戶確認當流動保安編碼被設置及啟動，客戶的保安裝置（除非客戶另外要求）將自動被停用，保安裝置將不能再用於進入或使用任何網上企業銀行服務。

生物憑據認證服務的提供 [（如適用）](#)

	現有條款		新條款
9	<p>客戶確認並同意如下：</p> <p>(a) 一旦啟動生物憑據認證服務，客戶的認可流動裝置上儲存的任何生物識別憑據均可被用於使用本行的網上企業銀行服務及使用客戶已啟動並與認可流動裝置綁定的任何流動保安編碼。客戶進一步確認並接受，任何獲得客戶認可流動裝置上的生物識別憑據或生物憑據認證驗證使用權限的人士均能夠使用本行的網上企業銀行服務、使用流動保安編碼（如有）認證身份，並就客戶的賬戶向本行作出指示，包括但不限於提取或另行處理客戶的資金；</p> <p>(b) 為提供生物憑據認證服務之目的，手機銀行應用程式及其內置功能（例如客戶啟動的任何流動保安編碼）將連接客戶的認可流動裝置上的生物憑據認證功能及資料。客戶同意本行為提供生物憑據認證服務而連</p>	13	<p>客戶確認並同意如下，連同流動保安編碼：</p> <p>(a) 一旦啟動生物憑據認證服務 （如適用），客戶的認可流動裝置上儲存的任何生物識別憑據均可被用於使用本行的網上企業銀行服務及使用客戶已啟動並與認可流動裝置綁定的任何流動保安編碼。客戶進一步確認並接受，任何獲得客戶認可流動裝置上的生物識別憑據或生物憑據認證驗證使用權限的人士均能夠使用本行的網上企業銀行服務、使用流動保安編碼（如有）認證身份，並就客戶的賬戶向本行作出指示，包括但不限於提取或另行處理客戶的資金；</p> <p>(b) 為提供生物憑據認證服務之目的，手機銀行應用程式及其內置功能（例如客戶啟動的任何流動保安編碼）將連接客戶的認可流動裝置上的生物憑據認證功能及資料。客戶同意本行為提供生物憑據認證服務而連</p>

客戶重要通知

Important Notice to Customers



<p>接及使用客戶的認可流動裝置上的該項功能及資料；</p> <p>(c) 本行可隨時酌情決定更新手機銀行應用程式及其內置功能。客戶必須安裝強制性的更新，以確保生物憑據認證服務正常運作。雖有前述規定，但本行並不對生物憑據認證服務的隨時可用作出陳述或保證，或與任何特定設備或型號、軟件或本行不時提供的其他網上銀行服務相容。客戶應負責確保其電子設備是足以滿足任何相容要求的認可流動裝置。如未能滿足這要求，或會導致生物憑據認證服務發生故障；</p> <p>(d) 客戶將錄入客戶的至少一種生物識別憑據以用於控制對認可流動裝置的登入；及</p> <p>(e) 客戶將根據本行的啟動指示，使用客戶的身份驗證訊息以及本行將向客戶發送的一次性密碼啟動生物憑據認證服務。</p>	<p>接及使用客戶的認可流動裝置上的該項功能及資料；<u>及</u></p> <p>(c) 本行可隨時酌情決定更新手機銀行應用程式及其內置功能。客戶必須安裝強制性的更新，以確保生物憑據認證服務正常運作。雖有前述規定，但本行並不對生物憑據認證服務的隨時可用作出陳述或保證，或與任何特定設備或型號、軟件或本行不時提供的其他網上銀行服務相容。客戶應負責確保其電子設備是足以滿足任何相容要求的認可流動裝置。如未能滿足這要求，或會導致生物憑據認證服務發生故障；</p> <p>(c) 客戶將<u>在生物憑據認證服務下</u>錄入客戶的至少一種生物識別憑據以用於控制對認可流動裝置的登入。；<u>—</u>及</p> <p>(e) <u>客戶將根據本行的啟動指示，</u>使用客戶的身份驗證訊息以及本行將向客戶發送的一次性密碼啟動生物憑據認證服務。<u>—</u></p>
---	--

保安

	現有條款		新條款
10	<p>客戶確認與客戶賬戶及/或交易記錄相關的資訊可能儲存在客戶的認可流動裝置上，如果儲存的資料在他人使用客戶的認可流動裝置時（不論是否經客戶授權）被洩漏，本行將不會對此承擔責任。為保護客戶的私隱和資產，客戶同意採取措施以確保客戶的認可流動裝置、密碼以及與銀行或賬戶相關資料的保密</p>	14	<p>客戶確認與客戶賬戶及/或交易記錄相關的資訊可能儲存在客戶的認可流動裝置上，如果儲存的資料在他人使用客戶的認可流動裝置時（不論是否經客戶授權）被洩漏，本行將不會對此承擔責任。為保護客戶的私隱和資產，客戶同意採取措施以確保客戶的認可流動裝置、<u>流動保安編碼密碼</u>、密碼以及與銀</p>

客戶重要通知

Important Notice to Customers



<p>性和安全性，並防止客戶的認可流動裝置遭到未經授權的使用，包括但不限於：</p> <p>(a) 確保客戶的認可流動裝置上僅儲存了客戶的生物識別憑據，客戶的認可流動裝置已妥善保管，且在可用於客戶的認可流動裝置上，以改變或增加生物識別憑據的任何密碼或安全碼均受到保護。如果由於客戶未對其認可流動裝置的登入權限加以保護，而導致發生任何未經授權的交易，本行對由此產生的任何損失不承擔任何責任；</p> <p>(b) 警惕面部辨識功能下的錯誤配對。作為替代性辦法，客戶可選擇使用其身份驗證資訊透過手機銀行應用程式登入網上企業銀行服務，或使用客戶流動保安編碼中的密碼，驗證客戶的身份以使用流動保安編碼；</p> <p>(c) 停用客戶的認可流動裝置上提供的任何有機會影響生物憑據認證安全的功能，並避免同意客戶的認可流動裝置上任何有機會影響生物憑據認證安全的設定（例如：於面部識別功能中停用能夠感知使用者注視的功能）；</p> <p>(d) 確保客戶的認可流動裝置在使用後立即上鎖，並確保客戶的認可流動裝置在不在客戶掌控期間亦應被鎖上；</p> <p>(e) 避免向任何其他人士披露或與任何其他人士分享客戶的認可</p>	<p>行或賬戶相關資料的保密性和安全性，並防止客戶的認可流動裝置遭到未經授權的使用，包括但不限於：</p> <p>(a) 確保（<u>在生物憑據認證服務的情況下</u>）客戶的認可流動裝置上僅儲存了客戶的生物識別憑據，客戶的認可流動裝置已妥善保管，且在可用於客戶的認可流動裝置上，以改變或增加生物識別憑據的任何密碼，<u>流動保安編碼密碼</u>或安全碼均受到保護。如果由於客戶未對其認可流動裝置的登入權限加以保護，而導致發生任何未經授權的交易，本行對由此產生的任何損失不承擔任何責任；</p> <p>(b) 警惕面部辨識功能下的錯誤配對。作為替代性辦法，客戶可選擇使用其身份驗證資訊透過手機銀行應用程式登入網上企業銀行服務，或使用客戶流動保安編碼中的密碼，驗證客戶的身份以使用流動保安編碼；</p> <p>(c) 停用客戶的認可流動裝置上提供的任何有機會影響生物憑據認證安全的功能，並避免同意客戶的認可流動裝置上任何有機會影響生物憑據認證安全的設定（例如：於面部識別功能中停用能夠感知使用者注視的功能）；</p> <p>(d) 確保客戶的認可流動裝置在使用後立即上鎖，並確保客戶的認可流動裝置在不在客戶掌控期間亦應被鎖上；</p>
---	--

客戶重要通知

Important Notice to Customers



<p>流動裝置的密碼或安全碼，或允許任何人士使用客戶的認可流動裝置上的生物識別憑據及/或生物憑據認證功能；</p> <p>(f) 在設定任何密碼時避免使用容易獲取的個人資料，例如客戶的生日、電話號碼或名字中任何可識別的部分等易於獲得的個人資料，亦不在使用任何其他服務時使用相同密碼（例如：用以連接互聯網或登入手機銀行應用程式）；</p> <p>(g) 避免在沒有適當保護措施的情況下寫下或記錄任何裝置密碼（例如流動保安編碼的密碼）或安全碼；</p> <p>(h) 在客戶的認可流動裝置上輸入任何密碼或安全碼之前，對客戶的四周環境保持警惕，以確保其保密性；</p> <p>(i) 定期更改登入認可流動裝置及生物憑據認證服務的密碼（如適用）；</p> <p>(j) 如客戶懷疑自己受到欺詐性網站、手機銀行應用程式、電子郵件或短訊/無綫應用協議 (WAP) 推送訊息的欺騙（例如：客戶在使用正確的生物識別憑據後無法登入手機銀行應用程式），立即更改客戶的密碼；</p> <p>(k) 如客戶懷疑自己的任何身份驗證資訊、任何其他安全碼（包括但不限於流動保安編碼的密碼）及/或認可流動裝置被入侵、丟失、被盜或未經客戶授</p>	<p>(e) 避免向任何其他人士披露或與任何其他人士分享客戶的認可流動裝置的密碼，流動保安編碼密碼或安全碼，或允許任何人士使用客戶的認可流動裝置上的流動保安編碼及/或生物識別憑據及/或生物憑據認證功能；</p> <p>(f) 在設定任何密碼或流動保安編碼密碼時避免使用容易獲取的個人資料，例如客戶的生日、電話號碼或名字中任何可識別的部分等易於獲得的個人資料，亦不在使用任何其他服務時使用相同密碼或流動保安編碼密碼（例如：用以連接互聯網或登入手機銀行應用程式）；</p> <p>(g) 避免在沒有適當保護措施的情況下寫下或記錄任何裝置密碼（例如流動保安編碼的密碼）或安全碼；</p> <p>(h) 在客戶的認可流動裝置上輸入任何密碼，流動保安編碼密碼或安全碼之前，對客戶的四周環境保持警惕，以確保其保密性；</p> <p>(i) 定期更改登入認可流動裝置、流動保安編碼及生物憑據認證服務的密碼和流動保安編碼密碼（如適用）；</p> <p>(j) 如客戶懷疑自己受到欺詐性網站、手機銀行應用程式、電子郵件或短訊/無綫應用協議 (WAP) 推送訊息的欺騙（例如：客戶在使用正確的生物識別憑</p>
---	---

客戶重要通知

Important Notice to Customers



<p>權被登入或使用，在合理可行的情況下儘快告知本行；</p> <p>(l) 嚴格遵照本行及/或客戶的認可流動裝置的製造商不時向客戶提供適用於客戶的認可流動裝置的安全建議、措施、指引及指示；</p> <p>(m) 如客戶的移動電話號碼有任何變更，立即通知本行；</p> <p>(n) 手機銀行應用程式及/或流動保安編碼因任何原因被終止時，在客戶的認可流動裝置刪除手機銀行應用程式及/或流動保安編碼；及</p> <p>(o) 如客戶更換或棄置其認可流動裝置，從該認可流動裝置刪除手機銀行應用程式。</p>	<p>據及/或流動保安編碼後無法登入手機銀行應用程式），立即更改客戶的密碼或流動保安編碼密碼；</p> <p>(k) 如客戶懷疑自己的任何身份驗證資訊、任何其他安全碼（包括但不限於流動保安編碼的密碼）及/或認可流動裝置被入侵、丟失、被盜或未經客戶授權被登入或使用，在合理可行的情況下儘快告知本行；</p> <p>(l) 嚴格遵照本行及/或客戶的認可流動裝置的製造商不時向客戶提供適用於客戶的認可流動裝置的安全建議、措施、指引及指示；</p> <p>(m) 如客戶的移動電話號碼有任何變更，立即通知本行；</p> <p>(n) 手機銀行應用程式及/或流動保安編碼因任何原因被終止時，在客戶的認可流動裝置刪除手機銀行應用程式及/或流動保安編碼；及</p> <p>(o) 如客戶更換或棄置其認可流動裝置，從該認可流動裝置刪除手機銀行應用程式；</p> <p>(p) 客戶須妥善保管其流動保安編碼密碼並確保其安全保密及處於客戶自主控制下，不可允許除客戶之外的任何其他人士使用該流動保安編碼。流動保安編碼任何時候均屬本行財產，並由本行自行酌情決定發出與否，客戶應在本行要求時，立即將之註銷或停用；及</p> <p>(q) 如果客戶(已啟用流動保安編碼)</p>
---	---

客戶重要通知

Important Notice to Customers



			<p><u>的流動裝置遺失或被竊，客戶應在合理可行情況下儘快撥打本行不時規定的電話號碼通知本行，並在本行要求時作出書面確認。如客戶未能在合理可行情況下儘快通知本行該等事件，或在其他情況下有欺詐或嚴重疏忽的行為，客戶可能需對因第三人使用其所遺失之(已啟用流動保安編碼的)流動裝置所進行的未經授權交易而所引致的所有直接損失負責。</u></p>
11	如客戶通知本行懷疑客戶的生物識別憑據、流動保安編碼或其他安全碼的安全性受到損害，本行有權（但無義務）要求客戶變更身分驗證資訊、重新錄入客戶的生物識別憑據或者暫停或停止使用生物憑據認證服務。	15	如客戶通知本行懷疑客戶的生物識別憑據、流動保安編碼或其他安全碼的安全性受到損害，本行有權（但無義務）要求客戶變更身分驗證資訊、 <u>重設流動保安編碼</u> 、重新錄入客戶的生物識別憑據或者暫停或停止使用 <u>流動保安編碼及</u> 生物憑據認證服務。
12	客戶應自行負責採取適當的保護措施（包括但不限於上文第 10 條所述之措施），並應對因客戶未採取並維持該等適當保護措施而在手機銀行應用程式、生物憑據認證服務及/或流動保安編碼內引起的未經授權的使用或披露所造成的任何損失承擔責任。	16	客戶應自行負責採取適當的保護措施（包括但不限於上文第 10 <u>14</u> 條所述之措施），並應對因客戶未採取並維持該等適當保護措施而在手機銀行應用程式、生物憑據認證服務及/或流動保安編碼內引起的未經授權的使用或披露所造成的任何損失承擔責任。

免責聲明及責任限制

現有條款		新條款	
14	客戶確認生物憑據認證服務是為方便客戶本人而提供。客戶應自行承擔使用生物憑據認證服務的所有風險。生物憑據認證服務是按「現狀」提供的。在監管規定允許的最	18	客戶確認 <u>流動保安編碼及</u> 生物憑據認證服務是為方便客戶本人而提供。客戶應自行承擔使用 <u>流動保安編碼及/或</u> 生物憑據認證服務的所有風險。 <u>流動保安編碼及/或</u> 生物

客戶重要通知

Important Notice to Customers



	<p>大範圍內，本行排除所有可能適用於生物憑據認證服務的明示或暗示的條件、保證（包括但不限於有關適銷性、適用於任何特定用途、準確性和不侵犯協力廠商權利的任何保證）、陳述或其他條款。</p>		<p>憑據認證服務是按「現狀」提供的。在監管規定允許的最大範圍內，本行排除所有可能適用於<u>流動保安編碼及/或生物憑據認證服務</u>的明示或暗示的條件、保證（包括但不限於有關適銷性、適用於任何特定用途、準確性和不侵犯協力廠商權利的任何保證）、陳述或其他條款。</p>
15	<p>在監管規定允許的最大範圍內，對於因客戶使用生物憑據認證服務、透過生物憑據認證服務向本行作出的指示或任何與生物憑據認證服務有關的未經授權的交易而導致客戶遭受的任何損失，本行將不承擔任何責任。</p>	19	<p>在監管規定允許的最大範圍內，對於因客戶使用<u>流動保安編碼及/或生物憑據認證服務</u>、透過生物憑據認證服務向本行作出的指示或任何與<u>流動保安編碼及/或生物憑據認證服務</u>有關的未經授權的交易而導致客戶遭受的任何損失，本行將不承擔任何責任。</p>
16	<p>在監管規定允許的最大範圍內，對於與使用生物憑據認證服務有關而產生的任何作為、不作為、疏忽、違約、損害、損失（包括但不限於資料損失或洩漏）、訴因（無論是基於合同、侵權（包括但不限於疏忽）或其他原因，本行將不承擔任何責任。就生物憑據認證服務中的任何錯誤、截取、破壞、刪除或不準確之處、任何人對生物憑據認證服務的運用、依賴或無法運用，生物憑據認證服務運作過程中的任何中斷或受阻或延遲、任何不完整的傳輸、任何電路或系統故障或任何電腦病毒，本行將不承擔任何責任。就因與生物憑據認證服務相關的該等作為、遺漏、疏忽或失責引致的任何利潤、銷售額、業務、收入、業務機遇、商譽或聲譽方面的</p>	20	<p>在監管規定允許的最大範圍內，對於與使用<u>流動保安編碼及/或生物憑據認證服務</u>有關而產生的任何作為、不作為、疏忽、違約、損害、損失（包括但不限於資料損失或洩漏）、訴因（無論是基於合同、侵權（包括但不限於疏忽）或其他原因，本行將不承擔任何責任。就<u>流動保安編碼及/或生物憑據認證服務</u>中的任何錯誤、截取、破壞、刪除或不準確之處、任何人對<u>流動保安編碼及/或生物憑據認證服務</u>的運用、依賴或無法運用，<u>流動保安編碼及/或生物憑據認證服務</u>運作過程中的任何中斷或受阻或延遲、任何不完整的傳輸、任何電路或系統故障或任何電腦病毒，本行將不承擔任何責任。就因與<u>流動保安編碼及/或生物憑據認證服務</u>相關的</p>

客戶重要通知

Important Notice to Customers



<p>損失或任何特殊、相應而生或間接的損失或損害，本行均無須負責。</p>	<p>該等作為、遺漏、疏忽或失責引致的任何利潤、銷售額、業務、收入、業務機遇、商譽或聲譽方面的損失或任何特殊、相應而生或間接的損失或損害，本行均無須負責。</p>
---------------------------------------	---

服務可用性及終止

	現有條款		新條款
19	<p>本行可隨時不經事先通知或提供任何理由的情形下而暫停、終止、撤銷或修改生物憑據認證服務。本行沒有義務持續提供生物憑據認證服務。本行有絕對酌情權決定客戶是否合資格使用生物憑據認證服務，及在本行認為適當的情況下，本行有權暫停客戶使用生物憑據認證服務或其中任何部分，或不經事先通知而中止客戶對生物憑據認證服務的使用權限。本行在這方面所作的決定是最終的並對客戶具有約束力。本行將不對客戶因該等決定而遭受的任何損失或損害承擔責任。</p>	23	<p>本行可隨時不經事先通知或提供任何理由的情形下而暫停、終止、撤銷或修改<u>流動保安編碼及/或</u>生物憑據認證服務。本行沒有義務持續提供<u>流動保安編碼及/或</u>生物憑據認證服務。本行有絕對酌情權決定客戶是否合資格使用<u>流動保安編碼及/或</u>生物憑據認證服務，及在本行認為適當的情況下，本行有權暫停客戶使用<u>流動保安編碼及/或</u>生物憑據認證服務或其中任何部分，或不經事先通知而中止客戶對<u>流動保安編碼及/或</u>生物憑據認證服務的使用權限。本行在這方面所作的決定是最終的並對客戶具有約束力。本行將不對客戶因該等決定而遭受的任何損失或損害承擔責任。</p>

其他

	現有條款		新條款
		24	<p><u>本附件1可能隨時修訂，並可不定期進行更新。修訂後的條款將在本行向客戶發出合理通知後生效，包括在手機銀行應用程式、網站上發布經修訂後的本條款或在本行分行（如適用）展示經修訂後的條款。在符合監管規定的情況下，倘客戶</u></p>

客戶重要通知

Important Notice to Customers



			<u>繼續使用流動保安編碼及/或生物憑據認證服務，即被視為已同意經修訂後的條款。</u>
		25	<u>本附件1受香港特別行政區法律管轄。客戶同意對於與本附件1有關或由本附件1引起的任何爭議，須服從香港法院的非專屬管轄權，但本附件1可由任何有管轄權的司法管轄區的法院執行。</u>
		26	<u>本行及客戶之外的任何人士均不享有《合約（第三者權利）條例》項下強制執行本附件1之任何規定或享有其利益的任何權利。不論本附件1中有何規定，本附件1的撤銷或更改在任何時候均無須經本行及客戶之外任何其他人士同意。</u>
		27	<u>本附件1條款中的英文版本與中文版本如有任何不一致，則以英文版本為準。</u>

Table

	Original	New
NA		<u>The additional provisions (“Terms”) set out in this section 12 of Part B of the Master TC will apply if a Customer requests internet banking services.</u>
NA	IMPORTANT NOTES: Before you register to use the Online Enterprise Banking Services (as defined hereinafter), please read these terms and conditions (“Terms”) carefully. By registering to use or using the Mobile Banking App (as defined hereinafter), the Website (as defined hereinafter) and the Online Enterprise Banking Services, you will be deemed to have accepted and be bound	IMPORTANT NOTES: Before you register to use the Online Enterprise Banking Services (as defined hereinafter), please read these terms and conditions (“Terms”) carefully. By registering to use or using the Mobile Banking App (as defined hereinafter), the Website (as defined hereinafter) and the Online Enterprise Banking Services <u>(as defined hereinafter), you will be deemed to</u>

客戶重要通知

Important Notice to Customers



	by these Terms, our Privacy Policy and PDPO Notice.	have accepted and be bound by these Terms, our Privacy Policy and PDPO Notice.
--	---	--

Definitions and interpretation

	Original	New
12.4	(a) the individual(s) authorised by the Customer via the Online Enterprise Banking Services Application / Maintenance Form as described below in Clause 21 from time to time to use the Online Enterprise Banking Services through the Website or through the Mobile Banking App; and	(a) the individual(s) authorised by the Customer via the Online Enterprise Banking Services Application / Maintenance Form as described below in Clause 12.21 from time to time to use the Online Enterprise Banking Services through the Website or through the Mobile Banking App; and
12.4	“Authoriser” refers to the individual(s) nominated by the Master or the Customer via an Online Enterprise Banking Services Application / Maintenance Form (and/or any other form and/or materials as required by the Bank from time to time) and/or the Online Enterprise Banking Services directly and approved by the Bank to do all the things as described below at Clause 21(b), which may be amended from time to time.	“Authoriser” refers to the individual(s) nominated by the Master or the Customer via an Online Enterprise Banking Services Application / Maintenance Form (and/or any other form and/or materials as required by the Bank from time to time) and/or the Online Enterprise Banking Services directly and approved by the Bank to do all the things as described below at Clause 12.21(b) , which may be amended from time to time.
12.4	“Biometric Credential Authentication Service” has the meaning as defined in Clause 5 of Annex 1 (Terms and Conditions for Biometric Credential Authentication Service) to these Terms.	“Biometric Credential Authentication Service” has the meaning as defined in Clause 5 of Annex 1 (the Terms and Conditions for Mobile Token and Biometric Credential Authentication Service) to these Terms.
12.4	“Biometric Credentials” has the meaning as defined in Clause 5 of Annex 1 (Terms and Conditions for Biometric	“Biometric Credentials” has the meaning as defined in Clause 5 of Annex 1 (the Terms and Conditions for Mobile

客戶重要通知

Important Notice to Customers



	Credential Authentication Service) to these Terms.	<i>Token and Biometric Credential Authentication Service</i> to these Terms.
12.4	<p>“Existing Terms” means, among others, the <i>“Terms and Conditions for Accounts and Related Services (For Enterprise Customers)”</i>, <i>“Master Terms and Conditions for Accounts and Services (Business Customers)”</i>, the <i>“Terms and Conditions for Bank Services relating to Faster Payment System”</i>, the <i>“Terms and Conditions for Investment Services”</i>, the <i>“Terms and Conditions in using WhatsApp Chatbot Service”</i>, and any other applicable agreements or terms and conditions that the Customer has entered into with the Bank, each as may be amended from time to time.</p>	<p>“Existing Terms” means, among others, the <i>“Terms and Conditions for Accounts and Related Services (For Enterprise Customers)”</i>, <i>“Master Terms and Conditions for Accounts and Services (Business Customers)”</i>, the <i>“Terms and Conditions for Bank Services relating to Faster Payment System”</i>, the <i>“Terms and Conditions for Investment Services”</i>, the <i>“Terms and Conditions in using WhatsApp Chatbot Service”</i>, <u><i>the “Terms and Conditions for Mobile Token and Biometric Credential Authentication Service”</i></u>, and any other applicable agreements or terms and conditions that the Customer has entered into with the Bank, each as may be amended from time to time.</p>
12.4	<p>“Maker” refers to the individual(s) nominated by the Customer or the Master via an Online Enterprise Banking Services Application / Maintenance Form (and/or any other form and/or materials as required by the Bank from time to time) and/or the Online Enterprise Banking Services directly and approved by the Bank to do all the things as described at Clause 21(c), which may be amended from time to time.</p>	<p>“Maker” refers to the individual(s) nominated by the Customer or the Master via an Online Enterprise Banking Services Application / Maintenance Form (and/or any other form and/or materials as required by the Bank from time to time) and/or the Online Enterprise Banking Services directly and approved by the Bank to do all the things as described at Clause <u>12.21(c)</u>, which may be amended from time to time.</p>
12.4	<p>“Master” refers to the individual(s) nominated by the Customer via an Online Enterprise Banking Services Application / Maintenance Form (and/or any other form and/or materials as required by the Bank from</p>	<p>“Master” refers to the individual(s) nominated by the Customer via an Online Enterprise Banking Services Application / Maintenance Form (and/or any other form and/or materials as required by the Bank from</p>

客戶重要通知

Important Notice to Customers



	time to time) and approved by the Bank to do all the things as described at Clause 21(a) , which may be amended from time to time.	time to time) and approved by the Bank to do all the things as described at Clause 12.21(a) , which may be amended from time to time.
12.4		"Mobile Token" has the meaning as defined in the Terms and Conditions for Mobile Token and Biometric Credential Authentication Service .
12.4		"Mobile Token Password" has the meaning as defined in the Terms and Conditions for Mobile Token and Biometric Credential Authentication Service .
12.4	"Online Enterprise Banking Services" means the banking products or services which the Bank enables a Customer to access via the Mobile Banking App or the Website as may be amended from time to time.	"Online Enterprise Banking Services" means the banking products or services which the Bank enables a Customer to access via the Mobile Banking App or the Website, and the relevant inbuilt features therein (including the Mobile Token and/or the Biometric Credential Authentication Service) , as may be amended from time to time.
12.4	"Password" means any confidential password, phrase, code or number or any other identification whether issued to the Customer by the Bank or adopted by the Customer (including any Security Code) which is used to access the Online Enterprise Banking Services.	"Password" means any confidential password, phrase, code or number or any other identification whether issued to the Customer by the Bank or adopted by the Customer (including any Security Code or (if applicable) any Mobile Token Password) which is used to access the Online Enterprise Banking Services.
12.4	"Security Code" means the one-time Password generated by the Security Device for use by the Authorised Representative to access the Online Enterprise Banking Services.	"Security Code" means the one-time Password generated or displayed by the Security Device or the Mobile Token (as applicable) for use by the Authorised Representative to access the Online Enterprise Banking Services.
12.4	"Security Device" means an electronic device designated and provided by the	"Security Device" means an electronic device in physical form designated and

客戶重要通知

Important Notice to Customers



<p>Bank for use by each Authorised Representative to generate the Security Code to access the Online Enterprise Banking Services.</p>	<p>provided by the Bank (upon request) for use by each Authorised Representative to generate the Security Code to access the Online Enterprise Banking Services.</p>
---	--

Use and Updates

	Original	New
12.7	<p>The Online Enterprise Banking Services (save for information provided by our licensors or by third-party service providers, such as market information and property valuation) are developed and solely owned by us. Any of the Online Enterprise Banking Services may be withdrawn, amended, suspended or terminated by the Bank at any time without prior notice. The Bank may at its absolute discretion decide whether the Customer or any of its Authorised Representatives is eligible to use any of the Online Enterprise Banking Services, and suspend its use of the Online Enterprise Banking Services, the Website and/or Mobile Banking App (or any part of them), or suspend its access to the Online Enterprise Banking Services, the Website and/or Mobile Banking App without prior notice. The decision of the Bank is final. The Bank will not be responsible for any loss or damage suffered by the Customer arising from such decisions.</p>	<p>The Online Enterprise Banking Services (save for information provided by our licensors or by third-party service providers, such as market information and property valuation) are developed and solely owned by us. Any of the Online Enterprise Banking Services may be withdrawn, amended, suspended or terminated by the Bank at any time without prior notice. The Bank may at its absolute discretion decide whether the Customer or any of its Authorised Representatives is eligible to use any of the Online Enterprise Banking Services, and suspend its use of the Online Enterprise Banking Services, the Website and/or Mobile Banking App (or any part of them), or suspend its access (including, via the Mobile Token and/or the Biometric Credential Authentication Service) to the Online Enterprise Banking Services, the Website and/or Mobile Banking App without prior notice. The decision of the Bank is final. The Bank will not be responsible for any loss or damage suffered by the Customer arising from such decisions.</p>
12.9	<p>Subject to Clause 65, the Bank does not charge any fee for the use of the Mobile Banking App nor the Website. However, the Customer will be</p>	<p>Subject to Clause 12.65, the Bank does not charge any fee for the use of the Mobile Banking App nor the Website. However, the Customer will be</p>

客戶重要通知

Important Notice to Customers



	responsible for the charges associated with using the data service on its Mobile Devices or any other electronic devices. The Customer should check with its network operator for details of the usage fees.	responsible for the charges associated with using the data service on its Mobile Devices or any other electronic devices. The Customer should check with its network operator for details of the usage fees.
--	--	--

The Mobile Banking App

	Original	New
12.11	The Mobile Banking App may only be used on compatible devices as specified by the Bank from time to time. The Bank does not guarantee that any specific device or model will be compatible with the Mobile Banking App. The Customer acknowledges that it is solely responsible for ensuring its Mobile Device meets the minimum requirements. Failure to do so may result in the malfunctioning of the Mobile Banking App.	The Mobile Banking App may only be used on compatible devices as specified by the Bank from time to time. The Bank does not guarantee that any specific device or model will be compatible with the Mobile Banking App. The Customer acknowledges that it is solely responsible for ensuring its Mobile Device meets the minimum requirements <u>and it shall only download the Mobile Banking App and its updates from the official App Store</u> . Failure to do so may result in the malfunctioning of the Mobile Banking App.

The Online Enterprise Banking Services

	Original	New
12.13	Without prejudice and in addition to Clause 58 below, the Bank is, in its absolute discretion, entitled to determine and update or modify from time to time the extent and type of the Online Enterprise Banking Services available to the Customer at any time including, without limitation:	Without prejudice and in addition to Clause <u>12.58</u> below, the Bank is, in its absolute discretion, entitled to determine and update or modify from time to time the extent and type of the Online Enterprise Banking Services available to the Customer at any time including, without limitation:
12.17	It is the Bank's policy to maintain the availability of the Online Enterprise Banking Services for use at all times. However, some functionalities of the	It is the Bank's policy to maintain the availability of the Online Enterprise Banking Services for use at all times. However, some functionalities of the

客戶重要通知

Important Notice to Customers



<p>Online Enterprise Banking Services may not be available outside of normal service hours and the Customer will be notified of these service outages on the Mobile Banking App or the Website (as the case may be). The Bank may also suspend the Online Enterprise Banking Services, including but without limitation where it suspects that there have been any security breaches, for routine or emergency maintenance checks or where the Bank is required to do so in compliance with Regulatory Requirements. The Bank will endeavour to notify the Customer on the Mobile Banking App or the Website (as the case may be) prior to any such service interruption or suspension, unless where it is not practicable or unlawful to provide such prior notice.</p>	<p>Online Enterprise Banking Services may not be available outside of normal service hours and the Customer will be notified of these service outages on the Mobile Banking App or the Website (as the case may be). The Bank may also suspend the Online Enterprise Banking Services (including Mobile Token or the Biometric Credential Authentication Service), including but without limitation where it suspects that there have been any security breaches, for routine or emergency maintenance checks or where the Bank is required to do so in compliance with Regulatory Requirements. The Bank will endeavour to notify the Customer on the Mobile Banking App or the Website (as the case may be) prior to any such service interruption or suspension, unless where it is not practicable or unlawful to provide such prior notice.</p>
--	--

Marketing functions on the Mobile Banking App

	Original	New
12.19	<p>Without limiting Clause 18, the Bank will send the Customer push notifications via the Mobile Banking App regarding general market information, promotional offers or other communications from the Bank. The Customer can turn off this functionality at any time by turning off the push notifications services on its Mobile Devices. The Bank will seek prior consent from the Customer before the sending of push notifications. The</p>	<p>Without limiting Clause 12.18, the Bank will send the Customer push notifications via the Mobile Banking App regarding general market information, promotional offers or other communications from the Bank. The Customer can turn off this functionality at any time by turning off the push notifications services on its Mobile Devices. The Bank will seek prior consent from the Customer before the sending of push notifications. The</p>

客戶重要通知

Important Notice to Customers



	Customer may withdraw this consent at any time by turning off the push notification services on its Mobile Devices.	Customer may withdraw this consent at any time by turning off the push notification services on its Mobile Devices.
12.20	[The social media sharing function in the Mobile Banking App will enable the Customer to share and repost certain information obtained from the Mobile Banking App on the Customer’s accounts on various social media platforms (as designated by the Bank from time to time). This functionality will remain disabled so long as the Customer refrains from clicking on the “sharing” button in respect of any or all of the permitted social media accounts on its Mobile Device. As different Mobile Devices and social media platforms may offer different means to disable the social media sharing function, the Customer should check the settings of its Mobile Devices and its respective social media account for more information. By using the social media sharing function, the Customer acknowledges and accepts that the Customer is solely responsible for any content the Customer shares and reposts via its social media accounts, as well as the comments and remarks the Customer makes in connection therewith. Without limiting Clauses 61 to 64 below, the Bank will not be liable for any losses suffered by the Customer in connection with its use of the social media sharing function. The Customer further agrees and undertakes to forthwith remove any such content, comments and/or remarks	{The social media sharing function in the Mobile Banking App will enable the Customer to share and repost certain information obtained from the Mobile Banking App on the Customer’s accounts on various social media platforms (as designated by the Bank from time to time). This functionality will remain disabled so long as the Customer refrains from clicking on the “sharing” button in respect of any or all of the permitted social media accounts on its Mobile Device. As different Mobile Devices and social media platforms may offer different means to disable the social media sharing function, the Customer should check the settings of its Mobile Devices and its respective social media account for more information. By using the social media sharing function, the Customer acknowledges and accepts that the Customer is solely responsible for any content the Customer shares and reposts via its social media accounts, as well as the comments and remarks the Customer makes in connection therewith. Without limiting Clauses <u>12.61</u> to <u>12.64</u> below, the Bank will not be liable for any losses suffered by the Customer in connection with its use of the social media sharing function. The Customer further agrees and undertakes to forthwith remove any such content, comments and/or

客戶重要通知

Important Notice to Customers



<p>disseminated via its social media accounts using the social media sharing function in the Mobile Banking App upon the request of the Bank in circumstances where the Bank reasonably determines that any such content, comments and/or remarks may be unlawful, inaccurate, misleading, inappropriate or prejudicial to the interests of the Bank in any respect. Currently, the social media sharing function in the Mobile Banking App can only be accessed in restricted mode and on designated mobile devices, the Bank will roll out the full version of the social media sharing function gradually.]</p>	<p>remarks disseminated via its social media accounts using the social media sharing function in the Mobile Banking App upon the request of the Bank in circumstances where the Bank reasonably determines that any such content, comments and/or remarks may be unlawful, inaccurate, misleading, inappropriate or prejudicial to the interests of the Bank in any respect. Currently, the social media sharing function in the Mobile Banking App can only be accessed in restricted mode and on designated mobile devices, the Bank will roll out the full version of the social media sharing function gradually.}]</p>
--	---

Appointment of Authorised Representative(s)

	Original	New
12.22	<p>If the Customer has more than one Authorised Representative, each of the Authorised Representatives will be given a unique User Name, Customer Number, Password and Security Device. The Bank will provide the respective sets of User Name, Customer Number, initial Password and Security Device to the Master, who shall be responsible for delivering the respective sets of User Name, Customer Number, initial Password and Security Devices to each of the nominated Authoriser(s) and/or Maker(s).</p>	<p>If the Customer has more than one Authorised Representative, each of the Authorised Representatives will be given <u>assigned</u> a unique User Name and Customer Number Password and Security Device. The Bank will provide the respective sets of User Name, and Customer Number initial Password and Security Device to the Master <u>Customer</u>, who shall be responsible for delivering the respective sets of User Name, and Customer Number, initial Password and Security Devices to each of the nominated <u>Master(s)</u>, Authoriser(s) and/or Maker(s).</p>

Instructions to the Bank

	Original	New
--	----------	-----

客戶重要通知

Important Notice to Customers



12.24	<p>The Bank will receive and act on Instructions with respect to the Customer's account(s) or other relationships or matters with the Bank, subject always to the following:</p> <p>a) the Bank shall ensure that before carrying out any Instruction, the Instruction is authenticated by the Bank through checking any one or more of the Customer's User Name, Customer Number, Password, Security Code and (if applicable) Biometric Credentials under the Biometric Credential Authentication Service (collectively, "Identity Verification Information"), but without the obligation to carry out any further inquiry, authentication or other steps as to the authority of person who submitted the Instruction;</p>	<p>The Bank will receive and act on Instructions with respect to the Customer's account(s) <u>Account(s)</u> or other relationships or matters with the Bank, subject always to the following:</p> <p>(a) the Bank shall ensure that before carrying out any Instruction, the Instruction is authenticated by the Bank through checking any one or more of the Customer's User Name, Customer Number, Password, Security Code, <u>(if applicable) Mobile Token Password under the Mobile Token</u> and (if applicable) Biometric Credentials under the Biometric Credential Authentication Service (collectively, "Identity Verification Information"), but without the obligation to carry out any further inquiry, authentication or other steps as to the authority of person who submitted the Instruction;</p>
-------	--	--

Security measures

	Original	New
12.29	<p>(a) changing its Password on a regular basis and refraining from disclosing its Password to any person who is not authorised to have access to the Password, including any member or officer of the Bank;</p> <p>(b) refraining from selecting any Password which has been used before, or which is likely to be guessed by anyone attempting to access the Online Enterprise Banking</p>	<p>(a) changing its Password <u>or Mobile Token Password (where applicable)</u> on a regular basis and refraining from disclosing its Password <u>or Mobile Token Password (where applicable)</u> to any person who is not authorised to have access to the Password <u>or the Mobile Token Password (where applicable)</u>, including any member or officer of the Bank;</p> <p>(b) refraining from selecting any Password <u>or any Mobile Token</u></p>

客戶重要通知

Important Notice to Customers



<p>Services. For example, an Authorised Representative should not choose a birthday or telephone number as a Password;</p> <p>(c) destroying any correspondence from the Bank concerning the Password as soon as possible;</p> <p>(d) informing the Bank immediately if the Customer or any Authorised Representative is aware of or suspects that anyone has access to its Password, Security Code or Security Device. The Online Enterprise Banking Services will be suspended immediately until a new Password has been set up;</p> <p>(e) never leaving a device or Mobile Device unattended, once the Customer has logged onto the Online Enterprise Banking Services nor allow others to use the Mobile Device and/ or any other electronic device until the Customer has logged out of the Online Enterprise Banking Services;</p> <p>(f) refraining from logging in to the Online Enterprise Banking Services on device or Mobile Device connected to a local area network or public terminal, without ensuring that no third parties can observe or copy a Customer's access. This includes being vigilant while logging into the Online Enterprise Banking Services via the Mobile Device and/or any other electronic device</p>	<p><u>Password (where applicable)</u> which has been used before, or which is likely to be guessed by anyone attempting to access the Online Enterprise Banking Services. For example, an Authorised Representative should not choose a birthday or telephone number as a Password <u>or a Mobile Token Password (where applicable)</u>;</p> <p>(c) destroying any correspondence from the Bank concerning the Password as soon as possible;</p> <p>(d) informing the Bank immediately if the Customer or any Authorised Representative is aware of or suspects that anyone has access to its Password, <u>Mobile Token Password (where applicable)</u>, Security Code, <u>Mobile Token</u> or Security Device. The Online Enterprise Banking Services will be suspended immediately until a new Password <u>or a new Mobile Token Password (where applicable)</u> has been set up;</p> <p>(e) <u>changing the Password and the Mobile Token Password (if applicable) immediately if the Customer suspects that it has been deceived by any fraudulent website, mobile application, email or SMS/WAP push message (for example, if the Customer fails to log on to the Mobile Banking App after using the correct Biometric Credentials, with or without any alert messages)</u>;</p> <p>(f) never leaving a device or Mobile Device unattended, once the Customer has logged onto the</p>
--	--

客戶重要通知

Important Notice to Customers



<p>available at any of the Bank's branches or any other public areas;</p> <p>(g) informing the Bank if any Authorised Representative leaves its employment, and revoking its mandate to act on behalf of the Customer. The Customer must ensure that these individuals do not have access to the Online Enterprise Banking Services;</p> <p>(h) ensuring that the computer system, Mobile Device and/ or any other electronic device used for accessing the Online Enterprise Banking Service has the latest security patches and that all reasonably practicable measures are taken to ensure that any device used to access the Online Enterprise Banking Service is free from any computer virus or other such malware;</p> <p>(i) informing the Bank immediately if a Security Device is not working, or there are any problems with logging onto the Online Enterprise Banking Services; and</p> <p>(j) complying with all other security safeguards as set out and updated from time to time on the Website, the Mobile Banking App and in the User Guide.</p>	<p>Online Enterprise Banking Services nor allow others to use the Mobile Device and/ or any other electronic device until the Customer has logged out of the Online Enterprise Banking Services;</p> <p>(g) refraining from logging in to the Online Enterprise Banking Services on device or Mobile Device connected to a local area network or public terminal, without ensuring that no third parties can observe or copy a Customer's access. This includes being vigilant while logging into the Online Enterprise Banking Services via the Mobile Device and/or any other electronic device available at any of the Bank's branches or any other public areas;</p> <p>(h) informing the Bank if any Authorised Representative leaves its employment, and revoking its mandate to act on behalf of the Customer. The Customer must ensure that these individuals do not have access to the Online Enterprise Banking Services;</p> <p>(i) ensuring that the computer system, Mobile Device and/ or any other electronic device used for accessing the Online Enterprise Banking Service has the latest security patches and that all reasonably practicable measures are taken to ensure that any device used to access the Online Enterprise Banking Service is free from any computer virus or other such malware;</p> <p>(j) informing the Bank immediately if a Security Device or a Mobile</p>
--	--

客戶重要通知

Important Notice to Customers



		<p>Token is not working, or there are any problems with logging onto the Online Enterprise Banking Services; and</p> <p>(k) referring to and complying with all other security safeguards as set out and updated from time to time on the Website, the Mobile Banking App and in the User Guide.</p> <p>The Customer may be held liable for the losses if it has failed to comply with any of the above safeguards.</p>
12.30	The Customer agrees to hold the Bank, its affiliates and/or its licensees (as applicable) fully indemnified against all losses, damages, costs and expenses (including professional and legal costs) if any person other than the Customer gains access to or acquires knowledge of the Customer's Identity Verification Information. The Bank will not be responsible for any losses arising out of any unauthorised transactions except due to any causes set out in Clause 61.	The Customer agrees to hold the Bank, its affiliates and/or its licensees (as applicable) fully indemnified against all losses, damages, costs and expenses (including professional and legal costs) if any person other than the Customer gains access to or acquires knowledge of the Customer's Identity Verification Information. The Bank will not be responsible for any losses arising out of any unauthorised transactions except due to any causes set out in Clause 12.61 .
12.31	The Bank may, in its sole discretion, require the Customer to use a Security Code to access the Online Enterprise Banking Services or give certain types of Instructions. It is the sole responsibility of the Customer to make a request for a Security Device.	The Bank may, in its sole discretion, require the Customer to use a Security Code to access the Online Enterprise Banking Services or give certain types of Instructions. It is the sole responsibility of the Customer to make a request for a Security Device or to set up a Mobile Token .
12.32	Any Security Device shall remain the property of the Bank and shall be returned to the Bank or disposed of in accordance with the Bank's instructions upon termination of the Online Enterprise Banking Services.	Any The Security Device or Mobile Token (where applicable) shall remain the property of the Bank and shall (in the case of the Security Token) be immediately returned to the Bank or disposed of in accordance with the Bank's

客戶重要通知

Important Notice to Customers



		instructions <u>or (in the case of the Mobile Token) be deregistered or otherwise disabled immediately</u> upon termination of the Online Enterprise Banking Services.
12.33	The Customer shall use the Security Device in a proper manner and not change, tamper or modify the Security Device without the Bank's prior written consent or cause any loss or damage to the Security Device. The Customer shall notify the Bank as soon as reasonably practicable after becoming aware of any loss, damage, corruption, compromise or failure of the Security Device. The Bank shall not be liable for any loss incurred by the Customer in connection with any loss, damage, corruption, compromise, failure, defect, malfunctioning or breakdown of the Security Device.	The Customer shall use the Security Device <u>or the Mobile Token (where applicable)</u> in a proper manner. <u>The Customer shall and</u> not change, tamper or modify the Security Device <u>nor interfere with, manipulate, damage, disrupt or reverse-engineer the Mobile Token (where applicable)</u> without the Bank's prior written consent or cause any loss or damage to the Security Device <u>and the Mobile Token (where applicable)</u> . The Customer shall notify the Bank as soon as reasonably practicable after becoming aware of any loss, damage, corruption, compromise, <u>unauthorised use</u> or failure of the Security Device <u>and/or the Mobile Token</u> . The Bank shall not be liable for any loss incurred by the Customer in connection with any loss, damage, corruption, compromise, failure, defect, malfunctioning or breakdown of the Security Device, <u>the Mobile Device or the Mobile Token</u> .

Biometric Credential

Authentication Service

Mobile Token and Biometric

Credential Authentication Service

	Original	New
12.34	Further terms and conditions of services in relation to biometric credential authentication for accessing the Mobile Banking App are set out in Annex 1 (Terms and Conditions for Biometric Credential Authentication Service) to	Further terms and conditions of services in relation to <u>the biometric credential authentication for</u> accessing <u>of</u> the Mobile Banking App <u>via the Mobile Token and/or the Biometric Credential Authentication Service</u> are set out in <u>Annex 1 (the</u>

客戶重要通知

Important Notice to Customers



	these Terms.	<i>Terms and Conditions for <u>Mobile Token and Biometric Credential Authentication Service</u> to these Terms.</i>
--	--------------	---

Data Collection

	Original	New
12.36	By using the Mobile Banking App, the Website or any of the Online Enterprise Banking Services, the Customer consents to the Bank, its affiliates and/or its licensees' collecting and using the location of its Mobile Devices and/or any other electronic device and technical information such as IP address, advertising ID, unique device identifier, and device type, information about the operating system and application software used on its Mobile Device and/or any other electronic device and other non-personal information, related software, hardware and peripherals for the Online Enterprise Banking Services in the Mobile Banking App or the Website that are internet-based or wireless to facilitate the Bank, its affiliates and/or its licensees in improving its products and services to the Customer.	By using the Mobile Banking App, the Website, <u>the Mobile Token</u> or any of the Online Enterprise Banking Services, the Customer consents to the Bank, its affiliates and/or its licensees' collecting and using the location of its Mobile Devices and/or any other electronic device and technical information such as IP address, advertising ID, unique device identifier, and device type, information about the operating system and application software used on its Mobile Device and/or any other electronic device and other non-personal information, related software, hardware and peripherals for the Online Enterprise Banking Services in the <u>Mobile Token, the</u> Mobile Banking App or the Website that are internet-based or wireless to facilitate the Bank, its affiliates and/or its licensees in improving its products and services to the Customer.
12.42	The Customer further acknowledges and consents that its personal data and information will be collected, stored, accessed, used and handled for the purposes described in Clause 41. The Customer further acknowledges that, should it decide to withdraw its consent to such personal data or information collection, the Customer may change	The Customer further acknowledges and consents that its personal data and information will be collected, stored, accessed, used and handled for the purposes described in Clause <u>12.41</u> . The Customer further acknowledges that, should it decide to withdraw its consent to such personal data or information collection, the Customer

客戶重要通知

Important Notice to Customers



	<p>the settings on its Mobile Devices and/or any other electronic device. The Customer understands that as a result of the withdrawal of its consent, it may not be able to use certain function(s) of the Mobile Banking App and/or the Website.</p>	<p>may change the settings on its Mobile Devices and/or any other electronic device. The Customer understands that as a result of the withdrawal of its consent, it may not be able to use certain function(s) of the Mobile Banking App and/or the Website.</p>
--	---	--

The Customer's responsibilities

	Original	New
12.47	(a) not to use the Mobile Banking App, the Website and the Online Enterprise Banking Services in any way that breaches any applicable Regulatory Requirements, including all technology control or export laws and regulations that apply to the technology used or supported by the Mobile Banking App, the Website or any Online Enterprise Banking Services (“ Technology ”);	(a) not to use the Mobile Banking App, the Website and the Online Enterprise Banking Services <u>(including the access via the Mobile Token and/or the Biometric Credential Authentication Service)</u> in any way that breaches any applicable Regulatory Requirements, including all technology control or export laws and regulations that apply to the technology used or supported by the Mobile Banking App, the Website, <u>the Mobile Token, the Biometric Credential Authentication Service</u> or any Online Enterprise Banking Services (“ Technology ”);
12.47	(h) not to use the Mobile Banking App, the Website or the Online Enterprise Banking Services in any unlawful manner, for any unlawful purpose, or in any manner inconsistent with these Terms, or act fraudulently or maliciously, including but without limitation to hacking into the Mobile Banking App, the Website or any operating system;	(h) not to use the Mobile Banking App, the Website, <u>the Mobile Token, the Biometric Credential Authentication Service</u> or the Online Enterprise Banking Services in any unlawful manner, for any unlawful purpose, or in any manner inconsistent with these Terms, or act fraudulently or maliciously, including but without lim12.47itation to hacking into the Mobile Banking App, the Website or any operating system;

客戶重要通知

Important Notice to Customers



12.47	(i) not infringe the Bank's intellectual property rights or those of any third party in relation to its use of the Mobile Banking App, the Website or any Online Enterprise Banking Services (to the extent that such use is not licensed by these Terms);	(i) not infringe the Bank's intellectual property rights or those of any third party in relation to its use of the Mobile Banking App, the Website, the Mobile Token , the Biometric Credential Authentication Service or any Online Enterprise Banking Services (to the extent that such use is not licensed by these Terms);
12.47	(k) not to transmit any data, send or upload any material that contains viruses, Trojan horses, worms, time-bombs, keystroke loggers, spyware, adware or any other harmful programs or similar computer code designed to adversely affect the operation of the Mobile Banking App, the Website, any Online Enterprise Banking Services or any operating system;	(k) not to transmit any data, send or upload any material that contains viruses, Trojan horses, worms, time-bombs, keystroke loggers, spyware, adware or any other harmful programs or similar computer code designed to adversely affect the operation of the Mobile Banking App, the Website, the Mobile Token , the Biometric Credential Authentication Service , any Online Enterprise Banking Services or any operating system;
12.47	(l) not use the Mobile Banking App, the Website or any Online Enterprise Banking Services in a way that could damage, disable, overburden, impair or compromise the Bank's systems or security or interfere with other users;	(l) not use the Mobile Banking App, the Website, the Mobile Token , the Biometric Credential Authentication Service or any Online Enterprise Banking Services in a way that could damage, disable, overburden, impair or compromise the Bank's systems or security or interfere with other users;
12.47	(n) not to access without authority, interfere with, manipulate, damage or disrupt: (i) any part of the Mobile Banking App nor the Website; (ii) any device, Mobile Device or	(n) not to access without authority, interfere with, manipulate, damage or disrupt: (i) any part of the Mobile Banking App nor the Website; (ii) any device, Mobile Device or network on which the Mobile Banking App or the Website is

客戶重要通知

Important Notice to Customers



	<p>network on which the Mobile Banking App or the Website is stored;</p> <p>(iii) any software used in the provision of the Mobile Banking App or the Website; or</p> <p>(iv) any device, Mobile Device or network or software owned or used by any third party.</p>	<p>stored;</p> <p>(iii) <u>the Mobile Token or any software used in the provision of the Mobile Banking App or the Website;</u> or</p> <p>(iv) any device, Mobile Device or network or software owned or used by any third party.</p>
12.48	(c) the Customer becomes aware of any of the acts mentioned in Clause 47 being done or attempted by any person;	(c) the Customer becomes aware of any of the acts mentioned in Clause <u>12.47</u> being done or attempted by any person;
12.48		<u>If the Customer fails to report such incidents to the Bank as soon as reasonably practicable, or has otherwise acted fraudulently or with gross negligence, the Customer may be held responsible for all such transactions and all direct losses as a result.</u>
12.49	The Customer acknowledges that the Online Enterprise Banking Services, the Website, the Mobile Banking App and the software comprised in them, are proprietary to the Bank. Where the Bank has reasonable ground to suspect that the Customer has breached any of its warranties and undertakings in these Terms (including Clause 47), the Customer agrees that the Bank shall be entitled to close any or all of the account(s) maintained by the Customer with the Bank immediately without notice to the Customer and take legal action against the Customer. The Customer undertakes to notify the Bank	The Customer acknowledges that the Online Enterprise Banking Services, the Website, the Mobile Banking App, <u>the Mobile Token</u> and the software comprised in them, are proprietary to the Bank. Where the Bank has reasonable ground to suspect that the Customer has breached any of its warranties and undertakings in these Terms (including Clause <u>12.47</u>), the Customer agrees that the Bank shall be entitled to close any or all of the account(s) maintained by the Customer with the Bank immediately without notice to the Customer and take legal action against the Customer. The

客戶重要通知

Important Notice to Customers



	immediately if the Customer becomes aware that any of the actions described above in Clause 47 is being perpetrated by any other person.	Customer undertakes to notify the Bank immediately if the Customer becomes aware that any of the actions described above in Clause <u>12.47</u> is being perpetrated by any other person.
12.50	The Customer acknowledges that the communication facilities adopted by the Bank (including the Internet) for the purpose of the transmission or communication of instructions or any information through the Online Enterprise Banking Services, the Website and the Mobile Banking App may be unreliable or unavailable at any time, causing interruption, delay, corruption or loss of data, the loss of confidentiality in the transmission of data, or the transmission of malware may occur when transmitting data via such communication facilities. Also, transmission or communication of instructions or any information through the Online Enterprise Banking Services, the Website and the Mobile Banking App between the Customer and the Bank may be delayed as a result of a range of factors, including but without limitation to time zone differences, public holidays in Hong Kong SAR or overseas, or other reasons beyond the control of the Bank, and the Bank should not be liable for such delay or any interest thereon (if any). The Customer accepts all risks arising from its acceptance of any of the Online Enterprise Banking Services made available by the Bank, including but not limited to, any loss suffered as a result of any delay, error or omission of	The Customer acknowledges that the communication facilities adopted by the Bank (including the Internet) for the purpose of the transmission or communication of instructions or any information through the Online Enterprise Banking Services (including the access via the Mobile Token and/or the Biometric Credential Authentication Service), the Website and the Mobile Banking App may be unreliable or unavailable at any time, causing interruption, delay, corruption or loss of data, the loss of confidentiality in the transmission of data, or the transmission of malware may occur when transmitting data via such communication facilities. Also, transmission or communication of instructions or any information through the Online Enterprise Banking Services, the Website and the Mobile Banking App between the Customer and the Bank may be delayed as a result of a range of factors, including but without limitation to time zone differences, public holidays in Hong Kong SAR or overseas, or other reasons beyond the control of the Bank, and the Bank should not be liable for such delay or any interest thereon (if any). The Customer accepts all risks arising from its acceptance of any of the Online Enterprise Banking Services (including

客戶重要通知

Important Notice to Customers



	transmission and communication of instructions or any information through the Online Enterprise Banking Services between the Customer and the Bank.	the access via the Mobile Token and/or the Biometric Credential Authentication Service) made available by the Bank, including but not limited to, any loss suffered as a result of any delay, error or omission of transmission and communication of instructions or any information through the Online Enterprise Banking Services between the Customer and the Bank.
12.52	The Customer's use of the Mobile Banking App, the Website and the Online Enterprise Banking Services is wholly at its own risk. The Mobile Banking App, the Website and the Online Enterprise Banking Services are provided on an "as is" basis. To the fullest extent permitted by the Regulatory Requirements, the Bank disclaims all conditions, warranties (including, but not limited to, any warranties of merchantability, fitness for a particular purposes, accuracy and non-infringement of third party rights), representations or other terms which may apply to the Mobile Banking App, the Website and the Online Enterprise Banking Services, whether express or implied.	The Customer's use of the Mobile Banking App, the Website, the Mobile Token and the Online Enterprise Banking Services is wholly at its own risk. The Mobile Banking App, the Website, the Mobile Token and the Online Enterprise Banking Services are provided on an "as is" basis. To the fullest extent permitted by the Regulatory Requirements, the Bank disclaims all conditions, warranties (including, but not limited to, any warranties of merchantability, fitness for a particular purposes, accuracy and non-infringement of third party rights), representations or other terms which may apply to the Mobile Banking App, the Website, the Mobile Token and the Online Enterprise Banking Services, whether express or implied.

Intellectual property rights and information ownership

	Original	New
12.57	(a) all intellectual property rights (including but not limited to trade marks, logos and service marks) in the Mobile Banking App, the Website, the Online Enterprise	(a) all intellectual property rights (including but not limited to trade marks, logos and service marks) in the Mobile Banking App, the Website, the Mobile Token , the

客戶重要通知

Important Notice to Customers



	Banking Services and the Technology anywhere in the world belong to the Bank or its licensors;	Online Enterprise Banking Services and the Technology anywhere in the world belong to the Bank or its licensors;
	(b) the Mobile Banking App and the Website are licensed (and not sold) to the Customer for use only, as such the Customer has no rights in, or to, the Mobile Banking App, the Website, the Online Enterprise Banking Services or the Technology other than the right to use each of them in accordance with these Terms;	(b) the Mobile Banking App and the Website are licensed (and not sold) to the Customer for use only, as such the Customer has no rights in, or to, the Mobile Banking App, the Website, the Mobile Token , the Online Enterprise Banking Services or the Technology other than the right to use each of them in accordance with these Terms;

Service availability and termination

	Original	New
12.58	Subject to Regulatory Requirements, the Online Enterprise Banking Services may be suspended, terminated, withdrawn or amended by the Bank at any time without prior notice or providing any reason. Subject to Regulatory Requirement applicable to the Bank, the Bank is under no obligation to continuously provide the Online Enterprise Banking Services. The Bank may, in its absolute discretion, suspend the Customer's use of the Online Enterprise Banking Services or any part of it, or suspend the Customer's access to the Online Enterprise Banking Services without prior notice as the Bank considers appropriate. The Bank's decision in this regard is final and binding on the Customer. The Bank will not be responsible for any loss or damage	Subject to Regulatory Requirements, the Online Enterprise Banking Services (including its access via the Mobile Token and/or the Biometric Credential Authentication Service) may be suspended, terminated, withdrawn or amended by the Bank at any time without prior notice or providing any reason. Subject to Regulatory Requirement applicable to the Bank, the Bank is under no obligation to continuously provide the Online Enterprise Banking Services (including its access via the Mobile Token and/or the Biometric Credential Authentication Service) . The Bank may, in its absolute discretion, suspend the Customer's use of the Online Enterprise Banking Services or any part of it, or suspend the Customer's access to the Online Enterprise Banking Services without

客戶重要通知

Important Notice to Customers



	suffered by the Customer arising from such decisions.	prior notice as the Bank considers appropriate. The Bank's decision in this regard is final and binding on the Customer. The Bank will not be responsible for any loss or damage suffered by the Customer arising from such decisions.
12.59	(a) the Customer does not activate the Online Enterprise Banking Services after 60 days of receipt of the Security Device from the Bank or such other period as prescribed by the Bank;	(a) the Customer does not activate the Online Enterprise Banking Services after 60 days <u>from our notification of receipt of the Security Device from the Bank</u> or such other period as prescribed by the Bank;
12.60	Without limiting Clause 7, these Terms can be terminated by the Customer by giving prior notice to the Bank in the form and by means specified by the Bank from time to time. The Customer agrees that any notice of termination originated from the Customer will only become effective when the Bank confirms the termination. Any suspension or termination of the Online Enterprise Banking Services will not affect any of the rights or obligations which may have accrued on or before the date of suspension or termination, and the provisions of these Terms will continue to bind the Customer after the termination of these Terms to the extent that they relate to any obligations or liabilities of the Customer which remain to be performed or discharged.	Without limiting Clause <u>12.7</u> , these Terms can be terminated by the Customer by giving prior notice to the Bank in the form and by means specified by the Bank from time to time. The Customer agrees that any notice of termination originated from the Customer will only become effective when the Bank confirms the termination. Any suspension or termination of the Online Enterprise Banking Services will not affect any of the rights or obligations which may have accrued on or before the date of suspension or termination, and the provisions of these Terms will continue to bind the Customer after the termination of these Terms to the extent that they relate to any obligations or liabilities of the Customer which remain to be performed or discharged.

The Bank's rights and limitation of liability

	Original	New
--	----------	-----

客戶重要通知

Important Notice to Customers



12.61	Subject to Clauses 62 and 63 below, the Bank will only be liable where the Customer has suffered direct losses from its use of the Online Enterprise Banking Services and such losses are attributable to the gross negligence, fraud or wilful misconduct of the Bank.	Subject to Clauses 12.62 and 12.63 below, the Bank will only be liable where the Customer has suffered direct losses from its use of the Online Enterprise Banking Services and such losses are attributable to the gross negligence, fraud or wilful misconduct of the Bank.
12.62	Without prejudice to Clause 58 above, the Bank reserves the right to vary, cancel, terminate or suspend the whole or any part of the Online Enterprise Banking Services without giving notice or reason. The Customer agrees that, to the fullest extent permissible under the Regulatory Requirement applicable to the Bank, in the absence of gross negligence, fraud or wilful misconduct, neither the Bank, nor any of its officers or employees shall be liable for any loss, damage, cost or expense of any kind which the Customer or any other person may incur or suffer in connection with the Bank's exercise of the above mentioned right.	Without prejudice to Clause 12.58 above, the Bank reserves the right to vary, cancel, terminate or suspend the whole or any part of the Online Enterprise Banking Services without giving notice or reason. The Customer agrees that, to the fullest extent permissible under the Regulatory Requirement applicable to the Bank, in the absence of gross negligence, fraud or wilful misconduct, neither the Bank, nor any of its officers or employees shall be liable for any loss, damage, cost or expense of any kind which the Customer or any other person may incur or suffer in connection with the Bank's exercise of the above mentioned right.
12.63	In addition to Clause 62 above, the Bank will not be liable to the Customer for any loss or damages from the Customer's use of the Online Enterprise Banking Services in the instances including, without limitation:	In addition to Clause 12.62 above, the Bank will not be liable to the Customer for any loss or damages from the Customer's use of the Online Enterprise Banking Services in the instances including, without limitation:
12.63	(a) any interruption, delay, suspension, interception, loss or other failure in the Bank providing the Online Enterprise Banking Services, in transmitting any Instructions or information via the Online Enterprise Banking Services, which are beyond the reasonable control	(a) any interruption, delay, suspension, interception, loss or other failure in the Bank providing the Online Enterprise Banking Services (including its access via the Mobile Token and/or the Biometric Credential Authentication Service) , in transmitting any Instructions or

客戶重要通知

Important Notice to Customers



	<p>of the Bank, including, without limitation, failures of communication networks, systems, any act or omission of third party providers, breakdown of equipment or any government order;</p>	<p>information via the Online Enterprise Banking Services, which are beyond the reasonable control of the Bank, including, without limitation, failures of communication networks, systems, any act or omission of third party providers, breakdown of equipment or any government order;</p>
--	---	---

Annex 1— Terms and Conditions for [Mobile Token and Biometric Credential Authentication Service](#) (“Annex 1”)

Original	New
	<p>This Annex 1 is the Terms and Conditions for Mobile Token and Biometric Credential Authentication Service referred to in clause 12.34 of the Specific Terms and Conditions for Online Enterprise Banking Services, as the same may be amended from time to time.</p>

General

Original	New
<p>1 This Annex 1 applies to Customers who use the Biometric Credential Authentication Service (as defined in Clause 3 in this Annex) made available by the Bank</p>	<p>1 This Annex 1 applies to Customers who use (1) the Mobile Token and/or (2) the Biometric Credential Authentication Service (each as defined in Clause 3 in this Annex 1) made available by the Bank.</p>
<p>2 This Annex 1 is in addition and supplemental to the Terms. For the avoidance of doubt, in the event that there is any inconsistency between the provisions set out in this Annex 1 and the provisions set out in other parts of the Terms, this Annex 1 shall prevail in relation to the Biometric Credential Authentication Service.</p>	<p>2 This Annex 1 is in addition and supplemental to the Specific Terms and Conditions for Online Enterprise Banking Services (the “Terms”). For the avoidance of doubt, in the event that there is any inconsistency between the provisions set out in this Annex 1 and the provisions set out in other parts of the Terms, this Annex 1 shall prevail in</p>

客戶重要通知

Important Notice to Customers



		relation to the Mobile Token and the Biometric Credential Authentication Service .
--	--	--

Definitions and Interpretation

Original		New	
5	“Permitted Mobile Device” means any Mobile Device which the Bank may permit for use with the Biometric Credential Authentication Service from time to time, including, without limitation, the operating system or software that the Mobile Device operates on.	5	“Permitted Mobile Device” means any Mobile Device which the Bank may permit for use with the Mobile Token and/or Biometric Credential Authentication Service from time to time, including, without limitation, the operating system or software that the Mobile Device operates on.
5		5	<p>“Mobile Token” means a feature in-built within and linked to the Mobile Banking App which is used to generate a Security Code or otherwise to authenticate and grant the Customer access to and/or use of any Online Enterprise Banking Services.</p> <p>“Mobile Token Password” means the personal identification number self-selected and designated by the Customer for the purpose of utilizing the Mobile Token.</p>
5	Please visit “Settings and Others” > “Manage Biometric Credential Authentication” > [“Biometric Credential Authentication Service FAQ”] for the current list of such Permitted Mobile Devices.	6	Please visit https://www.asia.ccb.com/hongkong/doc/commercial/faq_oeps_mb.pdf “Settings and Others” > “Manage Biometric Credential Authentication” > [“Biometric Credential Authentication Service FAQ”] for the current list of such Permitted Mobile Devices.

客戶重要通知

Important Notice to Customers



~~Provision of Biometric Credential Authentication Service Eligibility~~

Original		New	
7	To use the Biometric Credential Authentication Service, the Customer must have:	7	To use the Mobile Token and/or the Biometric Credential Authentication Service (if applicable) , the Customer must have:
	(c) installed the Mobile Banking App where the Bank offers the Biometric Credential Authentication Service and latest updates on the Customer's Permitted Mobile Device;		(c) installed the Mobile Banking App where the Bank offers the Mobile Token and Biometric Credential Authentication Service and latest updates on the Customer's Permitted Mobile Device;
7	(d) a Permitted Mobile Device with the biometric authentication function enabled;	7	(d) (only applicable to Biometric Credential Authentication Service) a Permitted Mobile Device with the biometric authentication function enabled;
7	(e) registered at least one of the Customer's Biometric Credentials to control access to the Permitted Mobile Device; and	7	(e) (only applicable to Biometric Credential Authentication Service) registered at least one of the Customer's Biometric Credentials to control access to the Permitted Mobile Device; and
7	(f) activated the Biometric Credential Authentication Service according to the Bank's activation instructions using the Customer's Identity Verification Information and a one-time Password sent by the Bank to the Customer.	7	(f) set up and activated the Mobile Token and Biometric Credential Authentication Service (if applicable) according to the Bank's activation instructions using the Customer's Identity Verification Information and a one-time Password sent by the Bank to the Customer.
8	To facilitate the provision of the Biometric Credential Authentication Service, the Customer agrees that the Bank may require the Customer to execute such forms and/or documents,	8	To facilitate the provision of the Mobile Token and Biometric Credential Authentication Service, the Customer agrees that the Bank may require the Customer to execute such forms and/or

客戶重要通知

Important Notice to Customers



	provide such information and perform such acts as the Bank may consider reasonably necessary.		documents, provide such information and perform such acts as the Bank may consider reasonably necessary.
		9	<p><u>The Customer acknowledges that the Bank may, at its discretion, from time to time prescribe updates to the Mobile Banking App or the Website and their in-built features which must be installed in order to enable the proper functioning of the Mobile Banking App, the Mobile Token and the Biometric Credential Authentication Service. The Customer acknowledges that it is the Customer's sole responsibility to update the Mobile Banking App and/or access the latest updated version of the Website to access the Online Enterprise Banking Services using the Mobile Token and/or the Biometric Credential Authentication Service and the Bank shall not be liable to the Customer for any loss or damage caused to the Customer due to its inability to access any Online Enterprise Banking Services if the Customer fails to (A) install any required updates to the Mobile Banking App or (B) access the latest version of the Website. Notwithstanding the foregoing, the Bank does not represent or warrant that the Mobile Token and/or the Biometric Credential Authentication Service will be available at all times, be compatible with any particular device or model, software or other online banking services that the Bank may offer from time to time. The Customer shall be responsible for ensuring that the Customer's Mobile Device is a Permitted Mobile Device</u></p>

客戶重要通知

Important Notice to Customers



		<p>which meets any compatibility requirements. Failure to do so may result in malfunctioning of the Mobile Token or the Biometric Credential Authentication Service.</p>
--	--	--

Provision of Mobile Token

Original		New	
		10	<p>The Mobile Token is a digital security token which is offered by the Bank to Customers for the Customer as one of the means to authenticate his or her identity for accessing and/or using the Online Enterprise Banking Services on the Mobile Banking App. Customer may set up its Mobile Token on any Permitted Mobile Device by:</p> <ul style="list-style-type: none"> (a) logging on to the Mobile Banking App and accepting all applicable terms and conditions for the set-up and use of the Mobile Token; (b) entering a Security Code which will be sent to the Customer at his or her designated mobile number registered with the Bank; (c) designating a Mobile Token Password, (d) (only applicable to Biometric Credential Authentication Service) applying the Customer's Biometric Credentials for authentication purposes; and (e) (only applicable to Biometric Credential Authentication Service) where the Customer's Mobile Device carries a biometric authentication function and if the Customer has

客戶重要通知

Important Notice to Customers



		<p>agreed to the terms and conditions under this Annex 1, enabling access to and use of the Mobile Token via the Biometric Credential Authentication Service, or otherwise in accordance with any other steps or instructions as may be prescribed by the Bank from time to time.</p>
	<p>11</p>	<p>Set up and activation of the Mobile Token involves the creation and storing of a digital security token in the Permitted Mobile Device. The Customer acknowledges that each Mobile Token may only be bound to and activated by only one Mobile Device at a time. Once a Mobile Token is bound, the Permitted Mobile Device will be recognized by the Bank for the purposes of authenticating such Customer's identity on a continuous basis in relation to the access and use of any Online Enterprise Banking Services by such Customer. The Bank shall have no obligation or duty to enquire or verify the identity or authority of any person accessing the Online Enterprise Banking Services via the use of the Mobile Token. Should the Customer wish to terminate its use of the Mobile Token or otherwise to unbind a Permitted Mobile Device, the Customer may only do so by deregistering the Mobile Token from the applicable Permitted Mobile Device under the Online Enterprise Banking Services or otherwise contacting the Bank by calling the Bank's customer hotline posted by the Bank from time to time in the Website or Mobile Banking App for assistance.</p>

客戶重要通知

Important Notice to Customers



		12	The Customer acknowledges that once a Mobile Token is set up and activated, the Security Device of the Customer (unless otherwise requested by the Customer) will be automatically disabled and may no longer be used to access or use any Online Enterprise Banking Services.
--	--	----	--

Provision of Biometric Credential Authentication Service [\(if applicable\)](#)

	Original		New
9	The Customer acknowledges and agrees as follows: (a) once the Biometric Credential Authentication Service is activated, any Biometric Credentials stored on the Customer's Permitted Mobile Device can be used to access the Online Enterprise Banking Services and use of any Mobile Token which the Customer has activated and bound to the Permitted Mobile Device. The Customer further acknowledges and accepts that any person who gains access to the biometric credentials or the biometric authentication controls of the Customer's Permitted Mobile Device will be able to access the Online Enterprise Banking Services, authenticate their use of the Mobile Token (if any) and give Instructions to the Bank in respect of the Customer's accounts, including, without limitation, withdrawing or	13	The Customer acknowledges and agrees as follows, along with the Mobile Token : (a) once the Biometric Credential Authentication Service (if applicable) is activated, any Biometric Credentials stored on the Customer's Permitted Mobile Device can be used to access the Online Enterprise Banking Services and use of any Mobile Token which the Customer has activated and bound to the Permitted Mobile Device. The Customer further acknowledges and accepts that any person who gains access to the biometric credentials or the biometric authentication controls of the Customer's Permitted Mobile Device will be able to access the Online Enterprise Banking Services, authenticate their use of the Mobile Token (if any) and give Instructions to the Bank in

客戶重要通知

Important Notice to Customers



<p>otherwise dealing with the Customer's funds;</p> <p>(b) for the purpose of providing the Biometric Credential Authentication Service, the Mobile Banking App and its in-built features (such as any Mobile Token activated by the Customer) will interface with the biometric authentication function and data on the Customer's Permitted Mobile Device. The Customer consents to the Bank's access and use of such function and data in the Customer's Permitted Mobile Device for the provision of the Biometric Credential Authentication Service;</p> <p>(c) the Bank may, at its discretion, update the Mobile Banking App and its in-built features at any time. The Customer must install the mandatory updates to ensure the proper functioning of the Biometric Credential Authentication Service. Notwithstanding the foregoing, the Bank does not represent or warrant that the Biometric Credential Authentication Service will be available at all times, be compatible with any particular device or model, software or other online banking services that the Bank may offer from time to time. The Customer shall be responsible for ensuring that the Customer's electronic equipment is a Permitted Mobile Device which meets any compatibility requirements. Failure to do so may result in malfunctioning of the</p>	<p>respect of the Customer's accounts, including, without limitation, withdrawing or otherwise dealing with the Customer's funds;</p> <p>(b) for the purpose of providing the Biometric Credential Authentication Service, the Mobile Banking App and its in-built features (such as any Mobile Token activated by the Customer) will interface with the biometric authentication function and data on the Customer's Permitted Mobile Device. The Customer consents to the Bank's access and use of such function and data in the Customer's Permitted Mobile Device for the provision of the Biometric Credential Authentication Service; <u>and</u></p> <p>the Bank may, at its discretion, update the Mobile Banking App and its in-built features at any time. The Customer must install the mandatory updates to ensure the proper functioning of the Biometric Credential Authentication Service. Notwithstanding the foregoing, the Bank does not represent or warrant that the Biometric Credential Authentication Service will be available at all times, be compatible with any particular device or model, software or other online banking services that the Bank may offer from time to time. The Customer shall be responsible for ensuring that the Customer's electronic equipment is a Permitted Mobile Device which meets any compatibility requirements. Failure</p>
--	---

客戶重要通知

Important Notice to Customers



	<p>Biometric Credential Authentication Service;</p> <p>(d) the Customer will register at least one of the Customer's Biometric Credentials to control access to the Permitted Mobile Device; and</p> <p>(e) the Customer will activate the Biometric Credential Authentication Service according to the Bank's activation instructions using the Customer's Identity Verification Information and the one-time Password sent by the Bank to the Customer.</p>	<p>to do so may result in malfunctioning of the Biometric Credential Authentication Service;</p> <p>(c) the Customer will register at least one of the Customer's Biometric Credentials to control access to the Permitted Mobile Device via the Biometric Credential Authentication Service. ; and</p> <p>the Customer will activate the Biometric Credential Authentication Service according to the Bank's activation instructions using the Customer's Identity Verification Information and the one-time Password sent by the Bank to the Customer.</p>
--	---	--

Security

Original		New	
10	<p>The Customer acknowledges that information in relation to the Customer's accounts and/or transaction records may be stored on the Customer's Permitted Mobile Device and the Bank shall have no liability if the stored data is exposed when the Customer's Permitted Mobile Device is used by another person (whether with or without the Customer's authorisation). To protect the Customer's privacy and assets, the Customer agrees to take steps to keep confidential and secure the Customer's Permitted Mobile Device, Passwords, and bank or account related information and to prevent unauthorised use of the</p>	14	<p>The Customer acknowledges that information in relation to the Customer's accounts and/or transaction records may be stored on the Customer's Permitted Mobile Device and the Bank shall have no liability if the stored data is exposed when the Customer's Permitted Mobile Device is used by another person (whether with or without the Customer's authorisation). To protect the Customer's privacy and assets, the Customer agrees to take steps to keep confidential and secure the Customer's Permitted Mobile Device, Mobile Token Password, Passwords, and bank or account related information and to prevent unauthorised use of the</p>

客戶重要通知

Important Notice to Customers



<p>Customer's Permitted Mobile Device, which include, without limitation:</p> <ul style="list-style-type: none"> (a) ensuring that only the Customer's Biometric Credentials are stored on the Customer's Permitted Mobile Device, the Customer's Permitted Mobile Device is securely and safely kept and any Password or Security Code allowing access to altering or adding biometric credentials on the Customer's Permitted Mobile Device is protected. The Bank will not be responsible for any losses arising out of any unauthorised transactions due to the Customer's failure to secure access to the Customer's Permitted Mobile Device; (b) being vigilant of false matches under the facial mapping function. As an alternative, the Customer may choose to use its Identity Verification Information to access the Online Enterprise Banking Services via the Mobile Banking App, or authenticate the Customer's identity for use of the Mobile Token using the Customer's Mobile Token Password; (c) disabling any function provided by, and refraining to consent to any settings of, the Customer's Permitted Mobile Device that would otherwise compromise the security of the use of the biometric authentication (e.g. disabling "attention-aware" feature for facial recognition); (d) ensuring that the Customer's Permitted Mobile Device is locked immediately after use and when it is not in the Customer's possession; 	<p>Customer's Permitted Mobile Device, which include, without limitation:</p> <ul style="list-style-type: none"> (a) ensuring that (in case of the Biometric Credential Authentication Service) only the Customer's Biometric Credentials are stored on the Customer's Permitted Mobile Device, the Customer's Permitted Mobile Device is securely and safely kept and any Password, Mobile Token Password or Security Code allowing access to altering or adding biometric credentials on the Customer's Permitted Mobile Device is protected. The Bank will not be responsible for any losses arising out of any unauthorised transactions due to the Customer's failure to secure access to the Customer's Permitted Mobile Device; (b) being vigilant of false matches under the facial mapping function. As an alternative, the Customer may choose to use its Identity Verification Information to access the Online Enterprise Banking Services via the Mobile Banking App, or authenticate the Customer's identity for use of the Mobile Token using the Customer's Mobile Token Password; (c) disabling any function provided by, and refraining to consent to any settings of, the Customer's Permitted Mobile Device that would otherwise compromise the security of the use of the biometric authentication (e.g. disabling "attention-aware" feature for facial recognition);
--	---

客戶重要通知

Important Notice to Customers



<p>(e) refraining from disclosing or sharing the Customer's Permitted Mobile Device Passwords or Security Codes with any other person or allow any other person's access to the Customer's Biometric Credentials and/or biometric authentication function on the Customer's Permitted Mobile Device;</p> <p>(f) avoiding using easily accessible personal information such as date of birth, telephone number or any recognisable part of the Customer's name in setting any Password or use the same Password to access any other services (for example, to connect to the internet or to access to the Mobile Banking App);</p> <p>(g) avoiding putting down or recording any device Passwords (e.g. the Password of the Mobile Token) or Security Codes without proper safeguard;</p> <p>(h) being vigilant of the Customer's surroundings before entering any Passwords or Security Codes on the Customer's Permitted Mobile Device to ensure their secrecy;</p> <p>(i) regularly changing the Passwords of accessing the Permitted Mobile Device and Biometric Credential Authentication Service (if applicable);</p> <p>(j) changing the Customer's Passwords immediately if the Customer suspects that the Customer has been deceived by a fraudulent website, Mobile Banking App, email, or SMS/WAP push message (for example, where the Customer fails to</p>	<p>(d) ensuring that the Customer's Permitted Mobile Device is locked immediately after use and when it is not in the Customer's possession;</p> <p>(e) refraining from disclosing or sharing the Customer's Permitted Mobile Device Passwords, Mobile Token Passwords or Security Codes with any other person or allow any other person's access to the Customer's Mobile Token and/or Biometric Credentials and/or biometric authentication function on the Customer's Permitted Mobile Device;</p> <p>(f) avoiding using easily accessible personal information such as date of birth, telephone number or any recognisable part of the Customer's name in setting any Password or any Mobile Token Password or use the same Password or the same Mobile Token Password to access any other services (for example, to connect to the internet or to access to the Mobile Banking App);</p> <p>(g) avoiding putting down or recording any device Passwords (e.g. the Password of the Mobile Token) or Security Codes without proper safeguard;</p> <p>(h) being vigilant of the Customer's surroundings before entering any Passwords, Mobile Token Password or Security Codes on the Customer's Permitted Mobile Device to ensure their secrecy;</p> <p>(i) regularly changing the Passwords and Mobile Token Password of accessing the Permitted Mobile Device, the</p>
--	---

客戶重要通知

Important Notice to Customers



<p>logon to the Mobile Banking App with the use of the correct biometric credentials);</p> <p>(k) notifying the Bank as soon as reasonably practicable if it suspects that any of the Customer's Identity Verification Information, any other security codes (including, without limitation, the Password of the Mobile Token) and/or the Permitted Mobile Device have been compromised, lost, stolen, or accessed or used without the Customer's authorisation;</p> <p>(l) strictly adhering to all security advice, measure, guidelines and instructions from time to time provided to the Customer by the Bank and/or the manufacturer of the Customer's Permitted Mobile Device applicable to the Customer's use of its Permitted Mobile Device;</p> <p>(m) notifying the Bank without delay if the Customer changes the Customer's mobile phone number;</p> <p>(n) upon termination of the use of the Mobile Banking App and/or the Mobile Token for any reason, removing the Mobile Banking App and/or the Mobile Token from the Customer's Permitted Mobile Device; and</p> <p>(o) removing the Mobile Banking App from the Customer's Permitted Mobile Device if the Customer changes or disposes of its Permitted Mobile Device.</p>	<p>Mobile Token and Biometric Credential Authentication Service (if applicable);</p> <p>(j) changing the Customer's Passwords or Mobile Token Password immediately if the Customer suspects that the Customer has been deceived by a fraudulent website, Mobile Banking App, email, or SMS/WAP push message (for example, where the Customer fails to logon to the Mobile Banking App with the use of the correct biometric credentials and/or Mobile Token Password);</p> <p>(k) notifying the Bank as soon as reasonably practicable if it suspects that any of the Customer's Identity Verification Information, any other security codes (including, without limitation, the Password of the Mobile Token) and/or the Permitted Mobile Device have been compromised, lost, stolen, or accessed or used without the Customer's authorisation;</p> <p>(l) strictly adhering to all security advice, measure, guidelines and instructions from time to time provided to the Customer by the Bank and/or the manufacturer of the Customer's Permitted Mobile Device applicable to the Customer's use of its Permitted Mobile Device;</p> <p>(m) notifying the Bank without delay if the Customer changes the Customer's mobile phone number;</p> <p>(n) upon termination of the use of the Mobile Banking App and/or the Mobile Token for any reason,</p>
---	---

客戶重要通知

Important Notice to Customers



		<p>removing the Mobile Banking App and/or the Mobile Token from the Customer's Permitted Mobile Device; and</p> <p>(o) removing the Mobile Banking App from the Customer's Permitted Mobile Device if the Customer changes or disposes of its Permitted Mobile Device;</p> <p>(p) <u>ensuring that the Mobile Token Password are kept secure and under the personal control of the Customer and will not permit any person other than the Customer to use the Mobile Token. The Mobile Token shall at all times remains the property of the Bank and issued at the Bank's discretion and the Customer shall immediately unregister or otherwise disable immediately upon the Bank's request; and</u></p> <p>(q) <u>notifying the Bank in the event of loss or theft of the Permitted Mobile Device to which a Mobile Token is bound as soon as reasonably practicable by telephone at such telephone number as the Bank may from time to time prescribe and confirm the same in writing if requested by the Bank. If the Customer fails to report such incidents as soon as reasonably practicable to the Bank or has otherwise acted fraudulently or with gross negligence, the Customer may be responsible for all direct losses as a result of all unauthorised transactions involving the use of, as the case may be, the lost of the</u></p>
--	--	---

客戶重要通知

Important Notice to Customers



			Permitted Mobile Device to which a Mobile Token is bound by any person.
11	Upon the Customer notifying the Bank that the security of the Customer's Biometric Credentials, Mobile Token or other security code was suspected to be compromised, the Bank is entitled (but not obliged) to require the Customer to change the Identity Verification Information, re-register the Customer's Biometric Credentials or suspend or cease the use of the Biometric Credential Authentication Service.	15	Upon the Customer notifying the Bank that the security of the Customer's Biometric Credentials, Mobile Token or other security code was suspected to be compromised, the Bank is entitled (but not obliged) to require the Customer to change the Identity Verification Information, re-set the Mobile Token , re-register the Customer's Biometric Credentials or suspend or cease the use of the Mobile Token and Biometric Credential Authentication Service.
12	The Customer shall be solely responsible for using, and shall be liable for any loss that results from any unauthorised use of the Mobile Banking App, the Biometric Credential Authentication Service and/or the Mobile Token due to the Customer's failure to adopt and maintain appropriate safeguards (including, without limitation, to the measures in Clause 10 above).	16	The Customer shall be solely responsible for using, and shall be liable for any loss that results from any unauthorised use of the Mobile Banking App, the Biometric Credential Authentication Service and/or the Mobile Token due to the Customer's failure to adopt and maintain appropriate safeguards (including, without limitation, to the measures in Clause 14 10 above).

Disclaimer and limitation of liability

	Original		New
14	The Customer acknowledges that the Biometric Credential Authentication Service is for the purpose of the Customer's personal convenience. The Customer's use of the Biometric Credential Authentication Service is wholly at the Customer's own risk. The Biometric Credential Authentication Service is provided on an "as is" basis.	18	The Customer acknowledges that the Mobile Token and the Biometric Credential Authentication Service is for the purpose of the Customer's personal convenience. The Customer's use of the Mobile Token and/or the Biometric Credential Authentication Service is wholly at the Customer's own risk. The Mobile Token and/or the Biometric

客戶重要通知

Important Notice to Customers



	To the maximum extent permitted by the Regulatory Requirements, the Bank disclaims all conditions, warranties (including, without limitation, any warranties of merchantability, fitness for a particular purposes, accuracy and non-infringement of third party rights), representations or other terms which may apply to the Biometric Credential Authentication Service, whether express or implied.		Credential Authentication Service is provided on an “as is” basis. To the maximum extent permitted by the Regulatory Requirements, the Bank disclaims all conditions, warranties (including, without limitation, any warranties of merchantability, fitness for a particular purposes, accuracy and non-infringement of third party rights), representations or other terms which may apply to the Mobile Token and the Biometric Credential Authentication Service , whether express or implied.
15	To the fullest extent permitted by the Regulatory Requirements, the Bank will not be responsible for any loss the Customer may suffer in connection with the Customer’s use of the Biometric Credential Authentication Service, the Customer’s Instructions to the Bank or any unauthorised transactions made through or in connection with the Biometric Credential Authentication Service.	19	To the fullest extent permitted by the Regulatory Requirements, the Bank will not be responsible for any loss the Customer may suffer in connection with the Customer’s use of the Mobile Token and/or the Biometric Credential Authentication Service , the Customer’s Instructions to the Bank or any unauthorised transactions made through or in connection with the Mobile Token and/or the Biometric Credential Authentication Service .
16	To the fullest extent permitted by the Regulatory Requirements, the Bank will not be liable for any act, omission, negligence, default, damages, losses (including, without limitation, loss or leakage of data), causes of action, whether in contract, tort (including, without limitation, negligence), or otherwise arising in connection with the use of Biometric Credential Authentication Service. The Bank shall not be liable for any error, interception, corruption, deletion or inaccuracy in the Biometric Credential Authentication	20	To the fullest extent permitted by the Regulatory Requirements, the Bank will not be liable for any act, omission, negligence, default, damages, losses (including, without limitation, loss or leakage of data), causes of action, whether in contract, tort (including, without limitation, negligence), or otherwise arising in connection with the use of the Mobile Token and/or the Biometric Credential Authentication Service . The Bank shall not be liable for any error, interception, corruption, deletion or inaccuracy in the Mobile

客戶重要通知

Important Notice to Customers



<p>Service, any person's use of, or reliance on or inability to use the Biometric Credential Authentication Service, any interruption or hindrance of or delay in the operation of the Biometric Credential Authentication Service, any incomplete transmission, any circuit or system failure or any computer virus. The Bank shall not be responsible for any loss of profit, sales, business, revenue, business opportunity, goodwill or reputation, or any special, consequential or indirect loss or damage arising out of such act, omission, negligence or default with respect to the Biometric Credential Authentication Service.</p>	<p>Token and/or the Biometric Credential Authentication Service, any person's use of, or reliance on or inability to use the Mobile Token and/or the Biometric Credential Authentication Service, any interruption or hindrance of or delay in the operation of the Mobile Token and/or the Biometric Credential Authentication Service, any incomplete transmission, any circuit or system failure or any computer virus. The Bank shall not be responsible for any loss of profit, sales, business, revenue, business opportunity, goodwill or reputation, or any special, consequential or indirect loss or damage arising out of such act, omission, negligence or default with respect to the Mobile Token and/or the Biometric Credential Authentication Service.</p>
--	---

Service availability and termination

	Original		New
19	<p>The Biometric Credential Authentication Service may be suspended, terminated, withdrawn or amended by the Bank at any time without prior notice or providing any reason. The Bank is under no obligation to continually provide the Biometric Credential Authentication Service. The Bank may in its absolute discretion decide whether the Customer are eligible to use the Biometric Credential Authentication Service and as the Bank considers appropriate, the Bank is entitled to suspend the Customer's use of the Biometric</p>	23	<p>The Mobile Token and/or the Biometric Credential Authentication Service may be suspended, terminated, withdrawn or amended by the Bank at any time without prior notice or providing any reason. The Bank is under no obligation to continually provide the Mobile Token and/or the Biometric Credential Authentication Service. The Bank may in its absolute discretion decide whether the Customer are eligible to use the Mobile Token and/or the Biometric Credential Authentication Service and as the Bank considers appropriate, the Bank</p>

客戶重要通知

Important Notice to Customers



<p>Credential Authentication Service or any part of it, or suspend the Customer's access to the Biometric Credential Authentication Service without prior notice. The Bank's decision in this regard is final and binding on the Customer. The Bank will not be responsible for any loss or damage suffered by the Customer arising from such decisions.</p>	<p>is entitled to suspend the Customer's use of the Mobile Token and/or the Biometric Credential Authentication Service or any part of it, or suspend the Customer's access to the Mobile Token and/or the Biometric Credential Authentication Service without prior notice. The Bank's decision in this regard is final and binding on the Customer. The Bank will not be responsible for any loss or damage suffered by the Customer arising from such decisions.</p>
--	---

Others

Original	New
	<p>24 This Annex 1 may be amended at any time and from time to time. The amended terms and conditions will become effective upon the Bank giving reasonable notice to the Customer, including posting the amended terms and conditions on the Mobile Banking App, on the Website or displaying the amended terms and conditions in the Bank's branches (where appropriate). By continuing to use the Mobile Token and/or the Biometric Credential Authentication Service, subject to Regulatory Requirements, the Customer is deemed to have agreed to the amended terms and conditions.</p>
	<p>25 This Annex 1 is governed by the laws of the Hong Kong Special Administrative Region. The Customer agrees to submit to the non-exclusive jurisdiction of the Hong Kong courts in relation to any dispute in respect of or arising from this</p>

客戶重要通知

Important Notice to Customers



			<u>Annex 1, but these terms and conditions may be enforced in the courts of any competent jurisdiction.</u>
		26	<u>No person other than the Bank and the Customer will have any right under the Contracts (Rights of Third Parties) Ordinance to enforce or enjoy the benefit of any of the provisions in this Annex 1. Notwithstanding any provision contained herein, the consent of any person who is not a party to this Annex 1 is not required to rescind or vary the terms.</u>
		27	<u>In the event of any inconsistency between the English version and the Chinese version of these terms and conditions in this Annex 1, the English version will prevail.</u>