

# 客戶重要通知

## Important Notice to Customers



### 更改「網上銀行服務的條款及條件」通知

本行將於 2022 年 8 月 19 日 (星期五) (「生效日」) 修訂「網上銀行服務的條款及條件」(簡稱「條款和條件」)的條文。

#### A. 條款和條件主要更新的摘要

1. 修訂條文以列明與使用流動保安編碼有關的保安措施；及
2. 修訂條文以使某些條文涵義更清晰。

新增條文及完整修訂請參閱 B 部分。

#### B. 條款和條件內已修訂的條文(新加內容已劃上底線，移除內容已被劃掉)：

「網上銀行服務的條款及條件」

原有項目號碼	修訂或新增項目號碼	修訂內容
1.1	不變	「銀行」指中國建設銀行(亞洲)股份有限公司， <u>包括其承繼人、承讓人、受讓人及從前述任何人取得所有權的任何其他人。</u>
N/A	1.2	<u>新增「生物識別憑據」的定義，並更新其後條文的項目號碼：</u> <u>「生物識別憑據」指在客戶流動裝置上註冊的指紋、面部辨識或任何其他生物識別數據。</u>
N/A	1.3	<u>新增「生物憑據認證服務」的定義，並更新其後條文的項目號碼：</u>

# 客戶重要通知

## Important Notice to Customers



		<u>「生物憑據認證服務」指銀行不時根據中國建設銀行(亞洲)生物憑據認證服務條款及條件就使用客戶生物識別憑據進入銀行的網上銀行服務所提供的認證方式。</u>
1.9	1.25	「客戶名稱」指用來進行任何網上銀行交易的登記身份號碼。
N/A	1.14	<b>新增「流動保安編碼」的定義，並更新其後條文的項目號碼：</b> <u>「流動保安編碼」指銀行流動應用程式內建並連接銀行流動應用程式的功能，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/或使用任何網上銀行服務。</u>
N/A	1.15	<b>新增「流動保安編碼密碼」的定義，並更新其後條文的項目號碼：</b> <u>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>
1.17	1.20	「保安編碼」指於有關時間由 <u>流動保安編碼自動計算，或由保安編碼器自動計算和顯示的或向指定流動電話號碼發出之一次性密碼，以用作使用銀行不時指定的某類網上銀行服務。</u>
1.18	1.21	「保安編碼器」指銀行根據客戶要求所提供給客戶用來計算及顯示保安編碼的 <u>實體電子儀器。</u>
2(e)	不變	銀行可在不通知客戶情況下不時釐定或更改銀行提供的服務範圍及類別、使用服務限制、最高或最低交易限額、某一類別服務的適用截止時間及 / 或日期、適用服務收費及網上銀行服務的其他特色（ <u>更改服務收費或影響客戶責任及義務的改動除外</u> ）。 <u>，但須受本條款及條件第 18 條所述修訂本條款及條件的通知要求規限。...</u>
3(c)	不變	為了使用轉賬服務，客戶必須使用有效保安編碼。 <u>或透過使用流動保安編碼另行認證客戶身份。</u> 銀行可能要求客戶使用有效保安編碼或流動保安編碼，以進入任何其他網上銀行服務。
N/A	3A	<b>新增以下 3A(a)至 3A(f)條：</b> 進入網上銀行服務/使用流動保安編碼

# 客戶重要通知

## Important Notice to Customers



N/A	3A(a)	<p>取決於客戶希望進入及/或使用網上銀行服務的類型，客戶將需採取由銀行獨自酌情要求之下列一項或多項步驟：</p> <p><u>(i) 輸入客戶名稱和私人密碼的正確組合；</u></p> <p><u>(ii) 透過銀行提供的銀行生物憑據認證服務使用客戶的生物識別憑據來進行認證；</u></p> <p><u>(iii) 輸入由保安編碼器計算或發送至客戶指定流動電話號碼的保安編碼；或</u></p> <p><u>(iv) 輸入由流動保安編碼透過(1)輸入正確的流動保安編碼密碼；或(2)透過銀行生物憑據認證服務使用客戶的生物識別憑據計算的保安編碼。</u></p>
N/A	3A(b)	<p>流動保安編碼是由銀行向已經下載及註冊銀行流動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兼容流動裝置上設置其流動保安編碼：</p> <p><u>(i) 登入客戶的銀行流動應用程式及接受為設置和使用流動保安編碼的所有適用條款及條件；</u></p> <p><u>(ii) 將客戶的生物識別憑據用於認證；</u></p> <p><u>(iii) 輸入發送至客戶指定及已在銀行登記之流動電話號碼的保安編碼；及</u></p> <p><u>(iv) 指定流動保安編碼密碼，及/或在客戶的流動裝置具備生物認證功能且客戶已同意中國建設銀行（亞洲）生物憑據認證服務條款及條件的情況下，允許透過生物憑據認證服務進入並使用流動保安編碼，</u></p> <p><u>或遵循銀行不時規定的任何其他步驟或指示。</u></p>

# 客戶重要通知

## Important Notice to Customers



N/A	3A(c)	<p>客戶可在 <a href="https://www.asia.ccb.com/hongkong/doc/personal/banking_channels/compatible-android-devices.pdf">https://www.asia.ccb.com/hongkong/doc/personal/banking_channels/compatible-android-devices.pdf</a> 查詢與銀行流動應用程式的流動保安編碼功能兼容的流動裝置清單。但是，銀行不保證任何特定型號或品牌的流動裝置與流動保安編碼兼容或就流動保安編碼而言具適用性，客戶應獨自負責確保其為設置和使用流動保安編碼所指定的流動裝置能兼容流動保安編碼的任何及所有軟件或硬件要求，且在任何時候就流動保安編碼而言具適用性。</p>
N/A	3A(d)	<p>客戶確認銀行可不時規定必須安裝的銀行流動應用程式或銀行網站更新，以使銀行流動應用程式正常運行。客戶確認，客戶須獨自負責更新其銀行流動應用程式及/或進入銀行網站的最新更新版本以使用流動保安編碼進入網上銀行服務。如果客戶(A)未有安裝銀行流動應用程式的任何要求安裝的更新，或(B)未進入銀行網站的最新版本，對於客戶因不能進入任何網上銀行服務而招致之任何損失或損害，銀行概不對客戶承擔任何責任。</p>
N/A	3A(e)	<p>設置和啟動流動保安編碼會創建並保存一個數碼保安編碼，該編碼將與客戶用於該等設置和啟動的流動裝置綁定。客戶確認流動保安編碼每次僅可在一個流動裝置綁定並啟動。一旦綁定該流動保安編碼，客戶被綁定的流動裝置將被銀行為在進入和使用任何網上銀行服務持續用於認證客戶身份的目的而認定。如果客戶希望停止使用流動保安編碼或將流動裝置與相關流動保安編碼解除綁定，客戶可在相關流動裝置上註銷流動保安編碼或致電銀行於銀行網站或銀行流動應用程式發佈之客戶熱線與銀行聯繫以獲取進一步協助。</p>
N/A	3A(f)	<p>客戶確認當流動保安編碼被啟動，客戶的保安編碼器將自動被停用，不能再用於進入或使用任何網上銀行服務。</p>
4	不變	<p><b>更改標題：</b> 客戶名稱、私人密碼、<u>流動保安編碼密碼</u>、保安編碼及保安編碼器</p>
4(a)	不變	<p>客戶應採取合理措施以將客戶名稱、私人密碼、<u>其流動保安編碼密碼</u>及任何保安編碼保密。客戶應該：</p>

# 客戶重要通知

## Important Notice to Customers



4(a)(ii)	不變	設定難以猜測（例如：設定新密碼時，切勿選用如出生日期、電話號碼或客戶姓名中可認知的部份等資料）及有別於其他服務所使用的 <u>私人密碼和流動保安編碼密碼（如適用）</u> ；
4(a)(iii)	不變	熟記客戶名稱及 <u>私人密碼和流動保安編碼密碼（如適用）</u> 並銷毀發給客戶的客戶名稱及私人密碼通知；
4(a)(iv)	不變	不向任何人透露、分享及容許獲得或使用信用卡、客戶名稱、私人密碼、 <u>流動保安編碼密碼（如適用）</u> 或保安編碼；
N/A	4(a)(vi)	<b>新增以下 4(a)(vi)條，並更新其後條文的項目號碼：</b> <u>不要將流動保安編碼密碼（如適用）寫在流動保安編碼上或將流動保安編碼密碼與流動保安編碼放置在一起；</u>
4(a)(vi)	4(a)(vii)	不要不加掩飾地寫下或記錄客戶名稱、私人密碼、 <u>流動保安編碼密碼（如適用）</u> 或保安編碼；
4(a)(vii)	4(a)(viii)	定時更改私人密碼和 <u>流動保安編碼密碼（如適用）</u> ，且不要將私人密碼和 <u>流動保安編碼密碼（如適用）</u> 儲存於電腦、流動電話或當眼處；
4(a)(x)	4(a)(xi)	如銀行向客戶的流動裝置發送 <u>一次性的密碼保安編碼</u> ，不要將該 <u>一次性密碼保安編碼</u> 傳送至另一流動裝置；
4(a)(xiii)	4(a)(xiv)	採取防範社交工程技術的措施，避免遭受虛假或可疑電郵、網站或網上理財流動應用程式或偽冒銀行職員或警務人員索取 <u>任何客戶資料（如：客戶名稱、私人密碼、流動保安編碼密碼（如適用）或保安編碼）</u> ；
4(a)(xv)	4(a)(xvi)	只連結至由銀行指定或認可的銀行網站或應用程式商店下載的銀行流動應用程式；及
N/A	4(a)(xvii)	<b>新增以下 4(a)(xvii)條，並更新其後條文的項目號碼：</b> <u>如果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銀行流動應用程式，無論是否有任何警告提示），立即更改私人密碼和流動保安編碼密碼（如適用）；</u>

# 客戶重要通知

## Important Notice to Customers



4(a)(xvi)	4(a)(xviii)	<p>即時查閱銀行向客戶發出的相關通知及<u>任何賬單或通知書及客戶最後登入網上銀行服務的日期及時間的資料</u>，並在發現不尋常交易或狀況時，在可行情況下儘快致電銀行於銀行網站或銀行流動應用程式發佈之客戶熱線通知銀行。<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>；及</p>
N/A	4(a)(xix)	<p><b>新增以下 4(a)(xix)條：</b>  <u>參閱並遵守銀行不時提供之任何額外安全建議。</u></p> <p><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></p>
4(b)	不變	<p>客戶明白及<u>承認確認</u>客戶的信用卡、客戶名稱、私人密碼、<u>流動保安編碼密碼和流動保安編碼（如適用）及/或保安編碼有被未獲授權人士濫用不當使用或被用於未獲批准的用途的風險</u>。如果有<u>下列任何情形</u>，客戶應在合理可行情況下儘快通知銀行：<u>(i) 客戶得知或懷疑信用卡、客戶名稱、私人密碼、流動保安編碼密碼（如適用）、保安編碼器（如適用）及/或保安編碼已被遺失、被竊、受損害、被洩露給任何未獲授權人士或被任何未獲授權人士取得；(ii) 或有人用信用卡、客戶名稱、私人密碼、流動保安編碼密碼（如適用）及/或保安編碼作出任何未獲授權的指示或交易；或(iii) 流動保安編碼受到任何損害或未獲授權的使用</u>。客戶應在合理可行情況下儘快可透過下列任何方式或銀行不時通知的任何其他方式向銀行<u>發送該等通知：</u></p> <p><u>(I) 致電銀行於銀行網站或銀行流動應用程式發佈之客戶熱線。</u></p> <p><u>(II) 聯絡銀行任何分行。</u></p> <p>若客戶未能在合理可行情況下儘快通知銀行該等事情，或存在欺詐或嚴重疏忽行為，一切由他人使用<u>任何信用卡、客戶名稱、私人密碼、流動保安編碼密碼（如適用）、流動保安編碼（如適用）及/或保安編碼進行的交易及所引致的直接損失</u>，可能需由客戶負責。</p>



# 客戶重要通知

## Important Notice to Customers



4(c)	不變	如銀行根據本條款及條件的第 4(b)條所述收到通知並且有合理機會就該通知採取行動之前，任何人使用客戶任何信用卡、客戶名稱、私人密碼及/或、 <u>流動保安編碼密碼及/或保安編碼發出的</u> ，或透過任何未獲授權使用客戶的流動保安編碼發出的所有指示將被銀行所依賴或執行，而有關指示不可被撤銷。假如所使用的信用卡、客戶名稱、私人密碼及/或保安編碼正確， <u>或者透過使用正確的流動保安編碼密碼或生物識別登入憑據來使用流動保安編碼</u> ，銀行並無責任核證向銀行作出指示的人士的身份或授權。
4(d)	不變	客戶的信用卡、客戶名稱、私人密碼、 <u>流動保安編碼密碼（如適用）</u> 、 <u>流動保安編碼（如適用）</u> 或保安編碼器於未被客戶更改或取消(以銀行已收到客戶的更改或取消通知且銀行有合理機會就通知採取行動為條件)或未被銀行或其他發出機構取消之前將一直有效。
4(f)(i)	不變	安全保管任何客戶名稱、保安編碼器、保安編碼、私人密碼、 <u>流動保安編碼密碼（如適用）</u> 、 <u>流動保安編碼（如適用）</u> 及網上銀行服務；
4(f)(iii)	不變	確保沒有其他人在未授權的情況下進入網上銀行服務或指定戶口(不論以電腦系統或其他方式)，包括但不限於 <u>客戶名稱、私人密碼、保安編碼器、保安編碼、流動保安編碼密碼（如適用）</u> 、 <u>流動保安編碼（如適用）</u> 或其他進入網上銀行服務之 <u>認證方式</u> ；
4(f)(iv)	不變	使用任何保安編碼器、 <u>流動保安編碼（如適用）</u> 、軟件、電腦系統、用戶指引或銀行向客戶提供之任何其他設備，以便客戶可執行任何交易，及按銀行要求立即向銀行交還該等設備；
N/A	4(f)(viii)	<b>新增以下 4(f)(viii)條：</b> <u>遵守所有適用法律法規，不得將網上銀行服務用於或有關任何不合法、未經授權或欺詐性目的或活動。</u>
5(a)	不變	若銀行有合理理由，銀行可酌情在任何指定戶口結束時或任何時間暫停或終止所有或部分網上銀行服務（包括銀行網站、銀行流動應用程式，使用及取用 <u>流動保安編碼</u> ），而無須給予客戶事先通知或理由。

# 客戶重要通知

## Important Notice to Customers



5(c)	不變	除本條款及條件的第 5(a) 及 5(d) 條所述之情況外，銀行將盡合理努力給予客戶任何有關網上銀行服務、銀行網站及/或、銀行流動應用程式及/或流動保安編碼的任何更改、修改、暫停、限制或終止的預先通知，...
5(e)	不變	<u>在適用法律法規允許的最大範圍內</u> ，客戶若因任何原因自願或非自願暫停或終止任何網上銀行服務而蒙受或引致任何損失或損害，銀行概不承擔責任。
6(a)	不變	對於只需一名戶口持有人簽字就可運用的聯名戶口，經任何一名或多名戶口持有人要求，銀行將就 <u>使用</u> 網上銀行服務分別發給每一戶口持有人：
N/A	6(a)(ii)	<b>新增以下 6(a)(ii) 條，並更新其後條文的項目號碼：</b> <u>獨立的流動保安編碼；及</u>
9(a)	不變	如客戶需要作出任何網上銀行指示，客戶必須（在銀行要求下）引用 <u>正確的客戶名稱、私人密碼、保安編碼及/或透過流動保安編碼進行的認證及銀行就進行網上銀行交易所要求的其他資料</u> 。...
9(f)	不變	雖然銀行會合理地努力確保網上銀行指示被適時執行，但數據在網上的傳遞可能有時間的差距。網上銀行服務（包括 <u>但不限於轉賬服務、銀行網站、銀行流動應用程式、使用保安編碼器和流動保安編碼</u> ）亦可能會受到干擾、硬件或軟件失靈、誤差、傳遞阻塞、因互聯網線路繁忙導致傳遞延遲或因互聯網的公開性質導致數據傳遞錯誤、市場交易量或波動、系統故障、提升或維修或其他原因而所影響（並可能因導致指示、通訊或資料的處理及/或傳遞上產生故障或延誤）。...
9(g)	不變	雖然銀行已盡力避免網上銀行服務（包括 <u>但不限於透過銀行網站、銀行流動應用程式、保安編碼器及/或流動保安編碼進入</u> ）被中斷，但銀行的網上銀行服務仍可能發生故障或延誤或間歇性的機件失常或運作中斷。...但在任何情況下， <u>在適用法律法規允許的最大範圍內</u> ，銀行不會就取消網上銀行指示、或沒有就取消網上銀行指示作出通知或客戶無法收到取消轉賬指示的通知（無



# 客戶重要通知

## Important Notice to Customers



		論是否因為客戶沒有提供有效的電郵地址及/ 或可接收短訊的流動電話號碼) 而負上任何責任。...
10(a)	不變	客戶承諾在使用網上銀行服務 (包括但不限於銀行網站、銀行流動應用程式、保安編碼器及流動保安編碼) 時遵守本條款及條件，以及銀行不時規定的有關網上銀行服務的使用政策及程序。
10(b)	不變	<p>客戶承諾不幹擾、修改、解讀、反向解構或以其他方式改動或擅自進入網上銀行服務、銀行網站、銀行流動應用程式的任何部分或其中之任何軟件。如果客戶違反此項承諾，銀行有權終止客戶使用網上銀行服務而毋須通知客戶，並可對客戶採取法律行動。</p> <p>客戶承諾：</p> <p>(i) 不會對網上銀行服務、銀行網站、銀行流動應用程式、流動保安編碼或前述所包含的任何軟件的任何部分進行干擾、修改、解讀、反向工程或以其他方式變動或未經授權進入網上銀行服務、銀行網站、銀行流動應用程式、流動保安編碼或前述所包含的任何軟件的任何部分；</p> <p>(ii) 不會以在流動裝置或作業系統供應商支持或確保的配置外進行過修改的任何裝置或作業系統 (例如，已經被「越獄」或「刷機」的裝置) 進入或使用銀行網站、銀行流動應用程式或流動保安編碼。被越獄或刷機的裝置指在未經流動服務提供商及/ 或電話製造商批准的情況下不再受限於其所設置之限制的裝置。在被越獄或刷機的裝置上使用銀行網站、銀行流動應用程式或流動保安編碼可能會損害安全並導致欺詐性交易；及</p> <p>(iii) 僅從官方流動電話應用程式網上商店 (例如 Google Play 或 Apple App Store) 下載銀行流動應用程式及其更新。</p> <p>如果客戶違反上述承諾，銀行有權終止客戶的網上銀行服務 (包括但不限於銀行網站、銀行流動應用程式、保安編碼器和流動保安編碼) 而不通知客戶，並就此對客戶採取法律行動。如果客戶未採取本行或客戶電子裝置製造商不時告知或公佈的任何安全措施，客戶須對因使用網上銀行服務而引致或與其相關的所有後果全權負責並承擔所有責任。</p>

# 客戶重要通知

## Important Notice to Customers



N/A	11(a)	在符合一般條款及條件及不影響本條款及條件第 4 條的情況下，如發生未經授權的網上銀行交易，而客戶方面並無嚴重疏忽、欺詐或錯誤（例如客戶未能妥善保管接駁網上銀行服務（ <u>包括但不限於銀行網站、銀行流動應用程式、保安編碼器及流動保安編碼</u> ）的設備），則客戶將無須負責其所蒙受的任何直接損失。
N/A	11(b)	客戶須賠償銀行、其管理人員、僱員及銀行委派的任何其他人士就有關銀行提供網上銀行服務及/（ <u>包括但不限於銀行網站、銀行流動應用程式、保安編碼器及流動保安編碼</u> ）及/或銀行根據本條款及條件行使其權力及權利而可能引致的一切訴訟、債務、索償、訴求、損失、損害賠償及稅務費用及任何銀行因此而合理引起的合理費用及支出（包括法律費用），除非該等債務、索償、費用、損害賠償、支出、訴訟或司法程序直接且完全因銀行的管理人員、僱員或代理人員的疏忽或故意犯錯造成，而客戶方面並無嚴重疏忽、欺詐或錯誤。
12	不變	<b>更改標題：</b> 保安編碼器和流動保安編碼（如適用）的擁有權
12	不變	保安編碼器和流動保安編碼（如適用）是及在任何時候均屬銀行財產並由銀行決定發出，客戶應在銀行要求時立即將之退還銀行（適用於保安編碼器），或立即將之註銷或停用（適用於流動保安編碼）。客戶須自行保管其保安編碼器和流動保安編碼（如適用）並確保其安全保密，不可準許除客戶之外的任何其他人士使用該保安編碼器和流動保安編碼（如適用）。
13	不變	<b>更改標題：</b> 保安編碼器及/或與流動保安編碼綁定之流動裝置遺失或被竊
13	不變	如果客戶的保安編碼器或與流動保安編碼綁定之流動裝置遺失或被竊，客戶應在合理可行情況下儘快撥打銀行不時規定的電話號碼通知銀行，並在銀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向銀行知會該等事項，或在其他情況下有欺詐或嚴重疏忽的行為，所有未經授權交易（ <u>包括因涉及任何人士使用其所失之保安編碼器或與流動保安編碼綁定的流動裝置</u> （視乎情況

# 客戶重要通知

## Important Notice to Customers



		而定 ) 所進行的未經授權交易) 而引致的直接損失，一律可能需由客戶負責。銀行補發新保安編碼器或流動保安編碼 ( 如適用 ) 時可收取費用。
14(b)	不變	客戶明白及接受，任何接觸到、擁有、知道或獲准許查找私人密碼及/或流動保安編碼密碼或可使用保安編碼器 ( 如有 ) 或流動保安編碼 ( 如適用 ) 之人士可能能夠啟用客戶的指定戶口，而銀行概不會就任何有關損失負責。
14(c)(iii)	不變	因未能提供網上銀行服務、或網上銀行服務 ( 包括但不限於銀行網站、銀行流動應用程式、保安編碼器及流動保安編碼 )、或網上銀行服務 ( 包括但不限於銀行網站、銀行流動應用程式、保安編碼器及流動保安編碼 ) 受到限制、修改、修定、暫時中斷或終止或變成不可運作；
14(c)(v)	不變	因使用或不能使用網上銀行服務，或機器、網上銀行服務、銀行網站、銀行流動應用程式、保安編碼器、流動保安編碼、互聯網、電腦系統、資料處理系統或傳送網絡的任何錯誤、不足或失靈，或任何工業糾紛或任何其他在銀行、其代理人或分包商控制範圍以外之任何原因 ( 不論是因疏忽或其他原因造成 ) 所引致的任何利潤或機會之損失或任何其他相應或間接之損失或責任。
14(d)	不變	如發現銀行對其任何行為或遺漏、疏忽或過失需要負責，其責任 ( 在適用法律允許的最大範圍內 ) 只限於直接損失或實際損害的數額或有關交易數額兩者之較少者。銀行毋須對由於該等行為、遺漏、疏忽或過失引致的任何利潤損失或任何特殊、相應或非直接的損失或損害負責。
15(a)	不變	互聯網是一種迅速改變、開放及公開的科技，而網上交通擠塞亦是不可預計的。客戶明白銀行會盡合理努力確保網上銀行服務 ( 包括但不限於銀行網站、銀行流動應用程式、保安編碼器及流動保安編碼 ) 會持續運作，但客戶亦接受：
15(a)(ii)	不變	網上銀行服務、銀行網站及、銀行流動應用程式、保安編碼器及/或流動保安編碼 ( 如適用 ) 未必能達到客戶的所有要求或期望；及

# 客戶重要通知

## Important Notice to Customers



15(a)(iii)	不變	網上銀行服務、銀行網站及、銀行流動應用程式、保安編碼器及/或流動保安編碼 (如適用) 的運作、操作及可靠性；
17(a)	不變	客戶確認所有在銀行網站、銀行流動應用程式、流動保安編碼及有關軟件之內容均屬銀行及/或第三者供應商之所有，並受制於知識產權。除非特別列明或銀行或該第三者供應商 (視情況而定) 以書面認可外，銀行網站、銀行流動應用程式或第三者網站將不會被當作給予客戶任何權利或許可證使用任何有關或顯示在銀行網站、銀行流動應用程式、保安編碼器、流動保安編碼或第三者網站之任何知識產權。
17(b)(iii)	不變	為未經銀行或任何第三者供應商授權的目的，闖入、進入或使用或企圖闖入、進入或使用任何網上銀行服務、銀行網站、銀行流動應用程式、保安編碼器、流動保安編碼、第三者網站、內容及/或銀行或任何第三者供應商的伺服器的任何數據區域；
17(b)(iv)	不變	在使用銀行網站、銀行流動應用程式、保安編碼器、流動保安編碼或任何內容時侵犯任何人士或任何一方之知識產權；
17(b)(v)	不變	在使用網上銀行服務、銀行網站及/或、銀行流動應用程式、保安編碼器及/或流動保安編碼時，違反任何適用司法管轄區之任何適用法律；及/或
18	不變	銀行可於任何時間及不時修訂本根據適用法律或適用於銀行的監管規定修訂或替換本條款及條件及/或加入附加增補額外條款及條件。銀行以實物或電子方式給予客戶合理通知後，本條款及條件的任何修改及增補隨即生效，該等通知可、在銀行網站上張貼或以銀行認為適當的該等其他方式發出、發佈及/或採取適用法律或適用於銀行的監管規定要求的任何其他行動後，本條款及條件的任何修訂、替換或增補隨即生效。若客戶在修訂、替換或增補條款及條件的生效日或之後繼續持有維持或使用網上銀行服務，該通知任何經修訂或增補的條款及條件即對客戶構成約束力。

# 客戶重要通知

## Important Notice to Customers



客戶可聯絡分行職員索取上述條款和條件之完整修訂本。客戶除可經分行查詢詳情，亦可致電客戶服務熱線+852 277 95533 或瀏覽 [www.asia.ccb.com](http://www.asia.ccb.com) 了解。若客戶於生效日或之後繼續使用電子理財服務及/或網上銀行服務，上述更改將對客戶具有約束力。倘客戶不接受上述修訂，客戶有權於生效日前根據條款和條件中列明的有關條款終止電子理財服務及/或網上銀行服務，請致電客戶服務熱線通知本行以作安排。

本通知之中英文文本如有歧異，概以英文本為準。

中國建設銀行(亞洲)股份有限公司

2022年7月



# 客戶重要通知

## Important Notice to Customers



### Notice of Amendments to Terms and Conditions for Online Banking Services

Please be informed that Terms & Conditions for Online Banking Services (collectively, the “Terms and Conditions”) will be amended with effect from **August 19, 2022 (Friday)** (“effective date”) as set out below:

#### A. Summary of the key changes to the Terms and Conditions

1. Provisions are amended to update security measures in relation to the use of Mobile Token; and
2. Provisions are amended to enhance clarity of the meaning of certain provisions.

#### B. Amendments to the Terms and Conditions (additions are underlined and deletions are crossed out):

##### Terms & Conditions for Online Banking Services

1.1	No Change	"Bank" means China Construction Bank (Asia) Corporation Limited, <u>which shall include its successors, assigns, transferees and any other person deriving title under any of them.</u>
N/A	1.2	<b>Add the definition of “Biometric Credentials” and update subsequent numbering accordingly:</b> <u>"Biometric Credentials" means fingerprint, facial map or any other biometric data that is registered in the Customer's mobile device.</u>
N/A	1.3	<b>Add the definition of “Biometric Credential Authentication Service” and update subsequent numbering accordingly:</b> <u>"Biometric Credential Authentication Service" means the authentication method for accessing the Bank's Online Banking Services using Customer's Biometric Credentials, as may be offered by the Bank from time to time in accordance with the Terms and Conditions for CCB (Asia) Biometric Credential Authentication Service.</u>
1.9	1.25	"Username" means the login ID number for the purpose of any Online Banking Transaction.
1.12	1.13	"Mobile App" means such mobile application software(s) as may be designated by the Bank from time to time.
N/A	1.14	<b>Add the definition of “Mobile Token” and update subsequent numbering accordingly:</b> <u>"Mobile Token" means a feature in-built within and linked to the Mobile 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 Banking Services.</u>

# 客戶重要通知

## Important Notice to Customers



N/A	1.15	<b>Add the definition of “Mobile Token Password” and update subsequent numbering accordingly:</b> <u>“Mobile Token Password” means the personal identification number self-selected and designated by the Customer for the purpose of utilizing the Customer’s Mobile Token.</u>
1.17	1.20	"Security Code" means a one-time password that is automatically generated <u>by a Mobile Token, or generated</u> and displayed on the Security Token, or sent to the designated mobile number at the relevant time to be used for the purpose of utilizing certain Online Banking Services specified by the Bank from time to time.
1.18	1.21	"Security Token" means <u>a physical</u> digital device provided by the Bank to the Customer at the Customer's request for the purpose of generating and displaying a Security Code.
2(e)	No Change	The scope and types of service made available by the Bank, the restrictions on the use of the service, the maximum or minimum transaction limits, the cut-off time and/or date applicable to a particular type of service, the applicable service fees and other features in respect of the Online Banking Services may be determined or varied by the Bank from time to time without prior notice to the Customer <del>(other than in the case of change of service fees or changes which may affect the liabilities or obligations of the Customer)</del> , <u>subject to the notice requirements for variations to these Terms and Conditions as set out in Clause 18 of these Terms and Conditions.</u> Updated information relating to the Online Banking Services is available from the Bank upon request.
3(c)	No Change	In order to use the Funds Transfer Services, the Customer must use a Security Code <u>or otherwise authenticate the Customer's identity through the usage of the Mobile Token.</u> The Bank may require the Customer to use Security Code <u>or the Mobile Token</u> in order to access any other Online Banking Services.
N/A	3A	<b>Add the following new clause 3A(a) to 3A(f):</b> <u>Accessing the Online Banking Services / Using the Mobile Token</u>
N/A	3A(a)	<u>Depending on the type of Online Banking Services which the Customer wishes to access and/or use, the Customer will be required to perform one or more of the following steps which the Bank may in its sole discretion require:</u> <u>(i) entering the correct combination of the Customer's Username and Password;</u> <u>(ii) applying the Customer's Biometric Credentials using the Bank's Biometric Credential Authentication Service offered by the Bank for authentication purposes; or</u> <u>(iii) entering a Security Code generated by a Security Token or which is sent to the Customer's designated mobile number.</u> <u>(iv) entering a Security Code generated by a Mobile Token where such Security Code is generated by either (1) entering the correct Mobile</u>

# 客戶重要通知

## Important Notice to Customers



		<u>Token Password; or (2) applying the Customer's Biometric Credentials using the Bank's Biometric Credential Authentication Service.</u>
N/A	3A(b)	<u>The Mobile Token is a digital security token which is offered by the Bank to Customers who have downloaded and signed up for the Mobile App as one of the means for the Customer to authenticate his or her identity for accessing and/or using the Online Banking Services. The Customer may set up his or her Mobile Token on any compatible mobile device acceptable to the Bank by:</u> <u>(i) logging on to the Customer's Mobile App and accepting all applicable terms and conditions for the set-up and use of the Mobile Token;</u> <u>(ii) applying the Customer's Biometric Credentials for authentication purposes;</u> <u>(iii) entering a Security Code which will be sent to the Customer at his or her designated mobile number registered with the Bank; and</u> <u>(iv) designating a Mobile Token Password, and/or where the Customer's mobile device carries a biometric authentication function and the Customer has agreed to the Terms and Conditions for CCB (Asia) Biometric Credential Authentication Service, enabling access to and use of the Mobile Token via 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.</u>
N/A	3A(c)	<u>The Customer may check <a href="https://www.asia.ccb.com/hongkong/doc/personal/banking_channels/compatible-android-devices.pdf">https://www.asia.ccb.com/hongkong/doc/personal/banking_channels/compatible-android-devices.pdf</a> for a list of mobile devices which are compatible with the Mobile Token function of the Mobile App. However, the Bank does not guarantee the compatibility or fitness-for-use of any particular model or brand of mobile device for the purposes of the Mobile Token and the Customer shall be solely responsible for ensuring that the mobile device designated by him or her for set up and use of the Mobile Token is compatible with any and all software or hardware requirements of the Mobile Token and is at all times fit-for-use for the purposes of the Mobile Token.</u>
N/A	3A(d)	<u>The Customer acknowledges that the Bank may from time to time prescribe updates to the Mobile App or the Website which must be installed in order to enable the proper functioning of the Mobile App. The Customer acknowledges that it is the Customer's sole responsibility to update his or her Mobile App and/or access the latest updated version of the Website to access the Online Banking Services using the Mobile Token and the Bank shall not be liable to the Customer for any loss or damage caused to the Customer due to his or her inability to access any Online Banking Services if the Customer fails to (A) install any required updates to the Mobile App or (B) access the latest version of the Website.</u>
N/A	3A(e)	<u>Set up and activation of the Mobile Token creates and stores a digital security token which is bound to the Customer's mobile device that is used for such set up and activation. The Customer acknowledges that the Mobile Token may only be bound to and activated only on one mobile</u>

# 客戶重要通知

## Important Notice to Customers



		<u>device at a time. Once bound to such Mobile Token, the Customer's bound mobile device will be recognized by the Bank for the purposes of authenticating the Customer's identity on a continuous basis in relation to the access and use of any Online Banking Services. Should the Customer wish to stop using the Mobile Token or otherwise unbind a mobile device from the relevant Mobile Token, the Customer may do so by deregistering the Mobile Token from the relevant mobile device or otherwise contacting the Bank by calling the Bank's customer hotline posted by the Bank in the Website or Mobile App for further assistance.</u>
N/A	3A(f)	<u>The Customer acknowledges that once the Mobile Token is activated, the Customer's Security Token will be automatically disabled and may no longer be used to access or use any Online Banking Services.</u>
4	No Change	<b>Change the heading to:</b> Username, <u>Password, Mobile Token</u> Password, Security Code and Security Token
4(a)	No Change	The Customer shall take reasonable steps to keep the Username, the Password, <u>his or her Mobile Token Password</u> and <del>the any</del> Security Code confidential. The Customer is advised:
4(a)(ii)	No Change	to set a Password <u>and Mobile Token Password (where applicable)</u> that is difficult to guess (e.g. not to select such information as birthday, telephone number or recognizable part of the Customer's name in selecting new password) and different from the ones for other services;
4(a)(iii)	No Change	to memorize the Username, Password and <u>Mobile Token Password (where applicable) and</u> destroy the notice to the Customer of the Username and Password;
4(a)(iv)	No Change	not to disclose to, share with, allow access <del>to</del> or use by anyone <u>to or of any</u> of the Card, Username, Password, <u>Mobile Token Password (where applicable)</u> or Security Code;
N/A	4(a)(vi)	<b>Add the following new clause 4(a)(vi) and update subsequent numbering accordingly:</b> <u>not to write down the Mobile Token Password (where applicable) on the Mobile Token or keep the Mobile Token Password and Mobile Token together;</u>
4(a)(vi)	4(a)(vii)	not to write down or record <u>any of</u> the Username, Password, <u>Mobile Token Password (where applicable)</u> or Security Code without disguising it;
4(a)(vii)	4(a)(viii)	to change the Password <u>and Mobile Token Password (where applicable)</u> on a regular basis and not to store the Password <u>and Mobile Token Password (where applicable)</u> on computers, mobile phones or <u>place anywhere</u> in plain sight;

# 客戶重要通知

## Important Notice to Customers



4(a)(viii)	4(a)(ix)	to act in such manner so as to avoid shoulder surfing over the Username, Password, <u>Mobile Token Password (where applicable)</u> or Security Code;
4(a)(x)	4(a)(xi)	if the Bank sends a <del>one-time password</del> <u>Security Code</u> to the Customer's mobile device, not to send such <del>one-time password</del> <u>Security Code</u> from one mobile device to another mobile device;
4(a)(xiii)	4(a)(xiv)	to safeguard against social engineering techniques for obtaining <u>any of the Customer's information such as the Username, the Password, the Mobile Token Password (where applicable)</u> or a Security Code through fake or suspicious emails, websites or internet banking mobile applications or impersonating the Bank's staff or the police;
4(a)(xv)	4(a)(xvi)	to only connect to the Mobile App downloaded from the Website or app stores designated or approved by the Bank; <del>and</del>
N/A	4(a)(xvii)	<b>Add the following new clause 4(a)(xvii) and update subsequent numbering accordingly:</b> <u>to change the Password and Mobile Token Password (if applicable) immediately if the Customer suspects that he or she 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 App after using the correct Biometric Credentials, with or without any alert messages);</u>
4(a)(xvii)	4(a)(xviii)	to promptly check the relevant notification and <u>any account statement(s) or advice(s) the Bank sends to the Customer and information about the date and time of the last login to log on by the Customer into the Online Banking Services, and to notify the Bank as soon as practicable by calling the Bank's customer hotline posted by the Bank in the Website or Mobile App whenever unusual transactions or observations are detected. The Customer may be held liable for the losses if he has failed to comply with any of the above safeguards; and</u>
N/A	4(a)(xix)	<b>Add the following new clause 4(a)(xix):</b> <u>refer to and comply with any additional security advice(s) provided by the Bank from time to time.</u>  <u>The Customer may be held liable for the losses if he or she has failed to comply with any of the above safeguards.</u>
4(b)	No Change	The Customer understands and acknowledges that there are risks of the Card, Username, Password, <u>Mobile Token Password and Mobile Token (where applicable)</u> and/or Security Code of the Customer being <del>abused</del> <u>misused</u> by unauthorised persons or used for unauthorised purposes. The Customer shall notify the Bank as soon as reasonably practicable upon <u>(i) any notice or suspicion of the Card, Username, Password, Mobile Token Password (where applicable), Security Token (where applicable), and/or Security Code being lost, stolen, compromised or disclosed to or obtained by any unauthorised person; (ii) any unauthorised instruction given or transaction effected with the Card,</u>



# 客戶重要通知

## Important Notice to Customers



		<p>Username, Password, <u>Mobile Token Password (where applicable)</u> and/or Security Code; <u>or (iii) any compromise or unauthorised use of the Mobile Token. Such notice may be given by the Customer to the Bank via any of the following methods:</u></p> <p><u>(I) calling the Bank's customer hotline posted by the Bank in the Website or Mobile App</u></p> <p><u>(II) contact any of the Bank's branches</u></p> <p><u>or any other method notified by the Bank from time to time.</u></p> <p>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 involving the use of <u>any of the Card, Username, Password, Mobile Token Password (where applicable), Mobile Token (where applicable)</u> and/or Security Code and all direct losses as a result.</p>
4(c)	No Change	<p>All instructions given to the Bank by anyone using <u>any of the Card, Username, Password, Mobile Token Password</u> and/or Security Code of the Customer, <u>or otherwise through any unauthorised use of the Customer's Mobile Token</u>, prior to the Bank receiving notice as mentioned in Clause 4(b) of these Terms and Conditions and the Bank having a reasonable opportunity to take action in respect of such notice will be relied on or acted upon by the Bank and shall be irrevocable. The Bank shall have no duty to verify the identity or authority of the person giving an instruction to the Bank if the correct Card, Username, Password and/or Security Code of the Customer is used <u>or if the Mobile Token is utilized using the correct Mobile Token Password or biometric logon credentials.</u></p>
4(d)	No Change	<p>A Card, Username, Password, <u>Mobile Token Password (where applicable), Mobile Token (where applicable)</u> or Security Token shall remain effective until changed or cancelled by the Customer (provided that the Bank has received notice of the change or cancellation from the Customer and the Bank has a reasonable opportunity to act upon the notice) or cancelled by the Bank or any other issuing authority.</p>
4(f)(i)	No Change	<p>safeguarding the security of <u>any of the Username, Security Token, Security Code, Password, Mobile Token Password (where applicable), Mobile Token (where applicable)</u> and the Online Banking Services;</p>
4(f)(iii)	No Change	<p>ensuring that no other person has unauthorised access to the Online Banking Services or the Designated Account (whether by use of the Computer System or otherwise), including but not limited to <u>Username, Password, Security Token, Security Code, Mobile Token Password (where applicable), Mobile Token (where applicable)</u> or other authentication <u>methods</u> required to obtain such access;</p>
4(f)(iv)	No Change	<p>the use of any Security Token, <u>Mobile Token (where applicable),</u> software, computer system, user guide or any other facilities provided by the Bank to the Customer to facilitate him in effecting any transaction(s) and in returning the same to the Bank immediately upon its request;</p>

# 客戶重要通知

## Important Notice to Customers



4(f)(vi)	No Change	ensuring that the Customer signs off from the Website and exits the browser and/or Mobile App (as the case may be) immediately after each time he <u>or she</u> uses the Website and/or Mobile App; <del>and</del>
N/A	4(f)(viii)	<b>Add the following new clause 4(f)(viii):</b> <u>complying with all applicable laws and regulations and not using the Online Banking Services for or in connection with any illegal, unauthorised or fraudulent purpose or activity.</u>
5(a)	No Change	The Bank may at its discretion restrict, suspend or terminate all or any part of the Online Banking Service ( <u>including the Website, Mobile App and the use and access of the Mobile Token</u> ) upon closure of the Customer's Designated Accounts or at any time without notice or reason to the Customer if the Bank has reasonable grounds for doing so.
5(c)	No Change	Save and except for the circumstances set out in Clauses 5(a) and 5(d) of these Terms and Conditions, the Bank will use its reasonable endeavours to provide prior notice to the Customer of any changes, amendments to, suspensions, restrictions or terminations of the Online Banking Services, the Website, the Mobile App <u>and/or the Mobile Token...</u>
5(e)	No Change	<del>The</del> <u>To the maximum extent permitted by applicable laws and regulations,</u> the Bank shall not be liable for any loss or damage suffered by the Customer as a result of or arising out of any voluntary or involuntary suspension or termination of any Online Banking Service for any reason whatsoever.
6(a)	No Change	For joint accounts that may be operated on the signature of only one of the account holders, the following material, if required by any one or more of the joint account holders, will be issued to each joint account holder <u>for use with the Online Banking Services:</u>
N/A	6(a)(ii)	<b>Add the following new clause 6(a)(ii) and update the subsequent numbering accordingly:</b> <u>separate Mobile Token; and</u>
6(a)(ii)	6(a)(iii)	when applicable, separate Security Token <del>for the Online Banking Services</del>
9(a)	No Change	Any Online Banking Instruction must be given by the Customer to the Bank by quoting the <del>User Name</del> <u>correct Username</u> , Password, Security Code <u>and/or authentication via the Mobile Token</u> (if requested by the Bank) and other information required by the Bank to effect Online Banking Transactions....
9(f)	No Change	Although the Bank will use reasonable endeavours to ensure that the Online Banking Instruction is executed in a timely fashion, there may be a time lag in transmission of data online. The Online Banking Services ( <u>including but without limitation to the Funds Transfer Services the Website, the Mobile App and the use of the Security Token and the Mobile Token</u> ) <u>are</u> also subject to (and may suffer failure or delay in processing and/or transmitting orders, communications or information as a

# 客戶重要通知

## Important Notice to Customers



		result of) interruption, failure of hardware or software, errors, transmission blackout, delayed transmission due to online traffic or incorrect data transmission due to the public nature of the internet, market volume or volatility, system failure or upgrades or maintenance or for other reasons....
9(g)	No Change	Although the Bank <del>has endeavoured</del> endeavours to avoid interruptions to the Online Banking Services, <u>(including but without limitation to where accessed via the Website, Mobile App, the Security Token and/or the Mobile Token)</u> , the Online Banking Services may suffer failure or delays and periods of malfunction or outage... The Bank may (but is not obliged to) notify the Customer of such cancellation of Online Banking Instruction by any means that the Bank may consider appropriate (including but not limited to email message or short message via SMS) and in all the circumstances <u>and to the maximum extent permitted by applicable laws and regulations</u> , the Bank will not assume any liability or responsibility for such cancellation of Online Banking Instruction or the non-notification of such cancellation of Online Banking Instruction, or inability on the part of the Customer to receive notification of such cancellation of Online Banking Instruction (whether or not due to the failure of the Customer to provide valid email address and/or mobile phone number capable of receiving short messages via SMS whatsoever)....
10(a)	No Change	The Customer undertakes to use the Online Banking Services <u>(including but without limitation to the Website, Mobile App, the Security Token and the Mobile Token)</u> in accordance with these Terms and Conditions and the operation policy and procedure relating to Online Banking Services provided by the Bank from time to time.
10(b)	No Change	The Customer undertakes <del>not to tamper with, modify, decompile, reverse engineer or otherwise alter or gain unauthorized access to any part of the Online Banking Services, the Website, the Mobile App or any of the software comprised in them:</del>  <u>(i) not to tamper with, modify, decompile, reverse engineer or otherwise alter or gain unauthorised access to any part of the Online Banking Services, the Website, the Mobile App, the Mobile Token, or any of the software comprised in them;</u> <u>(ii) not to access or use the Website, Mobile App, or Mobile Token on any device or operating system that has been modified outside the mobile device or operating system vendor supported or warranted configurations (e.g. devices that have been "jail-broken" or "rooted"). A jail broken or rooted device means one that has been freed from the limitations imposed on it by the mobile service provider and/or the phone manufacturer without their approval. The use of the Website, Mobile App, or Mobile Token on a jail broken or rooted device may compromise security and lead to fraudulent transactions; and</u> <u>(iii) to only download the Mobile App and its updates from the official mobile application online stores (e.g. Google Play / Apple App Store).</u>

# 客戶重要通知

## Important Notice to Customers



		The Bank is entitled to terminate the use of the Online Banking Services ( <u>including but without limitation to the Website, Mobile App, the Security Token and the Mobile Token</u> ) by the Customer without notice and to take legal action against the Customer for breach of <del>this undertaking</del> <u>the above undertakings. The Customer shall also be fully responsible and liable for all consequences arising from or in connection with the use of the Online Banking Services if he or she fails to take any of the security measures communicated or published by the Bank or his or her electronic devices' manufacturer from time to time.</u>
11(a)	No Change	Subject to the General Terms and Conditions and without prejudice to Clause 4 of these Terms and Conditions, if there is no gross negligence, fraud or fault on the part of the Customer, such as failing to properly safeguard his <u>or her</u> device(s) for using the Online Banking Services ( <u>including but without limitation to the Website, Mobile App, the Security Token and the Mobile Token</u> ), the Customer will not be liable for any direct loss suffered by the Customer as a result of any unauthorised Online Banking Transaction.
11(b)	No Change	The Customer shall hold harmless and indemnify the Bank, its officers, employees and any other person appointed by the Bank against all actions, liabilities, claims, demands, losses, damages and taxes of any kind made against or incurred by the Bank and such reasonable costs and expenses reasonably incurred by <del>the Bank</del> (including legal fees) in connection with the Bank's provision of the Online Banking Services ( <u>including but without limitation to the Website, Mobile App, the Security Token and the Mobile Token</u> ) and/or the exercise of the powers and rights of the Bank under these Terms and Conditions, unless such liabilities, claims, costs, damages, expenses, actions or proceedings are caused directly <u>and solely</u> by the negligence or wilful misconduct of any officer, employee or agent of the Bank and without gross negligence, fraud or fault on the part of the Customer.
12	No Change	<b>Change the heading to:</b> Ownership of the Security Token <u>and the Mobile Token (where applicable)</u>
12	No Change	The Security Token <del>is</del> <u>and the Mobile Token (where applicable) are</u> and shall at all times remain the property of the Bank and issued at the Bank's discretion and the Customer shall <u>immediately (in the case of the Security Token), return #to the Bank, or (in the case of the Mobile Token)</u> deregister or otherwise disable immediately upon the Bank's request. The Customer will ensure that the Security Token <del>is</del> <u>and the Mobile Token (where applicable) are</u> kept secure and under the personal control of the Customer and will not permit any person other than the Customer to use the Security Token <u>and the Mobile Token (where applicable).</u>
13	No Change	<b>Change the heading to:</b> Loss or Theft of the Security Token <u>and/or mobile device bound to Mobile Token</u>

# 客戶重要通知

## Important Notice to Customers



13	No Change	In the event of loss or theft of the Security Token <u>or the mobile device to which a Mobile Token is bound</u> , the Customer shall as soon as reasonably practicable notify such loss or theft to the Bank 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 Security Token <u>or mobile device to which a Mobile Token is bound</u> by any person. If a replacement Security Token <u>or Mobile Token (where applicable)</u> is issued, the Bank may charge a fee for it.
14(b)	No Change	The Customer understands and accepts that any person who has access to, possesses, knows or is allowed to find out the Password <u>and/or the Mobile Token Password, or has access to the Security Token (if any) or Mobile Token (where applicable)</u> may be able to have access to the Designated Account(s) and the Bank shall not be responsible for any losses in relation thereto.
14(c)(iii)	No Change	the Online Banking Services <u>(including but without limitation to the Website, Mobile App, the Security Token and the Mobile Token)</u> not being available, being restricted, varied, amended, suspended or terminated or becoming inoperative;
14(c)(iv)	No Change	the Customer's failure to carry out his <u>or her</u> responsibilities as provided in these Terms and Conditions; and/or
14(c)(v)	No Change	any loss of profits or opportunity or any other consequential or indirect loss or liability caused by the use of or inability to use the Online Banking Services or from any errors, inadequacies or failures of any machine, Online Banking Services, Website, Mobile App, <u>Security Token, Mobile Token</u> , internet, the Computer System, data processing system or transmission link or any industrial dispute or any other factor outside the control of the Bank or outside the control of the agents or sub-contractors of the Bank, whether caused by negligence or otherwise.
14(d)	No Change	If the Bank is found liable for any act or omission, negligence or default, its liability shall be <u>(to the maximum extent permitted by applicable law)</u> limited to the lesser of the amount of the direct loss or actual damage and the amount of the relevant transaction. The Bank shall not be responsible for any loss of profit or any special, consequential or indirect loss or damage arising out of such act, omission, negligence or default.
15(a)	No Change	The Customer acknowledges that internet is a technology that is rapidly changing, open and public in nature and its traffic congestion is unpredictable. The Customer understands that the Bank will use its reasonable endeavour to make sure that the Online Banking Services



# 客戶重要通知

## Important Notice to Customers



		<u>(including the Website, Mobile App, the Security Token and the Mobile Token)</u> continue to function, but the Customer also accepts that:
15(a)(ii)	No Change	the Online Banking Services, the Website, the Mobile App, <u>the Security Token and/or the Mobile Token (where applicable)</u> may not meet all the requirements or expectations of the Customer; and
15(a)(iii)	No Change	the operation, functionality and reliability of the Online Banking Services, the Website, the Mobile App, <u>the Security Token and/or the Mobile Token (where applicable)</u> ;
15(b)	No Change	Given the circumstances set out in Clause 15(a) of these Terms and Conditions, the Customer understands and agrees that all transaction(s) through the Online Banking Services are made entirely at his <u>or her</u> own risk.
16(a)(iii)	No Change	the Customer accesses, enters or uses any links to Third Party Website(s) or deals with Third Party Provider(s) entirely at his <u>or her</u> own risk and the Bank is not a party to any arrangement between the Third Party Provider(s) and the Customer;
17(a)	No Change	The Customer acknowledges that all Content(s) on the Website, the Mobile App, <u>the Mobile Token</u> , and all related software(s) are proprietary to the Bank and/or Third Party Provider(s) and are subject to IP Rights. Unless otherwise expressly stated or approved in writing by the Bank or such Third Party Provider(s) (as the case may be), nothing on the Website, the Mobile App or Third Party Website(s) shall be implied as granting the Customer any right or license to use any IP Rights related to or shown on the Website, the Mobile App, <u>the Security Token, the Mobile Token</u> , or Third Party Website(s).
17(b)(iii)	No Change	break into, access or use or attempt to break into, access or use any part of the Online Banking Services, the Website, the Mobile App, <u>the Security Token, the Mobile Token</u> , the Third Party Website(s), the Content(s) and/or any data areas on the Bank's server(s) or those of any Third Party Provider(s) for any purposes unauthorised by the Bank or such Third Party Provider(s);
17(b)(iv)	No Change	infringe the IP Rights of any person or any party in using the Website, the Mobile App, <u>the Security Token, the Mobile Token</u> , or any Content(s);
17(b)(v)	No Change	violate any applicable law of any applicable jurisdiction in the use of the Online Banking Services, the Website, <u>the Mobile App, the Security Token</u> and/or the Mobile <u>AppToken</u> ; and/or
18	No Change	The Bank may revise <u>or replace</u> these Terms and Conditions and/or introduce additional terms and conditions at any time and from time to time. <u>Any revision in accordance with applicable laws or regulatory requirements applicable to the Bank. Any revision, replacement or addition to these Terms and Conditions shall become effective subject to the Bank giving reasonable notice to the Customer which may be given by</u>

# 客戶重要通知

## Important Notice to Customers



		<p><u>physical or electronic means</u>, posting it on the Website or by such other means as the Bank thinks fit, and/or <u>taking any other action required by applicable laws or regulatory requirements applicable to the Bank</u>. <u>Any revised or additional Terms and Conditions</u> shall be binding on the Customer if the Customer continues to maintain or use the Online Banking Services on or after the effective date of the revision, <u>replacement</u> or addition.</p>
--	--	---

Customers may contact our branch staff for a copy of the full version of the revised terms and conditions. For enquiries, please contact any of our branch staff or call customer service hotline at +852 277 95533 or visit [www.asia.ccb.com](http://www.asia.ccb.com).

The above amendments shall be binding on customers if they continue to use our Electronic Banking Services and/or Online Banking Services on or after the Effective Date. If customers decline to accept the above amendments, they have the right to terminate the use of the Electronic Banking Services and/or Online Banking Services in accordance with the respective terms and conditions before the Effective Date. Should customers wish to terminate their Electronic Banking Services and/or Online Banking Services, please notify us through the Customer Service Hotline.

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  
July 2022