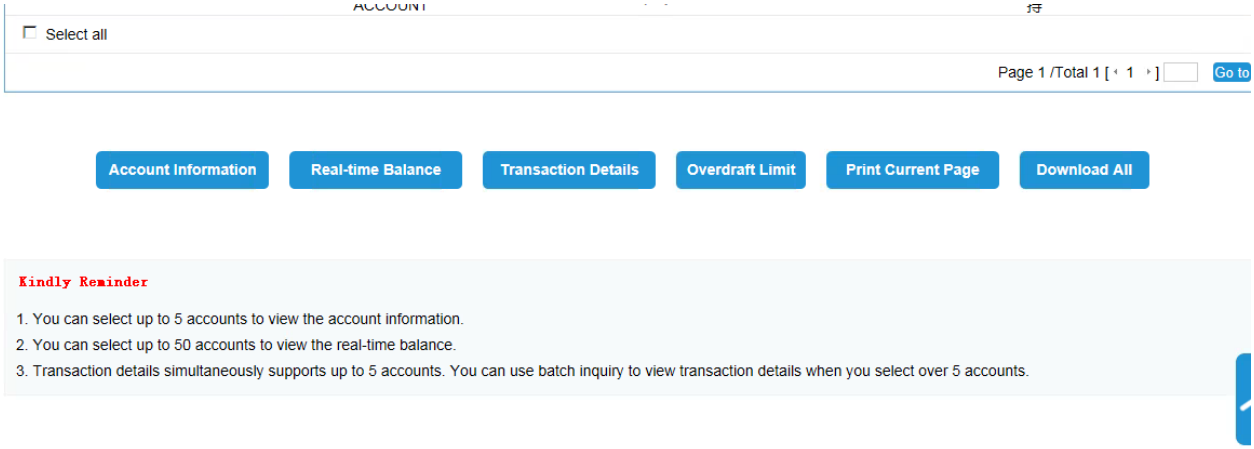
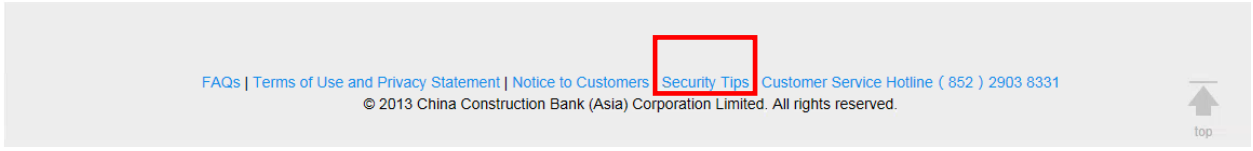
Contents

1 Internet Banking Security Tips





1. 1 What we have done to protect you?/我們為保護您的安全做了什麼？/我们为保护您的安全做了什么？

1.1.1 EN

- With the use of 128bit Secure Socket Layer (SSL) encryption, we ensure the security of your data during transmission.
- Our system will monitor each login attempt. If there are several consecutive login attempts with incorrect password, the online service will be suspended immediately.
- We will not ask for customers' account number, password or any personal information via emails.
- Our web servers are protected by firewall systems to prevent unauthorized access.
- CCB(Asia) Online Enterprise Banking Services provide one-time password (OTP) as one of your two-factor authentication tools for further verification when you need to conduct high-risk online transactions.
- You should not leave your Security Device unattended to avoid unauthorized use of such device by third party to conduct online transaction.

1.1.2 TC

- 通過使用 128 位安全套接字層（SSL）加密，我們確保您的資料在傳輸過程中的安全。

- 我們的系統會監視每個登陸嘗試。如果有多個連續的不正確的密碼嘗試登錄，線上服務將會暫停。
- 我們不會通過電子郵件詢問客戶的賬戶號碼，密碼或任何個人資訊。
- 我們的伺服器擁有防火牆系統的保護，可以防止未經授權的訪問。
- 當您需要進行高風險的網上交易時，中國建設銀行（亞洲）網上企業銀行會提供雙重身份核實的驗證工具之一的一次性密碼（OTP）來進行進一步確認。
- 隨時留意你的保安裝置，以避免未經授權的第三方使用這樣設備進行網上交易。

1.1.3 SC

- 通过使用 128 位安全套接字层（SSL）加密，我们确保您的资料在传输过程中的安全。
- 我们的系统会监视每个登陆尝试。如果有多个连续的不正确的密码尝试登录，线上服务将会暂停。
- 我们不会通过电子邮件询问客户的账户号码，密码或任何个人资讯。
- 我们的伺服器拥有防火墙系统的保护，可以防止未经授权的访问。
- 当您需要进行高风险的网上交易时，中国建设银行（亚洲）网上企业银行会提供双重身份核实的验证工具之一的一次性密码（OTP）来进行进一步确认。
- 随时留意你的保安装置，以避免未经授权的第三方使用这样设备进行网上交易。

1.2 What can you do to protect yourself?/你可以做些什麼來保護自己呢？/你可以做些什么来保护自己呢？

1.2.1 Password Protection/密碼保護/密码保护

1.2.1.1 EN

Password function is the key to your CCB(Asia) Online Enterprise Banking Services. It is important for you to safeguard your Customer Number, User Name, and Password. Please seriously consider the following suggestions:

- Destroy the original printed copy of your Password
- Change your initial password when you first access Online Banking Service.
- Change your Password regularly
- Use a combination of numbers, upper and lower case letters for your Password
- Avoid using a number or name that is likely to or can easily be guessed by others, for example birthday, ID number or telephone numbers
- Avoid to use the same Password for different web service accounts and systems
- Never read out your Password over the phone
- Never disclose your Password to anyone, including staff at CCB
- Never write down or record any Customer Number, User Name, and Password without disguising it
- Never include/send your Customer Number, User Name, and Password within an email message
- Ensure that no one is watching you while you key in your Customer Number, User Name, and Password

1.2.1.2 TC

密碼功能是保護您享受中國建設銀行（亞洲）網上企業銀行的關鍵。您需要仔細保護您的客戶號碼，用戶名稱和密碼。請認真考慮以下建議：

- 銷毀印有您密碼原始單據
- 當您第一次訪問網上銀行服務時更改您的初始密碼
- 定期更改您的密碼
- 使用數位，大寫字母和小寫字母的組合為您的密碼
- 避免使用容易地被他人猜到的號碼或姓名，例如出生日期，身份證號碼或電話號碼
- 避免將相同的密碼用於不同的網路服務賬戶和系統
- 切勿在電話中讀出你的密碼
- 切勿將您的密碼透露給任何人，包括建行的工作人員
- 切勿不加掩藏寫下或記錄任何客戶號碼，用戶名稱和密碼
- 切勿在電子郵件內容中包含或發送您的客戶號碼，用戶名稱和密碼
- 當您使用客戶號碼，用戶名稱和密碼時確保沒有人在看

1.2.1.3 SC

密码功能是保护您享受中国建设银行（亚洲）网上企业银行的关键。您需要仔细保护您的客户号码，用户名称和密码。请认真考虑以下建议：

- 销毁印有您密码原始单据
- 当您第一次访问网上银行服务时更改您的初始密码
- 定期更改您的密码
- 使用数位，大写字母和小写字母的组合为您的密码
- 避免使用容易地被他人猜到的号码或姓名，例如出生日期，身份证号码或电话号码
- 避免将相同的密码用于不同的网路服务账户和系统
- 切勿在电话中读出你的密码
- 切勿将您的密码透露给任何人，包括建行的工作人员
- 切勿不加掩藏写下或记录任何客户号码，用户名称和密码
- 切勿在电子邮件内容中包含或发送您的客户号码，用户名称和密码
- 当您使用客户号码，用户名称和密码时确保没有人在看

1.2.2 Fraudulent Website/詐騙網站/诈骗网站

1.2.2.1 EN

Fraudsters may send spoof emails pretending to be from China Construction Bank (Asia) Corporation Limited. Most of these emails appear to come from the true source of the bank.

Recipients of these emails will be requested to input their personal information such as their username, password, credit card number, etc through these emails.

Fraudsters through these emails may instruct the reader to visit the fraudulent websites via hyperlinks embedded in these emails and request users to input their personal and account information.

Please be reminded that the bank will NEVER ask customers to provide confidential data via emails, so do not respond to any suspicious emails that request for such information or click on an embedded hyperlink contained therein.

How to prevent?

- Make sure you are connected to the bank's official website at www.asia.ccb.com and/or m.asia.ccb.com for both desktop and mobile versions respectively before login or keying in any confidential data
- Do not access the website directly through hyperlinks embedded in e-mails. You should type www.asia.ccb.com and/or m.asia.ccb.com directly on the browser's address bar or access via a bookmark
- Verify the server certificate of our website (the locked padlock symbol at the bottom right hand corner of the browser)
- Update your anti-virus software and change your login password regularly

1.2.2.2 TC

詐騙者可能發送偽造的電子郵件，假裝是從中國建設銀行（亞洲）股份有限公司發出的。多數情況下這些郵件看上去像真的來自銀行。

郵件中會要求這些電子郵件的收件人輸入自己的個人資訊，如他們的用戶名稱，密碼，信用卡號碼等。

詐騙者通過這些電子郵件指導收件人通過訪問包含在郵件中的詐騙網站的超鏈結，要求用戶輸入他們的個人資訊和賬戶資訊。

請注意，銀行絕不會要求客戶通過電子郵件提供任何機密資料，所以不要回應任何可疑的、要求提供類似資訊的電子郵件，或單擊其中所含的超鏈結。

如何預防？

- 在登入及輸入任何保密資料前，請必須確保您是透過分別 www.asia.ccb.com 及/或 m.asia.ccb.com 桌面版或手機版進入本行的官方網站
- 不要使用藏於電郵內的超連結直接進入網站，您應在流覽器內的網址列內直接輸入 www.asia.ccb.com 及/或 m.asia.ccb.com 入或使用書簽
- 核實網站伺服器數位驗證（即流覽器右下角之「安全鎖」標誌）
- 經常更新您的防毒軟體並定期更改登入私人密碼

1.2.2.3 SC

诈骗者可能发送伪造的电子邮件，假装是从中国建设银行（亚洲）股份有限公司发出的。多数情况下这些邮件看上去像真的来自银行。

邮件中会要求这些电子邮件的收件人输入自己的个人资讯，如他们的用户名称，密码，信用卡号码等。

诈骗者通过这些电子邮件指导收件人通过访问包含在邮件中的诈骗网站的超链接，要求用户输入他们的个人资讯和账户资讯。

请注意，银行绝不会要求客户通过电子邮件提供任何机密资料，所以不要回应任何可疑的、要求提供类似资讯的电子邮件，或单击其中所含的超链接。

如何预防？

- 在登入及输入任何保密资料前，请必须确保您是透过分别 www.asia.ccb.com 及/或 m.asia.ccb.com 桌面版或手机版进入本行的官方网站
- 不要使用藏於电邮内的超连结直接进入网站，您应在浏览器内的网址列内直接输入 www.asia.ccb.com 及/或 m.asia.ccb.com 入或使用书签
- 核实网站伺服器数位验证（即浏览器右下角之「安全锁」标志）
- 经常更新您的防毒软件并定期更改登入私人密码

1.2.3 Spyware/間諜軟體/间谍软体

1.2.3.1 EN

Spyware is a computer software that monitors what users do with their computer and collects information of the computer users without the users' knowledge or consent. This software often comes from unseen components of "free download programs or applications".

The software will transmit the collected information to an unauthorized organization and more seriously, it can try to record what a user types in order to attempt to intercept passwords or credit card numbers.

How to prevent?

- Do not use public computers or mobile devices to logon to CCB(Asia) Online Enterprise Banking Services.
- Do not download any programs or software onto your computer from suspicious sources
- Install anti-virus and/or anti-spyware software programs in your computer and always run the programs before downloading programs or software or opening emails
- Regularly update your anti-virus and/or anti-spyware software programs and change your password

1.2.3.2 TC

間諜軟體是一種電腦軟體，它可以在使用者不知情或未經客戶同意的情況下監控用戶使用電腦並收集用戶資訊。該軟體往往來自於“免費下載程式或應用程式”的看不見的組成部分。

該軟體將收集到的資訊傳輸到未經授權的機構，更嚴重的是，它可以記錄用戶鍵入的內容，以試圖攔截密碼或信用卡號碼。

如何預防？

- 不要使用公用電腦或移動設備登錄到中國建設銀行（亞洲）網上企業銀行
- 不要下載任何來源可疑的程式或軟體到您的電腦
- 在您的電腦上安裝防病毒軟體和/或反間諜軟體程式，在下載程式或軟體或打開郵件之前運行該程式
- 定期更新您的防病毒軟體和/或反間諜軟體程式，並更改您的密碼

1.2.3.3 SC

间谍软体是一种电脑软体，它可以在用户不知情或未经客户同意的情况下监控用户使用电脑并收集用户资讯。该软体往往来自于“免费下载程式或应用程式”的看不见的组成部分。

该软体将收集到的资讯传输到未经授权的机构，更严重的是，它可以记录用户键入的内容，以试图拦截密码或信用卡号码。

如何预防？

- 不要使用公用电脑或移动设备登录到中国建设银行（亚洲）网上企业银行
- 不要下载任何来源可疑的程式或软体到您的电脑
- 在您的电脑上安装防病毒软体和/或反间谍软体程式，在下载程式或软体或打开邮件之前运行该程式
- 定期更新您的防病毒软体和/或反间谍软体程式，并更改您的密码

1.2.4 Unauthorized Access/未經授權的訪問/未经授权的访问

1.2.4.1 EN

In order to protect your computer and its contents and to stop unauthorized access to your computer, you should:

- Install anti-virus and/or anti-spyware software programs, a personal firewall, and security patches on your computer
- Install and regularly update anti-virus/anti-spyware software programs and security patches
- Run the anti-virus/anti-spyware software programs before downloading programs or software or opening emails

1.2.4.2 TC

為了保護您的電腦和它保存的擋，並阻止未經授權的訪問到您的電腦，您應該：

- 在您的電腦上安裝防病毒軟體和/或反間諜軟體，個人防火牆和安全補丁
- 安裝和定期更新防病毒軟體和/或反間諜軟體程式和安全補丁
- 下載程式或軟體，或打開電子郵件前運行防病毒軟體和/或反間諜軟體

1.2.4.3 SC

为了保护您的电脑和它保存的挡，并阻止未经授权的访问到您的电脑，您应该：

- 在您的电脑上安装防病毒软体和/或反间谍软体，个人防火墙和安全补丁
- 安装和定期更新防病毒软体和/或反间谍软体程式和安全补丁
- 下载程式或软体，或打开电子邮件前运行防病毒软体和/或反间谍软体

1.2.5 Other Preventive Actions/其他防護措施/其他防护措施

1.2.5.1 EN

Useful Security Tips to help you enjoy CCB(Asia) Online Enterprise Banking Services.:

- Remember to logout after you have completed your online activities
- Do not use sheared computers to access your CCB(Asia) Online Enterprise Banking Services.
- Do not leave your computer and/or mobile unattended when you are accessing your web service account
- Check the date and time of your last visit to the Company's official website every time after you have logged in
- Review the transfer limit for non-registered third party account and lower it if necessary
- Be alert of the SMS notification sent to you after each funds transfer to non-registered account via Online Banking

- Never install uncertain applications provided by any third party
- Review regularly and follow security tips published by the authorities, e.g. Hong Kong Association of Banks, the Consumer Council, the Hong Kong Police Force, the Hong Kong Monetary Authority, the Securities and Futures Commission or the Information Technology Services Department, etc.

1.2.5.2 TC

幫助您享受中國建設銀行（亞洲）網上企業銀行的一些有用安全提示：

- 完成線上活動後記得註銷
- 不要使用共用的電腦訪問您的中國建設銀行（亞洲）網上企業銀行
- 當你訪問你的網路賬戶服務時不要離開你的電腦和/或移動設備
- 每次登錄公司的官方頁面後都要檢查您上次訪問的日期和時間
- 審查非登記的第三方賬戶轉賬限額，並在必要時降低該限額
- 在每次通過網上銀行向非註冊賬戶進行資金轉移後，注意發送給您的短信通知
- 切勿安裝任何第三方提供的無法確定的應用程式
- 定期閱讀並遵循相關機構發佈的安全提示，例如：香港銀行公會，消費者委員會，香港警務處，香港金融管理局，證券及期貨事務監察委員會或資訊科技署等

1.2.5.3 SC

帮助您享受中国建设银行（亚洲）网上企业银行的一些有用安全提示：

- 完成线上活动后记得注销
- 不要使用共用的电脑访问您的中国建设银行（亚洲）网上企业银行
- 当你访问你的网路账户服务时不要离开你的电脑和/或移动设备
- 每次登录公司的官方页面后都要检查您上次访问的日期和时间
- 审查非登记的第三方账户转账限额，并在必要时降低该限额
- 在每次通过网上银行向非注册账户进行资金转移后，注意发送给您的短信通知
- 切勿安装任何第三方提供的无法确定的应用程式
- 定期阅读并遵循相关机构发布的安全提示，例如：香港银行公会，消费者委员会，香港警务处，香港金融管理局，证券及期货事务监察委员会或资讯科技署等

2 Public Website Security Tips

Remarks: The page layout will be revamped and to be developed by agency.

2.1 Password Protection/保護私人密碼/保护私人密码.

EN: http://www.asia.ccb.com/hongkong/personal/online_security/password_protection.html
TC: http://www.asia.ccb.com/hongkong_tc/personal/online_security/password_protection.html
SC: http://www.asia.ccb.com/hongkong_sc/personal/online_security/password_protection.html

2.1.1 Wording on banner

EN	TC	SC
Take measures to secure your passwords	小心保護您的私人密碼至關重要	小心保护您的私人密码至关重要

< New Banner image>

2.1.2 EN

Password function is the key to your Online Banking, Mobile Banking and Bank By Phone services. It is important for you to safeguard your Password and PINs. Please seriously consider the following suggestions:

How to MAKE your Password safe

<image>	• Use a combination of numbers, upper and lower case letters for your Mobile Banking / Online Banking Password • Avoid using a number or name that is likely to or can easily be guessed by others, for example, children's names, pets' names, birthday or telephone numbers • Avoid to use the same Password for different web service accounts and systems • Change your Password or PINs regularly

How to KEEP your Password safe

<image>	• Destroy the original printed copy of your Password or PINs • Never disclose your Password or PINs or any details of the Password or PINs to anyone • Never write down or record any Password or PINs without disguising it • Never store your password on computers, mobile phones, or placed in plain sight

How to USE your Password safe

<image>	• Ensure that no one is watching you while you key in your Password or PINs • Never read out your Password or PINs over the phone • Never include/send your Password or PINs within an email message

2.1.3 TC

私人密碼是您的「網上銀行」，「流動理財」及「電話銀行」服務之鑰匙，因此您必須小心選擇及保護您的私人密碼。請仔細考慮以下之提議:

如何設定安全的密碼

<image>	• 使用以數字、大楷及小楷字母組成的「網上銀行」及「流動理財」密碼 • 避免選取其他人能輕易猜中的數字或名稱，例如: 子女名字、寵物名字、生日日期或電話號碼 • 避免為各種不同網上服務賬戶及系統設定同一個私人密碼 • 定期更改您的密碼

如何安全地保存密碼

<image>	• 銷毀印有私人密碼的文件 • 切勿向任何其他人透露您的私人密碼或私人密碼的任何資料 • 切勿不加掩飾地寫下或記錄您的私人密碼 • 切勿記錄密碼在電腦、手機或當眼位置

如何安全地使用密碼

<image>	• 確保在沒有任何人士監察的情況下輸入您的私人密碼 • 切勿透過電話讀出任何密碼 • 切勿將密碼包含在/或透過電郵訊息發出

2.1.4 SC

私人密码是您的「网上银行」，「流动理财」及「电话银行」服务之钥匙，因此您必须小心选择及保护您的私人密码。请仔细考虑以下之提议:

如何设定安全的密码

<image>	• 使用以数字、大楷及小楷字母组成的「网上银行」及「流动理财」密码 • 避免选取其他人能轻易猜中的数字或名称，例如: 子女名字、宠物名字、生日日期或电话号码 • 避免为各种不同网上服务账户及系统设定同一个私人密码 • 定期更改您的密码

如何安全地保存密码

<image>	• 销毁印有私人密码的文件 • 切勿向任何其他人透露您的私人密码或私人密码的任何资料 • 切勿不加掩饰地写下或记录您的私人密码 • 切勿记录密码在电脑、手机或当眼位置

如何安全地使用密码

<image>	• 确保在没有任何人士监察的情况下输入您的私人密码 • 切勿透过电话读出任何密码 • 切勿将密码包含在/或透过电邮讯息发出

2.2 Fraudulent Website/偽冒網站/伪冒网站

EN: http://www.asia.ccb.com/hongkong/personal/online_security/fraudulent_website.html
TC: http://www.asia.ccb.com/hongkong_tc/personal/online_security/fraudulent_website.html
SC: http://www.asia.ccb.com/hongkong_sc/personal/online_security/fraudulent_website.html

2.2.1 Wording on banner

EN	TC	SC
Beware of fraudulent website and emails which may ask for your information	提防偽冒網站和 電郵套取您的資料	提防伪冒网站和 电邮套取您的资料

<New Banner image>

2.2.2 EN

What Fraudsters will do?

Fraudsters may send spoof emails pretending to be from China Construction Bank (Asia) Corporation Limited. Most of these emails appear to come from the true source of the bank.

Recipients of these emails will be requested to input their personal information such as their username, password, credit card number, etc through these emails.

Fraudsters through these emails may instruct the reader to visit the fraudulent websites via hyperlinks/ QR code embedded in these emails and request users to input their personal and account information.

Please be reminded that the bank will NEVER ask customers to provide confidential data via emails, so do not respond to any suspicious emails that request for such information or click on an embedded hyperlink/ QR code contained therein.

How to prevent?

	Make sure you are connected to the bank's official website at www.asia.ccb.com and/or m.asia.ccb.com for both desktop and mobile versions respectively before login or keying in any confidential data
<email with embed URL; a mouse courser with cross>	Do not access the website directly through hyperlinks/ QR code embedded in emails, internet search engines or suspicious pop-up windows. You should type www.asia.ccb.com and/or m.asia.ccb.com directly on the browser's address bar or access via a bookmark
	Verify the server certificate of our website (the locked padlock symbol at the upper left hand corner of the browser)

	Check the certificate information to ensure the certificate is issued to “online.asia.ccb.com” or “intl.ccb.com” and the certificate is still within a valid date.
<icon for anti-virus software >	Update your anti-virus and/or anti-spyware software programs and change your login password regularly

2.2.3 TC

騙徒會做甚麼?

有些欺詐集團會假冒中國建設銀行(亞洲)股份有限公司傳送偽冒電郵，這些電郵看似來自真實的機構。

偽冒電郵可能會要求您輸入您的用戶姓名、私人密碼、信用卡號碼等。

此外，有些騙徒更會透過偽冒電郵內的超連結/ 二維碼引導您進入偽冒網站，並要求您輸入一些個人資料或戶口資料。

請注意，本行絕對不會要求客戶透過電子郵件提供保密資料，客戶如收到此等要求提供保密資料的可疑電郵，切勿回覆，亦切勿使用有關之超連結/ 二維碼。

如何防止?

	在登入及輸入任何保密資料前，請必須確保您是透過分別 www.asia.ccb.com 及/或 m.asia.ccb.com 桌面版或手機版進入本行的官方網站
<email with embed URL; a mouse courser with cross>	不要使用藏於電郵、互聯網搜索引擎或快顯視窗內的超連結/ 二維碼直接進入網站，您應在瀏覽器內的網址列內直接輸入 www.asia.ccb.com 及/或 m.asia.ccb.com 入或使用書簽
	核實網站伺服器數位證書（即瀏覽器左上角之「安全鎖」標誌） 檢查數位證書，以確保證書是發給”online.asia.ccb.com”或“intl.ccb.com”和證書還在有效期內
<icon for anti-virus software >	經常更新您的防毒及/或防間諜軟件並定期更改登入私人密碼

2.2.4 SC

骗徒会做甚么?

有些欺诈集团会假冒中国建设银行(亚洲)股份有限公司传送伪冒电邮，这些电邮看似来自真实的机构。

伪冒电邮可能会要求您输入您的用户姓名、私人密码、信用卡号码等。

此外，有些骗徒更会透过伪冒电邮内的超连结/ 二维码引导您进入伪冒网站，并要求您输入一些个人资料或户口资料。

请注意，本行绝对不会要求客户透过电子邮件提供保密资料，客户如收到此等要求提供保密资料的可疑电邮，切勿回覆，亦切勿使用有关之超连结/ 二维码。

如何防止?

	在登入及输入任何保密资料前，请必须确保您是透过分别 www.asia.ccb.com 及/或 m.asia.ccb.com 桌面版或手机版进入本行的官方网站
<email with embed URL; a mouse courser with cross>	不要使用藏於电邮、互联网搜索引擎或快显视窗内的超连结/ 二维码直接进入网站，您应在浏览器内的网址列内直接输入 www.asia.ccb.com 及/或 m.asia.ccb.com 入或使用书签
 <>	核实网站伺服器数位证书（即浏览器左上角之「安全锁」标志） 检查数字证书，以确保证书是发给”online.asia.ccb.com”或“intl.ccb.com”和证书还在有效期内
<icon for anti-virus software >	经常更新您的防毒及/或防间谍软件并定期更改登入私人密码

2.3 Spyware/間碟軟件/间碟软件

EN: http://www.asia.ccb.com/hongkong/personal/online_security/spyware.html
TC: http://www.asia.ccb.com/hongkong_tc/personal/online_security/spyware.html
SC: http://www.asia.ccb.com/hongkong_sc/personal/online_security/spyware.html

2.3.1 Wording on banner

EN	TC	SC
Review your computer's security setting from time to time	不時檢查電腦的安全設定	不时检查电脑的安全设定

<New Banner image>

2.3.2 EN

What is Spyware?

<icon of spy>	Spyware is a computer software that monitors what users do with their computer and collects information of the computer users without the users' knowledge or consent. This software often comes from unseen components of "free download programs or applications". The software will transmit the collected information to an unauthorized organization and more seriously, it can try to record what a user types in order to attempt to intercept passwords or credit card numbers.

How to prevent?

<icon of download item from "?" site>	• Do not download any programs or software onto your computer from suspicious sources, or click on the hyperlinks and attachments from questionable sources including malicious SMS or MMS messages. Download and update CCB(Asia) Mobile App with "China Construction (Asia) Corporation Limited" as the trusted and verified developer at the official application store.
<anti-virus software with update mark>	• Install anti-virus and/or anti-spyware software programs in your computer and always run the programs before downloading programs or software or opening emails • Regularly update your anti-virus and/or anti-spyware software programs and change your password
<browser update>	• Use the latest versions of operating system, applications and browser
<computer login screen with many user head>	• Do not use public/ shared computers or mobile devices to logon to Online Banking and Mobile Banking

2.3.3 TC

甚麼是間諜軟件?

<icon of spy>	間諜軟件是一種在電腦用戶不知情或非允許下，監察用戶使用電腦之情況及搜集電腦用戶資料的電腦軟件。這些程式經常隱藏在「免費」程式內，間諜軟件可將搜集得來的資料傳送給他人，而它更可嘗試記錄用戶之輸入，從而得知用戶之私人密碼及信用卡號碼。

如何防止?

<icon of download item from "?" site>	切勿從不明來歷的來源下載任何程式或軟件在您的電腦上，或開啟來歷不明的超連結及附件，或開啟包含於惡意文字短訊或多媒體短訊內的超連結及附件。只從官方應用程式商店下載及升級由「China Construction (Asia) Corporation Limited」作為可信及已認證的開發商所推出的建行(亞洲)手機應用程式。 •
<anti-virus software with update mark>	• 在您的電腦上安裝防毒及/或防間諜軟件程式，並於下載程式或軟件或開啟電郵前，應先執行有關程式 • 定期更新您的防毒及/或防間諜軟件程式，並經常更改您的私人密碼
<browser update>	• 使用最新版本的操作系統、應用程式及瀏覽器
<computer login screen with many user head>	• 切勿使用公共/ 共享的電腦或流動裝置登入「網上銀行」及「流動理財」

2.3.4 SC

甚么是间谍软件?

<icon of spy>	间谍软件是一种在电脑用户不知情或非允许下，监察用户使用电脑之情况及搜集电脑用户资料的电脑软件。这些程式经常隐藏在「免费」程式内，间谍软件可将搜集得来的资料传送给他人，而它更可尝试记录用户之输入，从而得知用户之私人密码及信用卡号码。

如何防止?

<icon of download item from "?" site>	切勿从不明来历的来源下载任何程式或软件在您的电脑上，或开启来历不明的超连结及附件，或开启包含于恶意文字短讯或多媒体短讯内的超链接及附件。只从官方应用程式商店下载及升级由「China Construction (Asia) Corporation Limited」作为可信及已认证的开发商所推出的建行(亚洲)手机应用程式。 •
<anti-virus software with update mark>	• 在您的电脑上安装防毒及/或防间谍软件程式，并于下载程式或软件或开启电邮前，应先执行有关程式 • 定期更新您的防毒及/或防间谍软件程式，并经常更改您的私人密码
<browser update>	• 使用最新版本的操作系统、应用程式及浏览器
<computer login screen with many user head>	• 切勿使用公共/ 公享的电脑或流动装置登入「网上银行」及「流动理财」

2.4 Unauthorized access/未獲授權者侵襲/未获授权者侵袭

EN: http://www.asia.ccb.com/hongkong/personal/online_security/unauthorized_access.html
TC: http://www.asia.ccb.com/hongkong_tc/personal/online_security/unauthorized_access.html
SC: http://www.asia.ccb.com/hongkong_sc/personal/online_security/unauthorized_access.html

2.4.1 Wording on banner

EN	TC	SC
Install anti-spyware software and update on a regular basis	安裝防間碟軟件 並定期更新保安資訊	安装防间碟软件 并定期更新保安资讯

< New Banner image>

2.4.2 EN

In order to protect your computer and its contents and to stop unauthorized access to your computer, you should:

<icon of protector>	• Install anti-virus and/or anti-spyware software programs, a personal firewall, and security updates on your computer and/ or mobile devices • Run the anti-virus and/or anti-spyware software programs before downloading programs or software or opening emails • Regularly update anti-virus and/or anti-spyware software programs and install security patches
<icon with smart face>	• Keep your Username and Password confidential at all times • Check the date and time of your last visit to the Bank's Online Banking website and Mobile Banking App every time after you have logged in • Remember to logout after you have completed your online activities • Check your accounts from time to time and review alert messages and statements issued by the Bank in a timely manner
<icon with mobile phone>	• Opt for SMS One-Time password (OTP) verification for accessing Online Securities Trading Services

2.4.3 TC

為了保護您的電腦及所載的內容，並阻止未獲授權者進入您的電腦，您應該：

<icon of protector>	• 於您的電腦及/或流動裝置內安裝防毒及/或防間諜軟件程式，個人防火牆及安全更新 • 於下載程式或軟件或開啟電郵前，先執行防毒及/或防間諜軟件程式 • 定期更新防毒及/或防間諜軟件程式及安裝安全更新
<icon with smart face>	• 請將您的客戶名稱及私人密碼保密 • 每次登入後查閱您最近一次登入本行官方網上銀行網站和流動理財應用程式的日期及時間 • 每次使用網上服務後，請謹記登出 • 不時查核您的賬戶，並及時查閱銀行發出的提示訊息及結單

<icon with mobile phone>	• 選擇以手機短訊收取的一次性專用密碼作為核證以使用網上證券買賣服務

2.4.4 SC

为了保护您的电脑及所载的内容，并阻止未获授权者进入您的电脑，您应该：

<icon of protector>	• 于您的电脑及/或流动装置内安装防毒及/或防间谍软件程式，个人防火墙及安全更新 • 于下载程式或软件或开启电邮前，先执行防毒及/或防间谍软件程式 • 定期更新防毒及/或防间谍软件程式及安装安全更新
<icon with smart face>	• 请将您的客户名称及私人密码保密 • 每次登入后查阅您最近一次登入本行官方网上银行网站和流动理财应用程式的日期及时间 • 每次使用网上服务后，请谨记登出 • 不时查核您的账户，并及时查阅银行发出的提示讯息及结单
<icon with mobile phone>	• 选择以手机短讯收取的一次性專用密码作为核证以使用网上证券买卖服务

2.5 Other Preventive Actions/其它預防措施/其它预防措施

EN: http://www.asia.ccb.com/hongkong/personal/online_security/other_preventive_actions.html
TC: http://www.asia.ccb.com/hongkong_tc/personal/online_security/other_preventive_actions.html
SC: http://www.asia.ccb.com/hongkong_sc/personal/online_security/other_preventive_actions.html

2.5.1 Wording on banner

EN	TC	SC
Useful security tips to help you enjoy online banking	採用簡單實用的方法 令網上理財更安心	采用简单实用的方法 令网上理财更安心

< New Banner image>

2.5.2 EN

Access Online Banking Services safely

<icon of computer & mobile phone with protector>	• Avoid accessing Online Banking Services via public/ shared computers, and mobile devices or public Wi-Fi • Check the date and time of your last visit to the Bank's Online Banking website and Mobile Banking App every time after you have logged in • Do not leave your computer and/or mobile unattended when you are accessing your Online Banking Services • Remember to logout after you have completed your online activities • Review the transfer limit for non-registered third party account and lower it if necessary
<icon of mobile phone>	• Customer should provide a valid mobile phone and contact number for notification purpose. If any of these numbers is changed, please notify the Bank timely • Never install uncertain applications provided by any third party

Be aware of message from Bank

<icon of SMS>	• Be alert of the SMS notification sent to you after each funds transfer to non-registered account via Online Banking • If you have any suspicion or receive One-Time Password through SMS more than once, please contact us immediately • Be alert of the messages the Bank sent to you and verify your transaction records • Not to forward SMS One Time Password sent by the Bank to other mobile phone number • If you suspect anyone else has accessed your web service or you have found any suspicious transactions, please call our Bank By Phone at

	277 95533 or Credit Card 24-Hour Customer Service Hotline at 317 95533

Other related information

- To learn more about the e-leaflet of "Major Safety Tips on Using Internet Banking Services" published by Hong Kong Monetary Authority, please click here.
- To learn more about the publications published by The Hong Kong Association of Banks, please click here.

Peace of Mind Guarantee

Customers of Online Banking Service are fully protected against any third party fraud. You will not suffer any loss if money is withdrawn from your account without your authorization, provided that you have not acted with gross negligence or fraudulently. Any unauthorized transactions must be reported to the Bank within 90 days. Please refer to the Terms and Conditions for Electronic Banking Services.

Ensuring maximum online banking security is a joint effort and your cooperation is equally important. Please ensure that you observe the following precautionary measures so you can benefit from our online security service to its fullest.

2.5.3 TC

謹慎使用網上銀行服務

<icon of computer & mobile phone with protector>	• 避免使用公共/ 共用的電腦、流動裝置或公共無線網絡登入網上銀行服務 • 每次登入後查閱你最近一次登入本行官方網上銀行網站和流動理財應用程式的日期及時間 • 當您仍然使用網上銀行服務時，切勿離開你的電腦及/或放下您的手機不顧 • 每次使用網上服務之後，請謹記登出 • 評估您轉賬至非登記賬戶的限額，如有需要可降低其金額
<icon of mobile phone>	• 客戶需提供一個有效的手提電話及聯絡號碼，以作通知用途。如果有任何更改，請儘快通知本行 • 切勿安裝從第三者獲取而未經確定其安全性的應用程式

留意銀行訊息

<icon of SMS>	• 請留意透過「網上銀行」轉賬至非登記賬戶後發送給您的手機短訊通知 • 若遇任何可疑或透過短訊形式接受多個「一次性專用密碼」，請立即與我們聯絡 • 及時查閱本行發出的訊息並查核交易紀錄 • 請不要將手機短訊收取的「一次性專用密碼」轉傳至其他手提電話號碼

	• 若您懷疑您的網頁服務曾被其他人使用或發覺不尋常之交易，請即致電我們的「電話銀行」277 95533 或信用卡 24 小時客戶服務熱線 317 95533

其他相關資訊

- 有關香港金融管理局對「使用網上銀行的主要保安提示」所發行的電子小冊子，請按此了解更多。
- 有關香港銀行公會發行的參考刊物，請按此了解更多。

「安心保證」

本行保障網上銀行服務客戶不會蒙受任何因第三者欺詐所導致之損失。若客戶方面並無嚴重疏忽或欺詐，並於 90 日內向銀行舉報未受權之交易，您將毋須承擔任何未經受權而經其網上銀行戶口現金支出的損失。請參閱電子理財服務的有關條款和條件。

確保網上銀行保安完善需要客戶與銀行攜手努力，您的合作是同等重要。請您細心閱讀及採用以下預防措施，讓您盡享安全可靠的網上銀行服務。

2.5.4 SC

谨慎使用网上银行服务

<icon of computer & mobile phone with protector>	• 避免使用公共/ 共用的电脑、流动装置或公共无线网络登入网上银行服务 • 每次登入后查阅你最近一次登入本行官方网上银行网站和流动理财应用程式的日期及时间 • 当您仍然使用网上银行服务时，切勿离开你的电脑及/或放下您的手机不顾 • 每次使用网上服务之后，请谨记登出 • 评估您转账至非登记账户的限额，如有需要可降低其金额
<icon of mobile phone>	• 客户需提供一个有效的手提电话及联络号码，以作通知用途。如果有任何更改，请尽快通知本行 • 切勿安装从第三者获取而未经确定其安全性的应用程式

留意银行讯息

<icon of SMS>	• 请留意透过「网上银行」转账至非登记账户后发送给您的手机短讯通知 • 若遇任何可疑或透过短讯形式接受多个「一次性专用密码」，请立即与我们联络 • 及时查阅本行发出的讯息并查核交易纪录 • 请不要将手机短讯收取的「一次性专用密码」转传至其他手提电话号码 • 若您怀疑您的网页服务曾被其他人使用或发觉不寻常之交易，请即致电我们的「电话银行」277 95533 或信用卡 24 小时客户服务

	热线 317 95533

其他相关资讯

- 有关香港金融管理局对「使用网上银行的主要保安提示」所发行的电子小册子，请按此了解更多。
- 有关香港银行公会发行的参考刊物，请按此了解更多。

「安心保证」

本行保障网上银行服务客户不会蒙受任何因第三者欺诈所导致之损失。若客户方面并无严重疏忽或欺诈，并于 90 日内向银行举报未受权之交易，您将毋须承担任何未经受权而经其网上银行户口现金支出的损失。请参阅电子理财服务的有关条款和条件。

确保网上银行保安完善需要客户与银行携手努力，您的合作是同等重要。请您细心阅读及采用以下预防措施，让您尽享安全可靠的网上银行服务。

2.6 Mobile Banking Security/流動理財保安/流动理财保安

EN: http://www.asia.ccb.com/hongkong/personal/online_security/mobile_banking_security.html
TC:
http://www.asia.ccb.com/hongkong_tc/personal/online_security/mobile_banking_security.html
SC:
http://www.asia.ccb.com/hongkong_sc/personal/online_security/mobile_banking_security.html

2.6.1 Wording on banner

EN	TC	SC
Tips to help you bank on the go with confidence	助您隨時隨地安心理財	助您随时随地安心理财

< New Banner image>

2.6.2 EN

Secure access to your Mobile Banking

<icon of mobile with protector>	• Customer should provide a valid mobile phone and contact number for notification purpose. If any of these numbers is changed, please notify the Bank timely. • Avoid sharing of your mobile phone with others. If sharing is unavoidable, remember to set restrictions on your mobile phone. • Do not access Mobile Banking; disclose or enter any personal information (including Username and Password), if someone else nearby can read the screen of your mobile phone. • Always lock your mobile phone by password or pattern when it is not in use. • Closing the browser does not equivalent to logging out of Mobile Banking successfully. Click on the “Logout” button and follow the log out procedures to protect your account information. • Regularly remove all caches and browsing history stored in your mobile phone.

Safe usage of Touch Logon Service

	• Store only your own fingerprints on your mobile device so as to safeguard your account information and your personal details in your device. • When you change to a new mobile device, deactivate the Touch Logon Service on your old mobile device before you activate the Service on your new device. • If your mobile device with the Touch Logon Service activated is lost or stolen, please contact us immediately to suspend the Online Banking Services in order to prevent unauthorized access. • If you suspect the fingerprints in your mobile device are changed, you are advised to deactivate your Touch Logon Service and reset the fingerprint

	authentication setting of your mobile device. • Avoid activating the Touch Logon Service on jailbroken or rooted mobile devices as there may be security loopholes and it is less secure. • If your fingerprint settings in your mobile device have been changed (e.g. add or delete fingerprints), you have to reactivate Touch Logon Service with Online Banking username and password. • Do not disclose the Online Banking username and password to anyone. • Keep your mobile device properly and lock it with relatively complicated passcode.

Protect your Mobile system

<android & iOS icon with protector>	• Do not hack (or 'jailbreak' or 'root') your mobile device as this can make it open to infection from a virus or spyware. • Disable any wireless network functions (e.g. Wi-Fi, Bluetooth, NFC) not in use. Choose encrypted networks when using Wi-Fi and remove any unnecessary Wi-Fi connection settings.
<play store & app store with protector>	• Download mobile applications from reputable sources only, e.g. Apple App Store, Google Play and the Bank's website. • Install security software where available. • Download and install the latest system updates as soon as they become available. These include important security updates that help keep your device and data protected. • Examine carefully any app installation request before accepting it to make sure it's legitimate. • Read permission requests carefully when installing any apps. Be wary of apps that ask for permissions that seem unusual or unnecessary or that use large amounts of data or battery life.

Other related information

- To learn more about the e-leaflet of "Major tips on protection of your computers and mobile phones" published by Hong Kong Monetary Authority, please click here.
- To learn more about the publications published by The Hong Kong Association of Banks, please click here.

2.6.3 TC

安全使用流動理財

<icon of mobile with protector>	• 客戶需提供一個有效的手提電話及聯絡號碼，以作通知用途。如果有任何更改，請儘快通知本行。 • 盡量避免與他人共用您的手機。如您必須與他人共用手機，請於手機內設定權限以防止他們作非法使用。 • 切勿在他人視線範圍內登入流動理財服務、披露或輸入任何個人資料

	(包括用戶名稱及密碼)。 • 使用後以密碼或圖案鎖上您的手機。 • 關閉手機瀏覽器並不代表您已成功登出流動理財服務，您應直接按下「登出」及按照指示完成登出程序，以確保您的資料獲得妥善保障。 • 定期清除手機瀏覽器內的暫存檔案及瀏覽記錄。

安全使用指紋登入

	• 在您的流動裝置上只登記您本人的指紋，以保護您的賬戶資料及裝置上的其他個人資訊。 • 如要更換流動裝置，請您先在您原有的流動裝置上停用指紋登入服務後才於新的流動裝置啟動此服務。 • 如您遺失或失竊了已啟動指紋登入的流動裝置，請立即聯絡我們暫停此服務，以防止他人盜用。 • 如您懷疑手機的指紋被更改，您需要儘快停用指紋登入服務及重設流動裝置的指紋辨識功能。 • 我們建議您切勿於已越獄/破解的手機裝置啟動指紋登入，因為裝置系統可能存在安全性漏洞以及安全性較低。 • 如您更改了手機上的指紋紀錄（如：新增及/或刪除指紋），您需要以網上銀行客戶名稱及密碼重新啟動指紋登入服務。 • 切勿透露您的網上銀行客戶名稱及密碼予任何人。 • 請妥善保管您的流動裝置及使用比較複雜的密碼。

保護您的手機裝置

<android & iOS icon with protector>	• 請勿嘗試破解您手機內預設的操作系統(或稱「越獄」或「刷機」)，這可導致您的手機易受電腦病毒或間諜軟件感染。 • 關閉無需使用的無線網絡功能(如 Wi-Fi、藍芽、NFC)。如需使用 Wi-Fi，應選用加密的網絡，並移除不必要的 Wi-Fi 連線設定。
<play store & app store with protector>	• 只從信譽良好的來源下載應用程式，例如 Apple App Store、Google Play 及本行網站。 • 於您的手機內安裝適用的保安軟件。 • 盡快下載及安裝最新版本的系統更新軟件以獲得重要保安更新，以保護您的裝置及其資料。 • 接受軟件安裝請求前需留意該請求是否合理。 • 安裝軟件時小心留意權限細則，當軟件要求不尋常或不必要的權限，或需使用大量數據或耗電量高時，需特別提防。

其他相關資訊

- 有關香港金融管理局對「使用網上銀行的主要保安提示」所發行的電子小冊子，請按此了解更多。
- 有關香港銀行公會發行的參考刊物，請按此了解更多。

2.6.4 SC

安全使用流动理财

<icon of mobile with protector>	• 客户需提供一个有效的手提电话及联络号码，以作通知用途。如果有任何更改，请尽快通知本行。 • 尽量避免与他人共用您的手机。如您必须与他人共用手机，请於手机内设定权限以防止他们作非法使用。 • 切勿在他人视线范围内登入流动理财服务、披露或输入任何个人资料(包括用户名称及密码)。 • 使用後以密码或图案锁上您的手机。 • 关闭手机浏览器并不代表您已成功登出流动理财服务，您应直接按下「登出」及按照指示完成登出程序，以确保您的资料获得妥善保障。 • 定期清除手机浏览器内的暂存档案及浏览记录。

安全使用指纹登录

<android & iOS icon with protector>	• 在您的流动装置上只登记您本人的指纹，以保护您的账户资料及装置上的其他个人信息。 • 如要更换流动装置，请您先在您原有的流动装置上停用指纹登录服务后才于新的流动装置启动此服务。 • 如您遗失或失窃了已启动指纹登录的流动装置，请立即联络我们暂停此服务，以防止他人盗用。 • 如您怀疑手机的指纹被更改，您需要尽快停用指纹登录服务及重设流动装置的指纹辨识功能。 • 我们建议您切勿于已越狱/破解的手机装置启动指纹登录，因为装置系统可能存在安全漏洞以及安全性较低。 • 如您更改了手机上的指纹纪录（如：新增及/或删除指纹），您需要以网上银行客户名称及密码重新启动指纹登录服务。 • 切勿透露您的网上银行客户名称及密码予任何人。 • 请妥善保管您的流动装置及使用比较复杂的密码。

保护您的手机装置

<android & iOS icon with protector>	• 请勿尝试破解您手机内预设的操作系统(或称「越狱」或「刷机」)，这可导致您的手机易受电脑病毒或间谍软件感染。 • 关闭无需使用的无线网络功能(如 Wi-Fi、蓝芽、NFC)。如需使用 Wi-Fi，应选用加密的网络，并移除不必要的 Wi-Fi 连线设定。
<play store & app store with protector>	• 只从信誉良好的来源下载应用程式，例如 Apple App Store、Google Play 及本行网站。 • 於您的手机内安装适用的保安软件。 • 尽快下载及安装最新版本的系统更新软件以获得重要保安更新，以保护您的装置及其资料。 • 接受软件安装请求前需留意该请求是否合理。 • 安装软件时小心留意权限细则，当软件要求不寻常或不必要的权限，

	或需使用大量数据或耗电量高时，需特别提防。

其他相关资讯

- 有关香港金融管理局对「使用网上银行的主要保安提示」所发行的电子小册子，请按此了解更多。
- 有关香港银行公会发行的参考刊物，请按此了解更多。

2.7 Security Tips for ATM Cards/銀行卡保安提示/银行卡保安提示

EN: http://www.asia.ccb.com/hongkong/personal/online_security/atm_security.html
TC: http://www.asia.ccb.com/hongkong_tc/personal/online_security/atm_security.html
SC: http://www.asia.ccb.com/hongkong_sc/personal/online_security/atm_security.html

2.7.1 Wording on banner

EN	TC	SC
Take care your bank card protect you better	小心使用銀行卡 理財更大保障	小心使用银行卡 理财更大保障

< New Banner image>

2.7.2 EN

Keep your card safe

<Card with lock>	• Sign on the signature panel at the back of your bank card immediately with a permanent ink pen upon receipt of your bank card and keep the card in a secure place. Contact the Bank immediately if you lose your bank card/PIN • Do not keep the bank card and the PIN together. Never write down the PIN on the bank card or on anything usually kept with or near it • Do not allow anyone else to use your bank card and PIN • Call our 24-hour Bank By Phone at (852)277 95533 or notify any of our branches immediately if your bank card is retained by ATM, lost or stolen

Keep your PIN safe

<PIN code with safeguard>	• Change your PIN immediately when using your bank card for the first time and destroy the PIN letter • Do not use easily accessible personal information such as birthday, telephone number or recognizable part of your name for selecting password • Do not use your bank card PIN for any other cards, internet banking accounts, online memberships or internet services • Change your PIN regularly • Do not write down or record the PIN without disguising it • Do not disclose your card PIN to anyone else, including our staff

When you are using your card at ATM

<icon based on the content in right>	• Cover the keypad when entering the PIN • If the keypad cover (refer to below) is removed or damaged, stop the transaction and notify the Bank immediately

	 • If there is any suspicious device (e.g. Pinhole Camera, Skimming Device) or damage on card insert slot, cancel the transaction immediately and contact the Bank if you have any inquiry  • Do not accept any assistance from strangers

After use, before leaving the ATM

<icon based on the content in right>	• Remember to take out your bank card from ATM after every transaction • Count the banknotes immediately after each cash withdrawal. Do not take away any banknotes at the cash dispenser or bank card at the card insertion slot left behind by someone else. Let the banknotes or bank card return to the ATM automatically

Other Notices

<icon of Reminder>	• If you intend to withdraw cash from overseas ATMs, check with our bank whether your intended overseas destination can support cash withdrawal using your bank card. You should also activate the overseas bank cash withdrawal function in advance and set a prudent overseas ATM cash withdrawal limit and an activation period • Check the transaction records provided by our bank in a timely manner. Inform our bank immediately if you lose your bank card, or in case of any suspicious transactions or situations. Banks will not ask for any sensitive personal information (including passwords) through phone calls or emails

	• Call our 24-hour Bank By Phone at (852)277 95533 immediately or notify any of our branches during office hours if your bank card is retained by ATM, lost or stolen

Other related information

- To learn more about the e-leaflet of "Major safety tips on using ATMs" published by Hong Kong Monetary Authority, please click here.
- To learn more about the publications published by The Hong Kong Association of Banks, please click here.

<caution >	Please kindly note that, you will be liable for all losses if you do not act according to the security tips above and/or you have acted with negligence or fraudulently or have failed to inform us as soon as reasonably practicable after having found that the card has been lost or stolen. For your protection, please refer to our security advice from time to time.

2.7.3 TC

妥善保管你的卡

<Card with lock>	• 在收到銀行卡後，請立即於卡背簽名位置以不褪色原子筆簽署及把銀行卡保存於安全之地方，如有遺失，請即時通知本行 • 切勿把銀行卡與其私人密碼一起存放。絕不可在銀行卡上或任何其他經常與銀行卡放在一起或放在銀行卡附近的物件上，寫下個人密碼 • 不應讓任何其他人士使用你的銀行卡或個人密碼 • 如銀行卡被自動櫃員機沒收、遺失或被竊，請即致電本行 24 小時「電話銀行」服務(852) 277 95533 報失或於辦公時間內通知本行任何一間分行

妥善保管你的密碼

<PIN code with safeguard>	• 於首次使用銀行卡時，請立即更改密碼，並銷毀密碼函 • 設定新密碼時，切勿選用容易讓人取得的個人資料如出生日期、電話號碼或客戶姓名中可認知的部分資料 • 切勿將此銀行卡之私人密碼作為其他卡類產品、網上銀行戶口、網上會員或任何網上服務的客戶名稱及密碼 • 請定期更改銀行卡密碼 • 不應直接寫下或記下個人密碼，而不加掩飾 • 不應向任何人地透露你的密碼，包括本行職員

使用你的銀行卡時

<icon based on the	• 於輸入密碼時，請用手或其他物件遮蓋 • 如發現按密碼保護蓋(參考下圖)被移除或破壞，應停止交易並立即通知本行

content in right>	 • 如發現可疑裝置(如針孔攝影機、不尋常讀卡裝置)或入卡槽被破壞，應停止交易並立即通知本行  • 於交易期間，避免接受其他人仕的協助

使用後，離開自動櫃員機前

<icon based on the content in right>	• 每次使用完畢，請緊記從自動櫃員機取回銀行卡 • 提款後應即時點算鈔票。切勿取去別人遺留於出錢槽的鈔票或插卡口的銀行卡，應讓鈔票或銀行卡自動退回機內

其他注意事項

<icon of reminder>	• 如需境外提款，可向本行查詢當地櫃員機能否支援，並預先透過指定途徑啟動有關功能、設定審慎的提款限額和有效日期 • 及時查核銀行發出的交易紀錄。若發現遺失銀行卡、可疑交易或情況，應立即通知本行。本行一定不會以電話或電郵，要求提供任何敏感的個人資料(包括密碼) • 如銀行卡被自動櫃員機沒收、遺失或被竊，請即致電本行 24 小時「電話銀行」服務(852) 277 95533 報失或於辦公時間內通知本行任何一間分行

其他相關資訊

- 有關香港金融管理局對「使用網上銀行的主要保安提示」所發行的電子小冊子，請按此了解更多。
- 有關香港銀行公會發行的參考刊物，請按此了解更多。

<caution >	如您未有遵守以上保安貼士及未有於合理時間內通知本行，及/或有欺詐或嚴重疏忽的行為，您便須承擔所有因卡被盜用而引致的損失。 請緊記查閱本行提供的有關保安建議。

2.7.4 SC

妥善保管你的卡

<Card with lock>	• 在收到银行卡后，请立即于卡背签名位置以不褪色原子笔签署及把银行卡保存于安全之地方，如有遗失，请即时通知本行 • 切勿把银行卡与其私人密码一起存放。绝不可在银行卡上或任何其他经常与银行卡放在一起或放在银行卡附近的物件上，写下个人密码 • 不应让任何其他人士使用你的银行卡或个人密码 • 如银行卡被自动柜员机没收、遗失或被窃，请即致电本行 24 小时「电话银行」服务(852) 277 95533 报失或于办公时间内通知本行任何一间分行

妥善保管你的密码

<PIN code with safeguard>	• 于首次使用银行卡时，请立即更改密码，并销毁密码函 • 设定新密码时，切勿选用容易让人取得的个人资料如出生日期、电话号码或客户姓名中可认知的部分资料 • 切勿将此银行卡之私人密码作为其他卡类产品、网上银行户口、网上会员或任何网上服务的客户名称及密码 • 请定期更改银行卡密码 • 不应直接写下或记下个人密码，而不加掩饰 • 不应向任何人地透露你的密码，包括本行职员

使用你的银行卡时

<icon based on the content in right>	• 于输入密码时，请用手或其他物件遮盖 • 如发现按密码保护盖(参考下图)被移除或破坏，应停止交易并立即通知本行

	 • 如发现可疑装置(如针孔摄影机、不寻常读卡装置)或入卡槽被破坏，应停止交易并立即通知本行  • 于交易期间，避免接受其他人仕的协助

使用后，离开自动柜员机前

<icon based on the content in right>	• 每次使用完毕，请紧记从自动柜员机取回银行卡 • 提款后应实时点算钞票。切勿取去别人遗留于出钱槽的钞票或插卡口的银行卡，应让钞票或银行卡自动退回机内

其他注意事项

<icon of reminder>	• 如需境外提款，可向本行查询当地柜员机能否支持，并预先透过指定途径启动有关功能、设定审慎的提款限额和有效日期 • 及时查核银行发出的交易纪录。若发现遗失银行卡、可疑交易或情况，应立即通知本行。本行一定不会以电话或电邮，要求提供任何敏感的个人资料(包括密码) • 如银行卡被自动柜员机没收、遗失或被窃，请即致电本行 24 小时「电话银行」服务(852) 277 95533 报失或于办公时间内通知本行任何一间分行

其他相关资讯

- 有关香港金融管理局对「使用网上银行的主要保安提示」所发行的电子小册子，请按此了解更多。
- 有关香港银行公会发行的参考刊物，请按此了解更多。

<caution >	如您未有遵守以上保安贴士及未有于合理时间内通知本行，及/或有欺诈或严重疏忽的行为，您便须承担所有因卡被盗用而引致的损失。 请紧记查阅本行提供的有关保安建议。