BEA東亞銀行

BEA Credit Card/BEA Mobile Contactless Payment Service Usage Essentials

To safeguard your interests, please pay attention to the following tips when using your BEA Credit Card and/or the BEA Mobile Contactless Payment Service:

- When you first receive your credit card, sign the back of the card immediately.
- Set up your authentication identification such as a passcode, pattern, or biometric identification such as your fingerprint ("Authentication Credential"), when you activate the mobile contactless payment service.
- Do not use a smartphone or other near-field communication (NFC) – enabled device including mobile phones, computer tablets, or other mobile devices as specified by the bank from time to time (jointly, "Mobile Devices") which have any pirated, hacked, fake, or unauthorised applications, or on which the software lock has been overridden (such as jailbroken Mobile Devices), for the mobile contactless payment service.
- Your Mobile Device may need to connect to a cellular or wireless network when you activate the mobile contactless payment service or make a mobile contactless transaction.
- Do not download or use software or apps from untrustworthy sources. Keep your Mobile Devices' operating system and apps updated, and always have an up-to-date anti-malware and antivirus programme installed on your Mobile Devices.
- If possible, turn off NFC functionality when you do not want to conduct mobile contactless payments.
- To prevent your Mobile Devices from being accessed when they are not in use or unattended, always lock them and keep the auto-lock function activated.
- Take care of your credit card, your credit card information, and/or Mobile Devices with activated mobile contactless payment services, and never leave them unattended or lend them to anyone. Do not allow anyone else to use your credit card and/or Mobile Devices – this will help prevent any unauthorised attempts to make Card-Not-Present transactions. "Card-Not-Present" transactions are payments where the credit card is not physically presented (including but not limited to online and mobile payments, payments by telephone, physical mail, etc.; excluding recurring payments).
- Do not use your identity card number, telephone number, date of birth, driver's licence number, or any popular number sequences (such as 987654 or 123456) as your Personal Identification Number ("PIN") and/or passcode. Avoid using the same digit consecutively or the same sequence of numbers more than twice (such as 112233 or 383838).
- Do not disclose your PIN and/or passcode and/or pattern to anyone, nor write down/record the PIN and/or passcode and/or pattern without disguising it. In addition, do not send your PIN and/or passcode via email/SMS, and never use the same PIN and/or passcode and/or pattern to access other services.
- Do not permit any other person to use your Authentication Credential.
- Do not write down/record your PIN and/or passcode and/or the pattern of your credit card or Mobile Device, or on anything usually kept with or near them.
- For security reasons, change your PIN and/or passcode and/or pattern regularly.
- Do not, under any circumstances, disclose your PIN and/or passcode and/or pattern to anyone who claims to represent the Bank; or who claims to be the Bank's employee, nor to other authorised persons, nor the police. It is not necessary for anyone other than you to know your PIN and/or passcode and/or pattern. The Bank will never ask for your PIN and/or passcode and/or pattern by any means such as email, SMS, phone, etc.
- If your PIN and/or passcode and/or pattern is lost, stolen, or you suspect that it has been identified by another person, change the PIN and/or passcode and/or pattern immediately and call our Customer Services Hotline to report the case.
- Be alert to your surroundings before conducting any banking transactions. Make sure no one sees your PIN and/or passcode and/or pattern, and cover the keypad when you enter your PIN and/or passcode and/or pattern on any device, such as a personal computer, ATM, Mobile Device, or other self-service/point-of-sale terminal.
- Do not use a public computer or electronic device to enter your personal or credit card information.
- Ignore emails or phone calls seeking your personal or account information. Resist volunteering any personal information or financial information through email or over the phone.
- Check the total amount on the sales slip before signing/completing a transaction, and keep the sales slip for future reference.
- Do not sign any blank or incomplete sales slips.
- Ensure you get back your credit card once the purchase is completed, and check that the returned card is yours.
- Examine your statements and check all of the transactions carefully. Please call our Customer Services Hotline immediately if you detect any doubtful transaction.
- Inform the bank when your personal information, including but not limited to your address and mobile phone number, is changed.
- If your credit card or Mobile Device with activated mobile contactless payment service is lost or stolen, report this to the bank immediately by calling our Customer Services Hotline, or through our mobile banking (if your mobile phone number is recorded in our system and you have activated our mobile banking).
- If there is any actual or possible unauthorised use of your Authentication Credential or Mobile Device with activated mobile contactless payment service, report this to the bank immediately.
- Deactivate the mobile contactless payment service before disposing of any Mobile Devices on which this service has been activated.
- Please refer to these BEA Credit Card/BEA Mobile Contactless Payment Service Usage Essentials from time to time for updated security advice.

For enquiries, please call the BEA Credit Card Customer Services Hotline on 3608 6628.

Issued by The Bank of East Asia, Limited 東亞銀行有限公司

(01/2021)

BEA東亞銀行

東亞銀行信用卡/東亞銀行流動非接觸式付款服務使用須知

為保障你的利益：請留意下列有關使用東亞銀行信用卡及/或東亞銀行流動非接觸式付款服務的提示：

- 當收到你的信用卡後，立即在卡背面簽署。
- 在啟動流動非接觸式付款服務時，你須設定認證識別元素如認證密碼、圖形或生物識別元素如指紋(「認證憑據」)。
- 你不應在裝有盜版、破解版、偽造或未獲授權應用程式的智能手機或支援近場通訊(NFC)的裝置，包括手提電話、平版電腦及本行不時指定的流動裝置(「流動裝置」)或軟件保護被破解的流動裝置(例如「越獄」(jailbroken)流動裝置)安裝或使用流動非接觸式付款服務。
- 啟動流動非接觸式付款服務或進行流動非接觸式付款時，你的流動裝置可能需要使用電話網絡或無線數據網絡。
- 切勿下載或使用來歷不明的軟件或程式。 使用最新版本的流動裝置操作系統及程式，及安裝最新版本之惡意程式清除及防毒軟件。
- 在不需要進行流動非接觸式付款時，請盡可能關閉流動裝置的NFC功能。
- 為防止任何人士於你不使用或離開你的流動裝置時接觸或使用你的流動裝置，請鎖機及為你的流動裝置啟動自動上鎖功能。
- 小心保管你的信用卡、信用卡資料及/或已啟動流動非接觸式付款服務之流動裝置，切勿隨便亂放或借給任何人。不要讓任何人士使用你的信用卡及/或流動裝置，以防任何人企圖進行未經授權的「無卡支付」交易。「無卡支付」交易指不需要出示實物信用卡的支付交易(包括但不限於經網上/電話/郵購/手機支付之交易，但定期性支付交易除外)。
- 請勿以身份證號碼、電話號碼、出生日期、駕駛執照或任何常用數字組合(如987654或123456)作為私人密碼及/或認證密碼，及不應連續使用同一數字或同一組數字多於兩次(如112233或383838)。
- 切勿認將私人密碼及/或認證密碼及/或圖形告知任何人，以及不應直接寫下/記下私人密碼及/或認證密碼及/或圖形，而不加掩藏。另外，切勿將私人密碼及/或認證密碼以電子郵件/手機短訊傳送，或以相同之私人密碼及/或認證密碼及/或圖形使用其他服務。
- 切勿允許任何人士使用你的認證憑據。
- 切勿在信用卡或任何經常與卡放在一起或放在卡附近的物件上，寫下/記下私人密碼及/或認證密碼及/或圖形。
- 為保安理由，請定期更改私人密碼及/或認證密碼及/或圖形。
- 在任何情況下，切勿將私人密碼及/或認證密碼及/或圖形告知任自稱為本行代表或本行職員或授權人士或警察。任何人士均無須知悉你的私人密碼及/或認證密碼及/或圖形。本行絕對不會以電子郵件、手機短訊或電話要求你提供私人密碼及/或認證密碼及/或圖形。
- 若你的私人密碼及/或認證密碼及/或圖形遺失、被竊或懷疑已被別人得悉，請即更改私人密碼及/或認證密碼及/或圖形及致電客戶服務熱線通知本行。
- 進行交易時，須先留意四周環境，切勿讓他人得知輸入的私人密碼及/或認證密碼及/或圖形。在任何裝置如個人電腦、自動櫃員機、流動裝置或其他自助/銷售點終端機輸入私人密碼及/或認證密碼及/或圖形時，請遮掩按鍵。
- 切勿使用公共電腦或電子裝置輸入你的個人或信用卡資料。
- 不要理會任何要求索取個人資料或賬戶資料的電郵或來電。不要輕易於電郵及電話中透露你的個人資料及財務狀況。
- 簽署銷售單據或完成交易前，小心核對金額後方才完成交易，並保留存根作日後參考。
- 切勿簽署任何空白或未填妥的銷售單據。
- 每次購物後，必須盡快取回你的信用卡及查看該卡是否屬你所有。
- 小心核對結單上的簽賬交易。如發現任何可疑之簽賬，請立即致電客戶服務熱線。
- 更改個人資料(包括但不限於地址、手提電話號碼等)後，應立即通知本行。
- 如遇信用卡或已啟動流動非接觸式付款服務之流動裝置遺失或被竊，必須立即致電本行、或經由本行的流動理財(如你的流動電話號碼於本行系統已有記錄並已啟動流動理財)報失。
- 如發現任何未經授權人士已經或可能使用你的認證憑據或已啟動流動非接觸式付款服務之流動裝置，你應立即通知本行。
- 請於棄置任何已啟動流動非接觸式付款服務之流動裝置前解除此服務。
- 請不時參考東亞銀行信用卡/東亞銀行流動非接觸式付款服務使用須知以掌握最新保安資訊。

如有查詢，請致電東亞銀行信用卡客戶服務熱線：3608 6628。

The Bank of East Asia, Limited東亞銀行有限公司刊發

(01/2021)