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)