

Important Notice

Glossary

1. "The Bank" – means Banco Comercial de Macau, S. A. ("the Bank")
2. "This site" – means the internet website of Banco Comercial de Macau, S. A. (www.bcm.com.mo)
3. "e-Services" – means BCM Net e-Banking Services, BCM Mobile Banking Services, BCM eCorp Internet Banking Services, I-Securities Trading Services, Mobile Securities Trading Services, BCM JETCO Pay Service and BCM eEnquiry Service.
4. "E-Channels" – means Internet and/or mobile data network.

Viewing Notes

1. Some information of this site and e-Services may available in Chinese or English only.
2. This site and e-Services is best viewed with Internet Explorer 11.0 or above.
3. This site and e-Services web pages appearance may differ depending on the browser used.
4. Please install Adobe Acrobat Reader 5.0 or above to view some of the documents in downloadable forms.

Use of Information and Materials

All information and materials provided in this site and e-Services, whether provided by the Bank or any other information provider, are not intended to provide professional advice to its users. All investment products and services are not obligations of or guaranteed by the Bank and are subject to investment risks.

No Guarantee

All information and materials provided in this site and e-Services, whether provided by the Bank or any other information provider, are provided for general information purposes only and are subject to change without prior notice to its users. While the Bank has exercised every effort but no guarantee regarding the accuracy or completeness is given in connection with this information and materials.

Internet Communications

The Customer understands that due to unpredictable traffic congestion, openness and public nature of E-Channels and other reasons, E-Channels may not be a reliable medium of communication and that such unreliability is beyond the control of the Bank. This may be subject to delays in transmission, incomplete data transmission, delays in execution or execution of instructions at prices different from those prevailing at the time instructions were given, misunderstanding and errors in any communication between the Bank and the Customer, transmission blackouts, interruptions and so on.

Limitation of Liability

Under no circumstances, neither the Bank or its members will be liable or bear the responsibilities for any loss or damages of any kind, whether direct, indirect special, accidental, or consequential losses, arising from accessing this site and e-Services or use or inability to use by any party. Provision of hyperlinks to other web sites is for the interest and convenience of users. The Bank will not accept any responsibility or obligation for any hyperlink to any other web site within this site; the Bank does not verify, monitor, or endorse the content, opinions expressed, information, accuracy, and any other link provided by these linked web sites.

The Customer undertakes to: (a) keep and procure each of his authorized signatories and (where applicable) Delegated Person to keep his PIN, Security Passcode and any device(s) which including but not limited to personal computers and mobile devices for accessing internet services ("Devices") secure and secret and if the Customer and each of his authorized signatories and (where applicable) Delegated Person act in good faith and is diligent in safeguarding his PIN, Security Passcode and Devices, the Customer shall not be liable to the Bank for any unauthorized transactions made pursuant to instructions given through the Internet or electronic means; (b) inform the Bank as soon as reasonably practicable if the Customer knows or suspects that any unauthorized person knows the PIN and/or Security Passcode of the Customer or any of his authorized signatories or (where applicable) Delegated Person or that unauthorized transactions have been effected or finds or suspects that the PIN, Security Passcode and/or Devices have been compromised, lost or stolen and if the Customer fails to do so the Customer shall be liable for any unauthorized transactions made; and (c) be liable for all losses if the Customer or any of his authorized signatories or (where applicable) Delegated Person acts fraudulently or with gross negligence including failing to properly safeguard the PIN, Security Passcode and/or Devices of the Customer or any of his authorized signatories or (where applicable) Delegated Person.

Copyright

The ownership of all information and materials provided in this site and e-Services belong to the Bank or any other information provider and subject to the Copyright. Without the prior written approval by the Bank, neither party could copy, reproduce or distribute any of the information or materials provided in this site and e-Services.

Internet Security

Is it secure to make a transaction using the e-Services?

Our e-Services provide the following measures to ensure your banking information and account details are secure when you are using our e-Services:

Transport Layer Security (TLS) & Strong Encryption (128 bit)

Transport Layer Security version and 128 bit encryption is employed to ensure confidentiality. All data and information transmitted between you and the Bank through E-Channels is encrypted by using 128-bit encryption. To ensure your online transaction information is encrypted, look for the 'lock icon' in the status bar on the right hand corner of your Internet browser of your PC while you are connected.

User Name and Password and Security Passcode

To strengthen internet security, you are required to set up a "Username" and change your "Password" / "Security Passcode" regularly.

Mobile Device Fingerprint Authentication (Biometric Authentication)

Fingerprint can provide a high level of security and protection feature for identity verification. Only fingerprint(s) stored on your device can be used to login to BCM Net / Mobile Banking service. Your fingerprints data will not be stored in the BCM Mobile App or kept anywhere within BCM. You can enable or disable Fingerprint Authentication anytime in the "Security Authentication Settings" after logging into BCM Mobile Banking (two-factor authentication is required for service activation).

Mobile Device Face ID Authentication (Biometric Authentication)

Face ID can provide a high level of security and protection feature for identity verification. Only the Face ID stored on your device can be used to login to BCM Mobile Banking service. Therefore, it is strongly recommended that you should only store your own Face ID on your device and should not store or allow any third-party Face ID to be stored on your device. Your Face ID will not be stored in the BCM Mobile App or kept anywhere within BCM Bank. You can enable or disable Face ID anytime in the "Security Authentication Settings" after logging into BCM Mobile Banking (two-factor authentication is required for service activation). However, you are reminded that in using Face ID Authentication, there is possibility of false match due to certain circumstances, e.g. twins or siblings that look alike and the disabling of "Require Attention for Facial Recognition" function on your device settings. Please read the Terms and Conditions carefully and accept the associated risks and consequences before you enable Face ID.

Mobile Device Facial Recognition (Biometric Authentication)

Facial Recognition can provide a high level of security and protection feature for identity verification. Only the facial map stored on your device can be used to login to BCM Mobile Banking Service. Therefore, it is strongly recommended that you should only store your own Face map on your device and should not store or allow any third-party Face map to be stored on your device. Your facial map will not be stored in the BCM Mobile App or kept anywhere within BCM Bank. You can enable or disable Facial Recognition anytime in the "Security Authentication Settings" after logging into BCM Mobile Banking service (two-factor authentication is required for service activation). However, you are reminded that in using Facial Recognition, there is possibility of false match due to certain circumstances, e.g. twins or siblings that look alike. Please read the Terms and Conditions carefully and accept the associated risks and consequences before you enable Facial Recognition.

Automatic time out

e-Services will be automatically logoff when there is no activity for 15 minutes in order to protect you against unauthorized access.

Digital Certificates

The certificate on our web servers serve to prove to your customers that we are who we claim to be, i.e. to confirm our identity.

Does BCM bank present any policy to fight against computer hacker?

Security is one of the main concerns for both the Bank and its customers when banking over E-Channels is concerned. This is one of the easiest and most convenient ways of banking, however, can be very sensitive to hack and online frauds if not properly protected and secured. The Bank adopted physical, technological and managerial security means and measures in order to maximize the security of our site and e-Services.

Security Support

To fight against computer hacker, BCM Network Security Team will keep track to any attempts that would break into our security systems in order to ensure the security. If you suspect there are unusual activities in your account, please contact us immediately.

Firewalls

Our servers are protected behind two-layer firewalls of world-leading brands. They are constantly monitored to prevent any unauthorized access.

Encryption

Communication between customer's browser and our servers is secured by using TLS (Transport Layer Security) protocol and encryption with 128-bit encryption keys, the industry standard for encryption of data over E-Channels. It means that any and all information exchanged between the customer and the Bank during e-Services session is always encrypted.

Cookies

e-Services use cookies to store session identifier and to identify the user during the life of this particular session. Once the session is closed, the cookie will expire.

Secure email

As the security of an ordinary email cannot be guaranteed, our secure Internet solution BCM Net e-E-Banking service contains also email facility under "Contact us" options, included in encryption mechanism. The Bank will use this facility to send any personal or transaction-related information to our BCM Net customers.

Password security

The password security is strengthened by implementing rules that protect and prevent our customers from using easy to guess passwords, like for example strings of the same number or letter, or consecutive numbers. We also strongly advise our customers not to use their date of birth, telephone number or name as passwords, as other people can easily know this information.

Last Logon Information

e-Services also provide you with the information required to be vigilant. Each time you logon, we provide information related to your last banking session. If you find any discrepancies, please contact us immediately.

Channel for customers to report actual and/or suspected security incidents

Customers should promptly call our TeleBCM Hotline at 8796 8888 to report the incidences. If they notice any unusual activities in their accounts (e.g. find or believe their PIN or devices have been compromised. Lost or stolen, or that unauthorized transactions have been conducted over their account etc).

What should I do to keep safe my password?

To avoid unauthorized access to your account(s), you should refer to the security advice provided by the Bank from time to time and pay attention to the following points:

Take good care of your Password

The Password of e-Services are used to secure your online banking and execute of transactions, please do not disclose. You shall take all reasonable steps to keep the Password / Mobile Device with the following security tips:

- Do not disclose your Password / Security Passcode in any occasion or to anyone else including your relatives, friends or our staff. You are suggested to change your Password after first successful login to respective e-Services, memorize your Password and destroy the physical pin mailer thereafter.
- Avoid using easy-to-access numbers as your Password / Security Passcode, such as your birthday, ID No., Phone No., or similar numbers or a recognizable part of your name as your Password / Security Passcode.
- Do not write down or record your Password / Security Passcode without disguising it.
- Do not use same set of User Name / Password / Security Passcode from other Internet sites (e.g. connection to the internet or accessing other websites).
- Do not allow any person to use your Password / Security Passcode.
- Set a Password / Security Passcode that is difficult to guess and different from the ones for other services. The Password / Security Passcode should be changed regularly.
- Use both lowercase and capital letters with a combination of letters and numbers.
- Do not write down your Password / Security Passcode on any device (e.g. Personal Computers) or other mobile device for accessing e-Services, etc or anything usually kept with or near the device or any personal belongings such as handbag or wallets.
- Regularly change your Password / Security Passcode via respective e-Services (e.g. 30 days).
- Contact the Bank immediately if you believe that your e-Services password has been compromised, lost or stolen. At the same time, please change your Password / Security Passcode immediately to prevent unauthorized access to your e-Services.
- Safeguard your Personal Computers / Mobile Device and do not leave your Personal Computers / Mobile Device unattended.
- Avoid using "Remember your password" options on Internet browsers. Do not click "yes" to "Remember your password" options on computers.

Never disclose your PIN and personal information

- The Bank will never contact you and ask you for your Password / Security Passcode and personal information for e-Services, phone banking, or ATM Services. These include your User Name, Password, Security Passcode account number, identification / passport number, address, phone number etc.
- Watch out for suspicious phone calls, email messages, SMS or phishing sites requesting for passwords / Security Passcode and/or other personal information.
- The Bank will never disclose such information in our e-mails other than your name for personalization purpose, nor ask you to confirm any personal data by replying to our email.

Protect your computer

- Install a personal firewall on your computer. Personal firewall software is designed to prevent hackers from accessing the computer it is installed on. Installing a personal firewall is recommended especially if you are using a broadband connection. You should contact your computer or software provider for a suitable personal firewall. When installing such software, follow the manufacturer's recommendations for a 'conservative' accesses control.
- Install and regularly update virus detection software. Virus detection software scans your computer and your incoming email for viruses and then deletes them. You can download anti-virus software from the websites of software companies or buy it in retail stores. To be effective, anti-virus software must be updated routinely. As a matter of precaution, avoid opening any emails with attachments that you are not expecting, even if they are from known people.

- Be very cautious about opening attachments in emails from unfamiliar or suspicious sources which may be a virus or worm.
- Avoid visiting suspicious websites or downloading software or file from such websites.
- If any unusual screens pop up and/or the computer responds unusually slow, please log out from e-Services and scan the computer with the most updated version of virus protection software.

Protect your online transactions

- Beware of the site and e-Services of any unusual login screen or process (e.g. a suspicious pop-up window or request for providing additional personal information) and whether anyone is trying to peek at your password.
- Do not access e-Services from public places or from shared computers such as those in cyber cafes. You never know what malicious programs might be installed on the PC you use there.
- Avoid using public Wi-Fi to access e-Services.
- Always use the 'Logout' button to ensure you exit each e-Services session securely. Closing of your internet browser only does not mean complete logout from your e-Services.
- When you've finished using the Internet, always disconnect. Avoid leaving your connection on, especially with broadband access, unless you're actively using it.
- Always check the date and time of your last visit to respective e-Services (we track it at all times and display it on the Welcome Page). If you suspect anything unusual, please contact us immediately.
- Please take attention to review the transactions before confirmation. When your instructions have been accepted and confirmed online, they cannot be reversed and cancelled.
- For your protection, kindly login e-Services and check your bank statement regularly and report any unusual transaction to the Bank immediately. For statement information and customer enquiries, please call customer service hotline during office hours.
- Check the SMS messages and other messages sent by the Bank in a timely manner. Verify your transaction records and inform the Bank immediately in case of any suspicious transaction identified.
- Do not forward telephone calls or SMS to devices or phone numbers provided by unknown others. When travelling abroad, it is advisable to use the same SIM card and cell phone in receiving phone calls and SMS instead of forwarding all SMS to another mobile phone or SIM card.
- Follow the internet banking logon instructions and security tips published by the banks when conducting internet banking transactions.

Alert to Email Scam



Email is one of the main communication channels for both personal and commercial dealings. Nowadays, fraudsters would hack into email accounts, and cheat recipients by all possible means to make remittances. Some victims have suffered significant amount of losses in some cases. You shall be alert to suspicious emails and raise your awareness in preventing this kind of scam, such as taking the initiative to confirm the true identities of recipients by telephone, facsimile or other means before effecting remittances so as to prevent such kind of scam. Please read "**What should I do to keep safe my password?**" and preventive measures to mitigate the risk of hacking.

Make sure you are connected with BCM

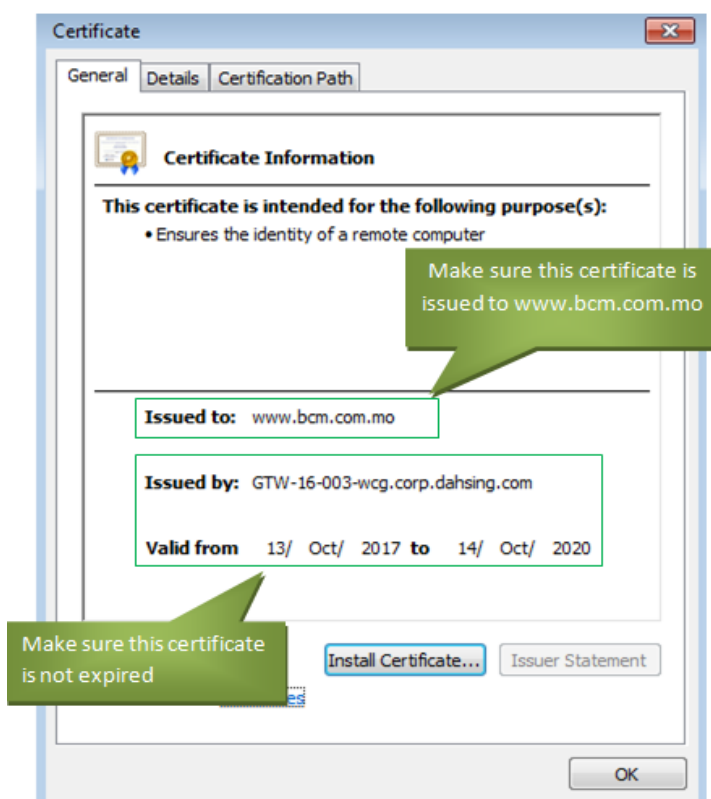
- If encounter some fraudulent websites that mimics the look of the financial institution's website to capture your usernames, Password and other personal and confidential banking details. Thus, it is important to make sure that you are connecting with BCM.
- To stay away from connecting with a fraud website, never access the internet banking accounts through hyperlinks embedded in email, Internet search engines, suspicious pop-up windows or any other doubtful channels to start BCM e-Services session.

- Customers should connect to a bank website through typing the authentic website address in the address bar of the browser or by bookmarking the genuine website and using that for subsequent access. If customers find the website of the bank suspicious, they should not enter any information (including user ID, password and OTP) to the website and should report to the bank immediately. Always logon directly from your browser or select from your favorite if you have already added BCM website to your list of favorite Internet sites. This will avoid you from being sent to a false site.

Remember: No e-mail from the Bank will contain a hyperlink to our e-Services logon page.

To ensure that you are connecting with the Bank, look for closed security padlock  at the top right corner of your Web browser before you enter your User ID and Password or important personal information. A closed security padlock  indicates a secure connection. Clicking the closed padlock will show you the digital certificate details.

Sample screen shot of Internet Explorer's certificate for your reference:



Note: After clicking the security padlock and you find the certificate contains any message different from what is illustrated above, please contact the Bank for more information or assistance.

To prevent logging into the fraudulent online services, please do not click any link in emails or from other websites for logging into internet banking services.

If you find the website of the Bank suspicious, you should not enter any information (including usernames, Password) to the website and contact the Bank immediately.

Security measures for specific services

Security Tips for using Mobile Securities Trading Services:

Customers shall take the following security measures for using Mobile Securities Trading Services, include:

- You shall take all the above-mentioned reasonable steps to keep your respective Password used for accessing Mobile Securities Trading Services safe, secure and secret to prevent fraud.
- Immediately logout from Mobile Securities Trading Services after using the service or respective app.
- Do not click on links from malicious SMS or MMS messages which may be a virus or worm or malware.
- Read and evaluate the requested permissions carefully before installation of any Apps.
- Check what Apps are running in the background mode and stop unnecessary Apps from running.
- Regularly login to check the account balances, stock holdings, order activity and transaction history.
- Only use authorized or official Apps from recognized suppliers on your mobile device.
- Do not jailbreak, root or pirate your mobile device. Only use legitimate and unaltered operating system.
- Keep the operating system of your mobile device and Apps up-to-date. Only download and upgrade your operation system and Apps from official App stores or reliable sources.
- Properly configure your mobile devices, e.g. disallow installation of Apps from unknown source etc.
- Do not leave your mobile device unattended.
- Activate the automatic locking function with a password on the mobile device that is difficult to guess.
- In public areas, please use secure network to connect with the internet on the mobile device. Avoid using public Wi-Fi to access Mobile Securities Trading Services.
- Disable any wireless network functions (e.g. Wi-Fi, Bluetooth, NFC) when not in use. Choose encrypted networks when using Wi-Fi and remove any unnecessary Wi-Fi connection settings.

Security Tips for using BCM JETCO Pay Services:

Customers shall take the following security measures for using BCM JETCO Pay, include:

- Always keep your Mobile PIN and Activation Code secure and secret. Never store them on your mobile handset. Also, don't write down or disclose them to other persons or parties.
- Set Mobile PIN that cannot easily be guessed by anyone and should be different from other services. Change your Mobile PIN regularly.
- Don't forward your One Time Password (OTP) and push notification to anyone.
- Do not click on links from malicious SMS or MMS messages which may be a virus or worm or malware.
- Don't leave your mobile device unattended after logon to the BCM JETCO Pay App. Always quit from the App when you have finished BCM JETCO Pay transactions.
- Avoid sharing your mobile device with others and use your own mobile device to register BCM JETCO Pay service.
- To prevent unauthorized access to your mobile device and BCM JETCO Pay App, activate the automatic locking function with a secure password.
- Read and evaluate the requested permissions carefully before install the BCM JETCO Pay or any app.
- Download and upgrade the BCM JETCO Pay App from official App stores or reliable sources only. Please be aware of the search keywords when download the App. Please search the keyword of "BCM JETCO Pay" in Apple App Store or Google Play Store to download the App.
- Delete BCM JETCO Pay App on your old mobile device before you donate, resell or recycle it.
- Properly configure your mobile devices, e.g. disallow installation of Apps from unknown source etc.
- When using Wi-Fi Internet connection, use trusted Wi-Fi networks or service providers and enable security protection such as Wi-Fi Protected Access (WPA), if possible. Use secure network and avoid using public Wi-Fi to access BCM JETCO Pay service.
- Review and where necessary update your mobile number registered with the Bank. If your personal contact details have been changed, please contact the Bank for update immediately.

- Notifications will be sent by JETCO after you have successfully "Send Money" via the App. Check the corresponding messages sent in a timely manner, verify your transaction records and inform the Bank immediately in case of any suspicious transaction identified.
- Check and verify the transaction details via the "Transaction Info" in BCM JETCO Pay App regularly. After you have successfully "Send Money" and "Collect Money", you should verify the corresponding transaction via BCM Net e-Banking / BCM Mobile Banking or Mobile Securities Trading Services.

Security Tips for using BCM Mobile Banking Services:

Customers shall take the following security measures for using BCM Mobile Banking Services, include:

- You shall take all the above-mentioned reasonable steps to keep your respective Password used for accessing BCM Mobile Banking Services safe, secure and secret to prevent fraud.
- You should only store your own fingerprint(s) / Face ID / facial map on your device in order to maintain the highest security level of Security Authentication to login to BCM Mobile Banking Services and authorize the online transaction. When you activated Security Authentication, any fingerprint / Face ID / facial map stored on your mobile device, now or in the future, can be used for Fingerprint Authentication / Face ID Authentication / Facial Recognition. Therefore, you should not store or allow any third-party fingerprint(s) / Face ID / facial map to be stored on your mobile device.
- Immediately logout from BCM Mobile Banking Services after using the service or respective app.
- Do not click on links from malicious SMS or MMS messages which may be a virus or worm or malware.
- Read and evaluate the requested permissions carefully before installation of any Apps.
- Check what Apps are running in the background mode and stop unnecessary Apps from running.
- Regularly login to check the account balances and transaction history.
- Only use authorized or official Apps from recognized suppliers on your mobile device.
- Do not jailbreak, root or pirate your mobile device. Only use legitimate and unaltered operating system.
- Keep the operating system of your mobile device and Apps up-to-date. Only download and upgrade your operation system and Apps from official App stores or reliable sources.
- Properly configure your mobile devices, e.g. disallow installation of Apps from unknown source etc.
- Do not leave your mobile device unattended.
- Activate the automatic locking function with a password on the mobile device that is difficult to guess.
- In public areas, please use secure network to connect with the internet on the mobile device. Avoid using public Wi-Fi to access BCM Mobile Banking Services.
- Disable any wireless network functions (e.g. Wi-Fi, Bluetooth, NFC) when not in use. Choose encrypted networks when using Wi-Fi and remove any unnecessary Wi-Fi connection settings.
- Please contact our Customer Services Representatives immediately if your Fingerprint Authentication / Face ID Authentication / Facial Recognition / Security Passcode Authentication-enabled mobile device is lost or stolen and your BCM Mobile Banking Services Security Authentication service may be suspended to prevent unauthorized access.

Last Update on July 2020