Octopus Online Service Safety Guide

This document aims to provide users with security tips and reminders when using online and mobile services provided by Octopus Cards Limited ("us", "we", "our", "our company", "OCL"). You may review information of particular interest to you:

Content

We may ask you to provide your personal information for customer service or operational purposes. If you wish to know the details of the purposes and use of your personal data, please refer to the Conditions of Issues of Octopus. If you have any questions or notice any suspicious activity when you use our services, please immediately call the Octopus Customer Service Hotline at 2266-2222. *OCL personnel will never ask for your password*.

1. When using online services provided by OCL

1.1. When accessing our online services

- Use only trusted mobile devices. Do not access our services through public computers.
- Access the OCL website only by entering http://www.octopus.com.hk in your web browser.
- Only download Octopus mobile applications (Octopus App, Octopus App for Tourists) through weblinks from the OCL website http://www.octopus.com.hk or authorised app stores, such as Google Play Store, Apple App Store or HUAWEI AppGallery.
- To use Octopus on iPhone or Apple Watch / Octopus on Android / Huawei Pay Octopus / Smart Octopus in Samsung Pay, only download authorised mobile payment apps from authorised app stores.
- When carrying out online transactions provided by us via an Internet browser, a padlock image will appear. When you click on the lock, a digital certificate issued to our company will be shown.
- When carrying out services with Octopus cards and products ("*Octopus*"), you are required to provide the Octopus number and the bracketed digit for validation and authentication. You can use your registered *Octopus ("R*egistered *Octopus")* for making online payments after successful registration.
- Remember to close the services and log-out (if applicable) after you have finished using them.
- To help you identify Octopus SMS instantly, we have joined the SMS Sender Registration Scheme, using registered sender IDs #Octopus and #OctopusOTP when sending SMS to local mobile users. If you receive SMS claiming to be from "Octopus" and the sender ID doesn't start with "#", please be vigilant.
- Please note that we will not display your personal information in any emails or short messages (SMS) sent by OCL, or ask you to confirm any personal data or credentials (such as password) by replying to or clicking embedded hyperlink in an email or SMS sent by OCL. If you notice any suspicious activity, please contact our Customer Service Hotline at 2266-2222.

1.2. When using Octopus Online Payment

- During the purchase process, the online merchant may request personal

information, such as your name, email address, phone number and shipping address, for the fulfilment of your purchase. Unless otherwise specified, this data will not be shared with or kept by OCL.

- Except for issuing a receipt for a charitable donation, OCL will not collect your personal information when you use the online payment service.
- If you wish to obtain a receipt for a charitable donation, you may choose to provide to the charity organisation your name, email address, phone number and postal address through us.
- Before confirming a payment, please verify the payment details, including the recipient, amount and donation type/bill type (if applicable).

1.3. When using Octopus Wallet Service

- Always apply your Octopus Wallet through the official Octopus App.
- During the application for an Octopus Wallet, OCL may request your personal information, such as your name, email address, mailing address, phone number, image(s) of your identification document and the applicant (i.e. yourself). These data will be securely stored in our servers for the purposes of Octopus Wallet application and customer service.
- If you apply to use the Fund Transfer with Bank Service under the Octopus Wallet, OCL will ask you to provide information such as your bank name and bank account number, and use your full name and Octopus Wallet number for setup and operation of the service.
- These data will be securely stored in our servers for operating the service. Details of the purpose(s) and use of your personal data can be found in the Terms and Conditions Relating to Fund Transfers with Banks under Octopus Wallet Service.
- Keep your password and one-time password (OTP) secure and do not disclose them.
- Do not write down your password and do change it regularly. Choose a strong password with an alphanumeric combination which is difficult to guess. *OCL personnel will never ask for your password*.
- Please be assured that we only rely on iOS / Android to store and authenticate your biometric data (e.g. fingerprint) and will not capture or store any of these data.

- Before enabling fingerprint, iOS Face ID or other biometric data for login to your Octopus Wallet, please ensure such data includes no one other than yourself, to prevent any unauthorised access to your Octopus Wallet.
- Review new requests carefully. When other users invite you as a friend, the mobile number will be shown for your review prior to approval. Please make sure any such user is someone you know and is trustworthy.
- You will receive payment requests and payment reminder notifications only in the Octopus App. These notifications will not be sent to you through email or SMS. You can review each payment request in the Wallet section of the Octopus App.
- Before accepting a payment request or sending a P2P payment, review the payment details carefully - including the recipient and the payment amount. All payment transactions of the Octopus Wallet are irreversible upon confirmation of the payment instruction.
- If you have changed your mobile phone number or other personal information, please call Octopus Customer Service Hotline at 2266-2222 at your earliest convenience, to ensure your contact information is up-to-date.
- If you have changed the email address you use, please update our record with the new email address through the Octopus App as soon as possible, to avoid missing any important notifications.
- Please ensure your mobile number is input correctly to receive SMS notifications for your Octopus Wallet.
- Please ensure you turn on “Notifications” in phone “Settings” to receive important notice of Octopus App.
- You can keep your Octopus Wallet monthly statement by downloading it through the Octopus App.
- Check your Octopus Wallet and Registered *Octopus* transactions regularly. If you have any question or notice any suspicious activity, please immediately call the Octopus Customer Service Hotline at 2266-2222.

1.4. When using Octopus on iPhone or Apple Watch / Octopus on Android / Huawei Pay Octopus / Smart Octopus in Samsung Pay

- Always access your authorised mobile payment service user account through an official or authorised app, or through the authorised mobile payment service

provider's website.

- Always use, if applicable, an Octopus App, Octopus App for Tourists or authorised mobile payment app for your Octopus on iPhone or Apple Watch or Octopus on Android or Huawei Pay Octopus or Smart Octopus in Samsung Pay.
- When you apply for a new Smart Octopus in Samsung Pay or Huawei Pay Octopus, OCL may request information for refund purpose such as your name and mobile number. Information you provide will be securely stored in our servers for refund purposes only. Read the Conditions of Issue to learn more.
- Your name and mobile number will be required if you apply for a refund of your Smart Octopus in Samsung Pay or Huawei Pay Octopus via the OCL website. The mobile number will be required for you to receive an SMS verification code during the refund application.
- For Smart Octopus in Samsung Pay or Huawei Pay Octopus user, if you have changed your mobile number, please update our record with the new mobile number through the authorised mobile payment app as soon as possible, to ensure the information required for you to apply for a refund of your Smart Octopus in Samsung Pay or Huawei Pay Octopus is up-to-date.
- Keep the authentication password and one-time password (OTP) (if applicable) for your authorised mobile payment app secure.
- Do not write down your password and change it regularly. Choose a strong password with alphanumeric combinations, which is difficult to guess. *OCL personnel will never ask for your password*.
- If you are using a mobile device that supports biometric data authentication such as face recognition, iris or fingerprint authorisation, you may choose to use it to authorise online transactions or other functions of Octopus on iPhone or Apple Watch or Octopus on Android or Huawei Pay Octopus or Smart Octopus in Samsung Pay. Be aware that Octopus relies on your authorised mobile payment service provider to store and authenticate your biometric data; Octopus does not capture or store any such data itself.
- Before applying the biometric data authorisation, ensure it only applies to you as an Octopus on iPhone or Apple Watch or Octopus on Android or Huawei Pay Octopus or Smart Octopus in Samsung Pay user. This is to prevent any unauthorised usage of the Octopus on iPhone or Apple Watch or Octopus on Android or Huawei Pay Octopus or Smart Octopus in Samsung Pay.
- Check your registered Octopus on iPhone or Apple Watch or Octopus on

Android or Huawei Pay Octopus or Smart Octopus in Samsung Pay transactions regularly. If you have any questions or notice any suspicious activity, please immediately call the Octopus Customer Service Hotline at 2266 2222.

2. What is OCL doing to protect you?

- Our servers and infrastructure are protected by firewall and intrusion prevention/detection systems to prevent unauthorised access.
- All communications among our servers, your device and *Octopus* are transmitted with an industry recognised encryption standard.
- If a transaction is not completed within a set period of time, it will be automatically cancelled.
- Our system will log the usage of each *Octopus* for online services. If the card registration via Octopus App records five attempts of invalid or unmatched input of the Octopus number, the online functions of the *Octopus* will be suspended for 24 hours.
- OCL may block your access if your mobile device is detected to be “rooted” or “jail-broken”. This is done to ensure transactions are carried out securely. We will not access other information in your mobile device when detecting your device’s status.
- OCL has suspended the screen mirror, capture and recording features on Octopus App via any Android devices for the following three types of screens to protect account security:
  - Involving input of any login credentials, including but not limited to user ID, password and one-time password (OTP).
  - Displaying direct payment information, including but not limited to Octopus MasterCard number, Octopus UnionPay QR code and eLaisee QR code.
  - Screens showing and for input of customer sensitive information, including but not limited to the application of services of JoyYou Card and Octopus Wallet Upgrade via electronic Know-Your-Customer (eKYC).

2.1. For Octopus Online Payment

- The merchant information and transaction amount will be shown on the Octopus App or website, allowing you to check the merchant name and amount prior to making a payment.

2.2. For Octopus Wallet Service

- You can access your Octopus Wallet from up to two registered devices at any time.
- When you login your Octopus Wallet, we will display the last login attempt and status. If you notice any suspicious activity, please immediately call the Octopus Customer Service Hotline at 2266-2222 for investigation.
- When using the service, your login session will expire after a set period of idle time.
- When you contact us to enquire about the operation of your Octopus Wallet, you will be asked for your authentication code or personal information to verify your identity. This is done to protect your account information.
- A verification code and the purpose of the verification code will be sent to your registered mobile number through SMS when you login from a new mobile device, or when you increase your daily transaction limit, or when you make high risk transactions (transactions which exceed the per-transaction limit or aggregate total limit as announced by us from time to time.). Please review the SMS content before entering the verification code in the Octopus App. If you receive any suspicious SMS related to the service, please immediately call the Octopus Customer Service Hotline at 2266-2222 for investigation.
- Please note that the verification code SMS will not be supported through the SMS forwarding instruction of your device or from your mobile network operator. You are also reminded not to forward the SMS verification code to other mobile devices.
- We will temporarily suspend your account if we detect a series of unsuccessful login attempts. In the event your account is locked, please contact our Customer Service Hotline at 2266-2222 for assistance.
- We will provide updates on your account activities via push notification messages / emails. For important transactions such as device registration / de-registration, and adding payee / friend, notifications will be sent via both push notifications and alternative channel, such as your registered email address.
- After you add a new friend or register a new *Octopus* to your Octopus Wallet, a daily summary will be sent to your registered email.
- We will never ask customers to validate their personal and/or account related information (e.g. ID number or login password) by emails or through any

hyperlinks embedded in such emails.

- Please check for updates and notifications in a timely manner. If suspicious activities are found, please immediately call Octopus Customer Service Hotline at 2266-2222.

2.3. For Octopus on iPhone or Apple Watch / Octopus on Android / Huawei Pay Octopus / Smart Octopus in Samsung Pay

- For Smart Octopus in Samsung Pay, each authorised mobile payment service user account can only link with one Smart Octopus in Samsung Pay.
- Like other Automatic Add Value Service (AAVS) users, Octopus on iPhone or Apple Watch or Octopus on Android or Huawei Pay Octopus or Smart Octopus in Samsung Pay holders can utilise the lost card reporting service and request a refund via the designated channels.
- You can opt to provide your name and mobile number (the name and mobile number may be subsequently updated from time to time) to us at the time of issuance of the Smart Octopus in Samsung Pay or Huawei Pay Octopus. The information will be used for the refund process. A verification code will be sent to the mobile number you provided, to verify your identity in case of refund.
- You will be asked to provide your Octopus on iPhone or Apple Watch or Octopus on Android or Huawei Pay Octopus or Smart Octopus in Samsung Pay number and personal information to verify your identity if you contact us to enquire about your Octopus on iPhone or Apple Watch or Octopus on Android or Huawei Pay Octopus or Smart Octopus in Samsung Pay operation.
- You will receive a notification via your registered email account in case you transfer your Octopus on iPhone or Apple Watch or Octopus on Android or Huawei Pay Octopus or Smart Octopus in Samsung Pay to a new mobile device. You are required to login to your authorised mobile payment service user account with the new device before transferring the Octopus on iPhone or Apple Watch or Octopus on Android or Huawei Pay Octopus or Smart Octopus in Samsung Pay to it.
- A push notification with transaction information will be sent to you after each transaction. You will be able to view a maximum of 40 transaction records at the Octopus on iPhone or Apple Watch or Octopus on Android or Huawei Pay Octopus or Smart Octopus in Samsung Pay enquiry page, if applicable, at your device's Octopus App, Octopus App for Tourists or authorised mobile payment app. You are advised to check your transaction records in a timely manner.

- Please note that the verification code SMS will not be supported through the SMS forwarding instruction of your device or from your mobile network operator. You are also reminded not to forward the SMS verification code to other mobile devices.
- OCL will never ask customers to validate their personal and/or account-related information (e.g. registered email or login password) via email or hyperlinks embedded in emails or SMS.

3. What to do to protect yourself?

- You should always keep an eye on your belongings. Leaving your Octopus cards and products unattended may result in unauthorised registration or online payment usage. If your mobile device with Octopus on iPhone or Apple Watch or Octopus on Android or Huawei Pay Octopus or Smart Octopus in Samsung Pay is left unattended, others might be able to use or retrieve the information you have stored in it, without your knowledge. You should also contact your mobile service operator to disable your SIM card if your mobile phone is lost.
- Never share with anyone your verification codes and one-time-password received in SMS or Push Notification via the Octopus App.
- Only access the Virtual Assistant Helen and Otto via Octopus App and Octopus App for Business, and the official website of Octopus Cards Limited (http://www.octopus.com.hk).
- Always enable the screen lock function for your mobile device, to prevent others accessing your personal information, such as messages, browser history, or your contact list.
- Enable “remote locate” or “remote erase” features if your mobile device is equipped with them. This can help identify your device location or prevent loss of your personal information in the event you lose your mobile device.
- To help you identify Octopus SMS instantly, we have joined the SMS Sender Registration Scheme, using registered sender IDs #Octopus and #OctopusOTP when sending SMS to local mobile users. If you receive SMS claiming to be from "Octopus" and the sender ID doesn’t start with "#", please be vigilant.
- Pay extra attention to any links in emails or SMS that ask you to start a payment transaction or request for personal data and credentials. OCL will not embed links in emails or SMS for these purposes.
- When using an online service on your mobile device, be extra careful regarding

the security arrangement. Your mobile device's security setting may not be the same as your personal computer's.

- Here are some tips for setting a password:
  - Avoid using the same password you use to access other services.
  - Do not create your password with personal information, such as your contact numbers, date of birth, HKID card number, licence number.
  - Do not write down your password or store your password on any computer or mobile device.
  - Change your password regularly.
  - Create a unique password and avoid using the same password for each website and online service.
- When using your Octopus Wallet, beware of any abnormal login process, suspicious pop-ups or request for additional personal information.
- Registration of partial *Octopus* number is required as a safety precaution for online payments and enquiries. For added protection, you may consider using a protective shield holder to further safeguard against potential unauthorised use of your *Octopus*.
- You have to register your Octopus on iPhone or Apple Watch or Octopus on Android or Huawei Pay Octopus or Smart Octopus in Samsung Pay with Octopus App for online payments and fund transfers.
- Always Check your *Octopus* transaction records. If you notice any suspicious transactions, call the Octopus Customer Service Hotline at 2266-2222 immediately.
- Always use legitimate software from original sources. This will reduce the chance of contamination by a computer virus or spyware. Pirated software or software from unknown sources may have been tampered with or modified by spyware, virus or other programme changes that are not included in the original software package. Using any such software may increase the risk of exposing your mobile device to viruses, spyware or other software that can result in damage to your device or theft of your personal information.
- Do not “jail-break”, “root” or “modify” the operating systems. These activities will reduce the system stability, making it vulnerable to computer virus and spyware attacks that might cause harm or theft of your personal information. We may be unable to provide the service you requested on a jail-broken or rooted mobile

device.

- Regularly update your operating system and Internet browser to maximise the security of your mobile device. Use the latest versions of operating systems and mobile applications. Download and apply security patches for mobile devices when they are available, for prompt protection against known security vulnerabilities.
- Use anti-virus software and update it regularly to protect your mobile device against computer virus attacks from numerous sources. Moreover, you also need to regularly update the “virus definition file” to effectively protect your mobile device. For details, please refer to the “Help” section of the software.
- Use anti-spyware software and update it regularly to help block malware or spyware from being installed on your mobile device and tracking your usage behaviour. Some anti-spyware software can also detect and block phishing websites and help you differentiate the official sites from fraudulent ones.
- Wi-Fi relies on radio signals. This means that there is a chance of people nearby accessing your network without your prior approval. When using your own wireless router, always safeguard the connections with password-protected secure access or encryption.
- Beware of fake / phishing SMSes, emails and social media posts. These may pretend to be sent from OCL, and attempt to trick you into providing your personal information. OCL will never ask for your personal information or password through emails or links in emails. Do not open, reply to or click within these emails.
- Spam emails may include links that attempt to divert you to fraudulent sites. They may be disguised as being from companies you have dealt with previously, attempting to gain your trust and obtain your information. Be extra careful regarding spam emails. You may minimise the chance of getting these by applying the spam blocking or filtering function of your email client or online email service provider.
- Carefully verify the payment details and whether the payee identity is trustworthy before each payment using Faster Payment System (FPS) proxy ID and use the most updated version of Octopus App containing the “Faster Payment System (FPS) Suspicious Proxy ID Alert” feature in order to receive the alert, if any, when making payment using FPS proxy ID. Under the mechanism of “Suspicious Proxy ID Alert”, you will be alerted of the high risk of fraud if the payee’s account / FPS proxy ID (including mobile phone number, email address, FPS Identifier

(FPS ID)) is related to a scam reported to Hong Kong Police Force and is listed as “High Risk” as per the scam prevention advice on “Scameter”. An alert message will be displayed, reminding you to think twice before deciding whether to cancel the transaction or continue with the payment.

- Beware of look-alike websites. Fraudsters and scammers may set up pages that look like websites you trust, asking for your personal or private information. Always check the URLs, to ensure the pages you visit are actually of your trusted companies.
- You can refer to Smart Tips on using Stored Value Facilitates by viewing Hong Kong Monetary Authority website at https://www.hkma.gov.hk.

- Ends -