Security Tips:

Resort employs a range of security features for its Payment Gateway and other channels. These measures extend from data encryption to firewalls. Resort uses encryption technology to ensure that the information exchanged between the customer's computer and the net-banking site over the Internet is secure and cannot be accessed by any third party.

Your Participation to Online Security

Resort recommends the following security measures to all its Internet/Payment Gateway Banking Users:

- Please create and maintain different passwords for Login and for Transactions. This provides additional security for financial transactions through Internet Banking.
- If you are accessing any website (including feetupholidays/index1.php) from cyber cafe, any shared computer or from a computer other than that of your own, please change your passwords after such use from your own PC at workplace or at house. It is very important to do so especially when you have entered your transaction password from such shared computer or cyber cafe computer. Change these Passwords from your own PC at workplace or at house.
- Make sure that your computer is protected with anti-virus and you have latest anti-virus software.
- Avoid clicking on links which are sent via E-mails. Type URL (Universal Resource Locator) of all such links directly on the browser.
- Avoid sending or furnishing personal and financial information on email. Also prior to providing any information (financial or personal) on a website, verify the bonafides of the website, its address and of the owners / operators of such websites. Make sure that the URL that appears in the "address" or "location" box on your browser window is the one you wish to access.
- Please do not reply / respond to communication or click on any link provided in any communication including
  - ✓ email, SMS or phone call informing you that your banking or other accounts will be closed unless you provide your
  - ✓ personal or banking information by responding to such communication or other email address/website/mobile
  - ✓ number/phone number, or any communication requiring furnishing of any information personal or otherwise, and representing to be from Bank
- Ignore any e-mail asking for your password or PIN and inform us of the same for us to investigate. Neither the police nor we will ever contact you to ask you to reveal your online banking or payment card PINs, or your password information.

- Beware of email attachments. It’s never a good idea to click on email attachments or free software from unknown sources. You could end up exposing your computer (and the information on it) to online fraud and theft.