General Safety Precautions for Online Transactions

- Make sure your computer has up-to-date antivirus software and a firewall installed.
- Install anti-spyware software on your machine.
- Download (from the internet) the latest security patches for your browser and your operating system. Set your computer/smartphone to automatically download these updates if possible.
- Ensure your browser is set at its highest level of security notification and monitoring. The safety options are not always activated by default.
- Use strong passwords. Do not use common passwords or a password that can easily be guessed. Use a combination of alphanumeric, upper and lower case characters and symbols and make sure the password length is at least 8 characters.
- Keep your passwords and PINs secret - do not write them down or tell anyone what they are.
- Be wary of unsolicited e-mails or phone calls asking you to disclose any personal details or passwords. Your bank or the police would never contact you to ask you to disclose your PIN or your online banking password.
- Always access your internet banking site by typing the bank's address into your web browser.
- Never go to a website from a link in an e-mail and then enter personal details.
- The login pages of bank websites are secured through an encryption process, so ensure that there is a locked padlock or a trust shield in your browser window when accessing your bank site. The beginning of the bank's internet address will change from "http" to "https" when a secure connection is established. This is a sign that the website has an SSL certificate, showing it is safer to use.
- Do not be fooled by convincing e-mails offering you the chance to make easy money.
- Never leave your computer/smartphone unattended when logged in to your online account.
- When making a payment, always double check that you have entered the correct account number and sort code - if you enter incorrect details the payment will go to a different recipient and it may prove difficult to get the money back.

- Ensure you log off from your online bank account before you shut down, especially if you are accessing your online bank account from a public computer or at an internet café.
- Check your bank statements regularly and thoroughly. If you notice anything irregular on your account, contact your back as soon as possible.
- Be aware that your card details are as valuable as cash in the wrong hands so store your cards securely at all times and try not to let them out of your sight.
- Sign up to "*Verified by Visa"* or "*MasterCard SecureCode"* whenever you are given the option whilst shopping online. This involves you registering a password with your card company. By signing up, your card will have an additional level of security that will help prevent you from being a victim of online fraud.
- Only shop on secure sites. Before submitting card details ensure that the locked padlock or unbroken key symbol is showing in your browser. (The locked padlock symbol is usually found at the top of the screen if you use Internet Explorer or Firefox). The beginning of the online retailer's internet address will change from 'http' to 'https' when a connection is secure. In some new browsers, the address bar may also turn green to indicate that a site has an additional level of security.
- Never disclose your PIN to anyone and never send it over the internet.
- Print out your order and keep copies of the retailer's terms and conditions, returns policy, delivery conditions, postal address (not a post office box) and phone number (not a mobile number). There may be additional charges such as local taxes and postage, particularly if you are purchasing from abroad. When buying from overseas remember that it may be difficult to roll back if problems arise, but having all the aforementioned information will help your card company take up your case if you subsequently have any difficulties.
- Ensure you are fully aware of any payment commitments you are entering into, including whether you are authorising a single payment or a series of payments.
- Consider using a separate credit card specifically for online transactions.