Fraudulent use of HSBC Name for Investment Solicitation

It has recently come to our attention that third parties are fraudulently portraying themselves as belonging to the HSBC Group for illegal financial gain through phone calls, social network systems (SNS), email and applications on smartphones. If you have been approached by such fraudulent third parties, please report it to the nearest police station. Should you have any doubt in relation to HSBC as the relevant party, please contact us here.

Following are the examples of fraudulent type of solicitation:

- You have won the HSBC lottery and require to send serial number of pre-paid cards through SNS as fee to receive winning money
- You have inherited money of the deceased who held account at overseas HSBC account
- Investing on FX using FX application with HSBC Logo being used

Protecting Oneself

Phishing/Spam Email

Fraudulent individuals can make an email look as if it comes from someone else. Identifying a fake email can be difficult and fraudsters constantly change their methods. Should you have received such email (spam email), please delete the email immediately, without opening any of the attachment. The fake emails often display some of the following characteristics:

- The sender's email address doesn't tally with the trusted organisation's website address.
- The email is sent from a completely different address or a free web mail address.
- The email does not use your proper name, but uses a non-specific greeting like "dear customer".
- A prominent website link. These can be forged or seem very similar to the proper address, but even a single character's difference means a different website.
- A request for personal information such as user name, password or bank details.
- You weren't expecting to get an email from the company that appears to have sent it.

Fake Websites

It is very easy for fraudulent individuals to develop a fake website. However, here are

some tips to help identify them:

- Look for evidence of a physical presence, for example, an address or telephone number. If in doubt, make a phone call or write a letter to establish whether they really exist.
- The website's address is different from what you are used to, perhaps there are extra characters or words in it or it uses a completely different name or no name at all, just numbers.
- Right-clicking on a hyperlink and selecting "Properties" should reveal a link's true destination – beware if this is different from what is displayed in the email.
- A request for personal information such as user name, password or other security details IN FULL, when you are normally only asked for SOME of them.