Our Ref.: B1/15C
B9/29C

20 May 2003

The Chief Executive
All Authorized Institutions

Dear Sir/Madam,

Overseas Fraud Cases involving Fake E-mails or Websites

The purpose of this letter is to draw your attention to a number of recent fraud cases which have occurred overseas and which made use of fraudulent e-mails or websites. This letter also proposes certain precautionary measures for your consideration.

In the recent weeks, customers of certain well known banks have been targeted by people sending out fake e-mails or using fake websites which are designed to trick bank customers into revealing private details such as e-banking login names and passwords. Such websites and e-mails can look genuine by using different techniques such as the following:

(a) using genuine logos and branding by grabbing the genuine graphics from the respective bank's website;

(b) redirecting customers to the real websites so that customers are communicating with the real bank concerned without knowing that their private details may be passing through the fake websites; and

(c) using domain names which are very similar to that of the real banks, or which may be regarded as those of banks. Customers may think they are communicating with their banks but in fact private details could have been passed to the fraudsters.

Institutions which provide transactional e-banking services or which may communicate with their customers through e-mails should be aware of such possible scams targeted at their customers. The HKMA is liaising with the relevant overseas authorities to understand more about

these cases and will incorporate the lessons learned into a new module on e-banking to be included in the Supervisory Policy Manual in due course. In the meantime, your institution may consider the following precautionary measures, if your existing procedures do not already include the same:

(a) ensuring that your e-banking customers are made aware that your institution or its agents/business partners will never ask for their sensitive account information (such as PIN numbers or passwords) by e-mail. They should be asked to contact your institution by phone if in doubt;

(b) advising your e-banking customers how to ensure that they are communicating with the official site, e.g. by clicking the padlock or key icon at the bottom of their web browsers to check the relevant details of the digital certificate of the transactional e-banking site, or by accessing your institution's website through the web browsers' bookmarks having satisfied themselves that the site bookmarked is genuine. Customers should be asked not to access your institution's transactional e-banking website through hyperlinks embedded in e-mails; and

(c) searching the internet regularly to see if there are third-party websites with domain names which could be mistaken for that of your institution or websites which have established hyperlinks to your institution's site. In these cases, your institution may consider blocking, through the firewall or router, any network traffic relayed by these websites to your institution's website. If the intent of these websites is doubtful, your institution should consider disputing the use of those similar domain names or seeking the assistance of the Police or the HKMA.

I hope you will find the above useful. If you have any questions on this letter, please feel free to contact Mr. Shu-Pui Li at 28781826 or Mr. Brian Lee at 28781651.

Yours faithfully,

(Raymond Li)
Executive Director (Banking Development)