



MAURITIUS BANKERS  
ASSOCIATION LIMITED

## COMMUNIQUÉ

### **BANKS WARN AGAINST FRAUDULENT E-MAIL AND WEBSITE**

The Mauritius Bankers Association (MBA), on behalf of its Members, would like to alert bank customers to various fraudulent e-mails which ask recipients to reveal their personal information, including full names and addresses, ID/passport details, debit and/or credit card details, personal identification numbers (ATM PIN) as well as user names and passwords for online banking users.

These e-mails, which are not originated from banks, instruct the readers to visit a website via a link and input personal details as described above. **Banks would never send e-mails asking for such confidential information to be recorded online and customers should NOT respond to such e-mails, even though they are sent repeatedly. The messages should simply be deleted immediately.**

- Bank customers are reminded to ensure they are connected to a valid site before keying in any confidential personal data.
- If customers are in doubt or are concerned that they may have revealed their security details to fraudulent websites, they should immediately contact their respective banks.

### **LES BANQUES METTENT EN GARDE CONTRE LES E-MAILS ET SITES WEB FRAUDULEUX**

La Mauritius Bankers Association (MBA), souhaite alerter les clients des banques au sujet de divers e-mails frauduleux demandant aux destinataires de révéler des informations personnelles, dont leurs noms et adresses, les détails concernant leur carte d'identité nationale/ passeport, les détails de leur carte de crédit et/ ou de débit, les codes confidentiels ainsi que les identifiants et mots de passe pour ceux qui se servent de services bancaires en ligne.

Ces e-mails n'émanant pas des banques, invitent les lecteurs à visiter un site web en cliquant sur un lien et à entrer leurs données personnelles comme indiqué ci-dessus. **Les banques n'enverraient jamais des e-mails demandant que de telles informations confidentielles leur soient soumises en ligne et les clients ne doivent PAS répondre à de tels e-mails, même s'ils sont envoyés plusieurs fois de suite. Ces messages doivent être supprimés immédiatement.**

- Nous rappelons aux clients des établissements bancaires de s'assurer qu'ils sont bien connectés à un site web valide avant d'entrer n'importe quelle donnée personnelle et confidentielle.
- Au moindre doute ou si les clients sont inquiets qu'ils ont pu révéler leurs données d'accès à des sites web frauduleux, ils doivent immédiatement prendre contact avec leurs banques respectives.