TELEPHONE CALLS FROM THE BANK

From time to time your bank may wish to contact you by telephone.

ALWAYS

- Take a note of the person's name and a telephone number. Then return the call USING A PUBLISHED CONTACT NUMBER FOR THE BANK. If the call is genuine, the bank will be more than happy if you do this and will probably be impressed with your vigilance!
- Report to your bank cases where you have been requested to disclose your PIN (Personal Identification Number) details by calling over a published telephone number. Bank staff should never ask for PIN details and such calls should be treated as fraudulent.

NEVER

- Divulge any details of your bank account, your password, PIN or personal details to anyone, even if the person purports to be from the bank or the police.

PREVENT IDENTITY THEFT

ALWAYS

- Lock your letterbox. If you cannot, then empty your mailbox as soon as possible after the mail is delivered.
- Take care to prevent third parties from accessing your bank statements, cheque books and general correspondence by keeping such information securely locked away.
- Check your bank statements promptly.
- In case you notice any error, report same immediately to your bank.

NEVER

- Leave behind printed receipts at bank machines.
- Disclose credit cards or other personal information on a website that is not secure.
- Throw your bank statements in paper baskets or garbage bins; shred or burn them instead.
- Disclose your personal data to third parties.

LES APPELS VENANT DE VOTRE BANQUE

De temps en temps, votre banque souhaiterait vous contacter par téléphone.

VEUILLEZ

- *Noter le nom de votre interlocuteur et son numéro de téléphone. Retourner l'appel en appelant au NUMERO DE LA BANQUE FIGURANT A L'ANNUAIRE TELEPHONIQUE. Si l'appel émane de votre banque, celle-ci apprécierait le fait que vous fassiez preuve d'une telle vigilance.*
- *Rapporter immédiatement tout appel vous demandant votre PIN (numéro d'identification personnel) en appelant la banque au numéro figurant à l'annuaire.*

Le personnel de la banque ne doit jamais vous demander des détails de votre mot de passe, et tout appel de ce genre doit être traité comme suspect.

NE JAMAIS

- *Divulguer des détails de votre compte bancaire, PIN, mot de passe ou tout autre détail personnel même si votre interlocuteur prétend être un préposé de la banque ou un agent de police.*

PREVENIR L'USURPATION D'IDENTITE

VEUILLEZ

- *Fermer votre boîte à lettres à clef. Si vous ne pouvez le faire, récupérez votre courrier dès qu'il est livré.*
- *Garder les documents contenant des renseignements personnels (par exemple, relevés bancaires, carnet de chèques) sous clef dans un lieu sûr.*
- *Passer en revue vos relevés bancaires sans tarder.*
- *Signaler immédiatement toute erreur à votre banque.*

NE JAMAIS

- *Laisser derrière vous des reçus/relevés d'opérations après avoir utilisé un guichet automatique.*
- *Divulguer les détails de vos cartes de crédit ou toute autre information personnelle sur un site internet non sécurisé.*
- *Jeter vos relevés bancaires sans les avoir déchirés ou déchiquetés.*
- *Révéler vos informations personnelles aux tiers.*

LIST OF OUR MEMBERS

LISTE DE NOS MEMBRES

Bank of Baroda
Banque des Mascareignes Ltée
Barclays Bank PLC
Deutsche Bank (Mauritius) Limited
First City Bank Ltd
Habib Bank Limited
Indian Ocean International Bank Limited
Investec Bank (Mauritius) Limited
Mauritius Post and Cooperative Bank Ltd
P.T Bank Internasional Indonesia
SBI International (Mauritius) Ltd
SBM Nedbank International Limited
South East Asian Bank Ltd
Standard Bank (Mauritius) Limited
Standard Chartered Bank (Mauritius) Limited
State Bank of Mauritius Ltd
The Hongkong and Shanghai Banking Corporation Limited
The Mauritius Commercial Bank Ltd

MBA
MAURITIUS BANKERS ASSOCIATION LIMITED

Mauritius Bankers Association Limited
3rd Floor, Plantation House
Duke of Edinburgh Street - Port Louis - Mauritius
Tel : (230) 210 9677, 211 2980, 213 0990
Fax : (230) 213 0968 - Email : ceo.mba@intnet.mu

PROTECTING YOUR FINANCES

PROTEGER SON ARGENT

MBA
MAURITIUS BANKERS ASSOCIATION LIMITED

INTERNET BANKING

Provided you keep your password confidential and ensure that others cannot see your PC screen and keyboard when you sign in, Internet Banking is just as safe as any other form of banking.

Take simple precautions such as:

ALWAYS

- Clear your browser's cache when you exit and if your browser is equipped to store passwords and user names, consider disabling this function.
- Log off from the Internet Banking site once all operations have been completed.
- Switch off your computer completely when you have finished using it.
- Consider setting up separate access accounts if your computer supports this feature.

NEVER

- Store your password on your computer's hard disk.
- Open emails with unusual attachments.

Your bank's help desk will always be happy to discuss the security levels in place and any other queries you may have.

LA BANQUE ELECTRONIQUE

Effectuer des opérations bancaires par Internet est aussi sûr que les autres services bancaires si vous ne divulguez à personne votre mot de passe et si vous êtes vigilant lors de votre connexion afin que personne ne puisse voir votre écran ou votre clavier.

RESPECTER LES RÈGLES DE PRUDENCE TELLES QUE :

- *Purger le fichier du navigateur avant de quitter. Si votre navigateur peut mémoriser vos mots de passe et noms d'utilisateurs, désactivez cette option.*
- *Se déconnecter aussitôt la consultation terminée.*
- *Éteindre votre ordinateur après utilisation.*
- *Créer des comptes à accès séparé si votre logiciel vous le permet.*

NE JAMAIS

- *Mémoriser votre mot de passe sur le disque dur de votre ordinateur.*
- *Ouvrir des emails qui comportent des pièces jointes suspectes.*

Votre banque sera toujours à votre écoute pour vous renseigner sur l'aspect sécurité ainsi que toutes autres questions complémentaires.

BUYING OVER THE INTERNET

ALWAYS

- Make sure your browser is set to the highest security level. This may not be the default security setting.
- Keep a record of the retailer's alternative contact details such as a (non-mobile) telephone number and street address. Beware if these are not available on the website and do not rely on an email address alone.
- Use only secure websites when transacting. Secure websites are indicated by a padlock or key at the bottom of the screen and the 'http'on the address bar becomes 'https'.
- If you have any concern, call the company for reassurance that it is legitimate before giving your card details.
- Print out a copy of your order and any details of terms and conditions and returns policy. Check to see whether VAT and postage or shipping costs will be added to your purchases.
- Be aware, that if you are buying from abroad, it may be difficult to seek redress in case of any problems. If you have any doubt about giving your card details, arrange for an alternative payment method.

TELEPHONE BANKING

ALWAYS

- Use the published telephone numbers and ensure that you provide only your bank with the security details requested.
- Ensure that you cannot be overheard.
- In case you have used a mobile phone, your phone set would have recorded your login details. Clear them out.

NEVER

- Write down your password or other security details.
- Divulge your password to anyone else.

ACHATS EN LIGNE

VEILLER A

- *Vous assurer que votre navigateur présente le niveau le plus élevé de sécurité. Cela n'est peut être pas la configuration de base de votre ordinateur.*
- *Identifier clairement l'entreprise, au moyen des détails tels que l'adresse postale, le numéro de téléphone fixe, correspondant au site marchand. Prenez garde si ces détails ne sont pas présents et ne vous fiez pas uniquement à l'adresse email.*
- *Utiliser uniquement les sites sécurisés pour vos transactions. Pour cela, vérifiez qu'un petit cadenas fermé ou une clef apparaît au bas de votre écran, et que le "http" de votre adresse devient "https".*
- *En cas de doute, appelez la société marchande pour vous rassurer qu'elle n'est pas fictive, avant de fournir les détails de votre carte.*
- *Imprimer une copie de votre commande et les conditions générales de vente, notamment les conditions de retour en cas de produits défectueux. A vérifier également si la TVA et/ou l'affranchissement/ les coûts d'expéditions seront ajoutés à votre achat.*
- *Vous rappeler qu'en cas d'achat de l'étranger, il vous sera difficile d'obtenir réparation en cas de difficultés. Donc, en cas de doute, il est préférable de choisir une autre méthode de paiement que sa carte bancaire.*

OPERATIONS BANCAIRES PAR TELEPHONE

VEILLER A

- *N'utiliser que les numéros de téléphone figurant à l'annuaire, et assurez-vous que vous ne fournissez des détails de sécurité qu'à votre banque.*
- *Vous assurer que votre conversation ne peut être entendue par d'autres personnes.*
- *Enlever les détails de votre compte bancaire de votre téléphone portable.*

NE JAMAIS

- *Faire figurer votre mot de passe ou d'autres détails de sécurité sur un document.*
- *Divulguer votre mot de passe.*