

## **Tips for Fraud Avoidance**

### **Important**

Please place your signature on the strip provided on the back of your credit card as soon as you receive it. Please remember to activate your card before use. If your card is replaced or renewed, please dispose of your old card by cutting it into four. Never permit any other person to use your credit card.

### **Informing your Credit Card details to third parties**

Transactions could be charged to your credit card account with the use of your card details (physical card or a signature is not needed). Therefore, please ensure that your card details are not shared with any other person.

### **Lost Card**

Report the loss of your credit card immediately to the Bank.

3 easy steps to report:

- Dial our Customer Service hotline 11 4 4722 75
- Press 1 – for English
- Press 2 – to report a lost card

### **Personal Identification Number (PIN)**

Never keep your credit card and PIN together (Memorize your PIN and destroy the PIN advice). If you change your PIN, do not use obvious numbers such as telephone numbers, ID card or date of birth.

### **Keeping your on-line banking secure**

There is much that your business can do to protect itself, and its users, whilst online. Some of these measures are simple; others may require a little time invested, or additional help from a PC support resource.

If nothing else, the business should be guided by five golden rules.

1. Make sure you have the latest security updates and patches
2. Install anti-virus software
3. Use personal firewalls
4. Read our password advice
5. Use an anti-spyware program

- **Keep user details and identity secure**

Identity theft is the act of stealing or using an individual's personal information without their knowledge or consent, for example, to illegally make purchases, or to gain access to funds.

- **Keep passwords secure**

Passwords are one of the keys to online account information. Your HSBC Internet banking password and digital certificate permit access to the bank accounts.

- **Keep your computer/network secure**

The Internet offers hackers the opportunity to access your systems. Whilst the probability of the happening may be small, the impact could be major. There are a number of key steps you can take to protect your business.

- **Keep your Internet Banking session secure**

You should ensure that you and your users are aware of potential pitfalls and know the best way to deal with them. There are two key areas to focus on.

Generally, email that is sent or received through a regular email address (e.g., yourname@yourbiz.com) is not secure or encrypted to protect the contents. Therefore, any sensitive information included in an email is at risk of being intercepted by unauthorized individuals. Never send Internet banking user names, passwords or digital certificates by email to anyone.

## **We are here to serve**

If for any reason you are not entirely satisfied with any aspect of our service, we want to hear from you as soon as possible. We will use this information to put matters right and take steps to prevent a recurrence.

## **Raising your concerns**

Our friendly and professional Customer Service staff (in our branches and call centre) are all geared to deal with your concerns. They will make every effort to resolve issues quickly and efficiently.

However, in the event that you are not entirely satisfied with the manner in which you have been served, or if our products do not meet your expectations, please mail your concerns to:

**The Manger Customer Service  
Personal Financial Services  
HSBC Centre  
525, Union Place  
Colombo 2**

Or

E-mail: [customersolutions@hsbc.com.lk](mailto:customersolutions@hsbc.com.lk)

Or

Call the Customer Solution hotline on: +94 11 4 511566

**Service Level Commitment**

If we are unable to resolve the matter immediately, we will provide you with a solution within three working days of receiving your feedback. However some issues may be more complex and could take a little longer to resolve. In this case, we will provide you with an estimated response time.