INTRODUCTIONS FOR SAFE TRANSACTIONS OF E- BANKING AND CARDS

To ensure the security and confidentiality, to protect the rights and interests of customers, for transactions through e- banking and cards of Indovinabank, Valued Customers please read introductions carefully and comply with them.

Indovinabank sincerely appreciates your concern.

TABLE OF CONTENTS

I. INTRODUCTIONS FOR SAFE TRANSACTIONS OF E- BANKING

1. Principles of Information Security

ABSOLUTELY NOT:

- Open a current account and register E- banking services for somebody else to use.
- Reveal PIN, password, username of E- banking services to somebody else through telephone, email, access link,…
- Click strange access link and declare personal information for any email address sent to you or telephone calls to you. Indovinabank never asks customers for declaring both username and password of E- banking service through telephone or email.
- Install software, tools from non-reliable sources and do not have licenses.
- Save username and log-in password on web browsers.
- Use unlocked mobile devices to download and use Ebanking application.
- Fund transfer, top - up to designated phone number for procedures to receive awards. Indovinabank never asks customers for funds transfer, top- up to any phone number to receive awards from any Promotion Program of Indovinabank.

CUSTOMERS SHOULD:

Use personal computer/mobile phone has installed anti-virus software to access IVB Ebanking service;

Only use public computer to access, make Ebanking's transactions in necessarily situations and after that use secure computer to change log-in account password

Protect secret of the secret code, OTP and maintains digital signature (PKI) like maintains cash.

- Setup password:

  + Use reliable password including: length of password (at least 6 characters) combination of capital letter, small letter and numbers.

  + Do not use a password containing personal information that others can guess easily as your birthday, phone number, registration number of vehicles, your name, your relatives' name like your husband/wife, simple representatives of sets of numbers as 123456.

- For password security:

+ Change password when you access E- banking program first within 24 hours since you received it.

+ Change your password constantly (at least once per 12 months) to ensure security for current account.

+ Avoid writing your password on paper or recording in any other form.

+ Change password of IVB E- banking service immediately after you find that you have just clicked on the links which you suspect they are falsified, or you in deliberately provide personal information for somebody else.

2. Principles of using the service safely

- To log in IVB Ebanking service, customers should visit the official website of Indovinabank (www.indovinabank.com.vn) and select "Internet Banking" module on the website or download IVB Mobile banking application;
- When you receive OTP message from Indovinabank, it is necessary for you to check content of message including: transaction type, transaction value, transaction channel. Unless information content of message coincides with current transaction, customer absolutely will not put OTP in any websites or reveal it to somebody else;
- When IVB system is processing your transaction, please do not log out the monitor transaction and wait result of transaction from IVB system before you carry out other transactions;
- Always remember log out/ exit the E- banking program after you access E- banking service.
- You should register Smart Notify service to receive messages with notification of changes in your account balance immediately that you can know transactions in your account to limit risks and loss in lowest level.

II. INTRODUCTION FOR SAFE TRANSACTION OF INDOVINABANK CARDS:

1. General principles:

- When you receive card, you need to:

  + Check information on your card to ensure compliance with the information you have registered before.

+ Change personal identification number (PIN) for debit card (ATM) which bank provided at automatic teller machine (ATM) in order to activate your card.

+ Do not setup your password concerning personal information as: your birthday, you telephone number, registration number of your vehicles…

+ Do not write password on your card or place close to your card for your information in order not to be discovered or exploited.

- Secure your card and personal identification number (PIN) at any time in any case:

+ Do not give your card to anybody except banking staff or cashier appointed to work with customer at merchant.

+ Do not reveal information on the card, also personal identification number (PIN) to anybody. A customer is the only person who knows that information.

- When you make transaction and you use PIN, please pay attention to:

+ Ensure that nobody can see your personal identification number (PIN) while you are making transaction (by cover your keyboard).

+ You should change your personal identification number (PIN) constantly.

+ If you enter your PIN incorrectly 03 times in a row, your card will become “locked” within 24 hours to ensure security absolutely for customers.

- Register and use E- banking service of Indovinabank (IVB Mobile Banking, SMS Banking…) to ensure:

+ Receive notification of changes concerning your personal account or transaction limit as soon as you have just made transaction.

+ Lock/Unlock internet transaction function of credit card proactively for you to control online payment transaction.

- Check details in credit card statement. In case you have any questions, please notify the bank in writing within 45 days since you made transaction.
- Please notify the bank of changes of residential address, statement delivery address, telephone number, and signature.

2. Principles of card maintenance:

- Do not bend, fold your card.

- Do not place your card near electronic devices which can broadcast or have strong magnetism, in fact, affect data on your card.
- Do not scratch magnetic stripe on the back of your card.
- Keep your card carefully and place your card at the position which helps you to find out stolen card easily.

3. Principles of transactions at automatic teller machine (ATM):

- Observe automatic teller machine (ATM) before you make transaction, especially positions as: magnetic stripe reader, keyboard, and camera. If you realize that ATM has strange devices or has any unusual signs, you stop to make transaction and notify Indovinabank through hotline 1900 588 879.
- You should use your hands to cover keyboard while you enter your personal identification number.
- ATM will return your card before it gives money to you, you should wait to get your cash and not go away immediately. In case ATM gives cash to you slowly, somebody else can take it.

4. Principles of card transactions for merchants:

- Please pay attention to check the information on the bills, ensure the information is accurate. You only sign your name on the bill when all of the information is correct.
- Ensure that all transactions for merchants have to be performed in the presence of you.
- Ensure that your card is given back to you after the transaction finished.
- Retain the bills and related vouchers in order that you can complain then if necessary.

5. Principles of card transactions on the Internet:

- Only use card information to make payment on the online websites which are verified by Visa/Master ("Verified by Visa/Master" icon on the websites) and your transaction is authenticated by OTP password of 3D Secure Service. You should not also use public computer when you make online transactions.
- Read payment policies and procedures carefully before you accept to make a payment.
- Always remember to log out/exit online website after the transaction finished.
- After you finish to make online transaction, you block "Internet Transaction" function of IVB cards by calling us 1900 588 879 or accessing our website.

III. WARNING OF ONLINE ATTACKS:

For customers to prevent risks actively and decrease overall damage, Indovinabank lists here various kind of attack that criminals usually use:

- International financial fraud: you receive a letter or an email that it seems to be sent to you actively. Actually, it is sent to many people to give a proposal: you will receive large amounts of money but you will not receive anything.
- Identity theft: that is the behavior of individuals and organizations obtaining personal information of customers to have financial benefits, mainly information of credit cards to create a huge debt for customers.
- Virus: that is the program or piece of code designed to replicate and copy itself to infected objects else. The virus frequently destroys infected computer to steal sensitive personal information, open the back door for hackers to take possession of control rights of your computer. That brings benefits to people spread virus. Lately, kind of viruses through email is common, it enters e- mail and often replicates itself in order to spread virus to those in customers' directory.
- Skimming: that is a method of stealing information account when you make a transaction at automatic teller machine (ATM). The bad guys use sophisticated electronic equipment to steal the information of the card including PIN in order to make falsified cards and withdraw cash from customers' current accounts at ATM.
- Phishing: using fake websites. When customers access these websites, somebody else steals customers' financial information.
- Hacking: illegal access to customers' computers by internet.

IV. SECURITY SOLUTIONS OF IVB:

- Use authentication security technology with two factors: password to log in and security equipment to receive OTP message or digital signature.
- Block a customer account automatically: when you enter wrong password 05 times, your current account is locked temporarily. To activate your account, you need to contact IVB nearby Branches/ Transaction offices for further instruction.
- 3D Secure Service: provide an extra layer of password. Provided that a customer has to enter it to online website, the transaction will be approved. 3D Secure service is only applicable if you make a transaction on online website verified by Visa/Master.
- Other solutions are carried out synchronously in designing and operating services, which based on modern technologies; risk warning and satisfied international practice.

V. CONTACT INDOVINABANK:

Please contact the Customer Service Center 24/7 of Indovinabank by telephone 1900 588 879 in the following cases:

- When you meet any problems in the course of using the service.

- If your phone is lost or there is any change to the registered phone number for the use of E- banking services.
- When there is any change of email address, telephone number, residential address, address for receiving card statement and signature.
- When the card is stolen, lost or you discover that the transaction is not done by you.
- When you suspect that your email address, your phone number which used for e- banking service are exploited.
- Accidentally, you click falsified links or you provide your personal information for people who you suspect that they impersonate somebody else.
- If you have any concerns, questions about using card services, E - banking of Indovinabank.

In all cases, only the phone number of the Customer Service Center 24/7 Indovinabank phone call you: 1900 588 879

Sincerely thank you for trusting, choosing to use the services of Indovinabank!

E- banking Service of Indovinabank – Solid Growth Together