Please take some time to read through the following important information

Risks of Internet Banking

While Internet Banking can bring you more convenience in terms of faster and easier access to your bank account(s), there are inherent risks that you need to be aware of.

Due to the open nature of the Internet, web-based systems such as Internet Banking are inherently subject to risks such as those related to virus attacks, hacking, unauthorized access and fraudulent transactions.

While Alpha Bank Cyprus Ltd has put in place the necessary security practices and measures to safeguard against these risks, the Bank is still unable to fully guarantee the complete security of your transactions against such malicious attacks. As the end-user, you also play a key role in safeguarding your account information.

Alpha Bank Cyprus Ltd Security Practices

At Alpha Bank Cyprus Ltd we know that the confidentiality of your personal information and security is very important to you and we are committed to provide you with a safe and secure online environment for your banking needs.

Your transactions and information are protected by industrial strength security technology that is used by leading banks. Alpha Bank Cyprus Ltd also implements a series of other security solutions like routers and firewalls to safeguard your interests.

The security features which we have put in place include:

- ***Industry's strongest 128-bit SSL encryption***
    - Alpha Express Banking is a VeriSign Secure Site. This is an assurance that the site runs legitimately under the care of Alpha Bank Cyprus Ltd. All information is sent in a Secure Socket Layer (SSL) session and is encrypted to protect you against unintentional information disclosure to third parties.
    - The 128-bit SSL encryption we use is currently the industry's strongest. Any data you send through Alpha Express Banking will be scrambled into an unrecognized form before it is transmitted to our server where only the Bank has the special key to decode it. The information we send to you is similarly protected.
      [128-bit encrypted messages are over septillion times (or 309,485,000,000,000,000,000,000,000 times) harder to break than 40-bit messages. It would take1 trillion x 1 trillion years to break using today's most sophisticated technology].
- ***Personal Identification Number (PIN) and unique User Identification (User ID)***
    - We have put in place a double-authentication login process whereby customer needs to enter his Alpha Express Banking PIN matched with his unique User ID in order to access his account information and/or transact online.
    - Alpha Express Banking access is based on a unique User ID that cannot be duplicated by any other user on the system, and a PIN tied to that User ID. The User ID and PIN combination is unique to each user.

Please take some time to read through the following important information

- ***One-Time Password (OTP) "Token" Device:***
  - The device combines the increased security and the ease of transaction execution. By activating your device, it is automatically connected to the "authorized user" subscription. Every time you want to perform a transaction through Alpha Express Banking you will be requested to enter an OTP code, generated from the device with a press of a button. You just, press the button, located on the left hand side of the device and a one-time password ("OTP") code is produced. The system will check the entered OTP code verifying that the transaction request is coming from the authorized customer that holds the specific OTP device.
- ***Automatic Logout Feature***
  - When our system detects that your login session has not recorded any activity for some time, your active session of Alpha Express Banking will be automatically terminated. You will need to login again using your User ID and PIN if you wish to access the service.

Your Role in Safeguarding Your Account Information

Apart from the security measures put in place by the Bank, you play an equally important role to ensure your online security and account information is not compromised.

You **SHOULD** adopt the following recommended security practices while banking online:

- Keep your PIN confidential at all times
- Always log off your online session
- Do not store your User ID/PIN when using Internet Explorer browsers
- Do not disclose your personal information to suspected websites
- Use a computer/ device that you trust
- Ensure adequate security for wireless network and devices
- Clear your browser's cache and history after each session
- Protect your computer from viruses and malicious programs
- Protect your critical data
- Disable the "File and Printer Sharing" feature on your Operating system
- Check your account and transaction history details regularly
- Update us when you change your contact particulars
- Let us know immediately if there's a problem!

- ***Keep your PIN confidential at all times***
  - Your PIN is like the key to your online safe. We identify you using your User ID and PIN. As such, protecting your online identity is very important and you need to safeguard your PIN at all times.
  - **Important Tips on how you can safeguard and protect your PIN:**
    - Never use the same PIN for other financial or non-financial web-based services such as for email, online shopping, digital identity and other online subscription services.
    - Do not choose a PIN that is easily guessed, like your telephone number, national ID number, date of birth, User ID plus or minus some digits, or other associated data. You should select a robust and unique PIN to make it difficult for anyone to guess.

- Do not use sequential numbers (e.g. 123456) or the same number more than twice (e.g. 121145).
- Do not share or divulge your PIN to anyone.
- Memorize your PIN. Do not write down your PIN or store it in computer hard-disk, diskette, mobile phone or other insecure means.
- Do not use your PIN when someone else can see you keying it in.
- Before entering your User ID and PIN, you should always check that the site you are visiting belongs to Alpha Bank Cyprus Ltd by verifying that the URL displayed in the browser is correct. The URL of Alpha Express Banking is https://online.alphabank.com.cy/
- When performing online transactions, always ensure that the URL is preceded by "https".
- For Netscape browsers, a security icon that looks like a lock or key should appear in the browser.
- For Internet Explorer browsers, you can check that your session is secured by right-clicking on the page and selecting properties.
- Always use the latest recommended Internet browser such as those that support 128-bit encryption so that you have the most updated security features available.
- Change your PIN regularly by using the 'Change of PIN' service (minimum 6 digits, maximum 9 digits).
- Change your PIN immediately if you suspect it has been exposed to others or the moment you suspect any unauthorized access.
- Block your PIN immediately if you suspect it has been exposed to others. This can be done by entering 3 sequential times an invalid PIN.

IMPORTANT: *No staff of Alpha Bank Cyprus Ltd should ever ask you for your PIN for whatever reasons.*

- ***Always log off your online session***
  - Log off your online session and close your web browser's window whenever you leave your computer, even for a short while. This immediately ends your Alpha Express Banking session and prevents further transactions from being carried out without a fresh login. You should also shut down your computer, when not in use, to prevent unauthorized access to your computer.
  - You can even set a password for your screen saver to prevent unauthorized access to your computer when you need to leave for a while. To do so, simply:
    - Right click at your desktop area
    - Select "Properties"
    - Click on the "Screen Saver" tab
    - Select your choice of screen saver from the "Screen Saver" drop-list
    - Check the "Password protected" option
    - Click on "Change..." to change your screen saver password if necessary
    - Under the "Wait:" option, select the period of inactivity before your screen saver is activated
    - Click "OK" to save your settings

Please take some time to read through the following important information

- ***Do not store your User ID/PIN when using Internet Explorer browsers***
  - Some browsers store and list possible matches from entries that you have typed previously. You can prevent any User ID/PIN from being stored in your browsers by de-activating the function:
    - Launch your Internet Explorer browser
      - Click on "Tools" >> "Internet Options" >> "Content".
      - Under "Personal Information", click on "AutoComplete".
      - Uncheck "User names and passwords on forms" and click on "Clear Passwords".
      - Click on "OK" to save your settings
    - Launch your Netscape browser
      - Go to "Netscape" or "Edit"
      - Select "Preferences"
      - Double click on "Privacy & Security"
      - Click on "Passwords"
      - Ensure that "Remember passwords" under "Password Manager" is unchecked
      - Click "OK" to save your settings

- ***Do not disclose your personal information to suspected websites***
  - To prevent your personal information from being captured by bogus websites, you should not disclose your personal, financial or credit card information to little-known or suspected websites.

- ***Use a computer/ device that you trust***
  - You should not conduct your Alpha Express Banking transactions on computers/ devices which cannot be trusted such as shared or public computers, especially computers located in unusual and bizarre places. If you have to, always clear your browser cache after each session on such computers to ensure your account information is removed. For Internet Explorer 5.x users, please also ensure that the "AutoComplete" function is deactivated after use.

- ***Ensure adequate security level for wireless network and devices***
  - Poorly configured wireless equipment may allow malicious entry into your computer directly through the air waves. If you are using a wireless network/ device, you are strongly advised to read your instruction manual, or consult your vendors if necessary, to configure your wireless network/ device to ensure that adequate security levels are established.

- ***Clear your browser's cache and history after each session***
  - Temporary files stored in your computer called cache files and history can retain information and data. Always remember to clear your browser's cache and history after

each session so that your account information is removed, especially if you are using a shared computer.

- ***Protect your computer from viruses and malicious programs***
  - Apart from destroying important data on your computer, viruses/malicious programs such as Trojan Horse may run a password sniffing program in the background to capture your password keystrokes without your knowledge. Being constantly online may increase your risk exposure for your computer. To avoid getting infected, you should:
    - Never download any file from sites (e.g. program, game, picture, mp3 song) or people (e.g. email attachments) which you aren't sure about.
    - Delete junk or chain emails.
    - Never use features in your programs that automatically get or preview files. For example, never turn on "auto DCC get" in mIRC and never enable the preview mode in Outlook and other mail programs.
    - Install firewall and virus detection software to protect against hackers, virus attacks or malicious "Trojan Horse" programs. You should also update your software's virus definition frequently.
    - Suggested Reference sites for Anti-Virus & Computer Protection Software*:
      - Trend Micro
      - McAfee
      - Symantec

      **The above are suggestions only and are not an official endorsement of the product whatsoever.*

- ***Protect your critical data***
  - Make regular backup of your critical data and ensure that these data in your computer is adequately protected.

- ***Disable the "File and Printer Sharing" feature on your Operating System***
  - This prevents an external party from gaining illegal control or access to your computer. You can refer to your computer vendor or instruction manual on how this is done.

- ***Check your account and transaction history details regularly***
  - Always check your transaction history details and statements regularly to make sure that all details are updated and there are no unauthorized transactions on your accounts.

- ***Update us when you change your contact particulars***
  - To make it easier for us to reach you whenever we detect unusual transactions in your account, always keep us updated with your latest contact numbers and mailing address.

- ***Let us know immediately if there's a problem!***
  - If you notice any unusual/unauthorized transactions, please change or block your PIN and notify us immediately. Where necessary, your Alpha Express Banking access can be suspended at your request to protect your interest. Contact us at:
    Tel1: 8000-3333 (domestic – toll-free)

Tel2: +357 22888610 (international)
Email: esupport@alphabank.com.cy

- ***Your Obligations, Responsibilities and Rights***
  - Your usage of Alpha Express Banking is subject at all times to the Terms and Conditions governing Electronic Services (the "Terms and Conditions") and the terms and conditions applicable to each product or service accessed by any of the Electronic Services. In addition, you are advised to comply with our recommended security practices to ensure you do not under any circumstances compromise your online security.