How we protect your online security

Keeping financial and personal information about you secure and confidential is one of our most important responsibilities. We take the following steps to protect our systems and their interaction with you:

- **Firewalls** are used to prevent unauthorized access by individuals or networks. UBS Financial Services Inc. uses firewall technology to help protect its systems as they interact with you over the Internet.

- **Virus protection software** is used to help identify, lessen the effect of or prevent known computer viruses. UBS Financial Services Inc. uses virus protection software across our network to help protect our computer systems from malicious code.

- **Secure Socket Layer (SSL)** technology is used by UBS Financial Services Inc. to encrypt the connection that we make with you over the Internet, as well as to encrypt the dedicated lines that connect to our systems. Encrypting transmission of data in this way makes it impossible for an unauthorized third party to decipher sensitive information as it travels between UBS Financial Services Inc. and you.

- A time-out feature is used to protect your accounts from unauthorized access should your PC be left unattended or should you be unable to exit a website by normal means. To provide additional protection, select parts of our website invoke a time-out feature.
  - Always remember to log off of Online Services when you finish your session. You can do this by clicking the "Logout" link in the upper right-hand corner of the site. In the event that you fail to log off, most activity on Online Services will time out after being idle for 30 minutes. This is done to provide additional security to you while you are online. To proceed following this timeout, you will need to log in again.
  - As an added precaution, when using our Online Trading and Bill Pay/Funds Transfer features, your session will time out if you are inactive for 15 minutes.
  - Always close your browser after completing a logon session.
  - Again, in order to proceed following a timeout, you will need to re-enter your password.

UBS Financial Services Inc. continues to explore and evaluate advances in security technology to ensure that we protect your information. We strongly believe that security is everyone's responsibility.

Your Computer

Anti-virus protection

If your computer becomes infected with a virus, you could possibly lose information and incur repair expenses. We recommend that you install an anti-virus protection program to reduce the risk of your computer becoming infected.

Automatic Upgrades

We recommend that you install software that automatically upgrades your virus protection. If you do not have this automatic upgrade feature, make sure you update your virus detection program weekly and whenever you hear of a new virus.

Attached Files

We advise that you do not open e-mail attachments or files on a storage device (i.e., CD, USB token, etc.) unless you are certain that you can trust the source. If you are unsure of the source, you should either delete those files or scan them for viruses.

Firewalls

A firewall blocks unauthorized access by individuals and networks. Placing a personal firewall on your computer can help prevent unauthorized access to your computer. If possible, do not keep sensitive information on any of your hard drives. Keep financial data on a removable diskette and place in a secure location.

- **DSL or cable modem.** If you use a digital subscriber line (DSL) or cable modem, your Internet connection is on whenever your computer is on. If you leave your computer on for long periods of time, the window of opportunity for malicious activity against your computer increases.

- **Dial-up modem.** If you use a dial-up modem, your risk to automated snooping programs (designed to steal information) is limited to the duration of your Internet connection. Though your exposure is limited, a firewall is recommended.

Additional Security Through Your Browser

Your browser provides access and the ability to navigate on the Internet. Most computers come with a browser already installed. An up-to-date and correctly configured Internet browser can add to your online security. For example, the latest versions support a higher level of encryption. To ensure that your browser provides the highest level of security:

- Always check which browsers are recommended for the websites you are visiting.

- Check your browser for built-in safety features.

- Update your browser regularly to take advantage of new safety features.

Spyware Protection

Spyware is computer software that can collect vital user information without the user's informed consent. Make sure that your computer has an anti-spyware protection program that can detect and remove all forms of spyware, and use this program to scan your computer frequently. Many software companies offer anti-spyware protection programs, and will also provide customer service in case you have questions.

Using Other Websites

Be careful when sending personal information such as your Social Security number, credit card information or other personal data over the Internet. We recommend that you:

- Validate the business reputation of the company by researching the company's history.

- Perform transactions in a secure website (generally denoted by an image of a closed lock in the lower right hand side of the browser window).

E-mail Security

In most cases, e-mail is not secure. Therefore, never include sensitive information such as your account number or your Social Security number.

In addition, e-mail viruses are commonplace in today's environment. You should not accept and open e-mail if you are not sure of the sender's identity or its content. If you receive an e-mail that seems suspicious, do not forward it. Instead, delete it immediately. You should also regularly check the website of any reputable anti-virus software company to stay informed about known viruses.

Secure Socket Layer (SSL)

An encrypted SSL connection requires all information sent between a client and a server to be encrypted by the sending software and decrypted by the receiving software, thus providing a high degree of confidentiality and integrity. In addition, all data sent over an encrypted SSL connection is protected with a mechanism that detects tampering.

The SSL protocol uses a combination of public-key and symmetric-key encryption. Symmetric-key encryption is much faster than public-key encryption, but public-key encryption provides better authentication techniques. An SSL session always begins with an exchange of messages called the SSL handshake. The handshake allows the server to authenticate itself to the client using public-key techniques, and then allows the client and the server to cooperate in the creation of symmetric keys used for rapid encryption, decryption and tamper detection during the session that follows. The handshake also allows the client to authenticate itself to the server.

ubs.com/fs
110602-3031-006