STATE OF HAWAII
Department of Commerce and Consumer Affairs
Office of the Securities Commissioner
Investor Education Program
Call toll free: 1-877-HI-SCAMS
www.investing.hawaii.gov

SIFMA Securities Industry and Financial Markets Association

FINRA Financial Industry Regulatory Authority

Keeping Your Account Secure

Tips for Protecting Your Financial Information

Your brokerage firm has an obligation to safeguard your personal financial information. But even the best procedures cannot prevent all instances of identity theft—especially if the vulnerability lies with you, the customer.

This brochure describes the critical steps you can take to safeguard your financial accounts and help prevent identity theft.

How Does Identity Theft Occur?

A host of ways. Some identity thieves use keystroke-logging software to capture usernames and passwords, disseminating these programs through instant messages, emails, or freeware. Others "phish" for sensitive information by sending phony emails that purport to come from a legitimate financial institution but which ask for information your firm would never request through email—such as confirmation of an account number, password, credit card number, or Social Security number. Still others use the old-fashioned method of "dumpster-diving" to recover your discarded account statements or other records that haven't been properly shredded.

How Can I Protect Myself?

Take the following steps to secure your brokerage accounts and your personal financial information:

- **Protect Your Passwords and PINs.** Do not share your passwords or PINs with others. You also should not store your passwords or PINs on your computer. If you need to write down your passwords or PINs, store them in a secure, private place. You should change your passwords and PINs regularly and use a different password and PIN for each of your accounts. Use passwords and PINs that contain numbers and letters or symbols.

- **Maintain Your Computer Security.** Personal firewalls and security software packages (with anti-virus, anti-spam, and spyware detection features) are a must for those who engage in online financial transactions. Make sure that your computer has up-to-date security software, including security patches, that the software is configured for automatic updates, and that the software is always turned on. For laptops, be sure to use encryption software. Computer hardware and software providers also maintain security pages on their Web sites with tips for checking and improving the security of your system.

- **Use Your Own Computer.** It is generally safer to access your brokerage account from your own computer. Avoid using public computers to access your brokerage account. Public computers may contain software that captures passwords and PINs, providing that information to others at your expense. If you do use another computer, be sure to delete your "Temporary Internet Files" or "Cache" and clear all of your "History" after you log off your account. You should occasionally check to make sure that no one else has attached any device or added programs to your computer without your knowledge or consent. Consult the Help function on your browser and operating system to learn how to delete this information.

- **Log Out Completely.** Always click the "log out" button to terminate your access to your brokerage firm's Web site. Access may not be terminated if you simply close or minimize your browser or type in a new web address when you're done using your online account. Other users of the computer might be able to re-enter the site and have access to your account online if you do not properly log out. You also potentially expose yourself to "session stealing" if you have multiple Web pages open while logged on to your brokerage account. Avoid multi-tasking on multiple Web pages when checking your financial accounts online—or, if you must visit another site, use a different type of browser rather than opening another window.

- **Be Prudent When Using Wireless Connections.** Wireless networks may not provide as much security as wired Internet connections. In fact, many "hotspots" - wireless networks in public areas like airports, hotels, internet cafes and restaurants - reduce their security settings so it is easier for individuals to access and use these wireless networks. This increases the possibility that someone may intercept your information. You may decide that accessing your online brokerage account through a wireless connection is not worth the security risk. If you use your own wireless network, make certain you secure the network with wireless encryption.

- **Check for Secure Web Sites.** When you access your brokerage account online, check to ensure that the log in page indicates that it is a secure site. The address of a secure Web site connection starts with "https" instead of just "http" and has a key or closed padlock in the status bar (which typically appears in the lower right-hand corner of your screen). When you click on the padlock, the security certificate should confirm the identity of the site you are visiting. In Microsoft Internet Explorer 7, look for the address bar to turn green.

- **Be Careful Downloading.** When you download a program or file from an unknown source, you risk loading malicious software programs on your computer. Download software only from sites you know. Be wary of free software because it can be accompanied by other software such as spyware. Do not install software unless you know what it is and what it does and do not click on links in pop-up windows. Using anti-spyware software helps protect you from such programs.

- **Don't Respond to Emails Requesting Personal Information.** Legitimate companies will not ask you to provide or verify sensitive information through email. If your financial institution actually needs personal information from you or your statement, call the company yourself - using the number in your files or on your statement, not the one the email provides! Do not respond to emails, such as "phishing" emails, seeking your password, PIN, or other personal information.

- **Read Your Statements.** Read all your monthly account statements (bank, brokerage, credit card, etc.) thoroughly as soon as they arrive to make sure that all transactions shown are ones that you actually made or authorized. Check to see whether all of the transactions that you thought you made appear as well. Be sure that your brokerage firm has current contact information for you, including your mailing address and email address. If you see a mistake on your statement or do not receive a statement, contact your financial institution or credit card issuer immediately and follow-up in writing, where necessary.

- **Secure Your Confidential Documents.** Keep all your financial documents in a secure place, and be careful how you dispose of any documents with financial or other confidential information. Shred documents that have confidential financial or identification information before throwing them away.

- **Safeguard Your Social Security Number.** Do not use your Social Security number as a username, password or PIN, and make sure that it does not appear on your printed checks. If your Social Security number appears on your driver's license, be sure to ask your state's Department of Motor Vehicles whether it can use an alternative number. Keep your Social Security card in a safe place and avoid carrying it with you. You should also be sure to safeguard the social security numbers of any dependents.

- **Do a Periodic "Identity Theft" Check.** Reviewing your credit report may alert you to inaccuracies and unauthorized activity. You can obtain a free credit report every 12 months from three different credit bureaus by contacting the Annual Credit Report Request Service at AnnualCreditReport.com. This is the only authorized online source for you to get a free credit report under federal law. Be aware that you will have to disclose your Social Security number to obtain this report.

What Should I Do If My Identity Has Been Compromised?

If you think that your personal information has been stolen, immediately contact your brokerage firm and other financial institutions, including credit card issuers, to notify them of the problem. You should also notify the credit bureaus to put a fraud alert on your file.

If you detect unauthorized transactions in or withdrawals from your brokerage account, ask the firm to investigate. Be aware that your firm will need time to determine what happened and may need your help in identifying family members or others who might have access to your account. In the meantime, be sure to change your username, password and PIN for the account.

Additional Resources

To obtain your free annual credit report:

- http://www.annualcreditreport.com

For more information on identity theft, including how to file a complaint:

- http://www.consumer.gov/idtheft

For more information on phishing, spyware, and other online threats:

- http://onguardonline.gov
- http://www.sec.gov/investor/pubs/phishing.htm

For more information on smart investing:

- http://www.finra.org/investor
- http://www.pathtoinvesting.org
- http://www.sec.gov/investor.shtml

SIFMA®
Securities Industry and Financial Markets Association

FINRA™
Financial Industry Regulatory Authority