Consumer Fraud Alert

Arbrook Realty Group, LLC (including its subsidiaries, "Arbrook Realty") knows you work hard for your money. That is why we want to provide you with some tips that may help you avoid being scammed.

Beware of Fraudulent E-Mails and Web Sites

"Phishing" is a rampant Internet scam that relies on "spoofed" e-mails, purportedly from well known firms, to lure individuals to fraudulent web sites that look and feel like the well known firm's web site. At such web sites, victims are asked to provide personal information about themselves, such as their name, address and credit card number. These fraudulent e-mails and web sites may also try to install malicious software on your computer that monitors your activities and sends sensitive personal information (your passwords, for example) to a remote location. With that information, criminals can commit identity theft, credit card fraud and other crimes.

You can protect yourself by following these best practices when using the Internet:

• *Be aware that e-mail is insecure and easy to forge. E-mail that appears to be from a friend or company you do business with may be fraudulent and designed to trick you into providing personal information about yourself or installing dangerous software.*
• *Do not respond to e-mails or pop-up messages that solicit your personal information: name, address, Social Security number, etc.*
• *Only access trusted web sites that you found other than by clicking on a web site address in an e-mail and then added to your browser's bookmarks. Otherwise, manually type the address into your browser and then bookmark it. When you receive an e-mail, rather than clicking on a web site address in the e-mail, which can bring you to a fraudulent site, use the bookmark to access that site.*

If you receive an e-mail claiming to come from Arbrook Realty or any of its affiliates that you are uncertain about, or which you believe to be fraudulent, please forward it to Roz@ArbrookRealty.com Arbrook Realty will investigate the e-mail and respond back to you.

Personal Computer Security Tips

No security practice is foolproof. You can, however, help protect yourself by following these best practices to secure your personal computer:

• *Install antivirus and anti-spyware software on your computer and make sure it is up to date with the most recent virus/spyware signatures.*
• *Make sure your computer is up to date with the most recent software patches. Patches are software updates that often address software vulnerabilities that phishing scams and viruses exploit.*
• *Install a firewall between your computer and the Internet. A firewall is software or hardware*

that acts as a buffer between your computer and the Internet that limits access to your computer and blocks communications from unauthorized sources.

Please contact the manufacturer of your computer for additional information and recommendations.

IMPORTANT NOTICE TO PROSPECTIVE HOMEBUYERS, HOMESELLERS, AND TENANTS REGARDING FRAUDULENT BANK WIRING INSTRUCTION SCHEMES

Recently, there have been increased reports across the nation of a theft scheme that involves hackers stealing email addresses and sending fraudulent wiring instructions to homebuyers, homesellers, and tenants. REALTORS®, lawyers, title agents and buyers could be affected. The criminal scheme has many variations and this notice is not intended to describe each situation. As an actual or prospective buyer or tenant, we want to alert you to the situation so that you can minimize the risk that you could be a victim.

We recommend that before you wire any funds to any party (including your own lawyer, real estate broker, agent or title agent whom you know to be involved in your transaction) that you personally call them to verify the wire instructions (you should confirm the ABA routing number or SWIFT code and the credit account number). You should call them at a number that you have obtained on your own (e.g., the sales contract, their website, etc.) and should not use the phone number that is contained in any email - even if the email appears to be from someone you know. A common aspect of the scheme involves the criminal hacking the sender's email (unbeknownst to them) and sending you an email that looks like other legitimate emails you have received from that party. The email contains the criminal's wire instructions and may contain the criminal's phone number and once your funds are wired by your bank to the criminal's account there may be no way to recover those funds.

PLEASE EXERCISE CAUTION BEFORE WIRING FUNDS TO ANY PARTY

This Important Notice is not intended to provide legal advice. You should consult with a lawyer if you have any questions.

Glossary of Terms

• ***Phishing:*** *Phishing attacks use "spoofed" e-mails and fraudulent web sites designed to fool recipients into divulging personal financial data such as credit card numbers, account usernames and passwords, Social Security numbers, etc. By hijacking the trusted brands of well-known banks, online retailers and credit card companies, phishers are able to convince up to 5% of recipients to respond to them.*

• ***Firewall:*** *A system designed to prevent unauthorized access to or from a private network. Firewalls can be implemented in both hardware and software, or a combination of both. Firewalls are frequently used to prevent unauthorized Internet users from accessing private networks connected to the Internet, especially intranets. All messages entering or leaving the intranet pass through the firewall, which examines each message and blocks those that do not*

meet the specified security criteria.

• ***Patch:*** *Also called a service patch, a fix to a program bug. A patch is an actual piece of object code that is inserted into (patched into) an executable program. Patches typically are available as downloads over the Internet.*

• ***Computer Virus:*** *A program or piece of code that is loaded onto your computer without your knowledge and runs against your wishes. Viruses can also replicate themselves. All computer viruses are manmade. A simple virus that can make a copy of itself over and over again is relatively easy to produce. Even such a simple virus is dangerous because it will quickly use all available memory and bring the system to a halt. An even more dangerous type of virus is one capable of transmitting itself across networks and bypassing security systems.*

• ***Antivirus Software:*** *A utility that searches a hard disk for viruses and removes any that are found. Most antivirus programs include an auto-update feature that enables the program to download profiles of new viruses so that it can check for the new viruses as soon as they are discovered.*

• ***Spoof:*** *To fool. In networking, the term is used to describe a variety of ways in which hardware and software can be fooled. IP spoofing, for example, involves trickery that makes a message appear as if it came from an authorized IP address (the numerical identifier for a computer).*

Most scams involve one or more of the following:

• *Inquiry from someone far away, often in another country.*

• *Western Union, Money Gram, cashier´s check, money order, shipping, escrow service, or a "guarantee."*

• *Inability or refusal to meet face-to-face before consummating transaction.*

Who should you notify about fraud or scam attempts?

• *FTC toll free hotline: 877-FTC-HELP (877-382-4357)*

• *FTC online complaint form (www.ftc.gov)*

• *Internet Fraud Complaint Center (www.ic3.gov)*

• *Non-emergency number for your local police department.*

• *The government agency in your country responsible for dealing with fraud*