SPILE, LEFF & GOOR, LLP
ATTORNEYS AT LAW

LOS ANGELES OFFICE

RIVERSIDE, SAN DIEGO & SAN BERNARDINO
41955 4th Street, Suite 310B
Temecula, CA 92590
Telephone (951) 699-0370

16501 VENTURA BLVD., SUITE 610
ENCINO, CALIFORNIA 91436-2072
Telephone (818) 784-6899 Facsimile (818) 784-0176 Email: counsel@spilelaw.com
www.spilelaw.com

Notice regarding Cyber Attacks

Instructions for the online or wire transfer of escrow deposits and down payments from buyers as well as seller proceeds to be disbursed from escrow have been known to be intercepted by hackers who alter them so that Buyer's or Seller's funds are actually wired to accounts controlled by criminals rather than the escrow company. Buyers and Sellers should exercise extreme caution in making electronic funds transfers, verifying that the organization they are transferring funds to is, in fact, the escrow company and that their own bank account information is not being exposed to third parties. The best way to accomplish this is to contact the escrow company by telephone and make sure to speak with the escrow officer in charge of the escrow in question. Buyers and Sellers should not respond to any disbursement instructions received via email, text, or mail. They should always check directly with the escrow officer in question to verify the current wiring information.

In addition, Buyers and Sellers and Brokers should refrain from placing sensitive personal and financial information in emails, texts or other correspondence subject to possible hacking by third parties. It is recommended that all such sensitive information be delivered by more secure means such as providing the information in person or by telephone directly with the escrow officer.

Landlords and Tenants are also advised to verify wiring instructions before wiring monies with regard to leases.

Brokers should have all Buyer and Sellers sign the CAR standalone form entitled Wire Fraud Advisory at the outset of all transactions.

Due to the increasing number of claims involving cyber attacks it is highly recommended that you consider obtaining a stand alone Cyber and Bond Policies. Many of the standard E & O policies exclude coverage for Cyber attacks and those that don't have very limited cyber coverage. Claims involving cyber attacks can be extremely large and very expensive to defend, and coverage for such situations is critical.

PROTECTING YOUR BUSINESS AND YOUR CLIENTS FROM CYBERFRAUD

LEGAL AFFAIRS DEPARTMENT

By 2019, cybercrime will cost businesses an estimated $2 trillion annually. Don't be a part of that statistic! Implement the following best practices to safeguard you, your clients, and your business from online criminals.

Best Business Practices: Develop and enforce formal policies for ensuring data security.

- ✓ Create, maintain and follow a comprehensive Data Security Program.*
- ✓ Create, maintain and follow a comprehensive Document Retention Policy.*
- ✓ Avoid storing clients' personally identifiable information for longer than absolutely necessary. When you no longer need it, destroy it.

Best Email Practices: Unsecure email accounts are open doors to cyber criminals. Follow these guidelines to help keep that door securely shut and locked tight.

- ✓ Whenever possible, avoid sending sensitive information via email.
- ✓ If you must send sensitive information via email, make sure to use encrypted email.
- ✓ Never trust contact information in unverified emails.
- ✓ If an email looks even slightly suspicious, do not click on any links in it, and do not reply to it.
- ✓ Clean out your email account regularly. You can always store important emails on your hard drive.
- ✓ Do not use free wifi to transact business.
- ✓ Avoid using free email accounts for business.
- ✓ Use strong passwords.
- ✓ Change your password regularly.

*** See NAR Data Security and Privacy Toolkit for guidance.** http://www.realtor.org/law-and-ethics/nars-data-security-and-privacy-toolkit

PROTECTING YOUR BUSINESS AND YOUR CLIENTS FROM CYBERFRAUD

LEGAL AFFAIRS DEPARTMENT

Best Transaction Practices: Real estate transactions require flurries of information between numerous parties. This makes for primetime opportunities for fraudsters. How do you secure your deal?

- ✓ From the very start of any transaction, *communicate and educate.* Get all parties to the transaction up to speed on fraud "red flags," and make sure everyone implements secure email practices.
- ✓ When wiring money, the person doing the wiring should pick up the telephone and call the intended recipient of the wired funds immediately prior to sending the funds in order to verify the wiring instructions.
- ✓ Remember to use only independently verified contact information.
- ✓ Stay paranoid. A few years back the director of the FBI almost got taken by an email banking scam. If it can happen to him, it can happen to us.

Best Damage Control Practices: It's happened. A breach of data, a successful scam, a hack. What to do?

- ✓ If a money wire has gone out, immediately contact the bank to try and stop the funds.
- ✓ Notify all affected or potentially affected parties. Many states have data breach notification laws.
- ✓ Change all of your passwords. If possible, change usernames as well.
- ✓ Talk to your attorney.
- ✓ Contact the police.
- ✓ Report the breach to the FBI Internet Crime Complaint Center: http://www.ic3.gov/default.aspx
- ✓ Report to your REALTOR® Associations.

CALIFORNIA ASSOCIATION OF REALTORS®

WIRE FRAUD ADVISORY

(C.A.R. Form WFA, 6/16)

Property Address: _____ ("Property").

WIRE FRAUD ADVISORY:

The ability to communicate and conduct business electronically is a convenience and reality in nearly all parts of our lives. At the same time, it has provided hackers and scammers new opportunities for their criminal activity. Many businesses have been victimized and the real business transaction is no exception.

While wiring funds is a welcome convenience, buyers and sellers need to exercise extreme caution. Emails attempting to induce fraudulent wire transfers have been received and have appeared to be legitimate. Reports indicate that some hackers have been able to intercept emailed wire transfer instructions, obtain account information and, by altering some of the data, redirect the funds to a different account. It also appears that some hackers were able to provide false phone numbers for verifying the wiring instructions. In those cases, the buyers called the number provided, to confirm the instructions, and then unwittingly authorized a transfer to somewhere other than escrow. Sellers have also had their sales proceeds taken through similar schemes.

ACCORDINGLY, BUYERS AND SELLERS ARE ADVISED:

1. **Obtain the phone number of the Escrow Officer at the beginning of the transaction.**
2. **DO NOT EVER WIRE FUNDS PRIOR TO CALLING YOUR ESCROW OFFICER TO CONFIRM WIRE INSTRUCTIONS. ONLY USE A PHONE NUMBER YOU WERE PROVIDED PREVIOUSLY. Do not use any different phone number included in the emailed wire transfer instructions.**
3. **Orally confirm the wire transfer instruction is legitimate and confirm the bank routing number, account numbers and other codes before taking steps to transfer the funds.**
4. **Avoid sending personal information in emails or texts. Provide such information in person or over the telephone directly to the Escrow Officer.**
5. **Take steps to secure the system you are using with your email account. These steps include creating strong passwords, using secure WiFi, and not using free services.**

If you believe you have received questionable or suspicious wire instructions, immediately notify your bank, the Escrow Holder and your real estate agent. The sources below, as well as others, can also provide information:

Federal Bureau of Investigation: https://www.fbi.gov/

National White Collar Crime Center: http://www.nw3c.org/

On Guard Online: https://www.onguardonline.gov/

By signing below, the undersigned acknowledge that each has read, understands and has received a copy of this Wire Fraud Advisory.

Buyer _____ Date _____

Buyer _____ Date _____

Seller _____ Date _____

Seller _____ Date _____

Published and Distributed by:
REAL ESTATE BUSINESS SERVICES, INC.
a subsidiary of the California Association of REALTORS®
525 South Virgil Avenue, Los Angeles, California 90020

Reviewed by _____

EQUAL HOUSING OPPORTUNITY