Wire Fraud Scams: How to Protect Your Buyer Clients

REBAC Connection

Jessica Edgerton, NAR Associate Counsel

NATIONAL ASSOCIATION of REALTORS®
Official Designation

ABR®

GOV GODWIN EMEFELE
<postmaster@cooky112.de>

URGENT NOTICE,

Is my pleasure to inform you that your deliveryman has arrived with your cash trunk boxes value $8.3 million dollars being your inheritance/ compensation payment?

Most importantly you are advised to send your full data to him, which include your Full Name, Current Residential Address, Direct Cell Number, and A copy of any identity card to verify that you are the right receiver to avoid mistakes and enable him deliver your cash consignment boxes to your house without any further delay.

CONGRATULATIONS.

MR.GODWIN EMEFELE,
EXECUTIVE GOVERNOR,
CENTRAL BANK OF NIGERIA

Best Email Practices

- Avoid sending sensitive information via email.
- Use encrypted email.
- Don’t open. Don’t click. Don’t reply.
- Clean out your email regularly.
- Use strong passwords.
- Change your password regularly.
- Do not do business over free wifi.
- Be aware that a free email service may have fewer protections in place than a business email account.

Best Business Practices

- Communicate and educate. Get all parties to the deal up to speed on fraud prevention.
- Call the intended recipient of wired funds immediately prior to sending the funds.
- Use an independently verified phone number.
- Implement technology security.
- Be paranoid.

Damage Control

- If money has been wired, call the banks immediately to stop funds.
- Contact all other parties to the transaction.
- Contact the police.
- Change all passwords.
- Report to FBI Internet Crime Complaint Center: http://www.fbi.gov/scams-safety/e-scams
- Report to REALTOR® Association(s).

Legal Exposure

- Negligence.
- Breach of fiduciary duty.
- Violations of state data security laws.
- Failure to maintain standards set forth in company security policy.
- FTC Action. (*FTC v. Wyndham Worldwide Corp.*, No. 14-3514 (3rd Cir. Aug. 24, 2015)).

Cyber Insurance?

- Cyber Insurance still in “wild west” territory.
- Don’t purchase without consulting specialist.
- Policies for small businesses are available.
- Policies may become outdated quickly in light of new threats so review often.
- As applicable, review coverage under NAR policy prior to purchase.

What to Watch For

Email Phishing still popular, but numbers going down. What's on the rise? Attacks via:

- Social media
- Mobile devices: Apps, SMS
- Compromised websites

…And what's next?

- Wearables
- Automobiles

Resources

http://www.realtor.org/videos/window-to-the-law-cyberscams-and-the-real-estate-professional

http://www.realtor.org/topics/data-privacy-and-security/resources

http://www.realtor.org/law-and-ethics/nars-data-security-and-privacy-toolkit

http://www.realtor.org/articles/request-to-redirect-funds-should-trigger-caution

http://www.realtor.org/topics/data-privacy-and-security

http://www.realtor.org/articles/internet-security-best-practice

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.