Security 1st Title

PROTECTING YOUR BUSINESS & CLIENTS FROM CYBERFRAUD

By 2019, cybercrime will cost consumers 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: Guidelines to help sensitive information safe.

- 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-andethics/nars-data-security-and-privacy-toolkit

BEST TRANSACTION PRACTICES: 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: 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.