**Cyber Security and Wire Fraud Policies and Procedures**

**This document is for informational purposes only.**

**Brokers may choose to implement some or all of the below policies and procedures as they see fit for their brokerage.**

**BROKERS SHOULD USE THE BELOW INFORMATION ONLY AFTER HAVING CONSULTED INSURANCE AND LEGAL PROFESIONALS.**

In order to protect yourself and your brokerage, the below provisions, which are not all-inclusive, are intended to assist Brokers in establishing office policies and procedures related to cyber security and wire fraud. These provisions are not a substitute for the retention of independent legal counsel. Brokers are strongly encouraged to seek the advice of an insurance professional regarding cyber fraud insurance coverage.

**Overview**

* Cyber security threats and wire fraud are on the rise. Criminals find creative ways to breach cyber security which could have negative results such as loss of monies, exposure of confidential information, identity theft, etc.
* The purpose of these policies is to outline the appropriate use of technology to safeguard business transaction files.

**Cyber Security**

1. Passwords
   1. Use strong passwords by making them unique and complex
   2. Regularly change passwords
   3. Do not use the same password for all accounts
2. Email Security
   1. Do not open any suspicious emails, click on any links, or open any attachments; delete these emails
   2. Clean out your email account on a regular basis
   3. Use encrypted emails when sending sensitive or confidential information
3. Wireless Use Security
   1. Use encrypted wireless for work matters
   2. Stay away from free / unsecured Wi-Fi (i.e., coffee shops, hotels, libraries, restaurants)
   3. Consider using a Virtual Private Network (VPN)
4. Use of Electronic Devices
   1. Lock your screen or log out when you walk away from your device to prevent unauthorized access
   2. Report stolen or lost devices
5. Software
   1. Antivirus and firewall software should be regularly monitored and updated
   2. Data should be backed up on several different platforms
6. Record Keeping/Disposal
   1. Shred any and all documents that contain personal information such as account numbers, driver’s license number, social security number, credit card, debit card numbers, etc.
7. Social Media
   1. Do not post transactional information on social media such as names and addresses as this information may be used by criminals
8. Other – Include any other items of importance

**Wire Fraud**

1. Client Discussions
   1. Discuss with your client your communication practices so the client knows what to expect and can exercise caution if contacted by a different means than previously discussed
   2. Provide a document to clients describing wire fraud risk
2. Transactional Wire Instructions
   1. Prior to wiring funds, advise your client to contact the intended recipient via a verified telephone number to confirm the wiring information is accurate
   2. Advise your client not to respond to any emails changing wire instructions by replying to that email or calling the number contained in the email
   3. Consider including in your email signature a warning about wire fraud
      * NAR suggests the following:

**IMPORTANT NOTICE:** Never trust wiring instructions sent via email. Cyber criminals are hacking email accounts and sending emails with fake wiring instructions. These emails are convincing and sophisticated. Always independently confirm wiring instructions in person or via a telephone call to a trusted and verified phone number. Never wire money without double-checking that the wiring instructions are correct.

1. Evaluate communications
   1. Thoroughly review emails, texts and other forms of communications for typos and suspicious links
   2. Do not click on links
   3. Only call trusted phone numbers
2. Other – Include any other items of importance

**Reporting Cyber Crime**

* If you become aware of a breach of data or wire fraud, you should:
  + Contact the sender of the funds so that they can contact their bank to try to stop the funds from being delivered
  + Notify your broker immediately
  + Notify all affected parties so that they may take appropriate action
  + Change all of your passwords and usernames
* Following a breach, you as the broker may want to:
  + Talk to an attorney as there may be notification laws
  + Contact the police
  + Report the breach to the FBI Internet Crime Complaint Center at <https://www.ic3.gov/default.aspx>
  + Report the breach to your REALTOR® Associations