Account Takeover Fraud -- Protect Your Clients' Information

Account takeover fraud occurs when a fraudster gains unauthorized access to an account, changes information such as log in credentials or personal information (i.e. address, telephone number, email, etc.), and then makes unauthorized transactions in that account. A common method fraudsters use to obtain another person's personal information is through a practice known as "phishing."

For example, a phishing e-mail might pose as an agent-support message from Microsoft that persuades the client to click a link to a fake website designed to "phish" for information. The client may be prompted to enter login credentials, which are then stolen by criminals who will have access to all the client's files and information.

As an agent serving the best interest of your clients, your diligence and awareness is crucial. Once a criminal has access to an account, they will quickly try and eliminate any Company contact with the true contract owner. From an agent's standpoint, being proactive is key to prevent account takeover fraud. The following are tips for prevention:

- Never use the same password for multiple accounts.
- Change your passwords frequently using a password manager.
- Don't click on links from suspicious emails as these could lead to phishing sites or download malware.
- Use a VPN, especially when connected to public wifi.
- Never provide login credentials (username and password) over email. Most IT departments or reputable companies will not ask you to provide this information.
- Exercise caution when opening email attachments. .Zip files are multiple documents combined into one folder. If you open an infected .Zip file, your device will be affected upon opening the attachment and can quickly spread to your network.
- Consult an IT or cybersecurity resource. These individuals can assist in advising on appropriate security measures.

Remember, one click could potentially grant access to all your clients' information. Don't give away your keys to the kingdom! If an e-mail appears to be of a suspicious nature, don't click on links or open any attachments.

For agent use only- not for use with the public