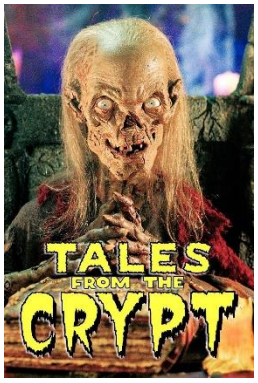

TALES FROM THE CRYPT – AGENT BEWARE!

By: Charles C. Whittington, Esq. and Amy S. Reinholdt, Realtor®, Broker Associate, ABR®, CIPS®, SRES®

If there is one thing everyone can agree upon, it is we are in the middle of an unprecedented market with record low inventory and a record number of buyers looking to purchase. The criminals know this and are seeking to take advantage of the situation at your expense and the expense of your customers. Many of you may have been the victim of cyber fraud or cybercrime, and others of you may be thinking it is only a matter of time. You've heard it before and you'll hear it again, vigilance, education and precautions are vital to protecting you and your customers.

Does the following sound familiar?

You receive a phone call from an international Seller (Canada or maybe Europe) who wants to have a piece of vacant land sold. The Seller asks you to please run the comps and let them know what you think of a listing price, and then once the price is set the Seller wants to get the property listed. Caller ID shows the name and location of the caller. Deed shows the home address (which matches the caller ID), all looks good. You are even excited because the Seller received your name from another customer. So far all is looking good. You review the comps and suggest a realistic list price, and send paperwork for review and electronic signatures. Then, suddenly, the Seller requests a price reduction before even giving the listing a chance at the very well-set price. The Seller also requests to use a closing company in another area well over 150 miles away because of the good experience the Seller's associate has had with them. In the course of your typical due diligence, you call the closing agent and all seemed normal. All the while photos are ordered, the sign is installed (all while the sinking feeling in your gut says something is not right). And of course, once the listing was live the calls started coming in. Not unexpected, the "Seller" accepted the first full price offer – again no surprise in this market. Sounds like a deal in this present market. Until . . . the phone rings, again caller ID showing the Seller's name and location but this time, it is the REAL Owner of the property who was surprised when he received a call from his neighbor because the sign in the front yard indicated that his property was for sale. Can you imagine the shock? Thankfully no money had yet been deposited! You immediately terminate the listing and sales contract, and, in this case, no one was hurt financially.

So how do you protect yourselves for this possibly happening to you? What procedures does your company have in place to ensure that the customer truly is the customer? Does your brokerage firm use a service to verify numbers, verify identity? Are you getting ID's, Passports, all previous sale documentation (survey, elevation certificate, title insurance policy, copies of trust paperwork or LLC operating agreements)?

Florida is seeing a very large increase in scams involving vacant land sales. These scams typically involve vacant land with no mortgage. Typically, the seller lives in a foreign country and wants to conduct all communications and the closing through electronic means (no personal contact or telephone calls). The seller (fraudster) may hold themselves out as the owner or may have forged a deed from the true owner to themselves. The seller will want to use a mail-away closing and not

come to the closing. If these scams are not uncovered and thwarted early in the process, thousands (if not hundreds of thousands) of dollars could be lost.

If you are asked to list vacant land, it is imperative that you undertake steps to verify that you are in communications with the true owner/seller of the subject property. This can include, but is not limited to, (a) independently finding contact information for the owner/seller to verify the contact information you received; (b) sending a letter to address where the property tax bills are sent; (c) set up a zoom (or similar) call with the owner/seller and not just communicate through emails; and (d) obtain copies of relevant backup documentation associated with the transaction (i.e. copies of seller identification, survey, elevation certificate, title insurance policy, copies of trust paperwork or LLC operating agreements).

Additionally, if you have customers who own vacant land, you may consider providing them with information on the property records monitoring services offered, free of charge, by the Clerks of Court for Collier County (https://app.collierclerk.com/recording/risk-alert-enrollment) and Lee County (https://or.leeclerk.org/LandMarkWeb/FraudAlert).

Another scam/crime that continues to affect, infiltrate and corrupt real estate transactions is business email compromise. This crime has resulted in the loss of billions of dollars and is becoming more sophisticated. The typical example is a fraudster sends a phishing email that requests the recipient click on a link. Once the recipient clicks on the link, the fraudster gains access, through a variety of means, to the recipient's computer and/or email account. Once into the recipient's email account, the fraudster will set up the ability to monitor the account and this allows the fraudster, in the case of real estate transactions, to know the details of the transaction and get involved with the wire transfers. Thereby diverting funds meant for the transaction.

There is no one-size fits all approach to protecting yourself from business email compromise scams. Technology plays a part through the use of appropriate email monitoring programs and use of secured email. Further, caution by the user in clicking on suspicious links or emails is vitally important. Additionally, use of strong passwords and updating them regularly helps in this area. It is important to check your email rules on a regular basis and before updating your password. In order to monitor compromised email accounts, fraudsters typically set up rules that will auto-forward emails to a designated account and then auto-delete any such auto-forwarded emails so the user has no idea what is occurring in the background. If you find you have such a rule affecting your email account, it is extremely important to immediately delete the rule and then immediately update your password.

If you or one of your customers has been the victim of a cybercrime, below is a non-exclusive list of resources available to victims.

https://www.fbi.gov/file-repository/cyber-incident-reporting-united-message-final.pdf/view

Secret Service Field Office:

- Miami – 305-863-5000
- Orlando – 407-648-6333
- Tampa – 813-228-2636

FBI Field Office:

- Tampa 813-253-1000; https://www.fbi.gov/contact-us/field-offices/tampa

Collier County Sheriff's Office – Financial Crimes Bureau

- 239-252-0069; https://www.colliersheriff.org/my-ccso/criminal-investigations-division/fraud-prevention-financial-crimes-bureau