REDUCING THE RISK OF REAL ESTATE WIRE FRAUD

Clareity Consulting

September 1, 2016

Updated November 29, 2016

Version 1.2

Contents

Background

Clareity Consulting has seen an ever-increasing rise in real estate wire fraud, involving both social engineering and hacking to get real estate professionals or consumers to wire money directly into a criminal's account. After having the increase in this type of activity brought to our attention in 2012, we took steps to address the problem. Clareity Consulting spread word of the issue through the brokerage and title community and asked NAR to spread the word through its communications channels. NAR did so, both directly to its members and to state and local associations, who also spread the word to their members. Still, we keep hearing reports of new cases. Last year, we saw articles being published about this issue both in the real estate and mainstream press such as the *Wall Street Journal* and *Washington Post*, threatening the reputation of all real estate professionals as a category. Yet, the problem persists and, anecdotally, awareness seems to remain low. Our industry must take action!

As part of its security audit practice, Clareity Consulting continues to find companies that do not have appropriate policies and procedures let alone appropriate technical countermeasures in place to help reduce the risk of real estate wire fraud. We believe business owners need concrete guidance on how to reduce their risk. That is why we are publishing this paper, which contains examples of what top companies around the country have done, as well as additional recommendations.

It is important to note that this type of fraud is not always the fault of any one party. Though real estate professionals – brokerages, title companies, and attorneys should take steps to improve security, many of these scams involve the criminal interacting directly with clients. Risk and the responsibility for mitigating that risk are shared by everyone.

A More Thorough Explanation of the Problem

NAR General Counsel Katie Johnson provided a summary of the problem recently on realtor.org:

> Hackers are gaining access to e-mail accounts through captured passwords, and they'll search inboxes for messages related to real estate transactions, Johnson said. Once they find a victim who's in the process of buying a home, they'll send a spoof e-mail that looks like it's from their agent, title representative, or attorney, and it will say there are "new" wiring instructions, which includes a fraudulent account. The home buyer will then unwittingly wire funds directly into the hacker's account, Johnson said. "Once they send it, the money is gone," she added. "Millions of dollars are lost on this."[1]

Following is an example of the type of email a consumer might see. In this case, the agent had an email address that incorporated the company domain, but the "from" was a Gmail address designed to make the recipient think it was legitimate correspondence.

```
From: [Agent Name] <[agent-name]@gmail.com>
Date: August 1, 2012 at 3:22:32 AM CDT
To: [CLIENT]
Subject: Urgent – regarding [Listing Address]
[First Name],
To move forward on [address] we need to have the money wired
immediately.
Once you wire [amount] to [wiring instructions] I will call you.
I am in a meeting and will not be available to talk until I call you
later.
[Agent's Email Signature – but using gmail.com and a phone number with
two digits transposed]
```

Following is another example of an email a consumer might see:

```
From: [Agent Name] <[agent-name]@[agent-company.com]>
Date: August 1, 2012 at 3:22:32 AM CDT
To: [CLIENT]
Subject: Time to Wire Funds
 [First Name] and [First Name],
Please wire the [amount] for [address] to [wiring instructions].
[Agent's Email Signature]
```

[1] http://realtormag.realtor.org/for-brokers/network/article/2016/05/threat-wire-fraud-real

In this case the hacker actually compromised the brokerage email system because the broker did not require encrypted connections to access email and did not enforce WPA2 encryption for wireless use[2]. As a result, the email looked legitimate because it was not "spoofed"[3] – it came directly from the broker's email server, from the agent's own account. The hacker then deleted the email from the "sent" folder so the agent wouldn't notice it, and monitored the agent's email account to answer any replies and delete them as well. Having the consumer look carefully at the email's "from" or "reply-to" information would have not helped in this case.

There are many other ways that hackers can involve themselves in communications.

There are many other ways that hackers can involve themselves in communications, including various ways of tricking the real estate professional into installing malicious software on their computer. As the paper will describe in more depth later, reducing wire fraud risk is just one aspect of a more comprehensive organizational information security program.

These are good illustrations of how many of the incidents start - but the problem is larger than that. There have been cases where instructions for escrow or other disbursements have been changed at the office of the real estate professional – and this occurs not only via email but by less sophisticated methods, including phone, fax, or even inter-office memo.

The Federal Trade Commission's description of the problem is better, but still focuses just on the most common aspect of the issue – email spoofing or hacking:

> Hackers have been breaking into some consumers' and real estate professionals' email accounts to get information about upcoming real estate transactions. After figuring out the closing dates, the hacker sends an email to the buyer, posing as the real estate professional or title company. The bogus email says there has been a last minute change to the wiring instructions, and tells the buyer to wire closing costs to a different account. But it's the scammer's account. If the buyer takes the bait, their bank account could be cleared out in a matter of minutes. Often, that's money the buyer will never see again.[4]

[2] There are many other steps needed to improve wireless security; lack of encryption just happened to be the particular issue in this case.
[3] "Spoofed" means that the sender's email address was forged. The email might seem to come from a legitimate account, but the email has not been sent through the legitimate account's email server.
[4] https://www.consumer.ftc.gov/blog/scammers-phish-mortgage-closing-costs

Following is an example of a spoofed *inter-office* email attempting to get an employee to change wiring information. Real names have been replaced with [items in brackets] to protect the privacy of those providing examples for this paper:

```
From: [Broker Name] <[Broker Name]@gmx.com>
Subject: [Listing Address]
To: [Internal Brokerage Employee Email]
Seller wants proceeds wired to their trading account how can you help
with this?
```

In that example, "gmx.com" is a site that provides email hosting – the criminal uses this to send the bogus email and correspond with brokerage employees.

A similar example:

```
From: [Brokerage Employee Name] <admin@private-use.org>
To: [Employee Name] <[Employee Email]>
Subject: Wire Request
[First Name],
I have an outgoing wire transfer request for a vendor payment. can you
handle this today? Kindly advice.
```

Sometimes the email address looks correct on first glance, but the "reply-to", which isn't displayed in most email programs, is from Gmail or similar email hosting company:

```
From: "[Broker Name]" <[Broker's Actual Email Address]>
To: [Internal Brokerage Employee Email]
Subject: DETAILS
Reply-To: "[Broker Name]" <[REDACTED]@gmail.com>
Hello,
Please i need you to do a quick wire transfer to a local bank for me.
Get back at me with the info's you need to do the wire transfer.
Thanks
Sent from my iPhone
```

The email exchange can even start off more innocently:

```
From: [Broker Name] <[Broker Name]@gmail.com>
To: [Internal Brokerage Employee Email]
Subject: Wire Transfer
[First Name], are you at the office?
```

Because this issue is *not* only about the consumer receiving bogus wiring instructions but also about wiring decisions made inside the real estate office, it's not only necessary to educate the consumer regarding the procedures for how wiring information is set or changed, but also to set policies and procedures inside the business to ensure anyone who may possibly affect wiring information understands how wiring instructions are established or changed. A sample policy will be provided later in this paper.

It's not only necessary to educate the consumer regarding the procedures for how wiring information is set or changed, but also to set policies and procedures inside the business.

There's a newer, sophisticated variant of the wire fraud scam that has only recently emerged. Following is the process that it follows, though as with other processes there is a high degree of variation:

1. A hacker obtains a Realtor's transaction management / eSignature system login credentials by using a phishing email that looks like it comes from the transaction management system.
    a. The user first types their credentials into the fake transaction management website, then are forwarded to the real one where their credentials work. They never even notice they've been phished, thinking they just mistyped a password the first time.
2. The hacker logs into the transaction system to identify target transactions and collect information to use to fool participants going forward.
3. If the agent has used the same credentials for both email and transaction system, they re-use credentials to access the agent's email.
    a. The hacker may set up an email filtering rule so emails from the client to 'skip the inbox' and forward emails from that client to themselves.
    b. Emails to clients can be sent from the agent's real email address – it's not a spoofed email.
    c. Changing email password at this point means that the hacker may need to spoof further emails – but unless the agent notices the filtering rule, the hacker still has access to client emails to the agent.
4. Because the hacker has information about the mortgage and title company from the transaction system, they can spoof an email from those parties to the client. When a client receives (spoofed) email from multiple parties that confirm each other's message, they are more likely to trust each of those emails – even if they are all bogus.
5. From that point it's a typical wire fraud scenario: at the appropriate time the client is told to wire funds to an account the hacker has access to.

Countermeasures for Consumers

Put consumers on notice early in the process. Educational materials should be included with contracts, in buyer handouts, and with closing instructions. Ideally, this should be a separate page that the client signs.

Following is an example that one broker puts in *all* **Buyer Agency Contracts** and **Listing Contracts**:

> **Anti-Fraud Disclosure Statement**
> Electronic communications such as email, text messages and social media messaging, are neither secure nor confidential. While [Brokerage] has adopted policies and procedures to aid in avoiding fraud, even the best security protections can still be bypassed by unauthorized parties. [Brokerage] will never send you any electronic communication with instructions to transfer funds or to provide nonpublic personal information, such as credit card or debit numbers or bank account and/or routing numbers.
>
> YOU SHOULD NEVER TRANSMIT NONPUBLIC PERSONAL INFORMATION, SUCH AS CREDIT OR DEBIT CARD NUMBERS OR BANK ACCOUNT OR ROUTING NUMBERS, BY EMAIL OR OTHER UNSECURED ELECTRONIC COMMUNICATION. EMAILS ATTEMPTING TO INDUCE FRAUDULENT WIRE TRANSFERS ARE COMMON AND MAY APPEAR TO COME FROM A TRUSTED SOURCE.
>
> If you receive any electronic communication directing you to transfer funds or provide nonpublic personal information, EVEN IF THAT ELECTRONIC COMMUNICATION APPEARS TO BE FROM [Brokerage], do not respond to it and immediately contact [Brokerage]. Such requests are likely part of a scheme to defraud you by stealing funds from you or using your identity to commit a crime.
>
> To notify [Brokerage] of suspected fraud related to your real estate transaction, contact: fraud@[Brokerage].com or [Phone Number].

Following is another company's disclosure, provided with their **contract package**:

Warning

Please be aware that there are numerous email, fax, text, and social media messenger scams involving wiring funds in conjunction with a real estate transaction. These scams involve authentic –looking, yet fake, emails to request information or direct users to a fake website (or a criminal's email) that requests information. Please note that [Company] will not send instructions to wire funds via email, fax, text, or social media message. [Company]'s affiliated licensees have been cautioned concerning computer hackers and will most likely not attempt to send you any wiring instructions of any kind via electronic means either.

Buyers, if you have received wiring instructions purporting to be from a settlement/title company, lender, attorney, or other entity, please verify the authenticity of the wiring instructions by at least one other independent means (i.e. telephone or personal visit to the office) prior to initiating any transfer of funds. ***Be especially aware of any change requests subsequent to the original wiring/money transfer information.***

Sellers, [Company] recommends that if you send wiring instructions of any kind (such as for the receipt of your proceeds from the transaction) via email or any electronic means to anyone, that you verify that the correct instructions were received by a known representative of the intended recipient. Also, it is important to confirm with the intended recipient that the wire instructions are not to be substituted without your verbal consent.

When wiring funds, never rely exclusively on an email, fax, text, or social media message communication.

IMMEDIATELY notify your banking institution if you are a victim of wire fraud.
If you believe you have received fraudulent wiring instructions, please notify wirefraud@[company].com.

Buyer or Seller	Buyer or Seller
Date	Date

Following is another broker's disclosure, provided early in the process to buyers:

WIRE FRAUD WARNING

Criminals engaged in identity theft and wire fraud frequently target the email accounts of parties involved in real estate transactions (e.g., lawyers, title agents, mortgage brokers, real estate agents), since these communications can be a source of highly sensitive, personally identifiable information. Among other strategies, these criminals have been known to provide instructions on making payments via wire transfer, causing consumers unknowingly to divert funds to the criminals' bank account. These emails may masquerade as legitimate communication from the proper party, but they are a fraud designed to enable theft.

[Company] strongly recommends that you, your lawyers and other professionals working on

<u>your transaction, refrain from placing any sensitive personal and/or financial information in an email, directly or through an email attachment.</u> When you need to share Social Security numbers, bank accounts, credit card numbers, wiring instructions or similar sensitive information, **use more secure means** such as providing the information in person, over the phone, or through secure mail or package services. In addition, **before you wire funds to any party** (including your lawyer, title agent, mortgage broker, or real estate agent) **personally call them to confirm that the transaction is legitimate** (i.e., confirm the ABA routing number or SWIFT code and credit account number). Call them at a number that you have obtained on your own (e.g., from the sales contract, their website, etc.) to confirm that you are contacting the intended party; do **not** use the phone number provided in the email.

Client/Customer Name _____ Date _____

Following is the text from a **buyer handout** provided by a title company:

Buyer Beware: Wire Fraud & Steps to Prevent It!

FBI officials warn of a dramatic rise in business e-mail compromise (BEC) and has seen a 270% increase in victims since January 2015. (fbi.gov) The scenario we all want to avoid is the one where the buyer's funds in a trans-action do not transfer to the rightful seller, and are unrecoverable.

According to the CIO for a national title insurance underwriter, one of the key indications of any wire fraud scam is the sense of urgency. It comes as an email that appears to be urgent, coming from someone of authority to the person who is responsible for wiring funds within the organization.

Fraudsters are getting more and more creative in their schemes. Recently, a bank's email was hacked and a fraudulent new mortgage payoff for a seller was sent to the title company with new information of where their pay-off should be wired. Luckily, this scheme was caught and thwarted.

Fraudsters are able to follow transactions in online listing sites and public records, or target Realtors and title companies to observe multiple transactions. This gives access to all parties in the transaction. The fraudster then waits patiently for a closing date to make his move…..change wiring instructions. Buyers should only receive wire instructions from a title company in a secure format (encrypted).

3 Steps to Prevent Falling Victim to Wire Fraud

1. Never accept wire instructions in a format other than secure/encrypted.
2. Always call Capital Title to confirm the wire instructions you received.
3. Wire Instructions will generally never change. If you receive an email stating wire instructions have changed, BEWARE!

Reference:

FBI Warns of Dramatic Increase in Business E-mail Scams. April 4, 2016; www.fbi.gov/phoenix/press-releases/2016/fbi-warns-of-dramatic-increase-in-business-e-mail-scams

Common Elements of a Suspicious Email

- Incorrect Grammar/Spelling/Text Body
- Email Format/Absence of Com-pany Logos/Plain Text Email
- Urgent Request for Personal Information
- Suspicious Attachments
- Links in the Email

Protect Yourself Online

- Don't use the same password more than once. This way, if your password is compromised on one website, fraudsters can't use it elsewhere.
- Always use second-factor authentication to sign in to your online email account.
- Don't use work email for personal business

Following is an example provided by another brokerage's affiliated title company as part of their **closing instructions**:

IMPORTANT NOTICE REGARDING WIRE TRANSFER INSTRUCTIONS FOR CLOSING FUNDS WITH [COMPANY] TITLE (NOT EARNEST MONEY)

DO NOT WIRE ANY CLOSING FUNDS UNTIL YOU HAVE CONFIRMED THE WIRE INSTRUCTIONS DIRECTLY WITH [COMPANY] TITLE SERVICES. THERE HAVE BEEN INSTANCES OF WIRE FRAUD, SO PLEASE NOTE THAT OUR BANK IS [BANK NAME], AND THE NAME ON OUR ACCOUNT IS [COMPANY] TITLE SERVICES AND THAT INFORMATION WILL NOT CHANGE. YOU SHOULD NOT WIRE ANY FUNDS, IF DIRECTED TO ANY OTHER BANK OR ANY OTHER ACCOUNT NAME. IF YOU RECEIVE AN EMAIL DIRECTING YOU TO WIRE TO ANY OTHER BANK OR ACCOUNT NAME, DO NOT RESPOND AND REPORT IT IMMEDIATELY TO [COMPANY] TITLE SERVICES. WIRE INSTRUCTIONS FOR EARNEST MONEY DEPOSITS SHOULD BE OBTAINED FROM THE [COMPANY] RESIDENTIAL SALES BRANCH OFFICE.

The California Association of Realtors® has released its own disclosure form:
http://www.car.org/media/pdf/legal/standard-forms/1020308/

Ongoing Notices

Professionals can continue to remind clients about the risk, especially during later phases of the transaction, by putting notices in their e-mail signature. Following are some examples to consider.

A sample notice from Realtor.org:

> **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.

From a brokerage:

> **CAUTION: Online banking fraud and cybercrime is on the rise. If you receive an email containing WIRE TRANSFER INSTRUCTIONS requesting personal/financial information or asking you to download, send, and/or do anything that may seem unusual to you, call your real estate agent or escrow officer immediately prior to acting on the suspicious email in order to verify the validity of the email. Please be diligent and exercise caution, especially when funds or financial information are involved. Phishing and other suspicious activity should be reported to the Federal Trade Commission.**

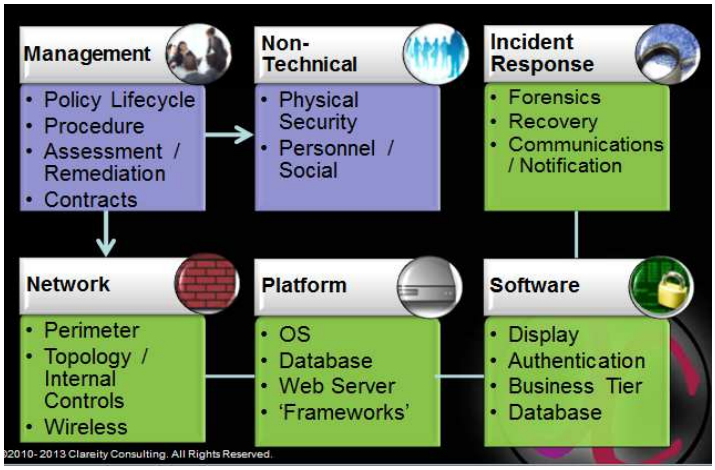
From a title company:

> *ALL funds to close exceeding $25,000.00 MUST BE WIRED to us for closing.*
> *Excess EMD over $5,000.00 MUST BE WIRED to us for closing.*
> **Customer wire instructions may only be presented in person to our closer with proper identification or returned with our package on mail away closings. Any change to initial request must otherwise be in person at our offices with proper ID. **

Using the preceding examples and adapting them to your own business process, craft a standard notice for your organization to use and, as will be later described, make it a policy to use that notice in the appropriate communications.

Countermeasures for Professionals

When most people think "information security" they automatically translate that to "computer security." This is where most security efforts go wrong – it's up to the business owner to take those first steps including assessment (security auditing) and risk remediation management, implementing policies and procedures, including information security in contracts, addressing physical security, and implementing appropriate personnel practices. Technical failures usually start as management failures.



Procedure Examples

Following is an example of a wiring procedure from one title company's employee handbook:

Disbursement or Receipt of Funds By Wire:

Purpose:

Wire transfer transactions usually involve large dollar amounts that must be processed quickly. There is also finality to a wire transfer transaction at the time of execution. Generally, wire transfers are not subject to a stop payment, recall, cancellation or adjustment; once a wire request has been executed the funds immediately become the property of the transfer recipient. Because of these concerns and to minimize the risk of loss from errors or fraud, wire transfer authority is to be centralized within a limited number of management, accounting or administration employees.

Procedure:

- No employee shall be unilaterally authorized to issue or accept a wire transfer.
- Customers are to communicate all wire transfer requests in writing and each closing attorney will then communicate the wire transfer information to one of the authorized employees in writing *or by fax* and confirmed in writing.
- In all cases of initiation of a wire transfer by a closing attorney or other authorized party, a reasonable security procedure must be used to validate the transfer.

Another company has initiated the following procedure, paraphrased here:

We require a specific signed wire request form and have also implemented a verbal password. If we receive wiring instructions from an owner or officer we call them and they must provide the verbal password in order for us to process the wire transfer. This provides confirmation that they are the actual requestor. Our wire process also requires 3 people: an initiator, a reviewer and an approver.

Company Policy Sample

Following is an example of the type of policy a company may wish to put in place to address wire fraud. Note that it needs to be tailored to the way a particular company operates – it is not meant for 'cut and paste' use with no adaptation, and it references various additional policies that would be put in place as part of a larger organizational information security program. Clareity Consulting grants readers permission to use and adapt this policy. Note that policies and contracts should only be implemented in consultation with a qualified attorney.

Wire Fraud Prevention Policy

1. Overview

It is essential that procedures are in place to prevent a hacker from tricking someone into wiring money to the wrong party.

2. Purpose

The Wire Fraud Prevention Policy describes required actions on the part of employees and contractors that will help ensure that money is wired only to the appropriate party during the real estate transaction. This includes procedures for raising awareness of the issue and methods to help ensure secure communications.

3. Scope

This policy applies to all employees and contractors that interact in any way with wiring instructions and communications internally and with clients. This includes temporary contractors and part-time employees.

4. Policy

4.1. Agents will provide the “Wire Fraud Warning” document with all buyer agency contracts and listing contracts and obtain client signature(s) on that document when other contracts are signed. This document must be submitted to the brokerage with those other contracts.

4.2. Title company staff will provide every new buyer with the “Wire Fraud” handout at the first opportunity, via email or in-person.

4.3. If communication with clients is via e-mail or other messaging service that allows for a "signature", the “Wire Fraud Signature” must be included in the signature, in close proximity to the rest of the message, in a font no smaller than the median size used in the email and of no lesser contrast. The “Wire Fraud Signature” is as follows:

IMPORTANT NOTICE: Online banking fraud and cybercrime is on the rise. Never trust wiring instructions or a request for other personal/financial information 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 (*not* the phone number that may be in the email you are concerned about). Never wire money without double-checking that the wiring instructions are correct.

4.4. You must configure your work email as instructed by the brokerage:
- Using a strong password, used only for this email account and not shared with others. The password and your activities around it must comply with the company's **Password Policy**.
- Using **encryption** (SSL or TLS) for the email connection. Please speak with [role] if you need help configuring your email client to meet this requirement.
- Using caution with regard to email attachments, as per the company's "**Email Policy**".

4.5. If the company has approved a Transaction Management system for all client communications related to the closing process, no other form of communication (other than telephone voice calling) should be used to communicate financial matters with clients.

4.6. If you use WiFi for work purposes, you must always use **WiFi encrypted using WPA2**. If you are unsure about the encryption level of your WiFi, you may not use it. See the company's **Wireless Security Policy**.

4.7. If you use a personal computer, tablet, phone, or other mobile device for business purposes, it must be compliant with the company's **"Bring Your Own Device (BYOD) Policy"**. This includes, but is not limited to, using and securing a unique, appropriately strong password for the device as per the company's **"Password Policy"**, setting the device lock timer, using anti-virus software, and using disk encryption.

4.8. Work computers configured by the company will be configured according to the "**Workstation Configuration Policy**". Employees are forbidden from attempting to bypass any aspect of workstation security.

4.9. Use extreme caution with regard to any request to establish or change wiring instructions not made through the following procedure:

1. Initiator provides wire transfer request form via [method].
2. The reviewer calls [role(s)] and they provide the verbal password to proceed. The reviewer signs off that they have received the verbal password on the wire transfer request form.
3. If the request is **invalid** (no password given), forward the request (email, voicemail, text message, etc.) to [role] for investigation and so they can attempt to block further attempts.
4. If the request is **valid** (password provided), forward the relevant documents to [role] who will file the request form and execute on the instructions.

Always obtain verbal confirmation via a phone number found via the company's phone directory – not by a number found any other way, especially not one provided in a form of communication such as email that might be suspect. Change of wiring instructions for seller proceeds [over $xx,xxx] must be made in person with proper seller ID.

4.10. In the event that you believe wiring instructions may have been compromised, inform the [role] immediately using every communications method possible, and they will take appropriate steps.

5. Policy Compliance

5.1 Compliance Measurement

The company will verify compliance to this policy through various methods, including but not limited to review of client communications, audit of computers and mobile devices and periodic drills including social engineering.

5.2 Exceptions

Any exception to any aspect of this policy must be approved by [name / role] in writing, in advance.

5.3 Non-Compliance

An employee or contractor found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

6. Related Standards, Policies and Processes

- Audit Policy
- Wireless Security Policy
- Workstation Configuration Policy
- Email Policy
- BYOD Policy
- Password Policy

7. Definitions and Terms

Encryption. The process of encoding a message or file so that it can only be read only by authorized parties. Examples include using TLS encryption to access websites via "https://", using the encryption setting on a computer or mobile device so only someone who logs in can read the files in storage, and using the encryption setting in an email program so that email login credentials and messages cannot be easily intercepted by a hacker.

8. Revision History

Date of Change	Responsible Party	Summary of Change

You can using the preceding policy example and adapt it to your own business processes. Note that this policy refers to a number of other policies or policy sections which provide stronger security practices, and which all companies that deal with financial information should employ. You may also wish to incorporate your final policies by reference in relevant contracts for non-employees.

Communications inside the Company

Internal communications is critical to improving awareness and decreasing risk. Education regarding risks and related procedures should be engaged in at least monthly. As an example, following is an email Coldwell Banker's CEO sent to brokers[5], raising awareness from the highest level:

DEAR COLDWELL BANKER® BROKER/OWNER,

Earlier this year, we communicated to you about wire fraud scams affecting real estate brokers, their agents and their customers. **Given the ongoing risks of wire fraud and email hacking, we wanted to reiterate the alert to our franchise network about this scam so that you can take measures to protect your company, independent agents and their clients.**

We strongly recommend that real estate agents, their clients and all those in communication about a home sale/purchase transaction (e.g., attorneys, mortgage brokers, title/escrow agents) avoid transmitting sensitive financial or personal information in an email, either directly or through an email attachment. If you need to send or request sensitive information such as Social Security numbers, bank accounts, credit card numbers or wiring instructions, you should only provide the information in person, by telephone, overnight mail or secure fax. As a reminder, the following precautions should be taken related to bank wire transfers:

[5] Thanks to Budge Huskey who allowed Clareity Consulting to re-print this email with attribution.

- **ALWAYS PERSONALLY VERIFY** wire instructions by calling the party who sent the instructions. Use only phone numbers that you have called before or can otherwise verify. Do not use the number provided in the sender's email. The hacker may have inserted a fraudulent telephone number in the email. Do not send an email to verify instructions because the sender's listed email address may be false or a hacker may intercept your email to the sender.
- **VERBALLY ASK** the party who sent the instructions to confirm the ABA routing number or SWIFT code and the credit account number. Because a hacker may have altered the attachment containing the wire instructions, simply asking the sender whether wire instructions were sent is not sufficient.
- **DO NOT AGREE** to requests to forward wire instructions to other parties (or their brokers) unless you have personally, verbally confirmed the instructions.
- **BE VERY SUSPICIOUS** of emails with purportedly updated, revised, or corrected wiring instructions. It is extremely rare that a title agent will change wire instructions during the course of a transaction.
- **MAKE SURE** you are not sending or requesting sensitive financial information in emails (e.g., Social Security numbers, bank accounts, credit card numbers, wiring instructions). Also, make sure to use strong passwords (e.g., 8 characters including both letters and numbers and nothing obvious) and frequently change your passwords.
- **DON'T** open attachments or click on links from unfamiliar sources because they could contain malware or be a phishing scheme, which once opened could allow a hacker the same access that you have to your computer and accounts.
- **CONSIDER** updating your company's disclosures and warnings to customers regarding these scams.

For more information on wire-fraud scams or to report an incident, please refer to the following links:

Federal Bureau of Investigation: http://www.fbi.gov
Internet Crime Complaint Center: http://www.ic3.gov
National White Collar Crime Center: http://www.nw3c.org
On Guard Online: http://www.onguardonline.gov

Sincerely,

Budge Huskey
President & CEO
Coldwell Banker Real Estate

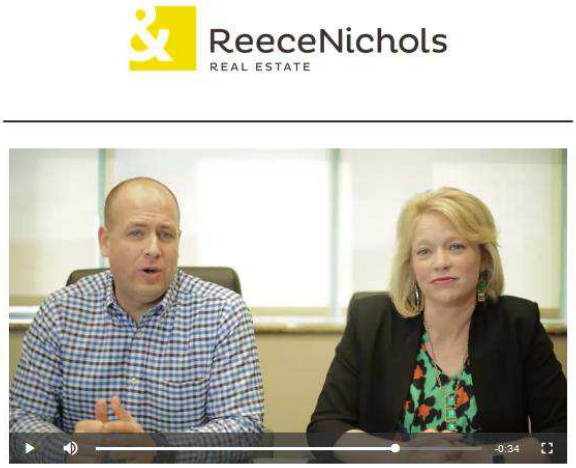
This Important Notice is not intended to provide legal advice. You should consult with a lawyer if you have any questions.

Following is an example letter sent to staff by a brokerage CFO to help raise awareness of the wire fraud problem and provide guidance on how to lower the risk:

> You've read a lot about hacking (stolen passwords, key-loggers, etc.) and while this is a concern it is not the most common driver of successful larceny. The most insidious form is "social engineering" where someone fraudulently poses as a familiar person and gets you to take action.
>
> Anyone can create an email account as below and put in a name that will command action and urgency – often the CEO's name is used. There are many, many telltale signs that these are not genuine.
>
> For example…
>
> 1) Look at the "From". The actual senders e-mail address is wrong. We all know [CEO]'s company email address. This is the #1 thing to look for – but there are ways from some email clients that it can look real.
>
> 2) [CEO]'s mobile sign off is incorrect and different than what we all normally see from [CEO]. It also omits the company name he is CEO for.
>
> 3) Finally…his e-mail within his reference information spells his name wrong.
>
> All wires can only be sent using a multi-layered and at least three-person approval process for security. I won't share the security protocol details lest we compromise security but please know we have many gates.
>
> Please continue to be vigilant. When you get this type of email, please share this with IT so that e-mail addresses can be blocked.
>
> …
>
> [Employee] is implementing recommendations to create and even more secure IT/communications environment as we implement opportunities identified during our recent risk audit.
>
> Thanks!

Video Training

ReeceNichols circulated this video (https://tinyurl.com/rn-fraud**)** to their agents over a period of 30-45 days – this was in addition to in-office training and discussions. This is a great way to help train employees and contractors about the issue and what risk mitigation steps were expected, including implementing new controls and providing a reporting method for detected attempts at wire fraud.



Compliance Monitoring

Implementing policy and procedure involves not only employee and contractor education, but compliance monitoring and enforcement. One company had their IT department create fake phishing scam emails (similar to the examples provided earlier in this paper) that are sent periodically to employees and agents of the brokerage and title company that mirror real phishing scams. If the employee or agent clicks on the link or attachment contained in the fake email, it directs them to some training materials that re-emphasizes the need to be diligent about this type of fraud. In addition, the broker receives reports on which people clicked on the links or attachments so they can better target future training.

In the Event of an Incident

While there are many steps you can take to reduce risks, there is no such thing as perfect security. If a wire fraud incident should occur, immediately contact the banks involved and let them know what has happened. Then talk to your attorney. Your attorney should understand all relevant laws and may help you craft notifications to anyone that may have been affected by the breach, as well as interact with others, such as your insurance company. Depending on your state and the state of those individuals affected by the breach, you may have to notify the attorney general and take other steps – again, your attorney can help guide you through the various state laws. Finally, inform law enforcement including, if the breach is "cyber", the FBI Internet Crime Complaint Center (http://www.ic3.gov/).

Conclusions –The Next Level

If companies in our industry follow the preceding advice consistently, the risk of real estate wire fraud can be decreased. However, the largest problem facing our industry with regard to addressing wire fraud risk – at least at the present time - is that the industry generally uses a variety of insecure tools for communication with clients, especially email and other messaging platforms. Brokerages and title companies may improve their own information security practices, but **unless the entirety of closing-related communications moves to more secure channels – for example, a more secure transaction management System with strong authentication – we will continue to have information security challenges around the closing**. Also, **addressing wire fraud is just one aspect of a more comprehensive organizational information security practice**.

Clareity Consulting hopes that companies in our industry will use both the preceding examples from franchises, brokerages and title companies, along with the draft company policy we have provided - using them to evaluate the steps they have already taken and considering how they can further reduce the risk of wire fraud for their clients.

For more information regarding Clareity Consulting's Security Assessment services, please contact Matt Cohen (matt.cohen@clareity.com).

About Clareity Consulting

Clareity Consulting brings clients fresh insights and wide perspective gained by serving clients throughout the industry: associations and MLSs, brokerages, franchises, technology vendors, and others. Clareity's services include:

STRATEGIC AND BUSINESS PLANNING

Clareity provides strategic, governance, and product/service business planning that bridges the gaps between strategy, tactics, and the timely activities needed to support your goals. Clareity also facilitates MLS regionalization and data shares.

SYSTEM SELECTION

From needs assessment and RFP to contract negotiation, for MLS, TMS, Public Records, and other offerings, Clareity's structured processes help your organization make a good business decision with stakeholder involvement.

PUBLIC SPEAKING

Clareity can address leadership or large groups on timely topics in an informative and fun way. Popular topics include MLS trends and system options, information security, and real estate technology trends, such as cloud computing and mobile technologies.

COMPLIANCE AND RISK AUDITS

Providing information security, risk management and business resumption planning, staffing and salary reviews, and VOW / IDX compliance audits, Clareity brings both an independent view and finely-honed technical skills.

PRODUCT / SERVICE / SOFTWARE REVIEW

Clareity performs customer surveys and market research, develops product strategies and specifications, performs usability and quality assurance, audits security, and facilitates user groups. Clareity also facilitates strategic alliances, mergers, and acquisitions.

RECRUITING

Your business is only as successful as your leaders and employees, and Clareity has discreetly helped recruit some of the brightest minds in our industry for their current positions, both executive and technical.

WEBSITE PLANNING AND REVIEW

Clareity helps improve website design, usability, and content, accounting for key factors such as SEO and mobile experience. Clareity also creates specifications and helps clients select the best partners to produce, and provide compelling content for, their web applications.

EXPERT WITNESS

Whether it's a matter of the policies and practice of organized real estate or a more technical software dispute, Clareity can provide an expert witness with integrity and experience to conduct research, write expert opinions, and provide depositions and testimony.

For more information, please contact:

Gregg Larson
480-368-8100
Gregg.Larson@clareity.com

Matt Cohen
612-331-1788
Matt.Cohen@clareity.com

Or visit: http://clareity.com