TITLE RESOURCES

Wire Fraud Prevention

Annette Aviles-Natal

VP-Florida Agency Representative

Our mission is to provide knowledgeable and responsive underwriting solutions to support our network of title insurance agents across America. Title Resources is dedicated to growing lifelong relationships and maintaining quality through integrity and financial stability.

Wire Fraud

Wire fraud happens.

You just don't want it to happen to you!

- How many of you have seen *attempted* or *successful* wire fraud?

Wire Fraud is on the Rise

Cyber fraud rose over 480% between 2015 and 2016

Wire fraud losses annually between $30 and $50 BILLION

Wire Fraud

Often wire fraud results from human behavior –

- Curiosity
- Desire to help
- Desire to please
- Human error

Social Engineering

Just how easy is it to get hacked?

YouTube video “Real Future: What Happens When You Dare Expert Hackers to Hack You (Episode 8)”

https://youtu.be/bjYhmX_OUQQ?t=1m24s

1:25 – 6:09

Wire Fraud Can Begin…

…with access to computers, laptops, computer networks *AND MOBILE DEVICES*.

Quicker, easier, better…?

In the past 20 years, the internet and computer technology have transformed how we do business –

- From in-person closings and telephone communication to relying on e-mail
- From issuing checks and deposit slips to funding and disbursing by wire
- Escrow has become speedier, more efficient, convenient, hassle free.

All good things!

But there is a trade-off

Criminals also have access to the internet and to our devices

if we aren't careful

Wire Fraud

Can start with phishing tactics –

- Clicking on a link in an e-mail from a friend (secure format)
- Clicking on a link in a news article (msn.com)
- Clicking on a .jpg file to open a photo
  - *Whose system was hacked?*

Wire Fraud # 1 – Buyer's Funds

- Buyer receives opening package with wire instructions
- Next day Buyer receives new wire instructions by e-mail
- Buyer calls – Why did we send him new wire instructions?
- Closer says – Didn't. Instructions in opening package / only instructions sent
- Buyer says – I just sent my $54K to your Texas bank yesterday!

Wire Fraud # 1 – Buyer's Funds

- What happened?
- Buyer received spoofed e-mail, claiming to be the Realtor
- Spoofed e-mail had red flags - buyer should have called to see if e-mail was real
- Funds never recovered
- NO title CLAIM!
- Buyer wired funds from another account

Wire Fraud # 2 – Seller Proceeds

- Closer receives email day of closing from Seller/Realtor (“S/R”) with new wire instructions
- Closer replies “need new wire instructions signed by her and her husband”
- New wire instructions received – initials match
- Closer calls S/R to talk about something else, but shares “received new wire instructions”
- S/R says “What?!”

Wire Fraud # 2 – Seller Proceeds

- S/R came straight to the escrow office
- While S/R sitting at the Closer's desk, Closer received email from S/R asking if the money has been wired
- S/R's email account had been hacked!
- Funds were wired to correct bank account
- No claim, but a close call!

Wire Fraud # 3 – Escrow Account

- Closer opened an email with malware
- Clicked on a .jpg file
- “Hobo spider” sat and watched
  - All email
  - All wires
- Hobo saw closer send request for wire to accounting
- Hobo saw accounting initiate the wire

Wire Fraud # 3 – Escrow Account

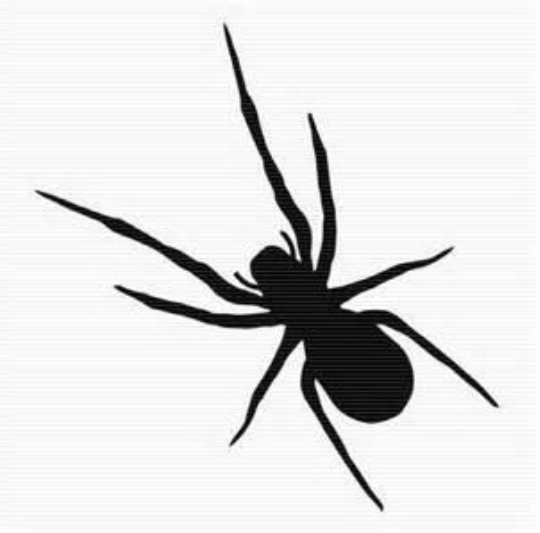
Hobo spider set up a $96,000 wire

- *Imitated* closer requesting the wire
- *Imitated* accounting initiating the wire
- Wire request was received by the bank

Wire Fraud # 3 – Escrow Account

But the hobo spider didn't know about the next step!

- The bank called the title company to confirm that the wire was legitimate.
- It was not legitimate, and the wire was not authorized!
- Loss avoided!



Wire Fraud # 4 – Title Co. Funds

- Mary Smith (M) received wire transfer request from Chris Jones (her dad) –
- Mary plays along – “Sure, what do you need?”
- Fraudster (F) sends wire instructions - $10,986
- F - “Is the transfer completed?”
- Mary – “Can’t find the file? File number? Closer?”

Wire Fraud # 4 – Title Co. Funds

- F – “Transfer completed?
- F – “Payment is for donation for medical support.”
- Mary – “I’m confused. What does this have to do with our company?”
- F - “Part of our social responsibility. I will send you paperwork. Waiting to read from you.”

Wire Fraud # 4 – Title Co. Funds

- Mary – If F would open an encrypted email, she could get F's IP Address
- Mary – Encrypted email sent, but he didn't open it
- F – Transfer completed?
- Mary – Chris, you know you need to open the link and authorize the transfer!
- F – Encrypted email opened

Wire Fraud # 5 – Buyer's Funds

- Title/escrow company computer infected with malware.
- Fraudster (F) monitored all activity on the computer.
- F set a rule moving all e-mail to the buyer into the computer's Junk Email folder.
- Escrow assistant doesn't monitor Junk Mail folder.
- From Junk Mail folder, F modifies some e-mail and forwards it to Buyer.
- F sent buyer new wire instructions!

Wire Fraud # 5 – Buyer's Funds

- F's new wire instructions instructed buyer to wire funds to F's account at new bank!
- New wire instructions were flawed – named two different banks.
- But buyer didn't notice.
- Buyer e-mailed F to ask "why the new instructions"?
- F replied, "Just disregard the prior instructions." Keep in mind this is all done from the Junk Mail folder, without escrow assistant's awareness.

Wire Fraud # 5 – Buyer's Funds

- So Buyer wired his $230,000 in funds to F's bank and told title company wire had been sent.
- Escrow company said, "Wire not received."
- Buyer tried to recall wire, but it was too late. F had already moved the funds.
- Is this an ESCROW CLAIM?

Wire Fraud Prevention – Tip #1

So what can be done to prevent wire fraud?

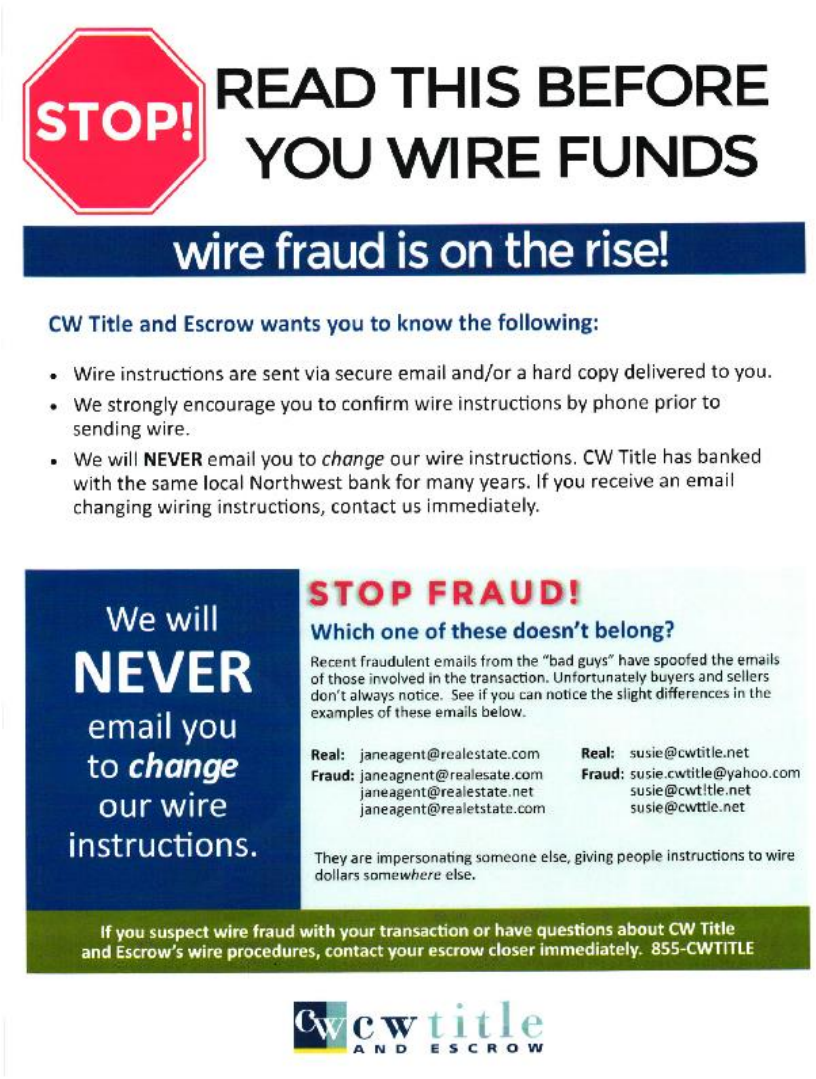
E-mail blurb

**BE AWARE! Online banking fraud is on the rise. If you receive an email containing WIRE TRANSFER INSTRUCTIONS, do not send funds until the instructions are verified.

Call your escrow closing team immediately to verify the information prior to sending funds.**

Wire Fraud Prevention - Tip # 2

- Post a flyer in your reception area
- Add a fraud alert to opening package



STOP! READ THIS BEFORE YOU WIRE FUNDS

wire fraud is on the rise!

CW Title and Escrow wants you to know the following:

- Wire instructions are sent via secure email and/or a hard copy delivered to you.
- We strongly encourage you to confirm wire instructions by phone prior to sending wire.
- We will **NEVER** email you to *change* our wire instructions. CW Title has banked with the same local Northwest bank for many years. If you receive an email changing wiring instructions, contact us immediately.

We will **NEVER** email you to ***change*** our wire instructions.

STOP FRAUD!

Which one of these doesn't belong?

Recent fraudulent emails from the "bad guys" have spoofed the emails of those involved in the transaction. Unfortunately buyers and sellers don't always notice. See if you can notice the slight differences in the examples of these emails below.

Real: janeagent@realestate.com
Fraud: janeagnent@realesate.com
janeagent@realestate.net
janeagent@realetstate.com

Real: susie@cwtitle.net
Fraud: susie.cwtitle@yahoo.com
susie@cwtltle.net
susie@cwttle.net

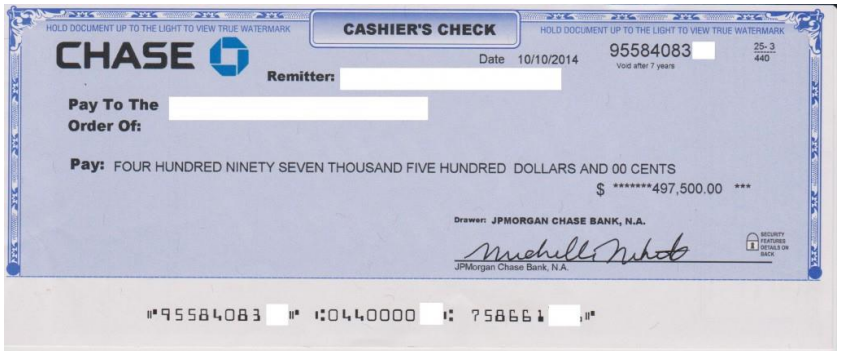
They are impersonating someone else, giving people instructions to wire dollars somewhere else.

If you suspect wire fraud with your transaction or have questions about CW Title and Escrow's wire procedures, contact your escrow closer immediately. 855-CWTITLE

cw title AND ESCROW

Wire Fraud Prevention – Tip # 3

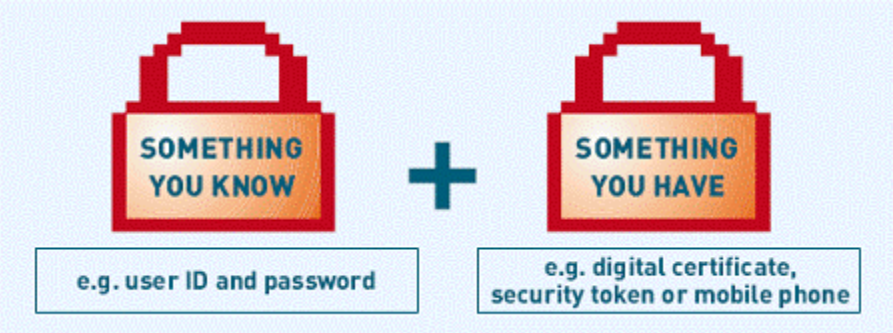
Discourage sending funds by wire transfer – request a cashier's check



Wire Fraud Prevention – Tip # 4

NEVER send wire instructions by e-mail. Always hand deliver wire instructions to the parties or to the person handling the signings.

Wire Fraud Prevention – Tip # 5

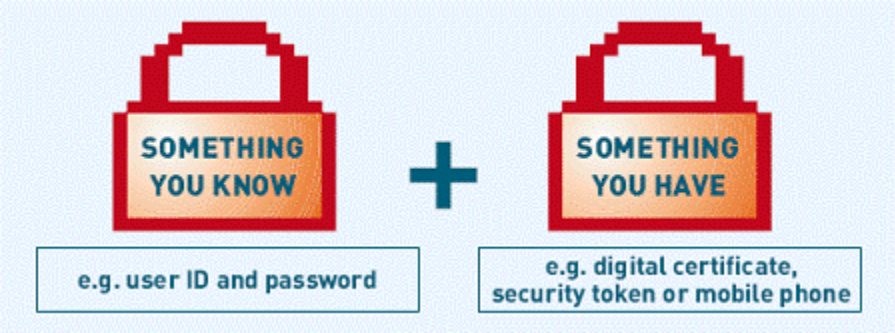


USE TWO FACTOR AUTHENTICATION (2FA) –

2FA you already know about –

- **Wire Fraud # 3 – Hobo spider sat on closer's computer. Imitated everything. Didn't know about the phone call to the bank.**
- **Debit cards with a PIN.**

Wire Fraud Prevention – Tip # 5



Other Forms of 2FA –

- **User ID and Password + Numbers in Cell Phone (RSA Token)**
- **User ID and Password + Numbers in a Key (RSA SecurID)**
- **User ID and Password + Fingerprint/Retina scan/Facial recognition software/Other biometrics**

Wire Fraud Prevention – Tip # 6

Everything is hackable!

Several times a day we receive

- Email that *appears* to come from someone we know
- Marketing e-mails that ask you to '*click on the link*' to receive more info or unsubscribe
- Fraudsters pretending to be your good friend
- **Be wary!**

Wire Fraud Prevention

Any questions?