Cyber Crime in Real Estate Transactions

Krista Christensen, Esq.
VP, Manager, Cyber & Wire Fraud Strategies
Fidelity National Financial

Headlines

"Cyberattacks on the rise during the Covid-19 pandemic"

"Cybercrime Will Cost the US $6 Trillion by the End of the Year: Study"

"Are You Remotely Secure?"

FBI Stats

- One of the most prevalent fraud scheme targeting businesses today.
  - In 2020, the IC3 received 19,369 BEC complaints with adjusted losses over $1.8 billion.
    - Over $1.2 billion more than the next highest reported crime.
- Title companies, law firms, realtors, sellers and buyers are some of the most often targeted victims of wire fraud.
  - Losses over $220 Million reported in real estate transactions through August 2020, which is a 13% increase from the same period in 2019

Social Engineering

- Phishing, Vishing and Smishing
- Spoofed emails
- Caller ID Spoofing
- Email Rule Manipulation

Phishing, Vishing and Smishing…oh my!

The IC3 has reported massive increase in phishing scams designed to get recipients to click on links/open attachments:

- This leads to the release of malware, which leads to
  - Exposure of login credentials
  - Exposure of corporate networks
  - Exposure of confidential data
  - Ransomware

Phishing Schemes: How to Recognize

- The domain in the sending email is not associated with the settlement service company referenced as the sender.
- The sender is not someone you have direct contact with or recognize.
- The email is highly generic. It references closing statements or other closing related documents but does not reference an active transaction.
- The email or attachment is unsolicited or not expected.

Spoofed Emails:

Email spoofing is the fabrication of an email header in the hopes of deceiving the recipient.

- The end game is to get the recipient to open an attachment, click a link or take action based on the information in the email
- Spoofing is successful since the Simple Mail Transfer Protocol (SMTP) does not authenticate email addresses.
- Fraudsters also set up own domains that mimic reputable companies.

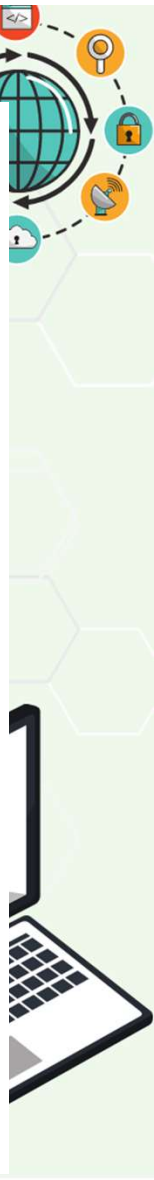
From: Escrow Officer <escrowofficer@fn-f.info>
Date: January 6, 2021 at 9:13:24 AM PST
To: Mortgage Broker@gmail.com
Cc: escrow assistant@fn-f.info, lender@aliancegroupinc.com, lender@aliancegroupinc.com, lender@aliencegroupinc.com
Subject: RE: ROBBINS #7000896353 1943 Huxley Ct San Jose CA

Hi Lender,
Our accounting department just notified me that the wire details I sent earlier have been compromised .. please use our subsidiary account in the attached instructions.
Sorry for the inconvenience.
Thanks

Senior Escrow Officer

Business Address
City and State

Direct: 800-867-5309
Fax: 800-123-4567
Email: escrowofficer@fnf.com



From: “Christensen, Krista" <krista.christensen@fnf.com>
Date: 1/16/21 9:00 AM (GMT-08:00)
To: Buyer@yahoo.com
Cc: broker@kmgloan.com
Subject: wire receipt

Note that only the correct email is visible in this example. It is not until the recipient hits the “reply” button that the fraudulent email is visible (see below)

Buyer,

Look at the receipt carefully, the account number is not correct. Please call your bank or go into the bank to rectify this. You mistakenly put ABA routing number in place of account number. It should be (Account Number: xxxx1779, Bank Routing Number: 263191387).

spoofed email address

From: Buyer<buyer@yahoo.com>
Date: 1/16/21 12:19 PM (GMT-08:00)
To: “Christensen, Krista" <krista.christensen@fn-f.com>
Subject: Re: wire receipt

Yes thank you. I will be fixing this by1:30pm today.

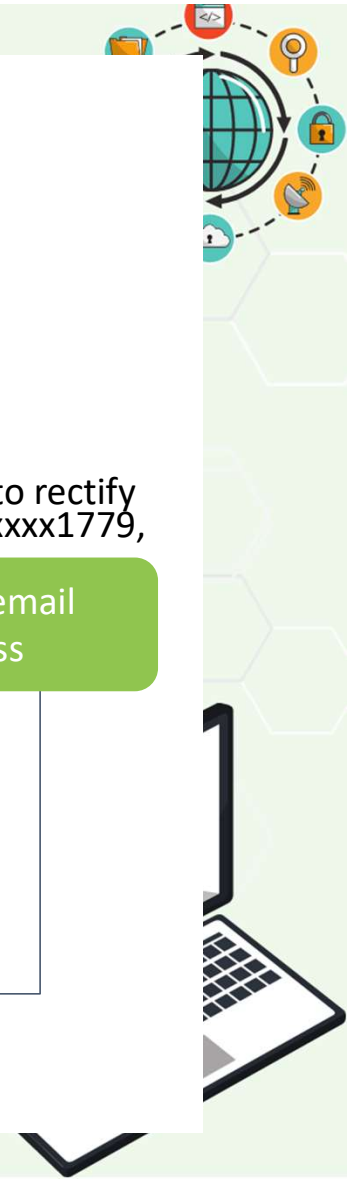
Krista Christensen

Fidelity National Title Group

(951)-248-0636

(866) 665-7637 FAX

Krista.christensen@fnf.com



Caller ID Spoofing

Email Rule Manipulation

Set up automatic forwarding

You can automatically forward your messages to another address. You can choose to forward all new messages, or just certain ones.

Note: You can only set up forwarding on your computer, and not on the Gmail app. If you have an account through work or school and have trouble, contact your administrator.

Turn automatic fowarding on or off

Only forward certain kinds of messages

Forward to multiple accounts

Forward emails from another email service to Gmail

Real Estate Scheme

- Criminals begin the wire fraud scheme long before the attempted theft occurs.
- The fraudsters are sending emails that look legitimate and include facts specific to the transaction.
- Targeting of all participants of a real estate transaction, gaining entry into their computer systems and posing as those parties via compromised emails
  - Real estate agents/ Brokers
  - Transaction coordinators
  - Buyers and sellers
  - Closing Attorneys
  - Escrow
  - Lenders/loan officers

Rethinking Communications

- Educate your clients!
- Talk with the escrow companies you do business with and learn procedures on the who, where, and when of closing funds and providing wire instructions.
- Don’t assume all emails received are legitimate. Be careful about opening attachments and downloading files from emails, even if it appears to be from someone you know.

Fraud using COVID

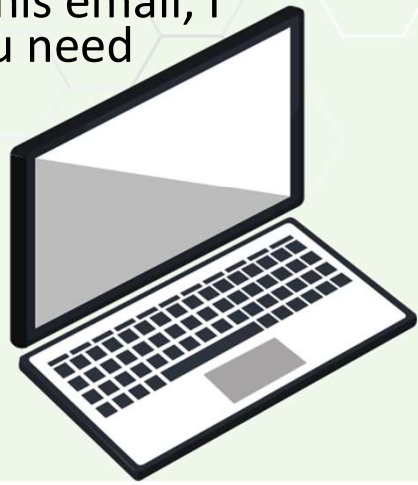
From: Sr. Escrow Officer<closing.com@gmail.com>
Sent: Tuesday, July 7, 2020 10:09 AM
To: Buyers 1, 2 and 3
Cc: Loan Broker<broker_gmccloan@gmx.com>', Real Estate Agent <agentbroker@gmail.com>
Subject: PROPERTY ADDRESS

Good Morning Buyers,

Due to the Covid-19 pandemic, All closing funds should be wired to our trust account today to avoid delay at closing, so that funds can clear in our account on time for closing. I will send the wire instructions once you have acknowledged the receipt of this email, I will be busy with limited access to my phone. You can send me an email if you need anything else.

Thank You!

Branch Manager | Sr. Escrow Officer



Rethinking Communications

- Communication outside of email whenever possible.
- Limit transmission of information to parties that need it.
- Use the “Forward” option rather than the “Reply”
- Immediately delete or report unsolicited e-mail (spam) from unknown parties. DO NOT open spam e-mail, click on links in the e-mail or open attachments.

Rethinking Communications

- Remind clients to never wire money without double-checking that the wiring instructions are correct directly with the intended payee.
- Consider implementing a standard warning notice to your customers of the scam

IT Security Suggestions

Work with IT and cybersecurity professionals to ensure that e-mail accounts, online systems, and business practices are as secure and current as possible- PATCH and UPDATE old programs and systems

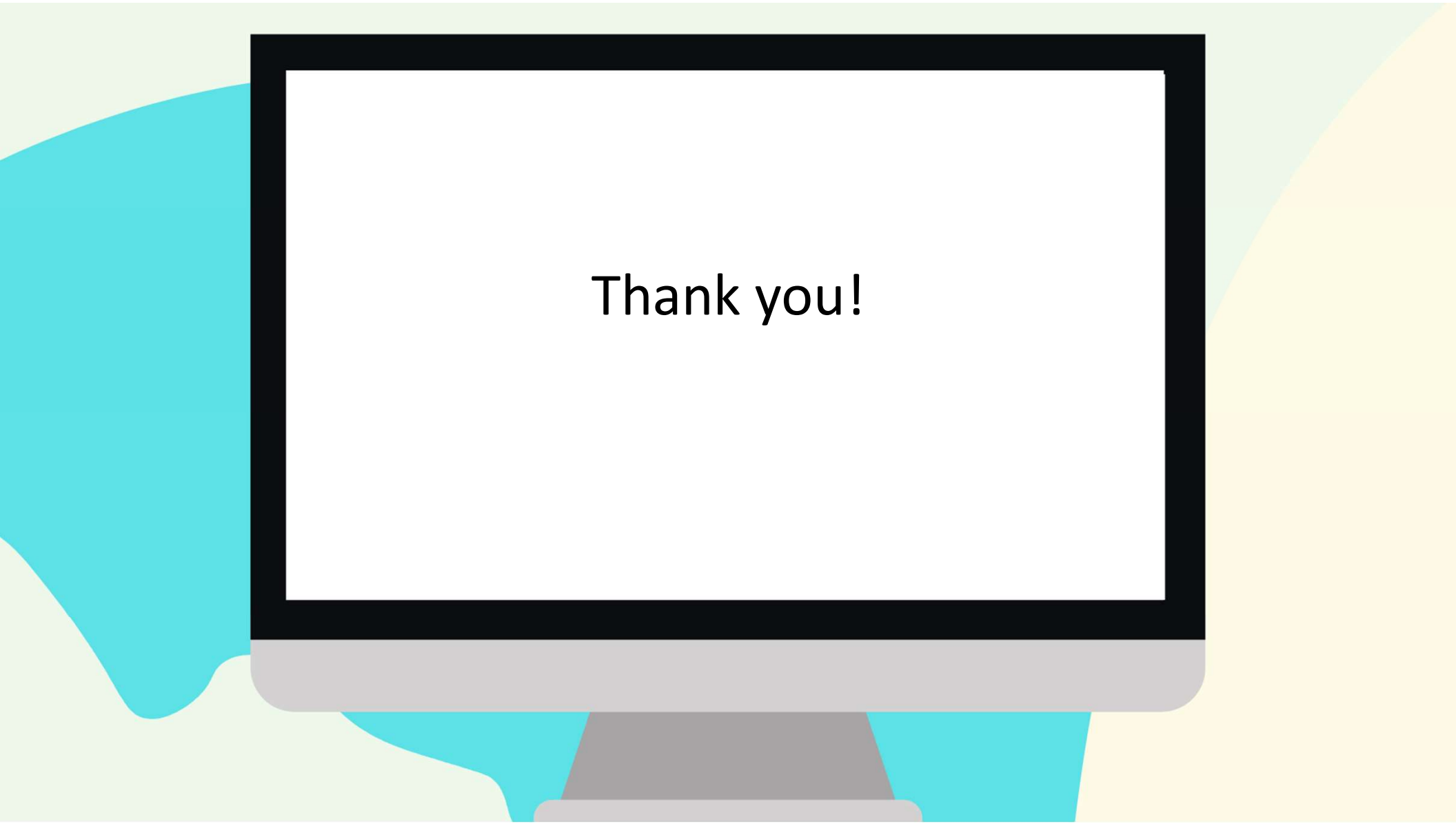
IT Security Suggestions

- **Use two-factor authentication for e-mail accounts.**
- Use secure email to transmit sensitive information.
- Regularly change passwords and review current Cybersecurity experts on password requirements.
- Be wary of free Wi-Fi. Use a Virtual Private Network (VPN) when using unsecured network.

Steps to take if fraud occurs:

See ALTA Rapid Response Plan for Wire Fraud Incidents:

- The account owner should contact the financial institution immediately upon discovering the fraudulent transfer and request a recall due to fraud.
- Request that the financial institution contact the corresponding financial institution where the fraudulent transfer was sent asking for an account freeze.
- Notify the title/escrow company involved in the transaction
- File a complaint with the Internet Crime Complaint Center at www.ic3.gov, regardless of the dollar amount.
- Contact the local police department and Federal Bureau of Investigation (FBI) office.


Thank you!