ALLIANT NATIONAL
TITLE INSURANCE COMPANY

# Ethical Considerations for Cyber Fraud Protection

**Credit: 1 hour CE (Ethics) / 1 hour CLE (Ethics, Technology, RE)**

Barbara Burke, PH.D., Esq.
Owner, Educator, Author, RELS Publishing
10 am – 11 am, Friday, August 9, 2019

UP!

# Barbara Burke, PH.D., Esq.

## Owner, Educator, Author

## RELS Publishing

Barbara Burke has a bachelor's degree in psychology from Vanderbilt University, Master's and Doctorate degrees in Communications from Florida State University, and a law degree from Florida State University. Deciding that was enough school, she joined a law firm in Naples, Florida, representing condominium associations. A year later, she moved to Orlando and began working in the title insurance industry.

Since then, Barbara has been Claims Counsel, Underwriting Counsel, and Commercial Closing Manager for national title insurers, and General Counsel for a large Florida title insurance agency, focusing on residential and developer business. In 2002, she established her own company, consulting for affiliated business arrangements and providing education on title insurance issues through her Real Estate Law Series® company. In 2012, Barbara sold her company and joined a national underwriter, creating online, webinar, and classroom training programs for employees and agents nationwide. In January 2019, Barbara returned to independent contractor life to focus on writing and public speaking training.

Barbara is a prior member of the Florida Bar's Ethics Committee, while currently serving as a member of the Bar's Unlicensed Practice of Law and Title Insurance Committees, in addition to the Property Records Industry Association's Standards Committee. In her spare time, she volunteers for the Adult Literacy League, helping adults improve their reading and writing skills.

# OVERVIEW

**Name of Provider:** Alliant National Title Insurance Company

**Name of Course:** Ethical Considerations for Cyber Fraud Protection (Classroom)

**Targeted audience:** Florida Title Insurance Agents

**Course Objectives:**

This course will be presented in a "scenario-based" format, to show the audience real-world situations in which title agents may find themselves dealing with cyber fraud attacks on their escrow accounts. The presenters will ask the audience members questions to enhance their understanding of how cyber fraud attacks can happen, and how title agents can protect themselves and their customers from loss. The ethical perspectives applicable to each scenario are also covered.

**Course Relevance:**

This course will present critically important information to Florida title insurance agents so that they recognize cyber fraud issues and protect their escrow accounts and business communications. The ethical duties of a title agent if a buyer loses funds or if the title agent loses funds are reviewed. Technology issues are discussed so that Florida title insurance agents, including attorneys, can establish best practices for computer systems, processes, and cyber liability insurance.

**Study Method**: Classroom

# OUTLINE

Ethical Considerations for Cyber Fraud Protection

**I.** Introduction **5 Min**

**II.** How Cyber Fraud Happens **15 Min**

A. Scenario

1. Buyer wires funds to close to cybercriminal in response to fraudulent wiring instructions

B. Discussion

1. How can this happen?
2. Legal and ethical responsibilities of title agent
    a. Duty to prevent?
    b. Duty to assist?
    c. Other duties?

**III.** Detecting and Resolving Cyber Theft **15 Min**

A. Understanding different perspectives

1. Banks
2. Law Enforcement
3. Customers/Clients

B. Discussion

1. What should buyers do?
2. What are the legal and ethical duties of a title/escrow agent
    a. To protect escrow funds?
    b. To protect email accounts?
    c. To carry cyber liability insurance?

**IV.** Stopping Cyber Theft Before It Happens **15 Min**

A. Be suspicious about changes to wiring instructions

B. Confirm changes via previously known telephone number

C. Contact law enforcement

D. Ethical duties to protect communications and funds, and to educate staff how to avoid following fraudulent instructions

**Total Instruction Time** **50 Min**

**Time for Break and Sample Scenarios/Questions** **10 Min**

**Total Time** **60 Min**

# Ethical Considerations for Cyber Fraud Protection

***Scenario One: The Fraud**

Buyer and seller are in the title agency's closing room. The agent asks the buyer for his 'cash to close' cashier's check– the buyer states that he wired the funds the day before, pursuant to the agency's emailed wiring instructions. The agent replies that she did not email any wiring instructions. She shows the buyer how he followed instructions from a fraudster by pointing out the difference between the title agency's correct email address and the fraudster's email address. The buyer asks the seller to delay the sale until the following day, promising to bring a cashier's check to close.

Scenario One - Questions for the Audience:

1. How could the fraudster intervene into the sale transaction's email stream?
2. Does the buyer have to complete the transaction?
3. Does the seller have to complete the transaction?
4. What are the title agent's legal and ethical responsibilities in this situation? To the seller? To the buyer? To the real estate agents, if any?

***Scenario Two: Detecting and Resolving Cyber Theft - Educating Your Customers**

The presenters will portray different industries' perspectives in preventing cyber fraud: IT (email security), banks, insurance (cyber liability), and law enforcement.

Questions for the Audience:

1. What should buyers do if they discover they have wired funds to a fraudster?
2. What are the banks' responsibilities, if any?
3. What is the impact of cyber liability insurance?
4. What law enforcement agencies should be contacted? Is there a minimum loss to contact law enforcement?
5. What are the legal and ethical duties of an escrow agent to protect the escrow funds?
6. What are the legal and ethical duties of an escrow agent if the buyer followed fraudulent instructions and the money was never received by the agent?

***Scenario Three: Stopping Cyber Theft Before it Happens**

The closing agent receives a suspicious email, instructing her to wire the seller's funds to a different bank account. She calls the seller, using a previously known telephone number, who tells the agent no change of wiring instructions were sent. The agent then contacts law enforcement.

Red flags and security steps to take to prevent cyber theft:

- Be suspicious of any changes to payment methods or changes to wiring instructions
- Confirm changes by telephone call to number not shown on fraudulent email message
- Contact law enforcement

Questions for the Audience:

1. Who has experienced cyber fraud?
2. Of those who have experienced cyber fraud, what steps did you take?
3. Were those steps effective?
4. Does a title agency/law firm have an ethical duty to protect its email account from hackers?
5. What are the ethical duties of a title agent/law firm to avoid following fraudulent wiring instructions?

*Scenarios taken from "Where's My Money? A Lesson in Cyber Crime," Title World Tale #1, by Barbara P. Burke

ALLIANT NATIONAL
TITLE INSURANCE COMPANY

**SPECIAL ALERT 14-01**

**TO:** All Alliant National Agents

**DATE:** January 10, 2014

**SUBJECT:** ***Fraud Scheme Using Real Estate Agents' Email Accounts***

Real estate transactions now seem to be attracting the attention of international cybercriminals. We recently learned of two fraud scenarios involving the hacking of a real estate agent's email account where the criminal is able to send email messages out of the real estate agent's account, with all of their normal links, logos, and contact information. It does not look like it is being generated by anyone other than the real estate agent. It works just like when you give an IT technician access to your computer and they can operate it remotely.

Scenario #1:

You, the settlement agent, receive a message from the buyer's real estate agent instructing you to release the earnest money deposit back to their client. They give you wire instructions for the buyer's account. It later turns out that the actual real estate agent did not send this message, though it came from their email address, and even had other attachments relating to this transaction. Their email account had been" highjacked" and a criminal was watching the email traffic in order to intervene at just the right moment and send their own message via the real estate agent's account. There is no way to distinguish that it is not really from the true real estate agent, unless the spelling or tone or style is different, or the message does not make sense.

Do not release funds unless you have written authorization from the buyers independent of their real estate agent. Of course, the seller should also consent to the release of the earnest money deposit. With regard to the release of escrowed funds, you should require a "wet" signature on your own document form – and not an electronically generated signature on a document coming out of the real estate agent's electronic delivery system, so common today with real estate contracts, using software such as Verisign and Docusign. That wet signature can be emailed, it does not need to be dropped off in person. You might also consider calling the real estate agent and/or buyer to confirm the instructions when funds are involved.

ALLIANT NATIONAL
TITLE INSURANCE COMPANY

**SPECIAL ALERT 15-01**

**TO:** All Alliant National Agents

**DATE:** February 13, 2015

**SUBJECT:** ***Fraud Scheme Using Real Estate Agents' Email Accounts – Part II***

This Special Alert supplements Special Alert 14-01 distributed on January 10, 2014. Cybercriminals continue to create new schemes to fraudulently obtain funds from escrow accounts. We recently learned of another scenario involving the hacking of a real estate agent's email account where the criminal is able to send email messages out of the real estate agent's account, with all of their normal links, logos, and contact information. It does not look like the email is being generated by anyone other than the real estate agent. It works just like when you give an IT technician access to your computer and they can operate it remotely.

Scenario #3:

You, the settlement agent, receive instructions from the seller regarding where to wire the seller's sale proceeds. Right before or after closing, you receive a message from the seller's real estate agent instructing you to wire the sale proceeds to a different account allegedly owned by the seller. It later turns out that the actual real estate agent did not send this message, though it came from their email address, and even had other attachments relating to this transaction. Their email account had been "highjacked" and a criminal was watching the email traffic in order to intervene at just the right moment and send their own message via the real estate agent's account. There is no way to distinguish that the email is not really from the true real estate agent, unless the spelling or tone or style is different, or the message does not make sense.

Do not release funds unless you have written authorization from the seller(s) independent of their real estate agent. You might also consider calling the real estate agent and seller(s) to confirm instructions when funds are involved.

The real estate agent rarely has any warning that malware has invaded their computer and their keystrokes and emails are being watched. The first notice they may get is a strange email reply that does not make sense to them. Please alert your real estate agent clients to the very real threat of a hacking of their email account, and make sure they instruct their clients to deal directly with the party who is going to wire into their account. Generally, real estate agents should not continue to be the go-between for their client relating to funds or closing documents, once an escrow is being opened. Please let us know if you hear of any fraudulent activity so we can alert our agents.

As always, please contact us with any questions or comments.

ALLIANT NATIONAL
TITLE INSURANCE COMPANY

**SPECIAL ALERT 15-03**

**TO:** All Alliant National Agents

**DATE:** March 30, 2015

**SUBJECT:** ***Fraud Scheme Using Email – Part III-Use of Fake Settlement Agent Email Address for Wire Instructions***

---

This Special Alert supplements Special Alert 14-01 distributed on January 10, 2014, and Special Alert 15-01 distributed on February 13, 2015. Cybercriminals continue to create new schemes to fraudulently obtain funds from escrow accounts. Last week we learned of another scenario that happened to an agent in Florida, involving the hacking of a buyer's email account where the criminal created an email address that looked like it was from the settlement agent (different email address, but very close), with all of their normal links, logos, and contact information.

Scenario #3:

The settlement agent sends wiring instructions for their escrow account to the buyer regarding where to wire the funds for closing. Then an hour later the buyer receives another message from the settlement agent reminding them not to bring a cashier's check and instructing them again to wire the sale proceeds, using the same wire instruction form that was attached before, but changing the account number. Luckily the buyer was very suspicious of the email and called the settlement agent to make sure they sent it. They noticed the minor difference in the email address. A generic example would be john@smithlaw.com vs johnsmithlaw@mail.com. Note that the end of the address is a general mail box, not the usual domain name of the recipient. But the email was written well, and looked legitimate if the buyer had not been looking carefully, and it did not state that there were updated or revised wire instructions, so it would be easy to miss that they had changed it.

Although there may be no liability for the settlement agent or the underwriter for funds that never went into their accounts, the loss to the parties could be devasting. Please encourage anyone to whom you send closing instructions to contact you by phone or correct email address, if they receive any further contact attaching wiring instructions, even if they look the same or look like they are coming from you. Also, remind them that if they get an email that has a generic domain at the end, like "gmail" or "mail", to check to see if it has the full correct email that has been on prior emails, because the generic domain a red flag that it is a fake, set up for just this scam.

As always, please let us know if you hear of any fraudulent activity so we can alert our agents, and contact us with any questions or comments.

Corporate Office | [illegible] | Longmont, CO 80501
Main: [illegible] | Toll Free: [illegible] | AlliantNational.com

  

ALLIANT NATIONAL
TITLE INSURANCE COMPANY

**SPECIAL ALERT 15-07**

**TO:** All Alliant National Agents

**DATE:** November 12, 2015

**SUBJECT:** ***New Scam – Business Email Compromise***

---

Businesses are being hit by a new email scam referred to by various names - "business email compromise," "corporate deception email," "CEO fraud." In this scam, the fraudsters impersonate a senior member of the company in order to deceive another employee to transfer money.

A typical pattern is –

- The fraudster sends an email to an employee whose job includes transferring funds, and the email appears to be from a senior officer, such as the CFO or CEO.
- Software is used to manipulate the characteristics of the email, including the sender's address, so that it looks genuine, arriving in the recipient's inbox just like a real email from the same contact.
- The email requests an urgent payment to be made outside of normal procedures, often giving a pressing reason.
- The account to which the payment is made is controlled by the fraudster, who quickly withdraws the funds.

Another twist on the scam is an email that appears to be from a vendor directing payment of an invoice.

The U.S. Federal Bureau of Investigation has identified Business Email Compromise as an emerging global threat, stating that businesses of all sizes are targeted, with fraudsters using extremely sophisticated methods.

From the FBI's report on Business Email Compromise -

> "They know how to perpetuate the scam without raising suspicions," FBI Special Agent Maxwell Marker said. "They have excellent tradecraft, and they do their homework. They use language specific to the company they are targeting, along with dollar amounts that lend legitimacy to the fraud. The days of these e-mails having horrible grammar and being easily identified are largely behind us."
>
> To make matters worse, the criminals often employ malware to infiltrate company networks, gaining access to legitimate e-mail threads about billing and invoices they can use to ensure the suspicions of an accountant or financial officer aren't raised when a fraudulent wire transfer is requested.

https://www.fbi.gov/news/stories/2015/august/business-e-mail-compromise/business-e-mail-compromise

ALLIANT NATIONAL
TITLE INSURANCE COMPANY

**SPECIAL ALERT 16-01**

**TO:** All Alliant National Agents

**DATE:** January 6, 2016

**SUBJECT:** ***Escrow Fraud Prevention-Wiring Seller Proceeds***

We recently received two reports of attempts to defraud settlement agents in connection with seller proceeds. The fraudsters, posing as sellers, emailed the settlement agents with requests to change wiring instructions; fortunately, these attempts were unsuccessful due to the settlement agents' good business practices.

These are the common factors in both scenarios:

- During or immediately after closing, the settlement agent received an email that appeared to come from the seller and included a subject line similar to that used in prior correspondence with the settlement agent.
- The settlement agent had previously received wiring instructions from the seller, including a copy of a voided check for the account to which the funds were to be wired.
- The email requested that the sales proceeds be wired to a different bank account.
- The email came from an email account apparently set up specifically for the purpose of the fraud.

In one case, the "seller" emailed the settlement agent requesting that the proceeds be wired to her corporate account instead of her personal account. Based on a company policy requiring that seller proceeds be paid only to the person or entity shown on the settlement statement, the settlement agent declined to do so. When the emails from the fraudster became increasingly demanding, the settlement agent called the actual seller—who confirmed that she had not sent the emails and had no corporate account.

In the other case, after the proceeds had already been wired to the account previously specified by the seller, the fraudster emailed the settlement agent requesting that the proceeds be wired to a completely different bank. When told the funds had already been sent, the fraudster became very agitated and demanded a copy of the wire confirmation. At this point, the settlement agent called the actual seller--who did not even own a computer or have an email account.

These good business practices will help prevent this fraud:

- Have a strict company policy that seller proceeds are to be paid only to the actual seller shown on the settlement statement.
- Decline to accept instructions to wire seller proceeds without a form physically signed by the seller to which a voided check from the indicated account is attached (sample form attached).
- Do not provide a copy of a wire confirmation (which contains all of the customer's bank account information) to anyone on the basis of an unconfirmed email.
- Pay close attention to email addresses; fraudsters typically use email addresses which closely resemble a seller's (or any party's) actual email address.

Please contact your Alliant National underwriter with any questions or concerns.

Corporate Office | Bay Left and Circle, Suite G | Longmont, CO 80501
Main: [illegible] | Toll Free: [illegible] | AlliantNational.com

  

ALLIANT NATIONAL
TITLE INSURANCE COMPANY

**SPECIAL ALERT 16–02**

**TO:** All Alliant National Agents

**DATE:** January 6, 2016

**SUBJECT:** ***Escrow Fraud Prevention-Wiring Buyer Funds to Settlement Agents***

---

In Special Alert 16-01, we discussed attempts by fraudsters to obtain seller proceeds by posing as sellers and emailing last-minute changes to wiring instructions previously given to settlement agents. These fraudsters had not hacked the "true" seller's email accounts but had instead set up email accounts specifically for the perpetration of the fraud.

This Special] Alert sets out another fraud scheme which instead targets buyers' funds. In this scheme, the fraudster actually hacks the email accounts of the settlement agent and/or the real estate agent and monitors the account(s) for upcoming real estate closings. As a closing date approaches, the fraudster—posing as the settlement agent or real estate agent–sends an email to the buyer requesting that the buyer wire his or her funds to a different bank account set up by the fraudster. In a recent reported transaction, the fraud was avoided only because the buyer questioned why the settlement agent had changed her wiring instructions.

Settlement agents need to make buyers aware of this scam and request that buyers immediately call them if such an email is received. Settlement agents should also consider the encryption of emails and wiring instructions.

Please contact your Alliant National underwriter with any questions or concerns.