From Deepfakes to Fake Deeds: AI's Role in Land Fraud & Ethical Concerns

Lynne Murphy Breen, Esq.

First American Title Insurance Company
800 Boylston Street, Suite 2820
Boston, MA 02199
(617) 780-1476
lymurphy@firstam.com

Lynne Murphy Breen is senior underwriting counsel with First American Title Insurance Company. Lynne works with agents in underwriting, for both commercial and residential transactions. She has worked in the title insurance industry for over twenty years.

Prior to joining the title insurance industry, Lynne was in private practice, specializing in real estate law and litigation. She is a member of the Abstract Club, the REBA Continuing Education Section, and the MCLE Curriculum Advisory Committee, and is a frequent lecturer for MCLE and REBA. A passionate advocate for those with Usher Syndrome, Lynne also served on the National Institute of Health NIDCD Advisory Council.

Lynne is a recipient of *Massachusetts Lawyers Weekly* and *New England In-House* 2017 In-House Leaders in the Law award. She received her J.D. from the John Marshall Law School, and her undergraduate degree from University of Massachusetts at Amherst.

Katherine Prifti, Esq.

First American Title Insurance Company
800 Boylston Street, Suite 2820
Boston, MA 02199
(617) 772-9210
kprifti@firstam.com

Katherine Prifti is Regional Underwriting Director for the Northeast Region of First American Title Insurance Company. She leads the Massachusetts underwriting team in providing agents with underwriting guidance and escrow services. Katherine works closely with the state manager to enhance agency relationships, and collaborates with regional counsel and senior underwriters to develop training for both agents and underwriters.

In 2013, Katherine joined First American as associate claims counsel for the New England states, and then served as area underwriting counsel. She also gained experience serving as claims counsel for a national title insurance underwriter, a paralegal for a Boston law firm, and intern in the Massachusetts Attorney General's office. Katherine routinely collaborates on complex commercial transactions with First American agents and employees. She also presents educational seminars on real estate topics, including title examination, complex endorsement coverages, foreclosure, probate and trusts.

Katherine is the Co-chair of the REBA Residential Conveyancing Section, and was the 2019 recipient of the Association's Emerging Leader Award. She is also a member of the MBA, American Land Title Association (ALTA), New England Land Title Association (NELTA) and Commercial Real Estate Women (CREW).

Katherine is an adjunct professor at Suffolk University, where she lectures on business and contract law. She received her J.D. from Suffolk University Law School, and her B.S., *magna cum laude*, from Suffolk University-Sawyer Business School.

From Deepfakes to Fake Deeds: AI's Role in Land Fraud & Ethical Concerns

FBI Boston
Kristen Setera
(857) 386-2905

April 1, 2025

FBI Boston Warns Quit Claim Deed Fraud is on the Rise

Landowners and Real Estate Agents Urged to Take Action to Protect Themselves

The Boston Division of the Federal Bureau of Investigation (FBI) is warning property owners and real estate agents about a steady increase in reports of quit claim deed fraud it has received—scams that have resulted in devastating consequences for unsuspecting owners who had no idea their land was sold, or was in the process of being sold, right out from under them.

Known as quit claim deed fraud or home title theft, the schemes involve fraudsters who forge documents to record a phony transfer of property ownership. Criminals can then sell either the vacant land or home, take out a mortgage on it, or even rent it out to make a profit, forcing the real owners to head to court to reclaim their property.

Deed fraud often involves identity theft where criminals will use personal information gleaned from the internet or elsewhere to assume your identity or claim to represent you to steal your property.

"Folks across the region are having their roots literally pulled out from under them and are being left with no place to call home. They're suffering deeply personal losses that have inflicted a significant financial and emotional toll, including shock, anger, and even embarrassment," said Jodi Cohen, special agent in charge of the FBI Boston Division. "We are urging the public to heed this warning and to take proactive steps to avoid losing your property. Anyone who is a victim of this type of fraud should report it to us."

Law enforcement and the FBI have been alerted to the fraud at all points in the process and have received reports involving a variety of fraudulent scenarios, including:

- Scammers who comb through public records to find vacant parcels of land and properties that don't have a mortgage or other lien and then impersonate the landowner, asking a real estate agent to list the property. Homeowners whose properties have been listed for sale don't know it until they're alerted, sometimes after the sales have gone through.
- Family members, often the elderly, targeted by their own relatives and close associates who convince them to transfer the property into their name for their own financial gain.
- Fraudsters known as "title pirates" who use fraudulent or forged deeds and other documents to convey title to a property. Often these scams go undetected until after the money has been wired to the scammer in the fraudulent sale and the sale has been recorded.

https://www.fbi.gov/contact-us/field-offices/boston/news/fbi-boston-warns-quit-claim-deed-fraud-is-on-the-rise-

The FBI's Internet Crime Complaint Center (IC3), which provides the public with a means of reporting internet-facilitated crimes, does not have specific statistics solely for quit claim deed fraud, but it does fall into the real estate crime category. Nationwide, from 2019 through 2023, 58,141 victims reported $1.3 billion in losses relating to real estate fraud. Here in the Boston Division—which includes all of Maine, Massachusetts, New Hampshire, and Rhode Island—during the same period, 2,301 victims reported losing more than $61.5 million.

- 262 victims in Maine lost $6,253,008.
- 1,576 victims in Massachusetts lost $46,269,818.
- 239 victims in New Hampshire lost $4,144,467.
- 224 victims in Rhode Island lost $4,852,220.

The reported losses are most likely much higher due to that fact that many don't know where to report it, are embarrassed, or haven't yet realized they have been scammed.

FBI Boston is working with property owners, realtors, county registers, title companies, and insurance companies to thwart the fraud schemes but it's no easy task. The COVID-19 pandemic changed the way business was and continues to be conducted. More and more people have grown accustomed to conducting real estate transactions through email and over the phone. The remote nature of these sales is a benefit to bad actors.

Tips for Landowners:

- Continually monitor online property records and set up title alerts with the county clerk's office (if possible).
- Set up online search alerts for your property.
- Drive by the property or have a management company periodically check it.
- Ask your neighbors to notify you if they see anything suspicious.
- Beware of anyone using encrypted applications to conduct real estate transactions.
- Take action if you stop receiving your water or property tax bills, or if utility bills on vacant properties suddenly increase.

Tips for Realtors:

- Avoid remote closings, if possible.
- Ask for in-person identity checks.
- Request copies of documents that only the property owner would have. This includes a copy of the most recent tax bill, utility bill, or survey from when the property was purchased, in addition to the individual's ID.
- Send a certified letter to the address of record on the tax bill.
- Look up the phone number by reverse search or through the phone carrier.
- Call to verify the public notary and confirm he/she attested to the documents.

The FBI can work with our partners to try to stop wire transfers and recover the funds within the first 72 hours. We urge folks to report fraud and suspected fraud to the FBI's Internet Crime Complaint Center at www.ic3.gov.

https://www.fbi.gov/contact-us/field-offices/boston/news/fbi-boston-warns-quit-claim-deed-fraud-is-on-the-rise-

First American Title™

AI-Driven Fraud: The Hidden Threat in Real Estate

The tools and technologies powered by artificial intelligence continue to evolve rapidly, and while the real estate industry is harnessing AI to automate everything from property valuations and predictive analytics to customer relationship management and fraud prevention, scammers are harnessing AI to identify targets, rapidly scale their schemes and avoid detection. For example, a Deloitte study estimated that generative AI could cause U.S. fraud losses to grow by 32% each year moving forward, reaching **$40 billion** by 2027.

What does this mean for the U.S. real estate and mortgage finance industries and the customers they serve? Sarah Franc, Vice President and Real Estate Fraud Expert at First American Title, shared her thoughts on the distinct threat AI fraud poses to home buyers and sellers, real estate professionals and lenders, providing concrete advice to help protect yourself from fraudsters.

MBA NewsLink: How are scammers using AI to commit real estate fraud?

Sarah Frano: AI tools make it easier to quickly fabricate correspondence, identification, deeds, mortgages, video and voices, which can be indistinguishable from a real document or person. Given the intrinsic value of real estate, property transactions and mortgages are attractive targets for scammers.

Armed with AI, scammers can commit broader and increasingly complex types of fraud. Deepfakes, for example, are created using deep learning algorithms that gather a large dataset of images or videos of a target person, which is then used to train an AI model to understand the person's voice, facial features, expressions and movements. In real estate transactions, scammers can use deepfake audio or video to impersonate real estate agents or other professionals involved in the transaction, leading to fraudulent communications that provide false information or instructions.

Scammers can also use deepfakes to impersonate home sellers. Recently, a Florida title company scheduled a video call to confirm the identity of a woman attempting to sell a vacant lot. They were shocked when they encountered an AI-generated person. The fraudsters likely used AI and **face-swapping** technology to create the alleged seller, but the face was actually that of a woman who had disappeared in 2018.

MBA NewsLink: What are the most common targets?

Sarah Frano: Properties without an owner-occupant, such as a vacant lot, a second home or a rental property, are common targets for scammers since it's less likely the owner will discover the fraud. Conversely, while owner-occupied properties are less susceptible to seller impersonation fraud, they may be at a greater risk of scammers taking out fraudulent loans and stripping the property's equity. Scammers are after money, not property, so high-equity and mortgage-free properties are attractive targets.

MBA NewsLink: How can I spot AI-driven fraud?

Sarah Frano: Detecting deepfakes can be challenging, but there are several techniques and tools that can help identify them, including visual and behavior analysis. Look for inconsistencies in blinking patterns, lip movements, reflections, shadows, skin texture and hair. Deepfakes often struggle to replicate natural blinking patterns and lip movements and may show overly smooth skin or inconsistencies in hair.

There are also specialized software and tools designed to detect deepfakes. These tools analyze videos for subtle artifacts and inconsistencies that are hard for humans to spot. Advanced machine learning models can also be trained to detect deepfakes by identifying patterns and anomalies in the data.

For a quick practical tip, perform a reverse image search to check if the image or video has been used elsewhere on the web.

MBA NewsLink: How can people protect themselves from AI-driven fraud?

Sarah Frano: To protect yourself from deepfake scams during the home buying and selling process, consider the following precautions, and tell those you work with to do the same.

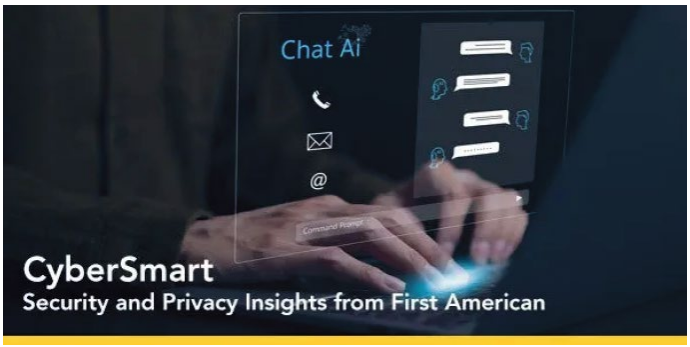
- Verify identities. Always verify the identity of the person you are dealing with through multiple sources. Whenever possible, meet in person to confirm details and verify identities.
- Use trusted platforms. Conduct transactions through trusted escrow services and their secure platforms. Be cautious of emails and content from unknown or unverified sources.
- Protect your title. Where available, always purchase a title insurance policy that covers fraud after you purchase your home.
- Stay informed. Keep up to date with the latest fraud schemes and how to detect them. Educate yourself and others about the signs of deepfakes and encourage a critical approach to consuming digital content.

By combining these techniques and staying vigilant, you can improve your ability to detect deepfakes and reduce the risk of real estate fraud powered by AI.

Originally published via Mortgage Bankers Association's (MBA) NewsLink Newsletter online on February 25, 2025. To read the full article, click here.

First American Title™

Exploring AI's Impact on Real Estate Security



Artificial Intelligence (AI) is revolutionizing industries, and the real estate sector is no exception. As the use of AI applications continues to soar, so will the use of AI in cyber scams aimed at homebuyers.

AI has been used in real estate for many years; however, it recently became a hot topic due to breakthroughs in generative AI technology, which is AI that can produce content. Generative AI has immense promise to streamline real estate transactions, but real estate leaders are adopting it slowly and cautiously. Let's explore the diverse range of applications for AI in real estate, examining both its potential benefits and possible security risks.

How AI Can Enhance Real Estate Transactions

Better Customer Service. AI chatbots can be used by real estate professionals for convenient, 24/7 customer support.

Faster Insights. “What are the top neighborhoods in California for a first-time homebuyer?” AI can analyze this data in seconds to help you make smarter decisions.

Dream Home Design. AI does not just produce text— it can draw architectural plans based on data, for example, to maximize sunlight in your kitchen.

Smart Home Integrations. You may already regularly use AI if you have smart home devices. For example, smart security systems use AI to track movement and tell you whether it is a pet or a person at your front door.

First American Title™

First American Title™

How AI Can Pose Security Risks

Deepfake Videos. Generative AI can turn a video of a cybercriminal into a video of your realtor, loan officer, or, even worse, a family member. These videos— called deepfakes— have been used to trick homebuyers and sellers into sending money straight into a cybercriminal's hands.

Voice Cloning. Similarly, generative AI can take a voice and mask it to sound like the voice of someone you know. You may first recognize this tactic from news stories where scammers masquerade as family members in need of bail. But, if buying a home, scammers may imitate your real estate professional, claiming something has gone wrong with your purchase and that they need money or your information to save the transaction.

Misinformation. Just like we can use generative AI to design a dream home, cybercriminals can use it to alter property listing photos, duping real estate buyers into thinking a home is in a better condition than it is.

Did you know?

The United States Patent Office awarded First American two patents in 2021 for our applications of AI to property data analysis.

Deepfake Scams

An unknowing employee at a multinational firm recently transferred millions of dollars to cybercriminals because of a deepfake video. Deepfake videos may be new, but this scam is just another form of phishing. Read more about phishing at our Security and Privacy Center.

More Cybercrime and Real Estate Trends

With evolving cybercrime tactics and shifting real estate trends, staying ahead of digital threats is more important than ever. Equip yourself with the knowledge and skills to be Cyber Smart.

Know Your Seller
Unencumbered and Vacant Land Checklist

The following checklist is a resource for combating potential fraudulent sales. While you are not required to satisfy all items, you are expected to complete any and all due diligence necessary for you to verify you are working with the rightful owner.

Initial Inquiries Upon Receipt of Contract

- ☐ Is the property unimproved or, if improved, not owner-unoccupied?
- ☐ Is the property unencumbered by a mortgage?
- ☐ How long has the current owner owned the property?
- ☐ Is Seller a US Citizen or Resident (e.g., U.S. Social Security Card Holder or Green Card Holder)?
- ☐ Where is Seller currently located?
- ☐ Did the contract come from a trusted referral, such as a known real estate agent or attorney?
- ☐ How did the real estate agent obtain the listing? For example, by phone call, email, or text?
- ☐ Does your referral personally know Seller? Have they met in-person? If so, how do they know each other and for how long?
- ☐ Does your referral personally know Seller? Have they met in-person? If so, how long have they known each other? If not personally known, how have they been communicating? Only by phone or email?
- ☐ Review Seller's emails for words, phrases, and grammar that indicate they may be a fraudster.
- ☐ Review Seller's emails for words, phrases, and grammar that indicate they may be a fraudster. Review *First American Underwriting Communication NA-2023-2005* for more information.
- ☐ Is the sales price reasonable?
- ☐ Are you being asked to close quickly?

Continued Due Diligence

- ☐ Obtain two separate valid forms of ID within three days of receipt of the contract.
  - Compare the IDs. Review photos and other information for inconsistencies.
  - Conduct reverse image search.
  - Visit https://www.emvlab.org/mrz as an additional resource to confirm passport data.
- ☐ Upon receipt of IDs, conduct a video call with Seller.
  - Compare the photo IDs to the person on video.
  - Look for anything unusual, such as the use of a still image or filter or a last-minute change to protocol.
  - Ask general questions that Seller should know without hesitation or review of documents, such as:
    - Seller's age and address
    - Date of purchase and purchase price
    - If improved, the approximate square footage or numbers of bedrooms; and
    - Seller's contact information.
- ☐ Send the Property Owner Notification Letter via overnight delivery (or international equivalent) to address on file with the property appraiser. Did you receive unsolicited confirmation of receipt?
- ☐ Conduct Internet research of Seller, including social media sites, to corroborate photos and other information.
- ☐ Do not use new contact information for Seller unless you receive satisfactory explanation for a change.
- ☐ Confirm the Seller's location on the day of closing. Does it match information previously received?
- ☐ Perform OFAC search for each Seller and any other name appearing on accounts from which closing funds are initiated and into which sales proceeds will be deposited.
- ☐ Validate Seller's cell phone: https://phonevalidator.com.
- ☐ Compare IP address on e-contract against Seller's purported location: https://www.whatismyipaddress.com.
- ☐ Consider engaging a third-party FIRPTA provider to add another layer of review.

Learn More at firstam.com/agency

First American Title™

AMD: 08/2023

Procedures for using a Notary - US Embassy or Consulate

- [ ] Participate in the scheduling of the appointment with the U.S. Embassy or Consulate.
- [ ] On the date of the signing, receive and review copies of executed and acknowledged documents and Seller's picture IDs from the U.S. Embassy or Consulate.
- [ ] Review the notarial certificate for obvious errors and confirm notary is not a known fraudulent notary.
- [ ] Contact the U.S. Embassy or Consulate to confirm that the official that notarized the documents is an employee authorized to perform the notarial act and that the seal is legitimate.
- [ ] Comply with all other First American requirements for foreign acknowledgments.

Notary Public in Foreign Country

- [ ] Obtain the name and contact information of the proposed notary public.
- [ ] Make independent contact with the notary public by phone.
- [ ] Review a copy of the executed and acknowledged documents and photo IDs while Seller is with the notary public. If appropriate, require an Apostille.
- [ ] Upon receipt of the original documents, confirm the information on the notarial seal and certificate match the purported location of the Seller and the country from which the original documents are sent.
- [ ] Comply with all other First American requirements for foreign acknowledgments.

RON - Remote Online Notarization

- [ ] Must be an approved RON "MISMO RON Certified Providers." – Visit: Certified eMortgage Technology Providers I MISMO
- [ ] If use of an approved RON is not possible, approval must be obtained in advance from Underwriting. Be prepared to provide sufficient due diligence evidencing valid identity of the signer.
- [ ] Either Agent or a trusted sourced who personally knows the signer, such as the real estate agent, must attend the RON session. If the attendee is someone other than the Agent, obtain Affidavit of Identity.
- [ ] Comply with all other First American and state-specific RON requirements.

Validation of the Bank Account to be Funded

- [ ] If the account to be funded is an account within the U.S., use a third-party validation platform to confirm the name of the account and when it was opened.
- [ ] If the account to be funded is located outside of the U.S., confirm that it is located within the country in which Seller resides and the date on which it was opened.
- [ ] If the wire is rejected, do NOT reinitiate wire or contact any party. Contact your local Agency underwriters.

SELLER IMPERSONATION FRAUD IN REAL ESTATE

FRAUDSTERS are impersonating property owners to illegally sell commercial or residential property. Sophisticated fraudsters are using the real property owner's Social Security and driver's license numbers in the transaction, as well as legitimate notary credentials, which may be applied without the notary's knowledge.

Fraudsters prefer to use email and text messages to communicate, allowing them to mask themselves and commit crime from anywhere.

Due to the types of property being targeted, it can take months or years for the actual property owner to discover the fraud. Property monitoring services offered by county recorder's offices are helpful, especially if the fraud is discovered prior to the transfer of money.

Where approved by state regulators, consumers can purchase the American Land Title Association (ALTA) Homeowner's Policy of Title Insurance for additional fraud protection.

WATCH FOR RED FLAGS

CONSIDER HEIGHTENED SCRUTINY OR HALT A TRANSACTION WHEN A PROPERTY

- Is vacant or non-owner occupied, such as investment property, vacation property, or rental property
- Has a different address than the owner's address or tax mailing address
- Has no outstanding mortgage or liens
- Is for sale or sold below market value

CONSIDER HEIGHTENED SCRUTINY OR HALT A TRANSACTION WHEN A SELLER

- Wants a quick sale, generally in less than three weeks, and may not negotiate fees
- Wants a cash buyer
- Is refusing to attend the signing and claims to be out of state or country
- Is difficult to reach via phone and only wants to communicate by text or email, or refuses to meet via video call
- Demands proceeds be wired
- Refuses or is unable to complete multifactor authentication or identity verification
- Wants to use their own notary

SHUTTERSTOCK / TANYA ANTUSENOK

www.alta.org

SELLER IMPERSONATION FRAUD
IN REAL ESTATE

AMERICAN LAND TITLE ASSOCIATION

TAKE PRECAUTIONS

CONTACT SELLER USING INDEPENDENT SOURCES

- Contact the seller directly at an independently discovered and validated phone number
- Mail the seller at the address on tax records, property address, and grantee address (if different)
- Ask the real estate agent if they have personal or verified knowledge of the seller's identity

MANAGE THE NOTARIZATION

- Require the notarization be performed by a vetted and approved remote online notary, if authorized in your state
- If remote online notarization is not available, the title company should select the notary. Examples include arranging for the seller to go to an attorney's office, title agency, or bank that utilizes a credential scanner or multifactor authentication to execute documents

VERIFY THE SELLER'S IDENTITY

- Send the seller a link to go through identity verification using a third-party service provider (credential analysis, KBA, etc.)
- Run the seller's email and phone number through a verification program
- Ask conversational questions to ascertain seller's knowledge of property information not readily available in public records
- Conduct additional due diligence as needed

USE THE PUBLIC RECORD

- Compare the seller's signature to previously recorded documents
- Compare the sales price to the appraisal, historical sales price, or tax appraisal value

CONTROL THE DISBURSEMENT

- Use a wire verification service or confirm wire instructions match account details on seller's disbursement authorization form
- Require a copy of a voided check with a disbursement authorization form
- Require that a check be sent for seller proceeds rather than a wire

FILE FRAUD REPORTS

- IC3.gov
- Local law enforcement
- State law enforcement, including the state bureau of investigation and state attorney general
- Secretary of state for notary violations

FIGHT FRAUD WITH INDUSTRY PARTNERS

- Educate real estate professionals in your community, such as county recorders, real estate agents, real estate listing platforms, banks, and lenders
- Host educational events at the local or state level
- Alert your title insurance underwriter of fraud attempts

SHUTTERSTOCK / TANYA ANTUSENOK

FRAUD AND FORGERY RED FLAGS

Fraud is generally defined as false representations of facts to induce another to rely on them, with the intention to deceive.

The various schemes invented by fraudsters are often difficult to navigate. Some involve cyber fraud, email hacking or other information security issues. Awareness, vigilance and due diligence are key to detect and avoid fraud traps. While your work as a settlement agent is done outside your relationship with First American, we think you might find the following information helpful in your business.

Closing/Settlement agents are entrusted with Non-Public Personal Information (NPI) and should be diligent in protecting that information. By taking some simple security measures, you can help reduce exposure to threats and loss of sensitive information.

- Use secure email or a secure portal when sending messages or attachments containing NPI.
- Pay close attention and be aware of possible Phishing emails.
- Avoid public Wi-Fi to improve network security
- Keep software, including security patches, up to date.

Distressed Properties/Foreclosure Issues

Properties involved in financial distress or mortgage defaults are often targeted by fraudsters.

RED FLAGS:

- Recently recorded Assignment of Mortgage/Security Deed/ Deed of Trust.
- Recently recorded Release, Reconveyance, Trustee Deed, Substitution of Trustee, or other foreclosure document.
- Request to rush the opening of a file and/or closing of a transaction.

LEARN MORE
www.firstam.com/cybersmart

First American Title™

www.firstam.com/agency

FRAUD AND FORGERY RED FLAGS

Wire Fraud

Fraudsters use compromised email accounts to deceive financial institutions, and their customers, in order to misappropriate funds through unauthorized wire transfers.

RED FLAGS:

- Changes to wiring instructions (language, timing, amounts, etc.).
- Wire account name payee differs from the principals on the transaction.
- Request to wire funds to foreign or unknown bank.
- Instructions sent by email, especially when sent late in the transaction process, when verification would be more difficult – at month end, for example.
- Instructions marked as *rush, urgent* or *secret.*

Closing Fraud Schemes

Free-and-clear properties are a target for fraudsters because of the obvious equity with no outstanding mortgage. Elder principals are also at a higher risk of abuse, as they may not be as transaction and tech savvy. In some cases, elder principals may be unaware that their property is being transferred.

RED FLAGS:

- Property has no mortgage to be paid.
- Seller(s) positioned to receive large cash out.
- Sales price on non-owner occupied property is *too good to be true*.
- Purchase contract has confusing counter offers, amendments or unusual terms.
- Property is immediately being transferred to another party after close of escrow.
- Use of a Power of Attorney (POA) to sign documents.
- You are unable to speak to, or communicate directly with, a principal at the request of another party (the principal is "*out of the county*" or "*very busy*").
- Chain of title reveals a recent purchase, or *flip*, indicating a sale price significantly different from the previous and/or current transaction.
- Recent transfer of title for *no consideration*.
- Parties involved are demanding a rush closing.
- Unexplained disbursements from seller proceeds. (Payments or repairs with no bill or documentation provided).
- Sales/Loan proceeds are paid to someone other than the borrower(s) or seller(s) of record.
- Principal appears disoriented, demonstrates a lack of understanding or unable/not allowed to speak on their own behalf.
- Change of contact person and/or authorized representative.
- Holder of POA requests funds be disbursed to him/her.

LEARN MORE

www.firstam.com/cybersmart

First American Title™

www.firstam.com/agency

ALTA Outgoing
Wire Preparation Checklist

Date:

File Number:

Company Name/Location:

Section 1	Provide the source of the wiring instructions
☐	I received the initial outgoing wire instructions directly from the **payee in person**. The instructions have not been modified or amended. ***Proceed to Section 2***.
☐	I received the initial outgoing wire instructions directly from the **payee via the United States Postal Service or a known overnight mail or messenger service** and **verified** the accuracy of the instruction by calling the payee at a phone number obtained independently from any phone number shown in the package. The instructions have not been modified or amended. ***Proceed to Section 2***.
☐	I received the initial outgoing wire instructions directly from the payee via fax and verified the accuracy of the instruction by calling the payee at a phone number obtained independently from any phone number shown in the package. The instructions have not been modified or amended. ***Proceed to Section 2***.
☐	I received the initial outgoing wire instructions from the **payee**, which have been modified or amended in writing in person at the following date/time: _____. ***Proceed to Section 2***.
☐	I received the initial outgoing wire instructions directly from the **payee by email** and **verified** the accuracy of the instruction by calling the payee at a phone number obtained independently from any phone number shown in the email. The instructions have not been modified or amended. ***Proceed to Section 2***.
☐	I received the initial outgoing wiring instructions **via a 3rd party** (e.g., attorney, realtor, lender) and have **verified** the accuracy of the instruction by **calling the payee** at a phone number obtained independently from any phone number obtained via the 3rd party. The instructions have not been modified or amended. ***Proceed to Section 2***.

Section 2	Verify instructions received by email or from someone other than the payee
☐	Wire Payee Name:
☐	Wire Amount:
☐	Payee Phone Number:
☐	Source of Phone Number (*never use the phone number included in an email*):
☐	Original Order or Contract:
☐	Secure Portal:
☐	Internet Search:
☐	Other (*describe*):
☐	Name of Person I Spoke With: Date:
☐	Wire Information confirmed. Account and ABA Routing Number, and Account Name match payee in the file. Wire instruction notes indicate correct payment information (e.g., loan number, beneficiary, other information).
☐	Wire Information confirmed. Account and ABA Routing Number match an entry on our company's list of validated wire instructions for common bank payoffs.

Visit the ALTA Website:
https://www.alta.org/business-tools/information-security.cfm

First American Title™

24-Agency-0074

Wire Creator: (Signature) (Date)

(Printed Name)

Wire Authorizer: (Signature) (Date)

(Printed Name)

Section 3		Verify Delivery of Wired Funds
☐	Date Wire Was Sent:	
☐	Date Wire Was Received:	
☐	Name of Person Who Confirmed Receipt:	
☐	Purpose of Wire:	
	☐	Loan Payoff
	☐	Equity Loan Payoff
	☐	Seller Proceeds
	☐	Real Estate Commission
	☐	Other (*describe*):

American Land Title Association
Protect your property rights

ALTA Rapid Response Plan for
Wire Fraud Incidents

Time is of the essence – every second and minute counts. Contact banks, transaction parties, and law enforcement immediately upon discovery.

STEP 1: Alert company management and your internal wire fraud response team. Contact your team according to a pre-arranged plan (group email; group text):

- Owner/Manager
- Accounting/Finance/ Treasurer
- IT/IT Security
- Legal Counsel

STEP 2: Report Fraudulent Wire Transfers to the Sending and Receiving Banks

- Contact the sending bank's fraud department and request that a recall of the wire be sent to the receiving bank because of fraud. Provide the details for the wire.
- Ask the sending bank to initiate the FBI's Financial Fraud Kill Chain if the amount of the wire transfer is $50,000 or above; the wire transfer is international; a SWIFT recall notice has been initiated; and the wire transfer has occurred within the last 72 hours.
- Also call the receiving bank's fraud department to notify them that you have requested a recall of the wire because of fraud. Provide the details for the wire and request that the account be frozen.
- If a client or consumer was a victim and your bank/accounts were not directly involved, your client or customer will need to contact the bank themselves but you may have helpful information to share, too. Coordinate quickly!

STEP 3: Report Fraudulent Wire Transfers and Attempts to Law Enforcement

- Local Police/Sheriff www.policeone.com/law-enforcement-directory
- FBI Field Office www.fbi.gov/contact-us/field-offices
- Secret Service www.secretservice.gov/contact/field-offices

STEP 4: Call the sending bank again to confirm that the recall request has been processed

STEP 5: Inform the parties to the transaction

Contact buyer, seller, real estate agents, broker, attorneys, underwriter, notary, etc., using known, trusted, phone numbers for verbal verification.

If you're unsure about what to say, here's a sample: "There appears to have been [attempted] wire fraud associated with this transaction. We recommend that you review your email security and update passwords and take any other appropriate security measures immediately. For the remainder of this transaction, all communication will occur using known, trusted, telephone numbers."

STEP 6: Review your Incident Response Plan

Determine if you need to update passwords, secure hardware, and review email logs to determine how and when email accounts were accessed.

STEP 7: Consider contacting your insurance carrier(s) and outside legal counsel

STEP 8: If funds were wired out of the U.S., hire an attorney in that country to help recover funds

STEP 9: Document your response using a Response Worksheet

- Customize the ALTA Rapid Response Plan and Worksheet for Wire Fraud Incidents, or create your own
- Assign each step to an appropriate person/entity
- Track progress through to completion or resolution
- Retain Response Worksheet for future reference/update

STEP 10: File a complaint with the FBI's Internet Crime Complaint Center (IC3)

Visit www.ic3.gov and provide the following information:

- Victim's name, address, telephone, and email
- Financial transaction information (e.g., account information, transaction date and amount, who received the money)
- Subject's name, address, telephone, email, website, and IP address
- Specific details on how you were victimized
- For Business Email Compromise (BEC) events, copy email header(s) (www.alta.org/file.cfm?name=HowToCopyEmailHeaders)
- Any other relevant information that is necessary to support the claimant

Wire Fraud Incident

Response Worksheet

Date/Time of Incident: _____

Date/Time Incident was Discovered: _____

Incident Discovered By: _____

Amount: _____

Transaction Affected (File Number): _____

Client/Parties Affected: _____

Systems/Devices Affected: _____

Response Coordinator: _____

Step	Task	Assigned To
STEP 1	**Alert Company Management** *Notes:*	
STEP 2	**Report to Sending and Receiving Banks** *Notes:*	
STEP 3	**Report to Law Enforcement** *Notes:*	
STEP 4	**Confirm recall request was processed by Sending Bank** *Notes:*	
STEP 5	**Inform clients/parties affected** *Notes:*	
STEP 6	**Review Incident Response Plan for next actions** *Notes:*	
STEP 7	**Contact insurance carrier(s) and legal counsel** *Notes:*	
STEP 8	**Hire counsel in country where funds were wired** *Notes:*	
STEP 9	**Document your response** *Notes:*	
STEP 10	**File a complaint with the FBI** *Notes:*	

Stop • Think • Verify

Wire Fraud

If you're on fire — Stop, Drop and Roll. If you detect the spark of a fraudster attempting to divert funds on your file — ***Stop, Think and Verify.***

Now, more than ever, you should be wary about fraudulent attempts to divert funds from your file or your client's. With many people working from home, the opportunity for fraudsters to infiltrate, what used to be a mostly in-person type of transaction, has now moved online via the internet and webcams.

> Fraudsters are getting good at creating trojan horses; do not let them behind the walls of your deal!

With several money transfers in a single transaction, fraudsters are wise to opportunities to infiltrate communication and divert bank funds. Stay vigilant and recognize the signs.

Red Flags Include:

- Changes to wire instructions (language, timing, amounts, etc.). Implement additional callback procedures using a known, independently verified telephone number.
- Instructions marked as rush, urgent or secret.
- SWIFT Codes. Only international accounts require Society for Worldwide Interbank Financial Communication Codes. These are not typical for domestic accounts or credit unions.
- Instructions sent by email, especially when sent late in the transaction process when verification would be more difficult, e.g., at month-end or hours before close.
- Requests to wire funds to an unknown, new, or foreign bank.
- Instructions with strange explanations like, *"I don't know what the international exchange rate will be, so let me just overfund."*

Additional Resources

Protect Your Real Estate Transaction
https://www.firstam.com/ownership/protect-your-transaction

These are only suggestions and best practices when corresponding with customers and should only be used as a secondary, after the Title Agent has followed their own internal business procedures related to fraud, information security and claims protocol. These red flags are not meant to replace or supersede any of the instruction from Agency Management.

AMD: 09/2021

First American Title™

www.firstam.com/cybersmart

SECURITY FOR MOBILE DEVICES

No matter which platform you're on, the security of your mobile device is crucial. Smart devices store emails, messages, family photos, and personal information. We also download apps, enabling us to shop online, manage finances and post to social media.

Protect mobile devices with the same defenses used to protect your computer.

1. **Antivirus**
   Install a reputable antivirus application for your smart device.

2. **Lock Your Screen**
   Use a numerical/alphabetical pin, fingerprint or facial recognition settings to unlock your screen and enable automatic lockout based on inactivity.

3. **Updates**
   Keep your operating system and applications updated to ensure the most recent security patches are installed.

4. **App Downloads**
   Only install apps from your device's official store or platform. Read reviews, note number of downloads, and check out authenticity of the developer.

5. **Permissions**
   Do not grant applications permissions they do not need. For example, does a mobile banking app really need access to your photo gallery?

6. **Storage**
   Some mobile devices have secure folders to store sensitive applications and data. Consider using this feature or encrypt the entire device.

Cybersecurity Incident Response Plan Template

Step 1: Preparation

Consider the following opportunities to prepare your company before an incident occurs:

1. Create a complete **IT Cyber System Overview** of your company's IT blueprint/architecture showing connectivity to understand all of the assets which could be at risk (e.g., in-house hardware, software, and data; phone system; online and cloud-based software and data; mobile devices; remote workforce)
2. Create a complete **IT Personnel Overview** for your company to document who is responsible for each of the various components of the computer systems (e.g., title production systems, email/messaging systems, network security) whether they be employees, consultants, or a Managed Service Provider (MSP)
3. Conduct a **Business Impact Analysis** to determine how a loss of access to hardware, software, or data for each system would impact everyday business
4. Establish a **Business Continuity Plan** to recover your daily business operations effectively after a limited-impact event (e.g., virus contained to one computer; power outage at a branch office; compromised system, device, or account)
5. Contact your insurance carrier(s) to determine if **Cyber Insurance Coverage** is in place or available to cover one or more types of potential cyber incidents and any requirements for an incident to be covered by the policy
6. Contact your attorney to identify requirements, draft notifications, and be prepared to distribute those notifications as documented in your company's **Breach Notification and Reporting Requirements** as applicable to the jurisdiction(s) where you do business or where your clients and customers reside[1]
7. Establish a **Disaster Recovery Plan** to recover from a catastrophic event (e.g., ransomware attack, network breach, email compromise, natural disaster affecting entire operation)
8. Establish **Roles & Responsibilities** for key functions in response to a cybersecurity incident (e.g., person responsible for coordinating response, talking with legal counsel, cyber insurance carrier, talking with customers, talking with media, talking with regulatory agencies, talking with law enforcement)
9. Create a **Crisis Communication Plan**, including:
    - Contact information for internal and external stakeholders
    - Prewritten communications for internal and external stakeholders
    - Strategy for maintaining confidentiality and privileged communications

Step 2: Analysis and Detection

1. Monitor critical systems and alerts as defined in the **IT Cyber System Overview** (e.g., logon failure/success, firewall logs, computer logs)
2. Ensure alerts are monitored in accordance with your **Business Impact Analysis**

[1] See also: CSR Data Breach Reporting: https://urisq.com/privacy-regulations/
See also: https://www.perkinscoie.com/images/content/2/4/246420/Security-Breach-Notification-Law-Chart-Sept-2021.pdf

- Refer to **IT Personnel Overview** to help monitor systems for alerts.
- Refer to **Roles & Responsibilities** and **Crisis Communication Plan** for reporting and escalation processes.

3. If an incident is detected, determine if the scenario is a limited-impact event or a catastrophic event

Step 3: Containment, Eradication, and Recovery

1. Containment strategies are designed to remove active attackers from your network and contain a cyber incident (e.g., isolating the affected devices, system, or network; resetting passwords; disabling accounts)
2. Eradication strategies are designed to remove the threat or vulnerability before restoring operations to full functionality (e.g., remove unauthorized access; consider disconnecting backup process to maintain quality backup; clean the affected machine(s) or device(s); rebuild machine(s) as needed; consider removing all access for specific users)
3. Recovery strategies are designed to restore systems back to normal operations as documented by a **Disaster Recovery Plan** and **Business Continuity Plan**

Step 4: Lessons Learned & Post-Event Activity

1. Documentation of Incident
   - Document incident and resolution including lessons learned and any changes made.
   - Report to proper stakeholders as reflected in **Breach Notification and Reporting Requirements**
2. What did we learn?
   - What went well?
   - What went poorly?
   - Did we maintain confidentiality and privilege during the incident and response?
3. What actions should we take?
   - Review policies
   - Review/update processes (e.g., password strength and updates; user and security access levels; periodic testing of backup restoration; data retention)
   - Review/update technology for additional features, potential upgrades, or replacement (e.g., software, hardware, services)
   - Review Roles & Responsibilities for adjustments (e.g., business, technology, third-party consulting assistance)
   - Review insurance coverage
   - Consider additional staff training