Beyond Fake Sellers: Protecting Landowners, Lenders, and Equipment Buyers from Modern Threats

Josh Bailey
General Counsel
Farm Credit of Western Arkansas

DISCLAIMER

This presentation is intended for educational purposes only and should not be construed as formal legal advice. The information provided herein is meant to offer general insights into legal and title issues relevant to lenders.

The views and opinions expressed are solely my own and do not necessarily reflect the views or positions of my employer, AgSouth Farm Credit.

For specific legal advice tailored to your situation, please consult with a qualified legal professional.

AG TRANSACTIONS ARE UNIQUELY VULNERABLE

Rural and agricultural deals are a ripe target for fraud:

- **Large tracts with absentee owners.**
- **High transaction values.**
- **Fewer repeat players at the closing table.**
- **Complex title histories.**
- **Equipment and chattel financing.**
- **Remote and digital transactions.**

WHERE DOES FRAUD IN THE TRANSACTION APPEAR?

Roadmap of Potential Fraud

Fraud in the Chain of Title — "Who Actually Owns This?"

Fraud in the Loan Application — "Who Is The Lender Actually Lending To?"

Fraud at the Closing Table — "Where Is The Money Going?"

Common Thread: Fraudsters succeed by exploiting the trust relationships, time pressures, and routine processes that characterize real estate and lending transactions.

Normalcy bias is a cognitive bias which leads people to disbelieve or minimize threat warnings. Consequently, individuals underestimate the likelihood of a disaster, when it might affect them, and its potential adverse effects.

FRAUD IN THE CHAIN OF TITLE — "WHO ACTUALLY OWNS THIS?"

Fake Sellers or Title Pirates

The "fake seller" or seller impersonation scheme has become the most widely discussed fraud type in the title insurance industry. The basic mechanics are straightforward:

- The fraudster identifies a property, typically vacant land, owned by an individual or entity with limited local presence.
- Using publicly available information (tax records, county assessor data, recorded deeds), the fraudster gathers enough detail to pose as the owner or an authorized representative.
- The fraudster contacts a real estate agent or responds to an inquiry about the property, representing themselves as the owner. They often propose an attractive below-market price and emphasize a desire for a quick cash closing.
- The fraudster provides identification documents: either forged government-issued IDs, stolen identity credentials, or fraudulently obtained real IDs using assumed identities.
- If a remote closing is arranged, the fraudster may use a notary who is either complicit or deceived, or may exploit remote online notarization (RON) platforms where identity verification can be circumvented.
- At closing, the fraudster executes the deed, receives the sale proceeds via wire transfer, and disappears.

FRAUD IN THE CHAIN OF TITLE — "WHO ACTUALLY OWNS THIS?"

Real Estate Seller Impersonation Red Flags

- Seller is unreachable by phone and communicates exclusively by email or text
- Seller is willing to accept a significantly below-market price
- Seller insists on a rush closing and resists standard due diligence timelines
- Property is vacant land with an out-of-state owner
- ID presented at closing shows signs of alteration or the individual does not match known descriptions
- Seller recently obtained a new government-issued ID (visible issuance date)
- No existing mortgage or lien on the property (no payoff to a known lender)

FRAUD IN THE CHAIN OF TITLE — "WHO ACTUALLY OWNS THIS?"

Fraudulent Deeds Recorded in Public Records

Fraudulent deed recording involves the fabrication and recording of a deed instrument in the county records without any legitimate transaction occurring. The forged deed purports to convey title from the true owner to the fraudster or an accomplice. Once recorded, the fraudulent deed creates a cloud on title that the fraudster can exploit in several ways:

- Using the apparent ownership to obtain mortgage financing against the property
- "Selling" the property to an innocent purchaser
- Recording additional instruments (such as deeds of trust or assignments) to create a more complex paper trail that obscures the fraud

Georgia clerks of superior court are generally not required to authenticate or verify the validity of instruments presented for recording. *Moore v. Hartford Acci. & Indem.* Co., 102 Ga. App. 514, 516(1960). O.C.G.A. § 44-2-14; O.C.G.A. § 15-6-6. The clerk's function is ministerial: if the instrument meets the formal requirements for recording (execution, attestation, notarization as applicable), it will be accepted and indexed. This means that a well-crafted forged deed will enter the public record without any gatekeeper review of its substantive legitimacy.

FRAUD IN THE CHAIN OF TITLE — "WHO ACTUALLY OWNS THIS?"

Fraudulent Deeds In Public Records -Red Flags

- Notary acknowledgements that don't match the county or state where the deed was purportedly executed
- Notary commissions that are expired
- Seller "has their own notary" – CONTROL THE NOTARY
- Witness signatures that appear in the same handwriting as grantor
- Formatting or language that does not match standard conveyancing practices for the jurisdiction
- Conveyance from an owner who has held the property for a long time with no prior activity, suddenly transferring to an unfamiliar LLC or individual
- Transfers for nominal consideration followed quickly by a mortgage or resale of significant value
- Multiple instruments recorded in rapid succession
- Quitclaim deeds used in what should be arm's-length transaction
- Multiple conflicting wills or probate documents recorded

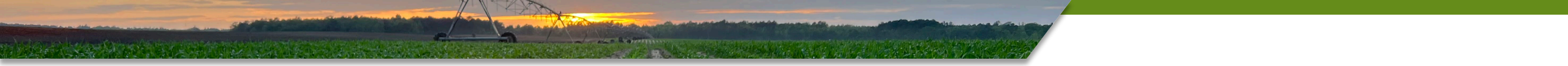
FRAUD IN THE CHAIN OF TITLE — "WHO ACTUALLY OWNS THIS?"

Impact of Forged Deed

Not Valid To Transfer Title: "[A] forged deed is a nullity and vests no title in a grantee. As such, even a bona fide purchaser for value without notice of a forgery cannot acquire good title from a grantee in a forged deed, or those holding under such a grantee, because the grantee has no title to convey." *Brice v. SSA NE Assets*, LLC, 376 Ga. App. 113, 118 (2025).

Requires Action to Remove: Under O.C.G.A. § 23-3-40, a proceeding quia timet can be brought to cancel any forged or iniquitous deed that casts a cloud over the complainant's title or subjects them to future liability or annoyance, where such cancellation is necessary for the owner's perfect protection Similarly, O.C.G.A. § 23-3-61 allows a proceeding in rem to establish title and remove any adverse claims or clouds on the title, including forged deeds . O.C.G.A. § 23-3-61.

Time Limit to Seek to Action to Remove: Equity requires that such remainderman shall proceed within a reasonable time to have such false, fraudulent, or forged deed removed as a cloud upon his title. *McDaniel v. Bagby*, 204 Ga. 750, 756 (1949). "[A]n action . . . seeking the cancellation of an alleged fraudulent deed, must be brought within seven years from the time the fraud became known." *Serchion v. Capstone Partners, Inc.*, 298 Ga. App. 73, 75. (2009). The seven years do not commence until the fraud is or should have been discovered. *Jones v. Spindel*, 239 Ga. 68, 68 (1977). Beyond statutory limitations, equity imposes its own standards through the doctrine of laches. Laches may bar a claim if there is an unreasonable delay in asserting rights, particularly when such delay prejudices the opposing party or renders the ascertainment of the truth difficult. Factors considered include the length of the delay, the sufficiency of the excuse for the delay, the loss of evidence, and whether the claimant acquiesced in the adverse claim. *Whitfield v. Whitfield*, 204 Ga. 64 (1948).



FRAUD IN THE CHAIN OF TITLE — "WHO ACTUALLY OWNS THIS?"

Protections from Fake Sellers / Forgery

- **ALTA 14 Future Advance Endorsement** protects lenders making future advances against fraudulent transfers impairing lien position
- **ALTA 11 Endorsement** (Mortgage Modification Endorsement) protects lender when modifying a loan if there is concern about intervening fraudulent conveyances
- **ALTA Homeowner's Policy (Enhanced OTP)** provide coverage for forgery that occurs after the policy is issued.
- **New ALTA 49 and 49.1** adds post-policy fraud coverage to a residential standard policy, either new or existing. This gives the standard policy the same fraud protection already included in the ALTA Homeowner Policy.
- Customized Endorsement to a lender policy may protect against post policy fraud and endorsements
- "Title lock insurance" is not true insurance but is a service that claims to monitor your deed to protect you against title fraud.

FRAUD IN THE CHAIN OF TITLE — "WHO ACTUALLY OWNS THIS?"

Virtual Vendor / Imposter Dealer

We have seen a rise of equipment 'fake sellers' that have the following scam pattern:

- Fraudster builds a convincing dealer site or marketplace presence using a real dealer's name, photos, and inventory listings copied from other sites.
- Sometimes the real dealer has no online sales presence, which the scammer exploits (buyers assume the website is real).
- Below-market pricing (or "need it gone this week"), often with a story: estate sale, downsizing, inventory liquidation.
- "We have multiple interested buyers," pressure to act quickly.
- Phone calls may route to voicemail first, then the scammer calls back selectively, helping them avoid angry victims and control the script.
- Buyer is pushed to wire funds (sometimes same day), then is ghosted and equipment never arrives.
- If a bank flags a mismatch between seller name and receiving account, criminals may use money mules / LLCs to make the recipient look plausible.

FRAUD IN THE CHAIN OF TITLE — "WHO ACTUALLY OWNS THIS?"

Virtual Vendor / Imposter Dealer Red Flags

- Price materially below market for model, hours, condition, location.
- Seller insists on wire/ACH only, resists escrow, or refuses in-person inspection.
- "We can ship anywhere" but can't provide credible pickup location, yard address, or verifiable inventory context.
- Domain / email feels "close enough," also newly created sites impersonating legitimate businesses.
- Communication control: won't answer live calls, calls back later, avoids video walkarounds.
- Wiring instructions change late in the process.

FRAUD IN THE LOAN FILE — "WHO IS THE LENDER ACTUALLY LENDING TO

ID Theft

- **Synthetic and Stolen Identities:** Synthetic identity fraud involves the creation of a fictitious identity using a combination of real and fabricated personal information: for example, a real Social Security number (often belonging to a minor, deceased person, or individual with limited credit history) combined with a fictitious name and date of birth. The synthetic identity is built up over time with credit accounts and a credit history, then used to obtain a significant loan before disappearing.
  - **Data Breach –** personal information stolen from hacked databases and sometimes put on dark web
  - **Phishing and Social Engineering –** Fraudster trick victims into revealing Social security numbers and other sensitive information
  - **False Identify;** criminals combined real and fake data to create a new identity that passes lender scrutiny to apply for a loan
- **Straw Borrowers:** A straw borrower is a real person who applies for credit on behalf of another individual who cannot qualify or who wishes to conceal their involvement. In the agricultural context, straw borrower arrangements may be used to circumvent lending limits, avoid regulatory scrutiny, or obtain credit that the true beneficiary could not access due to poor credit history or existing defaults. Often used in money laundering or to conceal a disqualified buyer.

FRAUD IN THE LOAN FILE — "WHO IS THE LENDER ACTUALLY LENDING TO

Rise of AI-Generated Fraudulent Documents

- **AI-Generated Fraudulent Documents:** The most concerning recent development in loan fraud is the use of artificial intelligence tools to generate highly convincing fraudulent documentation. AI can now produce realistic tax returns, bank statements, pay stubs, and financial statements that are difficult to distinguish from legitimate documents through visual inspection alone. Key characteristics of AI-generated fraudulent documents include:
  - Pixel-perfect formatting that matches genuine documents from specific institutions
  - Internally consistent financial data that passes basic reasonableness checks
  - Appropriate use of institution-specific logos, fonts, and formatting conventions
  - Metadata that may mimic legitimate document properties
- The traditional reliance on the "look and feel" of submitted documents is no longer sufficient.
- Verification must increasingly rely on independent confirmation: direct contact with the issuing institution, cross-referencing with third-party data sources, and analysis of document metadata and digital signatures.

FRAUD IN THE LOAN FILE — "WHO IS THE LENDER ACTUALLY LENDING TO

Red Flags ID Theft Mortgage Fraud

- Unverifiable employment or excessive job hopping
- Unrealistic borrower income for the job type
- Large, inconsistent bank deposits
- Discrepancies in personal information
- Title commitment or UCC record search shows undisclosed liens or unresolved legal issues
- Multiple loans for different properties within a short period
- Undisclosed relationships between the buyer, seller, and appraiser
- Use of a power of attorney or mail-away/virtual closing in unusual circumstances.

FRAUD IN THE LOAN FILE — "WHO IS THE LENDER ACTUALLY LENDING TO

Steps to Verify Identity of Buyer/Borrower

- Government photo ID, examined in person (**Gold Standard**)
- Use of a trusted intermediary when necessary: If the borrower is known to a lender, real estate agent, or prior counsel, obtain a direct confirmation from that person (not relayed through the borrower. **Be Careful with This!**
- Electronic identity verification (IDV) services: Use third-party tools that compare the borrower's identity against credit bureau or public records data (name, SSN, address history, phone, email).
  - Typical vendors used in financial transactions include LexisNexis, Experian, or similar services.
- Live video confirmation (when in-person is not possible)
  - Shows their ID on camera
  - States their name, date, and purpose of the transaction
  - Confirms key facts of the loan

FRAUD AT THE CLOSING TABLE — "WHERE IS MY MONEY GOING?"

Wire Fraud and Business Email Compromise

- **Email Account Compromise:** The most common vector involves the compromise of an email account belonging to one of the transaction participants: typically the real estate agent, the closing attorney, or the buyer. The attacker gains access through phishing, credential stuffing, or exploitation of weak passwords and lack of multi-factor authentication. Once inside the account, the attacker monitors email traffic, identifies pending closings, and waits for the optimal moment to intervene: usually when wire instructions are about to be sent.
- **Email Spoofing:** In some cases, the attacker does not compromise a legitimate account but instead creates a spoofed email address that closely resembles a real participant's address. Variations may be as subtle as a single transposed letter, an added character, or a different top-level domain (e.g., .co instead of .com). Under the time pressure of an imminent closing, recipients frequently fail to notice these discrepancies.
- **The Fraudulent Wire Instruction:** Whether through a compromised or spoofed account, the attacker sends what appear to be legitimate updated wiring instructions, typically claiming a last-minute change of bank or account number. The message often mimics the formatting, signature block, and tone of the impersonated party. If the recipient follows the fraudulent instructions, the funds are wired to an account controlled by the attacker and are typically moved through a series of transfers or converted to cryptocurrency within hours.
- **Limited Options for Recovery**: Under Georgia law, specifically , O.C.G.A. § 11-4A-202, once a wire transfer is executed in accordance with a bank's agreed-upon security procedures, recovery by the sender becomes extremely difficult. If the bank and its customer have agreed to verify the authenticity of payment orders using a security procedure, a payment order is effective as the order of the customer, even if it was unauthorized, provided that the security procedure is commercially reasonable, and the bank accepted the payment order in good faith and in compliance with its obligations under the security procedure and any relevant agreements or instructions.

FRAUD AT THE CLOSING TABLE — "WHERE IS MY MONEY GOING?"

Wire Fraud Red Flags

- A lender receives an email from "TitleCompany123@gmail.com" (instead of their usual domain)
- Spoofing an email address (e.g., jdoe@fãrmcredit.com instead of jdoe@farmcredit.com)
- Sending urgent, last-minute wiring instruction changes
- Using high-pressure language: "This must be done immediately to avoid closing delays."
- Common excuse: "We had a security breach and had to change our account."
- Spelling or grammatical errors in wiring instructions
- Emails sent outside of normal business hours (e.g., 2 AM)
- Mismatch between the account name and transaction details
- Funds directed to a personal or overseas account
- Title company or attorney office phone numbers that don't match public records (Google, state bar directories)

FRAUD AT THE CLOSING TABLE — "WHERE IS MY MONEY GOING?"

Wire Fraud Response: The Critical First 24 Hours

- When fraudulent wire instructions are followed, the window for recovery is extremely narrow. Practitioners should be prepared to take immediate action:
- Contact the sending bank immediately and request a wire recall or hold.
- File a complaint with the FBI's IC3 (ic3.gov) and request activation of the Financial Fraud Kill Chain, which can freeze funds in domestic accounts. https://www.ic3.gov/complaaint/default.aspx
- Notify the receiving bank and request a hold on the account.
- Contact local law enforcement.
- Notify the title insurance underwriter and all parties to the transaction.
- Preserve all email communications, headers, and metadata for forensic analysis
- Notify your E&O Carrier
- Do not communicate with "fraudsters"

FRAUD AT THE CLOSING TABLE — "WHERE IS MY MONEY GOING?"

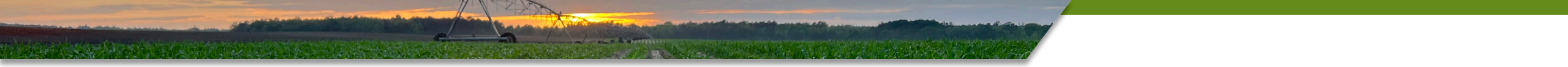
Preventative Procedures For Wire Fraud

- **Callback Verification:** The single most effective countermeasure against wire fraud is mandatory callback verification of all wiring instructions using a phone number obtained independently of the email communication. This means calling a number from the firm's existing records, a publicly listed number, or a number verified at the outset of the transaction: never a number provided in the same email that contains the wire instructions.
- **Standardized Wire Instruction Procedures:** Firms should establish and communicate clear policies: wire instructions are provided once at the outset of the transaction and will not change. Any purported change in wire instructions should trigger heightened verification, including in-person or video confirmation of the request.
- **Email Security Measures**
  - Domain-based Message Authentication (DMARC), SPF, and DKIM email authentication protocols
  - Email encryption for communications containing financial information
  - Staff training on identifying phishing attempts and spoofed email addresses
  - Automated warnings on emails originating from outside the organization
- **Client Education:** Closing attorneys and lenders should affirmatively warn clients about wire fraud at the earliest stage of engagement. Many firms now include wire fraud warnings in engagement letters, on their websites, and in separate written advisories provided to every client. For agricultural clients who may transact infrequently and be less familiar with these risks, this education is particularly important.

VERIFICATION MINDSET

Professional Obligations

- Georgia places primary responsibility for real estate and many secured-transaction closings in the hands of attorneys. This structure is justified in part because self-regulating attorneys provide enhanced competence, accountability, and control over high-risk transactions involving title, funds, and third-party representations. The lawyer's gatekeeping role is meant to reduce fraud, protect parties, and maintain public confidence in property and secured-lending systems.
- **Rule 1.1 – Competence**
  - Lawyers must provide representation with the legal knowledge, skill, thoroughness, and preparation reasonably necessary for the representation, including verifying key facts that affect client decisions.
- **Rule 1.3 – Diligence**
  - A lawyer must act with reasonable diligence and promptness, which in transactional practice includes meaningful verification of material facts, identities, documents, and payment instructions before advising a client to proceed.



VERIFICATION MINDSET

Always on Guard

- The common thread across all the fraud categories examined is that bad actors exploit trust, speed, and routine. The antidote is not the elimination of trust, which would make transactions impossible, but the systematization of verification so that trust is confirmed rather than assumed. This requires a shift in mindset from "verify when something seems wrong" to "verify as a matter of course."
- **Firm-Level Implementation:** For law firms implementing a fraud prevention framework requires attention to several areas:
  - **Written policies and procedures.** Document verification protocols, wire transfer procedures, identity confirmation requirements, and incident response plans. Policies that exist only as informal practices are difficult to enforce consistently and impossible to demonstrate to insurers and courts.
  - **Staff training.** Conduct regular training on fraud recognition, current threats, and firm procedures. Training should include all staff who handle closings, wire transfers, and loan processing, not just attorneys and senior personnel.
  - **Technology investment.** Implement email security (DMARC, MFA), document verification tools, and title monitoring services. The cost of prevention technology is trivial compared to the potential losses from a single successful fraud scheme.
- **Insurance review.** Review professional liability, cyber liability, and title insurance coverage to confirm that fraud-related losses are addressed. Understand policy exclusions and reporting requirements.
- **Incident response planning.** Develop and rehearse a response plan for wire fraud, identity theft, and other fraud events. The first hours after a fraud is discovered are critical, and a well-prepared team can significantly improve the chances of recovering funds and limiting liability.

APPENDIX A: KEY RESOURCES

Fraud Prevention and Control

- **FBI Internet Crime Complaint Center (IC3):** ic3.gov
- **FBI Financial Fraud Kill Chain Overview** ic3.gov/media/y2020/psa20201008
- **American Bankers Association Wire Fraud Guidance** aba.com/banking-topics/financial-crimes/wire-transfer-fraud
- **CISA (Cybersecurity & Infrastructure Security Agency) Phishing Guidance** cisa.gov/phishing
- **American Land Title Association (ALTA) Title Fraud Resources** alta.org/title-fraud
- **Georgia Bureau of Investigation Cyber Crime Unit:** gbi.georgia.gov
- **IRS Form 4506-C (Request for Transcript of Tax Return):** irs.gov
- **Financial Crimes Enforcement Network (FinCEN):** fincen.gov
- **FTC Identity Theft Resource Center** identitytheft.gov

APPENDIX B: SAMPLE WIRE FRAUD WARNING LANGUAGE

Wire Fraud Alert

The following is sample language that may be adapted for use in engagement letters, closing instructions, and client communications. This language is provided for educational purposes and should be reviewed by counsel before implementation.

IMPORTANT NOTICE REGARDING WIRE TRANSFER FRAUD: Criminals are actively targeting real estate transactions by intercepting email communications and sending fraudulent wire transfer instructions. Before wiring any funds, you must confirm all wire instructions by calling a verified phone number for the intended recipient. Do not rely on contact information provided in an email. Our firm will never send changes to wire instructions by email. If you receive an email appearing to be from our firm that requests a change to previously provided wire instructions, do not follow those instructions and contact our office immediately at [phone number]. We will not be responsible for losses resulting from fraudulent wire instructions that are not verified by telephone callback.

APPENDIX C: SELLER IDENTITY VERIFICATION CHECKLIST

Procedures

- Confirm the name and address of the record owner through independent title search
- Obtain and compare government-issued photo identification
- Verify identity through independent channels: contact the owner at a phone number or address obtained from tax records, prior correspondence, or other independent sources
- For out-of-state sellers, consider requiring an in-person appearance before a **notary known** to the closing attorney or title company
- Review the property tax payment history: sudden changes in mailing address or payment method may indicate impersonation
- Check the issuance date on the seller's identification: recently issued IDs in the context of a quick-sale transaction are a significant red flag
- For entity sellers, verify the entity's existence and authority through the Secretary of State's office and obtain certified organizational documents
- Confirm that the seller has knowledge of the property consistent with ownership: tax history, prior use, neighboring properties, access points
- Document all identity verification steps in the closing file