2024

Sued for Wire Fraud

CERTIFID

Table of Contents

Legal Disclaimer

The information provided in this report does not, and is not intended to, constitute legal advice: All information, content, and materials available in this paper are for general informational purposes only and may not constitute the most up-to-date information, legal or otherwise. The information provided herein is intended for educational and training purposes and is in no way meant to be a fully reflective or exhaustive analysis of the topics discussed herein. This report is not intended to be operationalized as an independent means of lowering risk, avoiding, or mitigating liability or expense relating to any of the topics covered herein.

Readers of this report should seek legal counsel to obtain advice with respect to any of the topics covered herein. Readers of this report should refrain from acting based on information in this document without first seeking legal advice from counsel in the relevant jurisdiction. Only your individual lawyer can provide assurances that the information contained herein–and your interpretation of it–is applicable or appropriate to your situation.

The content in this report is provided “as is;” no representations are made that the material is error-free, timely, accurate, or could lead to any benefit to the reader.

Executive Summary

There’s been an alarming rise in real estate wire fraud, and it’s having a devastating impact on buyers, sellers, and the industry as a whole. Those victimized by such scams are turning to the courts to seek damages after their life savings or business liquidity is stolen by scammers.

With this increasing pressure in and out of court, real estate firms can no longer be passive observers. The fallout from a single fraudulent transaction can lead to lost business and a tarnished reputation that takes years to rebuild. This means that the onus is on professionals to understand their risks and take action to prevent fraud before it happens.

This report delves into the intricacies of legal liability when funds are mistakenly wired to fraudulent bank accounts, suggesting that agents, brokers, and title companies are increasingly held accountable if a consumer loses money — but may not have success in recovering from banks or insurance companies when funds are diverted from their escrow accounts.

It will also advocate for stringent security measures, education, and collaboration between industry professionals to mitigate the risk of wire fraud and the wake of litigation and reputational risk that follows.

By understanding today’s legal landscape and taking proactive steps, professionals can better safeguard clients and their businesses. In the pages to follow, we’ll provide the necessary insights and recommendations to navigate this complex issue effectively.

I. Introduction: The New Reality of Real Estate Wire Fraud

Unveiling the impact and evolution of wire fraud from 2021-2024

I. Introduction: The New Reality of Real Estate Wire Fraud

> ***Cybercrime rings have taken aim at U.S. real estate transactions at an alarming rate.***
>
> *- Katie Pierce, Assistant to the Special Agent In Charge U.S. Secret Service Global Investigative Operations Center*[1]

As a real estate title agent or escrow attorney, could you afford the risk of a $250,000 judgment? How about two? These questions might seem hypothetical, but they underscore the real and growing threat of real estate wire transfer fraud.

Full Panic Mode

Consider the chilling experience of real estate attorney Nicole Quinn, which epitomizes the pervasive threat professionals now face.[2]

With just enough financial and personal information, a scammer posing as her client convinced Quinn and her paralegal to transfer $240,000 in client funds to the impersonator's account.

"I went into full panic mode," Quinn admits. "I called everyone… the state bar… the FBI… the police… I think they could all hear in my voice how distraught I was."

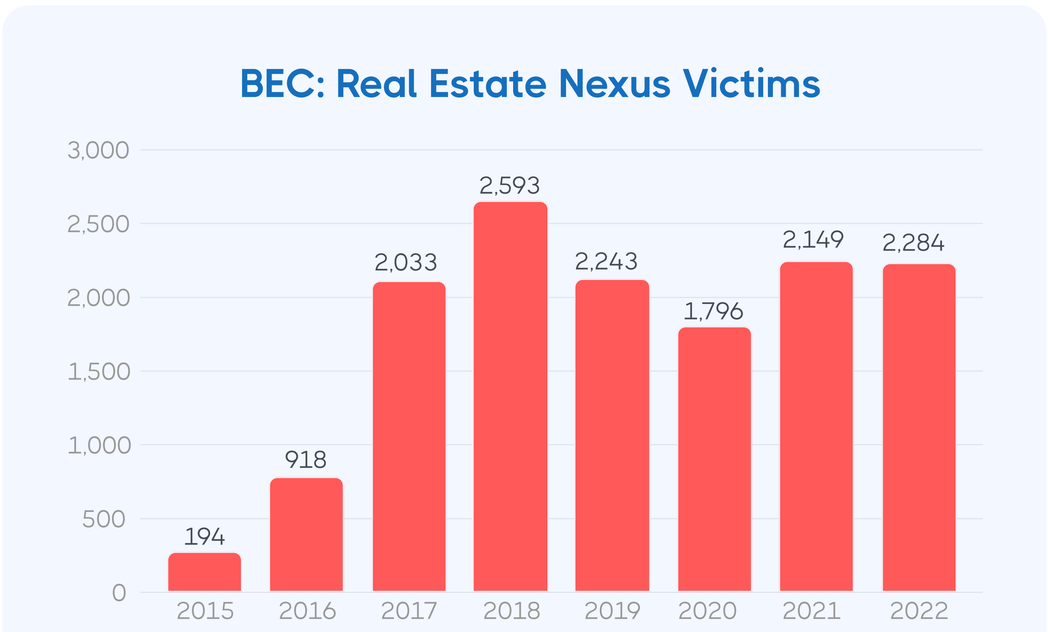
Big Problems With Business Emails

Fortunately, Quinn caught the error in time to retrieve her client's money, but other attorneys and firms aren't always so fortunate.

For criminals, routine business email is an easy access point.[3] The FBI's cybercrime division reports Business Email Compromise (BEC) accounts for **23% of all reported cybercrime losses.**[4]

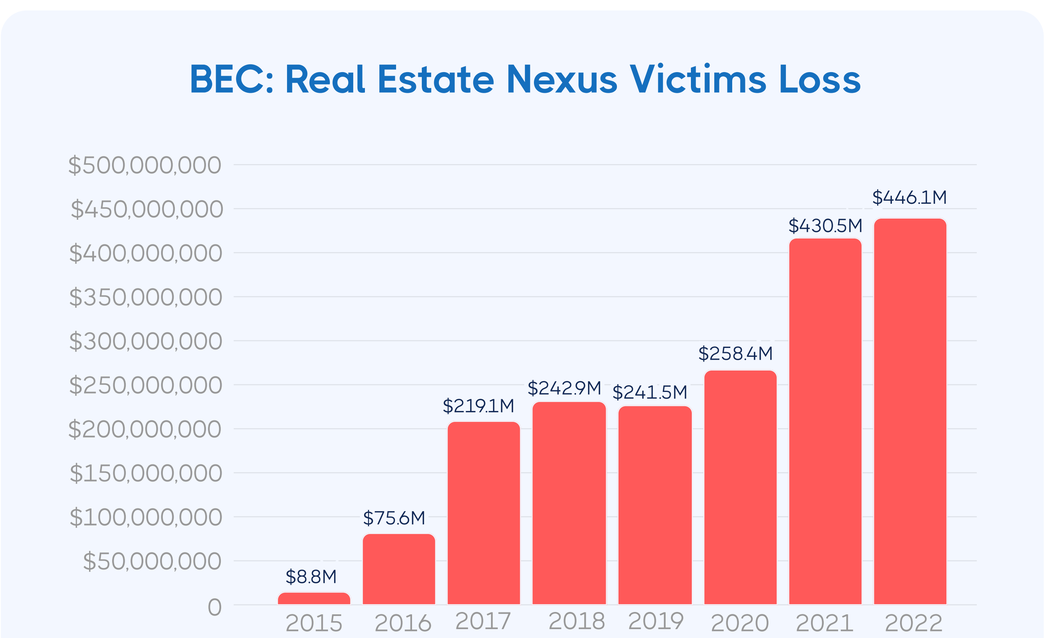
In 2023, the FBI investigated **21,489 BEC complaints**, with adjusted losses totaling over **$2.9 billion.**[4]

Real estate wire fraud is the new reality…



Source: F.B.I. IC3 Report, March 2024

… And the losses are staggering.



Source: F.B.I. IC3 Report, March 2024

Real Estate: A Lucrative Target

Of the $2.9 billion lost in business email compromise, **$446 million (or 17%)** of all scams involve **real estate**.[5]

Real estate transactions are a top target for fraud due to increasingly large sums of cash transferred between parties. The **median consumer loses $106,557**[6] in buyer down payments or seller net proceeds. Imagine you're on the hook for this loss—and shouldering the cost of your own defense in court.

The Silent Epidemic

Most of these cases will never be reported, much less go to trial, but they'll exact a hefty toll—costing real estate professionals significant sums in out-of-court settlements.[3]

As real estate wire fraud continues to climb, companies will need to pay close attention to potential legal liability in order to prevent drain on financial resources.

Who's Targeted and How It Happens

Buyers

Impersonation of title agency to provide fraudulent bank details to the buyer.

Scammer typically reaches out well before payment is required in an average closing process, making it less likely the fraud will be discovered until the buyer is at the closing table.

Sellers

Impersonation of a property owner in a fraudulent listing. Often called seller impersonation.

Scammer typically obtains property and owner identity details from public records, and creates an elaborate backstory to enable a quick remote sale.

Title and Law firms

Impersonation of lender-provided mortgage payoff instructions during a closing process.

Scammer intercepts and replaces payoff instructions to the closing agent. Title professionals miss the fraud because verification processes can be time-consuming and susceptive to manual error.

Source: 2024 CertifID State of Wire Fraud[6]

Contributing Factors: Why Real Estate?

- The pandemic-era housing boom led to soaring prices.
- Inflation is driving high interest rates, tightening housing inventory.
- There's extreme pressure to close transactions quickly.
- Digital currency and real-time payments accelerate money laundering.
- Property information is easy to obtain through data breaches and public records.
- Real estate wiring instructions are increasingly sent via email.
- Unprotected email systems are ripe for phishing-enabled breaches.
- Multiple parties in a transaction provide spoofing opportunities.
- Large sums of money are transferred in a single wire.
- Lack of transactional familiarity exposes buyers and sellers.

2024 Update: Patterns and Precedents Emerge in Courtrooms

Our investigation began with ***Sued For Wire Fraud***,[3] where we delved into the emerging real estate security threat and legal theories of liability for the resulting losses.

Through analysis of 100+ real estate wire fraud cases, it's become clear that title companies, law firms, banks, and real estate professionals may bear potential liability if client funds are diverted to fraudulent accounts.

This liability arises from legal theories such as:

Negligence:

Companies owe clients a "duty of care"—to educate consumers about wire fraud, clearly and securely communicate wiring instructions, and protect personally identifiable information.

Deceptive Business Practices:

Divergence between a business's representation and the actual service it provides, particularly when these discrepancies result in significant failures beyond reasonable expectations, can lead to heightened legal consequences.

Breach of Contract:

Contracts for escrow services may be oral, written, or implied. Parties must clarify the nature of the client relationship and reasonable business expectations to prove breach of terms.

Breach of Fiduciary Duty:

Agreeing to accept and disburse funds places a fiduciary obligation on real estate parties, requiring careful examination of shared information, technology, and processes.

Even though it's criminals who are orchestrating the business email compromise scams, recent court decisions suggest that the professionals involved in a real estate transaction are required to do more to protect consumers from wire fraud scams or face a potential court judgment for damages.

Over the last four years, fraudsters have become even more brazen in their attacks, prompting the courts to piece together more definitive standards of liability by looking outside of real estate fraud cases to draw upon well-established theories of duty and liability.

Expanding upon our previous work, we now scrutinize the evolving landscape of legal liability, combing through hundreds of pages of recent legal documents and decisions to analyze specific court opinions, trends, rulings, and key takeaways. Legal bright lines are emerging as it relates to liability for wire fraud losses, as title and escrow companies continue to bear more of the responsibility to protect the funds in their custody and mitigate the risk of a consumer falling victim to a scam.

By staying informed and proactive, real estate professionals put themselves—and their customers—in the best possible position to decrease the surface area of risk.

II. The Blame Game: Banks and Insurance Companies Pivot from Liability

II. The Blame Game: Banks and Insurance Companies Pivot from Liability

Exploring financial institution and insurance company liability in wire fraud cases

II. The Blame Game: Banks and Insurance Companies Pivot from Liability

"Almost any reasonable person would assume that a person who committed a fraud should be responsible for loss associated with the fraud. But fraudsters are not always easy to find, and not always easy to hold financially responsible."

- *Elisabeth Feeney, Cochair of the Payment Systems Litigation Subcommittee*[8]

Lawyers gearing up to take on banks in wire fraud cases must understand the ins and outs of Uniform Commercial Code Article 4A.[9]

What is UCC Article 4A?

UCC Article 4A governs the rights and responsibilities of parties involved in electronic funds transfers.

Who falls under its scope?

The article governs not only the big banks, but also smaller financial institutions, businesses, high-net-worth individuals, and payment processors.

What's missing from UCC Article 4A?

Within the UCC Article 4A framework, certain procedural and security requirements are missing. Notably, there's:

- ✕ No mandate for account matching;
- ✕ No duty to vet new account openings;
- ✕ No requirement to identify, monitor, or report suspicious account activity.

> Parties whose conflict arises out of a funds transfer should look first and foremost to Article 4A for guidance in bringing and resolving their claims.
>
> - ***Approved Mortgage v. Truist***[10]

Other Legal Theories in Wire Fraud Cases:

- State Consumer Protection Acts
- Breach of Bank Agreements
- Negligent Misrepresentation
- Unfair & Deceptive Conduct
- Aiding & Abetting
- Duty of Care

When your client loses money to fraud, what options are available for recourse?

In cases where the perpetrator cannot be identified, is it possible to allocate responsibility for the loss to the insured banks, which facilitate the transfer of funds?

In short, the courts are not in your favor. As we discovered in our case analysis, if your organization is suing a bank, it doesn't matter whether you are a consumer or real estate company—**you may lose**.

Commercial Court Cases

Let's take a look at nine landmark cases involving wire fraud and liability of financial institutions and other entities.

1. Approved Mortgage v. Truist [10]

> ***"Parties whose conflict arises out of a funds transfer should look first and foremost to Article 4A for guidance in bringing and resolving their claims."***

The plaintiff pursued recovery under Article 4A and common law negligence. The court ruled that under Article 4A, the reimbursement claim failed due to lack of privity (a direct relationship between the parties involved in the transaction). The court also noted that Article 4A of the UCC covers issues of bank liability and security procedures, leaving no room for additional negligence claims under common law. The case was dismissed without prejudice, as the purpose of Article 4A is to provide clear rules for banks in electronic transfers on behalf of customers.

2. Fragale v. Wells Fargo [11]

> ***"It is at least arguable that the plaintiff, rather than Wells Fargo, was in the best position to prevent the harm he allegedly suffered."***

The plaintiff transferred $166,054.96 to a fraudlent account after he received an email from a party falsely claiming to be his title company. In court, he contended that Wells Fargo should be held liable and enforce identity verification for significant withdrawals from new accounts.

However, the court disagreed, deeming such a duty was overly burdensome for banks. They also emphasized that the absence of a relationship between the bank and Fragale, along with the extensive regulation of the banking industry, made it inappropriate to impose a new common law duty on the bank to protect against wire fraud. Consequently, the plaintiff faced blowback, with the court suggesting they could have taken preventive measures to avoid harm.

3. Star Title Partners v. Illinois Union Insurance Co. [12]

> ***"Star Title made no attempt to verify the authenticity of CMS's alleged wire transfer instructions pursuant to its internal procedures."***

Star Title's insurance claim for deceptive transfer fraud was denied. As a mortgage lender, Capital Mortgage Services was not a "customer, client, or vendor," so the fraudulent communication fell outside policy requirements. Further, Star Title failed to call to authenticate wire information according to their standard operating procedures.

4. King v. Wells Fargo[13]

> ***"A plaintiff must demonstrate that the losses sustained were the foreseeable consequence of the defendant's deception."***

Wells Fargo invoked ***Chapter 93A*** of the Massachusetts General Laws, setting a high burden of proof. The courts concluded that the plaintiff's loss was caused by a third-party criminal who absconded with the funds, not "unfair and deceptive conduct" of Wells Fargo. This case emphasizes that the scammer — not the bank — was the proximate cause of the plaintiff's loss.

5. Helms v. Hanover Insurance[14]

> ***"The exclusion's plain language… states that no coverage is provided for claims based on or arising out of the theft, stealing, conversion, or misappropriation of funds."***

A mishap in a buyer cash-to-close real estate transaction led to a couple wiring $120,000 to fraudsters. They sued their broker and real estate agent, alleging negligence. Seeking defense from Hanover Insurance, the agent's E&O policy claims were flat-out denied, based on the terms of the insuring agreement. The agent's E&O insurance was never designed to cover wire fraud, containing unambiguous "fund misappropriation and fraudulent transfer policy" exclusions, ultimately causing the agent's bankruptcy.

6. Tracy v. PNC Bank[15]

> ***"PNC Bank's role here was limited, and those limitations were set forth in the account-holder agreement with its customer."***

Following the court's determination that PNC Bank hadn't breached its implied duty of good faith, Mr. Tracy refocused his claim on post-wire-transfer negligence. The court's summary judgment affirmed PNC acted in accordance with its consumer agreement and there was no account name matching duty owed.

7. Nicklas v. Professional Assistance LLC[16]

> ***"Not all federal circuits appear certain that the lack of adequate security measures equates to an 'unfair' act… Although some states allow recovery for failure to notify of a data breach."***

The plaintiffs' claims lack assertion of fraudulent practices, thus not qualifying for relief under the Wyoming Consumer Protection Act, which targets "deceptive marketing practices." The court also questioned why the FTC didn't file the consumer claim.

8. Thuney v. Lawyers Title of Arizona[17]

> ***"Chase released the funds to fraudsters even though Chase knew about the alleged fraud. Plaintiffs have stated a plausible aiding and abetting claim."***

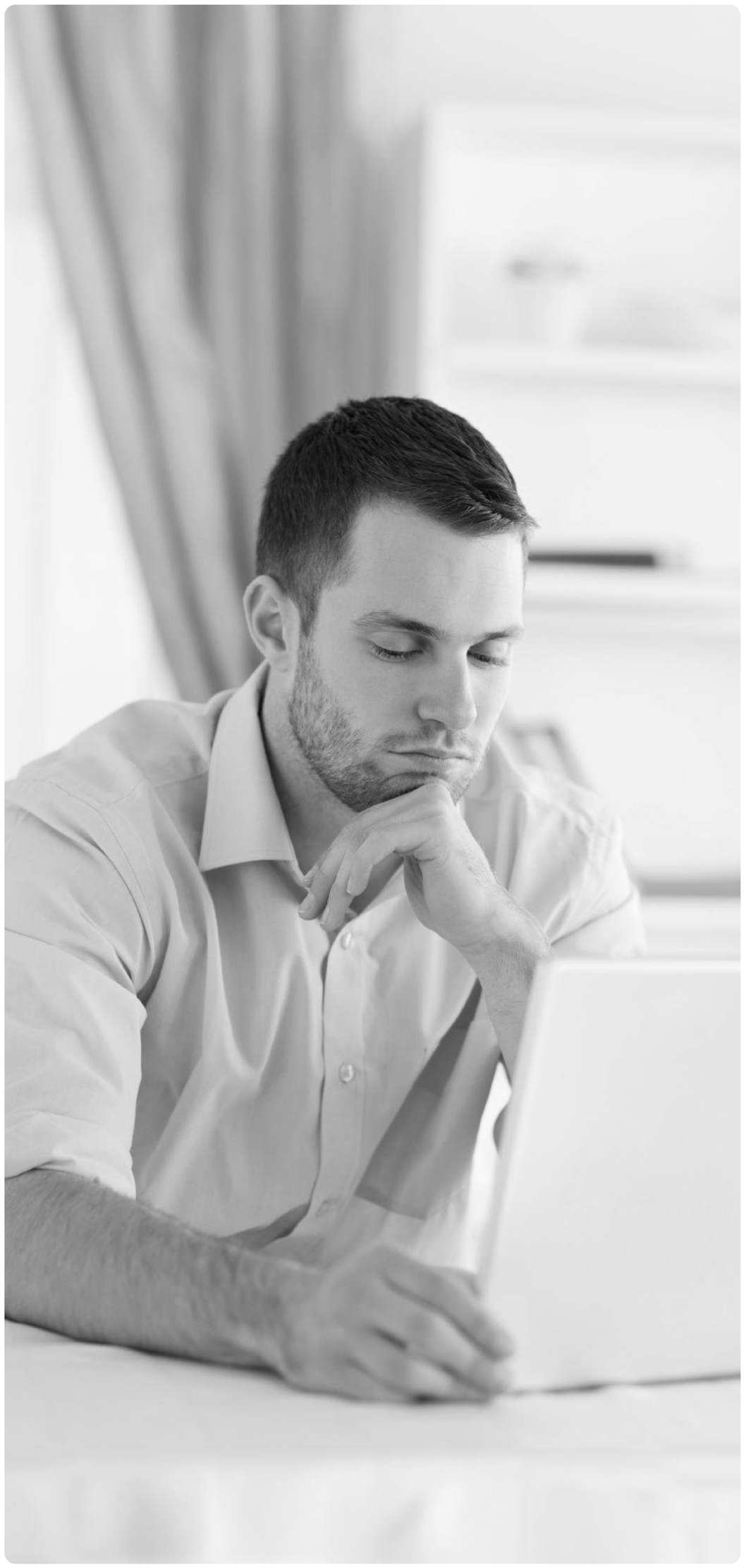
Chase argued that Article 4A governs their alleged release of funds to fraudsters. However, claims based on actions outside the funds transfer process, like aiding and abetting, aren't preempted. Plaintiffs' claims aren't dismissed, but must meet plausibility standards.

9. Authentic Title Services v. Greenwich Insurance[18]

> ***"The policy provided that the insurer had no obligation to pay any sums… for any claim… based upon or arising out of the actual or alleged theft."***

Authentic Title Services sought to reclaim $480,750.96 from their insurer after falling victim to an email spoofing scam, resulting in the transfer of real estate loan funds to a fraudulent account.

The court found there was no need for interpretation beyond plain language doctrine and no ambiguity in exclusion 14(a) stating the policy does not cover "claims related to stolen funds."



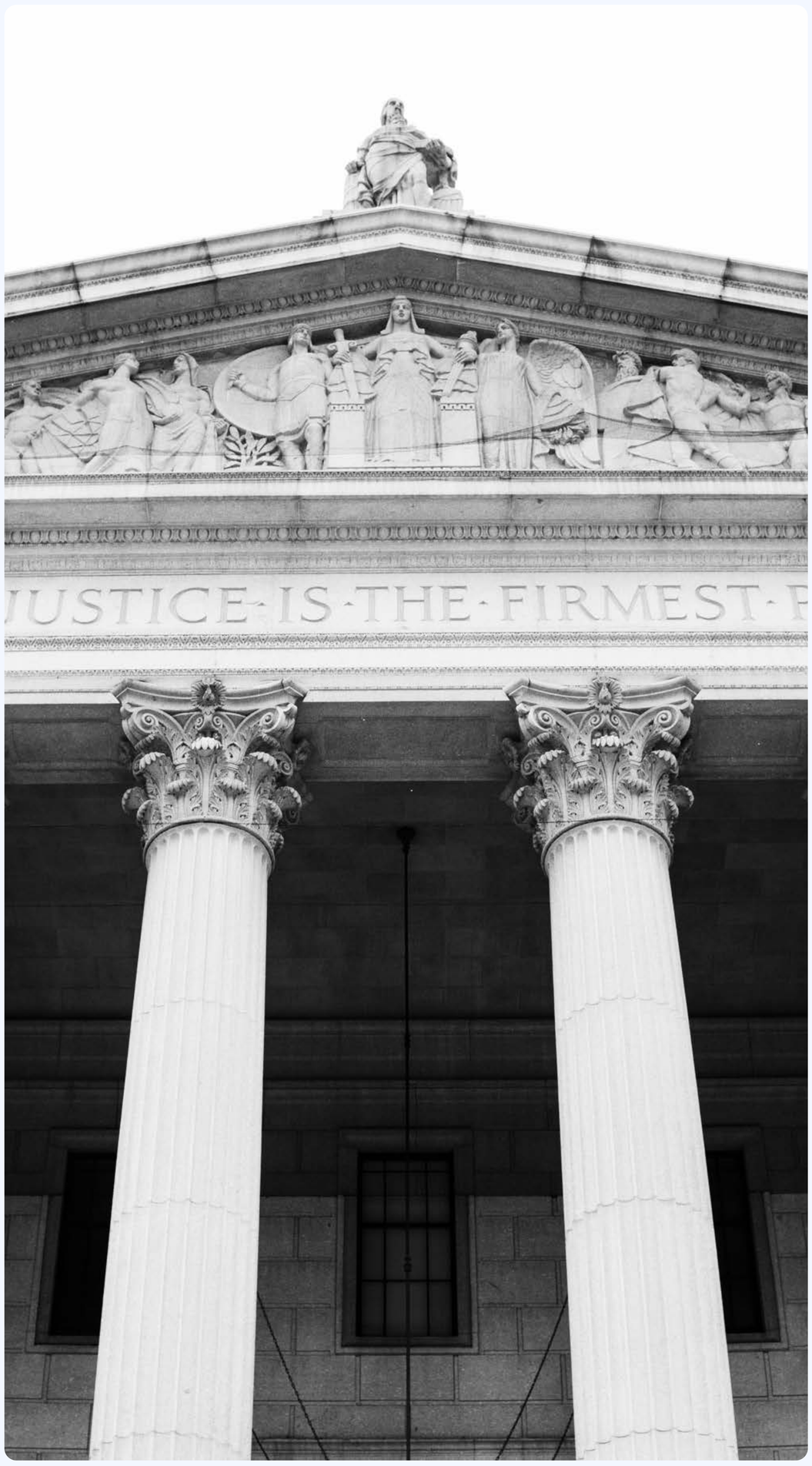
Conclusions

When a client is tricked into sending[1] funds to a fraudulent account, title and escrow companies often ask, "Will my bank or insurance company help me out or share in some of the risk exposure?"

The findings from the above court cases provide a harsh response to this question:

There is no practical way to hold a bank responsible for wire fraud losses if the account holder or authorized representative initiated the transfer. Likewise, unless there is specific insurance coverage for stolen funds and ***all requirements*** to coverage in an insuring contract are satisfied, a claim for damages will be denied.

Litigation involving financial institutions and liability for wire fraud losses boils down to the court's deference to **UCC 4A** and the determination of the relationships and duties that exist between parties, as spelled out in deposit and consumer agreement terms—and intentionally written in the bank's favor.



Under UCC 4A, banks are protected against wire fraud losses, provided they adhere to commercially reasonable security procedures—which include the verification of account ownership or authority before funds are transferred out of an account. This legal framework ensures that banks are shielded from liability as long as they follow the established protocols set forth by UCC 4A to authenticate wire transfers and detect fraudulent activity.[9]

If you attempt to sue the bank, the bank simply needs to demonstrate that the account holder or authorized representative requested the transfer—either online, in person, digitally, or over the phone. So long as it was the account holder or authorized representative requesting the transfer, **the bank is not liable for the loss**.

These court cases reflect what **an uphill battle** plaintiffs face when seeking expert witnesses that are qualified to testify as to industry best practices or uncover proof of bank negligence, deceptive practices, or misconduct.

The cases we analyzed ran the full gamut of possible factual scenarios that could have led to some form of bank liability including irregularities in account activity, failure to respond and render assistance after being notified of an unlawful transfer, failure to verify the status of funds before returning them back to a victim, and the failure of suspending or canceling accounts with unusual activity.

No matter the scenario or how shocking the fact pattern that was pleaded, **the courts seem to move quickly to provide summary judgment in favor of banks, time and time again.**

When could a bank be liable?

Feasibly, a bank ***could*** potentially be held liable if the person requesting the transfer is a bad actor and the movement of money can be traced back to flawed verification measures or a security failure that allowed hackers into the bank's system—though we have not seen any such cases come to light. A bank may also be held liable if they have actual "knowledge" of a mismatch between the beneficiary's name and account number and still process the transaction, as made evident in *Studco Building System U.S., LLC v. 1st Advantage Federal Credit Union*[28]. In this case, Studco was tricked into sending a large payment to a personal account of an unwitting money mule even though the ACH payment included a business name and specifically referenced a commercial transaction as part of the transfer.

Despite receiving alerts and having actual knowledge of potential fraud due to a mismatch between the account name and number, and placing a commercial payment into a personal account, the bank processed the transfer. The court ruled that the bank's failure to act on these red flags made it liable for the fraudulent transaction. While this decision may suggest that banks may have some sort of liability for name matching, it is contrasted by other decisions where courts have held that banks may solely rely upon account number matching and essentially disregard any notice of name mismatches.

As it stands, **common sense practices**—like monitoring irregular account activity, calling senders prior to transferring the money, or responding promptly to a freeze attempt after a transfer has initiated—**are not codified into law** and therefore, may not be admissible in court.

Though the notion that banks should do more to protect consumers from wire fraud has elevated to the state attorney general level in recent months[26], there is **no indication** that the conversation will ultimately translate to a heightened standard of care for wire transfers or actual liability in court.

The courts have held—and will likely continue to hold—that banks are simply completing a transaction, and the proximate cause for the loss is the fraudster who committed the crime. Since the fraudsters often abscond with the money and suing the banks rarely succeeds, the blowback often falls to the sender of funds—a title, escrow, or other real estate company (and sometimes even the consumers themselves)—for failing to exercise their due diligence in verifying where the money was headed.

As for insurance company liability? If you suffer a loss and file a claim against your errors and omissions policy, it will likely be denied unless the loss is specifically covered in the insurance policy and you satisfy all requirements to coverage. The courts will apply the four corners rule and examine the specific contractual language regarding covered claims, terms and conditions, and exclusions.

All too often, policies are written in a way that would seemingly cover a loss, but the steps title and escrow companies must take, and the amount of documentation required, often excludes policy coverage, as they are not able to satisfy all of them. What's more, if wire transfer or social engineering fraud is covered in the policy, it will likely be subject to a significant sublimit of coverage as compared to the overall policy limits, leaving the insured to self-insure any shortfall.

There is a clear, firm precedent set:

Banks and insurance companies will not come to your rescue.
If you're sued for wire fraud, assume you are on your own!

III. Winner and Losers: Recent Legal Battles

III. Winners and Losers: Recent Legal Battles

What legal pleadings reveal about lawyer, agent, broker, and intermediary liability

III. Winners and Losers: Recent Legal Battles

> *"The case presents a novel issue requiring the analysis of who bears the responsibility for escrow fraud that took place in this case."*
>
> - *Hoffman v. Atlas Title*[19]

Courts often empathize with victims of fraud, but deciding who should financially reimburse them for the loss is complicated. The cases involving banks establish that the proximate cause of the wire fraud loss is not the transferring of money itself, but rather the intentional and criminal act of the scammer.

But here's the twist: if you're entrusted with sharing wire instructions and collecting funds for a real estate closing, recent court cases suggest that you could be on the hook for some (or all) of the loss if funds are diverted into a fraudulent account—even if you were not responsible for the transfer of funds.

Legal Framework: A Glossary of Court Terms

Understanding the legal theories used in real estate wire fraud cases serves as a helpful guide for companies and individuals looking to improve communication processes and mitigate security risks.

Here are some common threads:

Breach of Contract

A contract dispute arises when two or more parties disagree over the terms or performance of a contract. Legal remedies may be sought when one party fails to fulfill their obligations, resulting in the other party's financial loss. Specific contractual terms apply.

Burden of Proof

The burden of proof is the responsibility to provide evidence and persuade the court of the truth of a claim or assertion in a legal proceeding.

Breach of Duty

A party that fails to fulfill their obligations as required by law or contract commits a "breach of duty." In real estate wire transfers, all parties involved generally owe a duty to "exercise reasonable care and judgment" as another person with similar knowledge, experience, and role.

Comparative Fault

Comparative fault is a legal principle used in certain states to determine responsibility for damages according to each party's level of fault in a lawsuit.

Breach of Fiduciary Duty

To make a breach-of-fiduciary-duty claim, you need to show three things: first, that there was a duty due to a *fiduciary* relationship; second, this duty wasn't upheld; and third, that harm resulted from this failure. Essentially, a breach of fiduciary duty is like a negligence claim with a higher standard of care in that the fiduciary must act in the best interest of the client.

Negligence

Parties that fail to exercise "the level of care that a reasonably prudent person would in similar circumstances," resulting in harm, may be held liable for general negligence. A plaintiff might argue that proper precautions were not taken to prevent fraudulent activities, to verify email addresses, or to take other steps that ensure the security of the transaction.

Negligent Infliction of Emotional Distress

To claim damages under this legal theory, a plaintiff must demonstrate that the defendant's conduct was "extreme or outrageous," "outside the bounds of decency," and is "utterly intolerable in a civilized community."

Plain Language

"Plain language" refers to clear, straightforward communication that is easily understandable to the average person and is the indisputable starting point for the court's analysis of a contract under state law.

Negligent Misrepresentation

Negligent misrepresentation involves providing false information or making misleading statements, which harms another party who reasonably relies on the information.

Punitive Damages

Punitive damages are awarded to punish a defendant for egregious behavior and deter similar conduct in the future. They may be sought if the actions of banks, title companies, or real estate agents were considered reckless or intentional and resulted in loss.

Consumer Court Cases

Let's take a closer look at six landmark cases involving escrow and title agent liability.

1. Hoffman v. Atlas Title

> ***"The escrow agent is a fiduciary agent for both parties to a purchase agreement… Although the economic-loss rule sweeps widely, it does not preclude all tort claims for economic damages."***[19]

Atlas Title, despite past breaches, sent unencrypted wire instructions, leading to interception and a loss of $289,772.19 for plaintiffs Hoffman and McMahon. The court dismissed breach of contract, due to the absence of a material contract, but allowed negligence and breach of fiduciary duty claims to proceed.

Key Takeaways:

"The case presents a novel issue requiring the analysis of who bears the responsibility for escrow fraud that took place in this case." The Court of Appeals confirmed that this is, in fact, a "novel" pattern—and there is no clearly defined case precedent in this area of law.

The economic loss rule says: if you have an agreement, and your agreement is clear, and you're harmed, then you're limited to economic losses. Under this legal framework, you can't say, "You've breached my contract—and I'm going to sue you for tort" and layer on the damages.

"Ohio courts have held that escrow agreements do not have to be in writing." Even without an escrow agreement, you may be obligated under breach of contract or fiduciary duty if the buyer loses their savings to wire fraud. The Ohio court holds that escrow agreements need not be formal or in writing, and "may be deemed to exist where there are only closing instructions."

"A plaintiff may pursue a tort claim, if based exclusively on a discreet pre-existing *duty* in tort and not any terms of contract or rights accompanying privity." Even if there wasn't an implied contract, there was at least an implied duty for professional services or fiduciary duty—for which the economic loss of the rule is not going to prohibit plaintiffs from seeking damages in tort. Tacit understandings and implied-in-fact contracts may proceed on counts of negligence, fraud, and breach of fiduciary duty.

2. Mago v. Arizona Escrow & Financial Corp

> ***"Mago waived his breach of contract claim… by failing to timely raise the specific theory… and instructing Arizona Escrow to perform in a manner contrary to the delivery-by-mail provision."***[20]

Mago's email hack led to Arizona Escrow wiring funds incorrectly during a Subway franchise sale. The court dismissed Mago's breach of contract claim, citing untimeliness and failure to follow mailing instructions, awarding $50,000 in attorney's fees to Arizona Escrow.

Despite the outcome, the case raised the question: Did the title company have a breach of fiduciary duty and a standard of negligence?—thus, opening the door for Mago to appeal these unresolved claims in district courts.

Key Takeaways:

This particular case featured a lower burden of proof due to its perceived simplicity. Though Mago presented expert testimony, the court asserted that the legal issue was understandable to laypersons. The transaction—characterized as a simple payment between a single buyer and seller—was "not complex," with the alleged breach stemming from the escrow agent's failure to recognize fraud indicators.

To prove breach of contract, Mago had to show that Arizona Escrow acted outside standard procedures. His claim unsuccessfully centered on a delivery-by-mail provision, which—as it was written, did not explicitly apply to wiring instructions.

Negligent standard of care is a lower threshold. Citing *Maganas v. Northroup, 135 Ariz. 573, 576 (1983)*: "The relationship of the escrow agent to the parties to the escrow is one of trust and confidence." On appeal, the court of appeals affirmed that the superior court did not expressly address Mago's breach of standard of care claim.

Comparative negligence may come into play. Arizona Escrow asserts that Mago failed to notify them about his compromised email account, introduced the imposter's email into the transaction, and instructed them to wire funds as directed by the imposter. Mago contests having prior knowledge of the hack, which the court ruled as a matter of fact for a jury to eventually decide.

3. Cook v. McGraw Davisson Stewart LLC

> ***"Cook failed to demonstrate… whether Defendants' email was hacked by fraudsters [and] whether Defendants' security measures, or alleged lack thereof, fell below the standard of care."***[21]

Plaintiff Cook had to prove defendants breached a duty of care by failing to safeguard his data. As some of the bank liability cases made clear, defendants can sometimes evade liability by claiming *the fraudster* was the "proximate cause of the loss," and shifting the burden back to the plaintiff. Lacking expert witnesses or evidence beyond a National Association of Realtors article warning of the rise in wire transfer fraud, the court required email security expert testimony—and granted summary judgment in favor of the defendant.

Breach of Duty

Negligence

Key Takeaways:

State decisions vary greatly—and when a negligence claim centers on a broker's "failure to maintain proper email account security," expert witnesses may be required to establish a standard of care and that a breach of such standard occurred. Offering stark contrast to the Arizona appeals court opinion in the Mago case, the Oklahoma court determined, "the average juror is unlikely to be familiar with industry standards for email security that one in broker and company's position would take, as well as whether failure to adopt such standards caused client's injury."

The case failed to pass summary judgment without expert testimony establishing both standard of care and a negligent security breach.

4. Wheeler v. Clear Title Company Inc.

> ***"Nevada does recognize a claim for negligent infliction of emotional distress, but under limited circumstances not present here."***[22]

Wheeler sued Clear Title Company for emotional distress due to a fraudulent wire transfer. Though the claim was brought in good faith, the court ruled that Wheeler failed to prove Clear Title's conduct was "extreme and outrageous, outside all possible bounds of decency." This case also highlights the importance of understanding state laws. In Nevada, there are separate title and escrow licenses. Because the escrow company handled the funds, the title company owed no duty to notify the plaintiff about the risk of wire fraud. The courts ruled in favor of the title company partly because the plaintiff sued the wrong party.

Key Takeaways:

A duty can exist even before a contract is signed. Clear Title tried to argue they owed no duty until the contract was formally signed—15 minutes after the funds had been unknowingly transferred to a fraudster. The courts disagreed, stating, "this interpretation would make the contract created by the escrow instructions meaningless."

What constitutes "reasonable duty of care" cannot be assumed. In the absence of expert testimony stating otherwise, the courts concluded the title company's only duty was to "safekeep any money that it received directly." There was no duty to ensure the money was transferred to the title company, let alone by a specified timeframe.

Escrow agents do not have a duty to investigate fraud. Though the plaintiff did request help in verifying the wire transfer instructions after the fact—to which the agent replied she'd "check the wires later," as per company protocol—that was deemed sufficient by the courts.

Negligence must directly cause the loss. The plaintiffs argued Clear Title was negligent "because they were [supposed] to work with the buyer in receiving money." However, the court determined the title company's actions (or inactions) did not cause the plaintiff's loss.

Extreme or outrageous conduct is difficult to prove. As distressing as the situation was, the plaintiff was unable to prove that the defendant's conduct directly caused the emotional distress because they were not responsible for the receipt of Plaintiff's funds.

5. Bain v. Platinum Realty

> ***"In forwarding wiring instructions, Ms. Sylvia could only have intended that plaintiffs would use those instructions to purchase her clients' house. A question of fact remains for trial."***[23]

Real estate agent Ms. Sylvia forwarded a hacker's altered wiring instructions to plaintiff Mr. Bain, who transferred $196,622.67 to the wrong account. Charges of punitive damages, breach of duty, and negligence were dropped, but the court allowed the negligent misrepresentation claim to proceed and a judgment was issued in favor of the Plaintiffs against the real estate broker and real estate agent involved in the transaction.

Key Takeaways:

Courts prioritize the reasonableness of a plaintiff's reliance over their level of experience. The defendants' attempt to argue for summary judgment was unsuccessful because, although Mr. Bain was an experienced investor, the court believed his reliance on Ms. Sylvia's correct wiring information was justifiable. The court disagreed that "he should have noticed red flags" in the correspondence.

These cases are not all-or-nothing. Tortfeasors can be added, dropped, or share the blame. Initially, the plaintiffs had pursued claims for breach of fiduciary duty, general negligence, and punitive damages against their title company and bank, invoking federal law for jurisdiction. But since the point of loss stemmed from the fraudulent wiring details, the plaintiffs later focused solely on pursuing claims against Ms. Sylvia and Platinum Realty, with summary judgment granted to the other counts.

6. Otto v. Catrow Law LLC

> ***"Petitioners failed to prove a breach of duty [with] specific evidence showing that the respondent had ever received bulletins warning of phishing schemes targeting closing funds."***[24]

Plaintiffs relied on the expert opinion of a lawyer whose disclaimer precluded him from assessing the standard of care in West Virginia. The circuit court also found that alleged insurance bulletins warning against fake wiring instructions were ineffective at proving a breach of duty.

Burden of Proof Negligence

Key Takeaways:

Negligence has a high burden of proof. The burden of proof for negligence was high in this case. According to *Calvert v. Scharf (2005)*, damages arising from the negligence of an attorney "are not presumed," and so the plaintiff "has the burden of proving both his loss and its causal connection to the attorney's negligence."

Standard duty of care claims are more straightforward to prove. Standard of care may have been a more straightforward argument, but under the theory of negligence, the Ottos needed to demonstrate that the defendant's actions "were a departure by members of the legal profession in similar circumstances," directly resulting in their loss. Since the plaintiffs did not take the extra step to produce any evidence that the defendant "actually knew about specific bulletins warning of phishing schemes," they lost the case.

Expert witness contracts must be entered into carefully, as proper jurisdiction matters. While it was the plaintiffs who failed to exercise due diligence in this case, the advice can apply to defendants as well. The circuit court found the hired witness placed a disclaimer in his retainer agreement that expressly stated he was "unable to render an opinion as to West Virginia law."

Navigating Legal Complexities

- A number of legal theories come into play in real estate wire fraud cases, with third parties quickly finding themselves swamped in document requests and depositions. The added pressure of reputational risk and potential media attention compounds the challenges.
- While some defendants appeared to have benefitted from plaintiffs that were unprepared and lacked expert witness testimony to support their legal claims, the path to success for a plaintiff is becoming clearer. Yet court opinions still vary wildly from jurisdiction to jurisdiction. Further laws and legal precedents are necessary to establish duty of care and standard security procedures among real estate parties.
- Nine out of 10 cases filed in the United States end in settlement because the cost of litigation could exceed the amount of damages requested by the plaintiff.[3] Settlements are further propelled by the reputational risk and potential loss of business for the title, escrow and real estate companies involved.

Conclusions

If a buyer loses cash-to-close or a seller loses their net proceeds, there is a strong issue of fact regarding breach of contract—whether that contract is implied or explicit—and breach of duty.

If you're in the position of receiving or sending funds on behalf of your client, you're considered "a legal custodian of funds," which heightens your standard of care as a fiduciary "in a position of trust," in the eyes of the court.

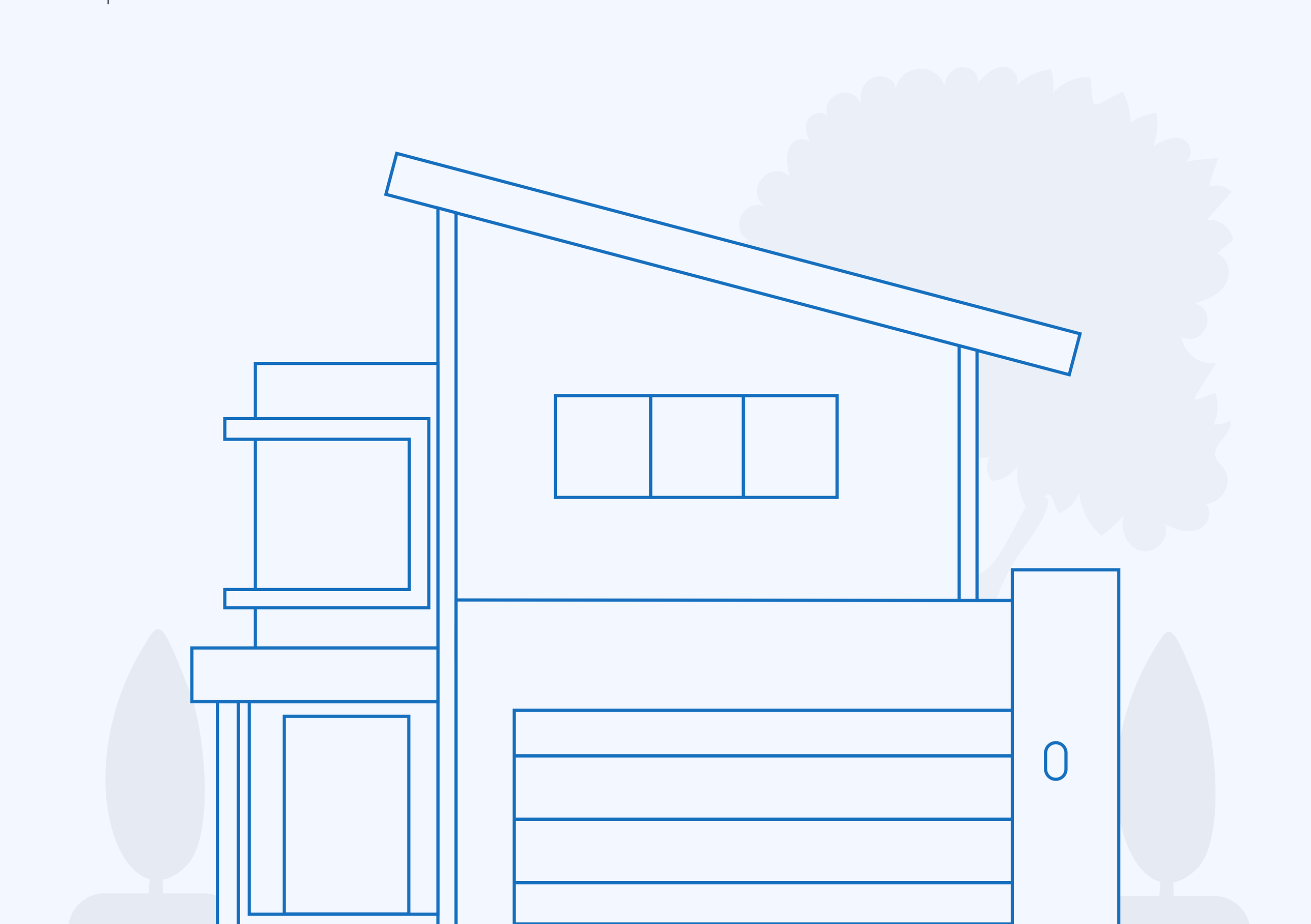
Real estate companies are held to a higher standard of care than banks.

Banks are well protected with UCC 4A. While some may be trying to change that today—as evidenced by a recent case against Citibank[26]—the precedent to protect financial institutions is mostly in place. The courts generally hold title and escrow companies to a higher standard of care in preventing and detecting fraudulent activities in real estate transactions.

Consumer court cases are a jump ball right now.

When a consumer is victimized by a wire fraud, their ability to obtain a legal judgment for monetary damages against the professionals involved in their real estate transaction will depend largely on the facts and circumstances surrounding their loss and the jurisdiction where the case is filed. Violation of state consumer protection act laws appears to be unsuccessful at the moment, but counts of breach of duty, professional negligence, and express or implied contract appear to have the likelihood of raising issues of fact that will require a judge or jury ruling.

There have been cases where it's determined no explicit escrow agreement is needed to apply a heightened negligence standard. Some courts lean heavily into the assumed duty of care argument, while others pick apart steps the consumer could have taken to prevent harm—and find no material point of fact in the claim. As it stands, there is not enough legal precedent or overarching laws to establish what is required of real estate parties in these transactions.



Kenigsberg v. 51 Sky Top Partners*[25] *sets a potential new direction for a real estate company's duty of care.

In the wake of rising consumer cases involving seller impersonation and deed fraud, a pivotal case is already shaping the legal landscape. In *Kenigsberg v. 51 Sky Top Partners, LLC et. al.*, a retired doctor's family land was fraudulently sold and a transferring deed was recorded by a licensed attorney that relied upon a forged document allegedly provided by the property owner. Shortly after the fraudulent land sale was closed, Sky Top Partners commenced construction of a $1.5 million single family residence on the property. Despite the buyer's innocence, the court granted quiet title in the name of Dr. Kenigsberg in order to void the fraudulent deed. In connection with the quiet title judgment, the parties settled the case for an undisclosed amount. A relevant portion of the stipulated order reads:

"The parties, as part of a settlement, hereby stipulate and agree that the Court may enter judgment on the First Count of Plaintiff's complaint [Quiet Title as to Sky Top Partners under Conn. Gen. Stat. § 47-31] confirming that Kenigsberg has a good and marketable title to the Property and that the Power of Attorney and the Monelli deed are declared void and of no effect."

The U.S. District Court of Connecticut affirmed Dr. Kenigsberg's ownership rights, dismissing all other claims such as slander, trespassing, conversion, and forgery. Kenigsberg, through a settlement, received substantial damages, allowing the completion of the house while preserving the buyer's rights.

This landmark decision underscores the responsibility of all professionals involved in a real estate transaction to confirm the identity of buyers and sellers, setting a crucial precedent in combating seller impersonation and deed fraud.

Decisions of wire fraud liability are still subject to individual district court scrutiny. As we await further legal precedent, it's important to take steps to mitigate the risks.

IV. Final Recommendations: Proven Strategies for Risk Mitigation

IV. Final Recommendations: Proven Strategies for Risk Mitigation

How to lock down security and fortify your defenses against wire fraud risks

IV. Final Recommendations: Proven Strategies for Risk Mitigation

> ***Wire fraud has become largely uninsurable in response to the alarming increase in claims. Wire fraud falls outside the scenarios of employee malfeasance and negligence or systems breaches that traditional professional and cyber policies cover. Carriers who serve this space now recommend partnering with technology providers to reduce their risks."***
>
> *- Chad Gaizutis, VP of Stateside Underwriting Agency*[6]

This discussion brings to light the growing risk of real estate wire fraud—as well as the many avenues that you can find yourself in court defending your standard of care should one of your clients become the next target.

If there is a silver lining, it's that federal law enforcement have focused on investigating and helping to recover funds. Notably, the U.S. Secret Service has recovered $210 million in stolen real estate funds since 2019.[27]

However, while law enforcement can certainly help, they can't be the only solution.

Since 2019, the U.S. Secret Service has recovered $210 million in stolen real estate funds.[27]

Despite the success stories, cooperation with these investigations can be time-consuming, costly, and may not always result in a full recovery—and this is just the tip of the iceberg.

The emotional toll on the affected clients and the reputational damage you may suffer as a real estate professional can be significant. Taking a proactive approach to prevent wire fraud incidents protects your clients' interests and your professional integrity.

Let's consider what you can do, right now, to batten down your hatches against the rising tide of bad actors.

Tips To Protect Against Wire Fraud

1. Educate, educate, educate

Notably, in *Mago v. Arizona Title*, the Arizona Supreme Court stated: **"An escrow agent cannot close her eyes in the face of known facts and console herself with the thought that no one has yet confessed fraud,"** and further suggested that scrutinizing and verifying email addresses could be interpreted as a reasonable standard of care.

The failure to spot trickery is a common thread in every single case of wire fraud.

- In Authentic *Title Services v. Greenwich Insurance*, harm could have been mitigated if Maryanski had noticed the email sender was Brittany "Clork" instead of Brittany Clark.
- Similarly, a mimicked seller email address in *Mago v. Arizona Escrow* inconspicuously substituted the letters "rn" for an "m."
- Ms. Sylvia in *Bain v. Platinum Realty* confessed she could've been more diligent in reviewing her contact's email address before passing along fraudulent wiring instructions to her client.
- A series of emails littered with spelling, punctuation, and capitalization irregularities were at issue in *Otto v. Catrow Law*.

Due to an expert witness disclaimer in *Otto v. Catrow*, the plaintiffs were unable to establish the elements of legal malpractice or prove breach of a duty owed to them, but their plea cited that the defendant "should have informed as to the prevalence of wire fraud schemes, and that if an email seemed suspicious, they should take no action until they confirmed, by independent means, that the communication was legitimate."

One of the easiest ways to protect your business from liability is to thoroughly train employees to check spelling and email addresses—and to verify instructions through another method rather than by email alone. Practicing "good digital hygiene" means limiting the amount of personal information that is publicly available, like email addresses, phone numbers, and account information, and therefore limiting the amount of data that can be hijacked by fraudsters.

As a custodian of funds, you are in a position of trust and knowledge. You hold a legal responsibility to not only train employees to spot red flags and follow proper protocols, but to counsel consumers on the risks they may face in light of the increase in scams as well.

2. Update standard operating procedures across your business

As highlighted in *Cook v. McGraw*, businesses sometimes rely on outdated security measures and don't realize how far their wire transfer procedures veer from industry standards and modern security protocols—until it's too late. Demonstrating adequate security measures "according to industry standards" is likely to come up in court.

The series of events in *Wheeler v. Clear Title* brought up a number of pertinent questions: Should the title company have told the client they hadn't sent out wire instructions prior to their in-person meeting? Looked over the alleged instructions? Educated the consumer on the dangers of potential wire fraud? State laws vary, but putting protective procedures in place costs precious little—while saving you a ton of trouble.

What are a few simple steps to lower your risk?

- **Edit Contracts**. Make sure all your contracts are clear and understood by all parties involved.
- **Look into Verification Technology**. Independently verify the phone and account numbers rather than relying on email. In *Authentic Title v. Greenwich*, Maryanski was asked to transfer the funds and confirm only by email—a common tactic used by cybercriminals.
- **Use Multi-Factor Authentication (MFA)**. Human-verify account digits and require passcodes to send funds.
- **Flag Errors**. Report suspicious emails that include spelling, capitalization, or punctuation mistakes.
- **Slow Down**. Rather than going through fast third-party payment processors or crypto platforms, go through standard channels—even if they take a few days extra.

There is no single procedural silver bullet that will save your business across all scenarios. A layered approach works best—putting yourself and your customer in the best possible position with a waterfall of steps to identify wire fraud, report to law enforcement, and quash the threat right away.

3. Reduce your risks with technology

Amid the hustle and bustle of a busy day, human eyes and basic email spam filters often fail to detect subtle email anomalies—but modern security systems will flag them.

Advanced technology can prevent fraud from becoming a costly legal issue. Implementing an advanced perimeter security system will safeguard enterprise data with web content filtering, antivirus scanning, and advanced threat protection.

CertifID is dedicated to fighting real estate wire fraud — providing advanced software, direct first-party insurance, and proven recovery services to protect buy side, sell side, and payoff transactions. CertifID ensures the safe transfer of funds in real estate transactions with robust identity verification, secure sharing of bank details, and verification of payoff and other business-to-business transactions. Since 2018, CertifID has protected over $300B in real estate transactions and recovered $60M in stolen funds.

The use of fraud protection software can help organizations identify suspicious transactions more effectively at scale. In the event of a legal dispute over wire fraud liability, the use of technology can also demonstrate your focus on security and client safety to the courts.

4. Mitigate impact with incident response planning and testing

It's your duty to have an incident response plan and protocols in place to minimize loss. Knowing how to respond effectively and freeze or recover funds potentially allows you to evade court altogether.

As we saw in *Hoffman v. Atlas Title*, cyberthreats need to be taken seriously and tended to immediately to prevent further harm. Two months prior to the transaction at issue in this case, Atlas Title had been notified of hacking and email-spoofing incidents involving the same fraudster.

They contacted their internet technology security provider, but did not believe the hacker obtained any information, despite being in their system for about an hour. As a result, they did not inform their clients, nor did they encrypt subsequent emails containing sensitive information. They also failed to notify the client they had not received the wire transfer on schedule until two days later—at which point, the banks were unable to freeze or recover the funds.

Unannounced, company-wide simulated testing is one way to pinpoint your team's baseline level of fraud awareness and rectify your company's weaknesses before a cybercriminal can exploit them. Incident response planning has become essential for every real estate firm operating in this era of wire fraud risks. Every organization must build a comprehensive understanding of key resources, owners, and steps to be able to act quickly when a fraud occurs.

5. Add first-party insurance to protect you from loss

If you try to sue your insurer for breach of contract, the court will dissect your policy's explicit terms—most often, not in your favor, as we saw with *Helms v. Hanover*.

Know your policy by asking your insurance agent the following questions:

- **What type of bond do I have?** Ensure you have either a Fidelity Bond or an Escrow Security Bond, distinct from a surety bond. Fidelity bonds, also referred to as escrow security bonds, safeguard businesses from losses due to employee theft, dishonesty, or fraud—which is particularly advisable for firms handling client funds or sensitive data.

- **Do I have coverage for wire fraud?** The insurance industry typically does not cover wire fraud. Where you don't have coverage, you'll need a technology partner to cover your liability. Insurance carriers may discount your premium if you have a technology solution for wire fraud.

- **Do I have coverage for owner/seller fraud?** The insurance industry also typically lacks coverage for owner/seller fraud, which is another reason to consider partnering with a tech solution provider.

- **What are my policy exclusions?** Insurance contracts typically have a long list of exclusions specifying coverage limits. For instance, your insurance policy may exclude coverage for situations where there's an unintentional violation of the terms outlined in the title underwriting contract. Look, specifically, for language which excludes claims based on "wire fraud," "social engineering," "breach of underwriting authority," and "negligent failure to prevent dishonest conduct" by any known or unknown non-insured party.

- **If I do have coverage, what are the sub-limits?** Even if wire fraud is covered, it may still be subject to a sub-limit. For instance, socially engineered wire fraud might be covered in a cyber policy with a $1 million limit. However, it could be capped at $100,000 or $250,000 with a higher deductible. Despite having insurance, the insured could still face significant losses. If you have a sub-limited policy, you may consider purchasing cyber gap insurance to help mitigate potential losses that exceed the primary policy limits.

- **What are my conditions precedent to coverage?** While terms are unique to each particular policy, every insurer will have some sort of stipulation that ensures you did your part to prevent fraud. Key conditions could include:

    - Timely reporting
    - Detailed documentation of the incident and proof of loss
    - Full cooperation with the insurer's investigation, providing evidence as requested
    - Meeting any and all agreed-upon conditions set forth by the policy

- **What are my reporting duties?** Most contracts stipulate that you report to the insurer any circumstances that could possibly give rise to a claim within 30-60 days. There may be additional documentation steps you must take in order to secure coverage for your claim.

While employee education and updated security measures are key, adding advanced verification tech and insurance will most effectively close the risk gap and protect your business from potential costly litigation.

Citations

Resources:

1. Yahoo! Finance, *1 in 10 Americans Targeted for Real Estate Fraud*, February 2024.
2. WRAL News - *'I went into full panic mode': Attorney loses $240,000 through wire fraud'*, March 2023.
3. CertifID, *Sued for Wire Fraud Whitepaper*, August 2020.
4. F.B.I., *Internet Crime Report 2023*, March 2024.
5. CertifID, *Infographic: FBI PSA Warns About The Rise in Business Email Compromise (BEC)*, September 2023.
6. CertifID, *2024 State of Wire Fraud Report*, February 2024.
7. CT Insider, *Fairfield case stands out amid sharp rise in real estate scams*, August 2023.
8. American Bar Association, *Escrow Agent Held 100 Percent Liable for Phishing Scam*, October 2023.
9. Cornell Law School, *UCC 4A - Authorized and Verified Payment Orders*, Retrieved May 2024.

Commercial Court Cases:

10. Approved Mortgage Corporation v. Truist Bank, No. 1:22-cv-00633-JMS-TAB, 638 F.Supp.3d 941 (S.D. Ind. Nov. 2, 2022), appeal filed (7th Cir. Dec. 1, 2022).
11. Fragale v. Wells Fargo Bank, N.A., Civil Action No. 20-1667, 480 F. Supp. 3d 653 (E.D. Pa. Aug. 19, 2020).
12. Star Title Partners of Palm Harbor, LLC v. Illinois Union Insurance Company, No. 8:20-cv-2155-JSM-AAS, 2021 WL 4509211 (M.D. Fla. Sept. 1, 2021).
13. King v. Wells Fargo Bank, N.A., Civil Action No. 19-cv-10065-ADB, 2019 WL 3717677 (D. Mass. Aug. 7, 2019).
14. Julie-Anne Helms, et al. v. Hanover Insurance Group Inc, et al., No. CV-20-01728-PHX-DWL, United States District Court, D. Arizona. Signed 08/20/2021.
15. Tracy v. PNC Bank, N.A., No. 2:20-CV-1960, 2024 WL 665227 (W.D. Pa. Feb. 16, 2024).
16. Nicklas v. Professional Assistance, LLC, No. 18-CV-0066-SWS, 2018 WL 8619646 (D. Wyo. Sept. 26, 2018).
17. Thuney v. Lawyer's Title of Arizona, No. 2:18-cv-1513-HRH, 2019 WL 467653 (D. Ariz. Feb. 6, 2019).
18. Authentic Title Services, Inc. v. Greenwich Ins. Co., No. 18-4131 (D.N.J. Nov. 17, 2020), 2020 WL 6739880.

Consumer Court Cases:

19. Hoffman v. Atlas Title Solutions, Ltd., No. 14-23-04, 2023-Ohio-1706, 214 N.E.3d 1271 (Ohio Ct. App. May 22, 2023).
20. Mago v. Arizona Escrow & Financial Corp., No. 1 CA-CV 19-0753, 2021 WL 829259 (Ariz. Ct. App. Mar. 4, 2021).
21. Warren Cook v. McGraw Davisson Stewart, LLC, et al., Case No. 119,216, Court of Civil Appeals of Oklahoma, Division No. 4. Filed April 5, 2021.
22 Sharon Wheeler, an Individual, Appellant, v. Clear Title Company, Inc., a Nevada Corporation, Respondent. No. 83684-COA, No. 84613-COA, Court of Appeals of Nevada, Filed March 24, 2023.
23. Bain v. Platinum Realty, LLC, No. 16-2326-JWL (D. Kan. Feb. 14, 2018), 2018 WL 862770.
24. Otto v. Catrow Law PLLC, 243 W.Va. 709, 850 S.E.2d 708 (2020).
25. Kenigsberg v. 51 Sky Top Partners, LLC, No. 3:23-cv-00939 (D. Conn. Apr. 5, 2024).

Resources:

26. Office of the NYS *Attorney General, Attorney General James Sues Citibank for Failing to Protect and Reimburse Victims of Electronic Fraud*, January 2024.
27. SecureWorld, *Real Estate Wire Fraud on the Rise, Secret Service Investigators Say*, May 2022.
28. American Bar Association. *Liability of the beneficiary bank for cybercrime involving fraudulent funds transfers*, May 2024.

Further Reading Material (Not Cited):

29. American Land Title Association, *Consumers Lose $106K on Average to Wire Fraud*, April 2023.
30. Fox News, *Real estate fraud risk is on the rise, and victims are sounding the alarm*, February 2024.
31. Housing Wire, *How scammers are using AI to commit new fraud in real estate*, December 2023.
32. CyberSecurity Dive, *LoanDepot caught in mortgage industry cyberattack spree*, January 2024.
33. US E&O Brokers, *What Should I Expect in 2022 for E&O Insurance Pricing?*, March 2022.
34. Insurance Journal, *Agency E&O Buyers Report Fewer Price Hikes But Overall Premiums Still Up*, November 2023.
35. Pittsburgh Post-Gazette, *Hacked Firm Can't Claw Money Back From Bank,* November 2018.
36. LexisNexis Report, *The True Cost of Fraud*, 2022.
37. Bloomberg Law, *Data Security, Professional Perspective - Key Takeaways from LabMD*, December 2018.

About the Author

T**om Cronkright** is the Executive Chairman of CertifID, a technology platform designed to safeguard electronic payments from fraud. He co-founded the company in response to a wire fraud he experienced and the rising instances of real estate wire fraud. He also serves as the CEO of Sun Title, a leading title agency in Michigan. Tom is a licensed attorney, real estate broker, title insurance producer and nationally recognized expert on cybersecurity and wire fraud.

About CertifID

CertifID is a leader in wire fraud protection. We safeguard billions of dollars every month from fraud with advanced software, insurance, and proven recovery services. Trusted by title companies, law firms, lenders, realtors, and home buyers and sellers, CertifID provides further peace of mind with up to $1M in direct coverage on every wire it protects.

Contact us at www.certifid.com to protect your business, or for help with a fraud incident.

CERTIFID

ALTA American Land Title Association

National Notary Association

Tips for Checking State Identification Cards During an In-Person Notarization

1. Use tools of the trade

- **Magnifying glass for microprint:** Many state driver's licenses and IDs have microprinting as a security feature, but you will need a magnifying glass to read it.
- **UV light for holograms:** Many IDs have holographic images that you can see only with a "blue" (UV) light.
- **ID Checking Guide:** Has pictures and information on drivers' licenses and state IDs of all 50 states. Use it to master your state's IDs and also to verify an out-of-state ID that is presented to you.

2. Know your state's IDs

- Most notarizations you will perform will involve state residents who present your state's driver's license or state ID to verify their identity.
- Know the versions of IDs that are currently valid in your state.
  - Real ID.
  - Non-Real ID.
  - Current but no longer issued versions.
- Know the security features of your state IDs, including: Ghost photos, microprinting, holograms, laser perforations and tactile security features.

3. Handle the ID

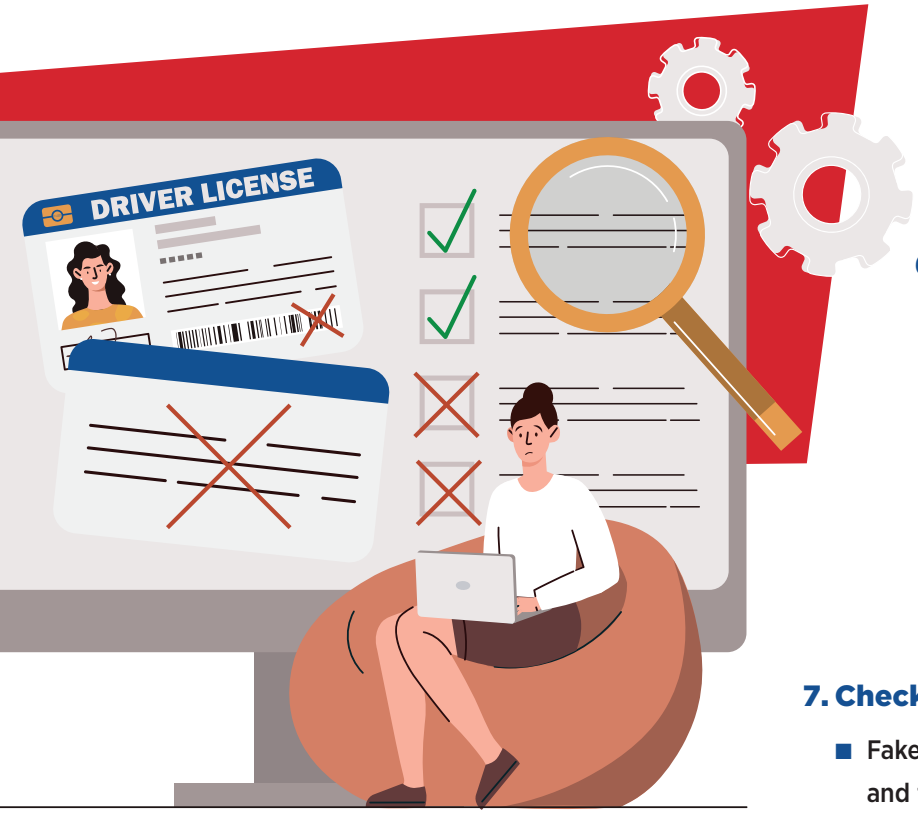
Ask the signer to take the ID out of their wallet or from behind the "ID window" of their wallet so you can handle it. To check the physical attributes of an ID, you must inspect the ID up close and touch it.

While handling the ID, check for tell-tale signs that the lamination is fake (ragged edges, peeling, air pockets underneath, creasing, etc.)

4. Compare the physical description, photo and signature

- The physical description of the person on the ID should reasonably match the appearance of the individual who appears before you.
- While a person may change their hair color, length or style, certain facial elements such as the position of the eyes, eyebrows, ears, nose and chin usually will not change. Focus on these elements in the photo and the person before you.
- Does the signature on the ID reasonably resemble the signature on the document being notarized and in the journal of notarial acts?

STOCK.ADOBE.COM / RUDZHAN



5. Inspect the front

- Physical attributes of the ID.
  - Thickness.
  - Rounded and smooth corners (a state DL or ID that does not have rounded corners is likely a fake).
  - Smoothness of photo: A "bump" could indicate an altered photo was placed on top.
- Design elements: For example, the current California driver's license has a fine-line state map, mountains, orchards, gold prospector, sailboats and California poppies on the front of the license.
- Fonts and color of fonts (mismatched and miscolored fonts are evidence of a fake ID).
- License number should reflect the proper type and number of characters. For example, in California, the first character is a letter followed by seven unspaced digits.
- Photo and ghost photo.
- Holograms and visual security features (laser perforations that require you to hold the ID at a certain angle or up to the light to see).
- Tactile security features such raised lettering that you can feel by touch.
- Overlapping elements and printing.
- License or ID term length.
- Does the signature on the ID reasonably resemble the signature on the document being notarized and in the journal of notarial acts?

6. Inspect the back.

- Fake IDs may compellingly reproduce the front of the ID but not the reverse side.
- Check the back side for the inclusion of all elements that should appear such as a magnetic swipe strip, barcode, and design and security elements (The ID Checking Guide will identify these elements).

7. Check for signs of tampering.

- Fake IDs may tamper with the signature, photo and typed information.
- If the ID contains overlapping type as a feature, the absence of overlapping type could be a sign of tampering.

8. Check the ID expiration date

9. Ask questions

- Ask the cardholder to verify personal data on the card. If they can't, it is a red flag.
- Ask the cardholder what the middle initial in their name stands for.
- Purposely mispronounce their name or misstate their middle initial to see if the cardholder instinctively gives the correct information.

10. Look for signs of deceit

- Nervousness.
- Lack of eye contact.
- Hesitation when answering questions.
- Eyes tracking upward (as a sign they may be trying to remember or make something up).

SELLER IMPERSONATION FRAUD IN REAL ESTATE

ALTA
American Land Title Association

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

For more information about real estate fraud, ask an ALTA member or visit **homeclosing101.org**

SELLER IMPERSONATION FRAUD IN REAL ESTATE

ALTA
American Land Title Association

TAKE PRECAUTIONS

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

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.

Wire Creator: _____
(Signature) (Date)

_____
(Printed Name)

Wire Authorizer: _____
(Signature) (Date)

_____
(Printed Name)

The Fund

Copyright © 2019 Attorneys' Title Fund Services, LLC / thefund.com / 800.336.3863

ALTA Outgoing Wire Preparation Checklist

Section 3:
Verify Delivery of Wired Funds.

- ☐ Date Wire Was Sent: _____
- ☐ Date Wire Was Received: _____
- ☐ Person Confirming Receipt: _____
- ☐ Purpose of Wire: _____
  - ☐ Loan Payoff _____
  - ☐ Equity Loan Payoff _____
  - ☐ Seller Proceeds _____
  - ☐ Real Estate Commission _____
  - ☐ Other (describe): _____

Verified By: _____
(Signature) (Date)

_____
(Printed Name)

MEMBER AMERICAN LAND TITLE ASSOCIATION

For more information and tools to prevent wire fraud, **visit the ALTA Website:**

alta.org/business-tools/information-security.cfm

Protect Your Practice From Wire Fraud Schemes

Every day, hackers try to steal your money by emailing fake wire instructions. Criminals will use a similar email address and steal a logo and other info to make it look like the email came from a reputable source you know.

Protect yourself and your firm by following these steps:

Be Vigilant

- **Call, don't email:** Confirm your wiring instructions by phone using a known number before transferring funds. Don't use phone numbers or links from an email.
- **Be suspicious:** If anything about the transaction doesn't feel right, STOP!

Protect Your Money

- **Confirm everything:** Ask the bank to confirm all info on the account before any money is sent.
- **Verify immediately:** Within four to eight hours, call and confirm the money was received.

What To Do If You've Been Targeted

- **Immediately call the bank** and ask them to issue a recall notice.
- **Report the crime to IC3.gov**
- **Call your regional FBI office and police.**
- Detecting that you sent money to the wrong account **within 24 hours** is the best chance of recovering your money.

The Fund

Copyright © 2019 Attorneys' Title Fund Services, LLC / thefund.com / 800.336.3863

The Fund® DON'T BE A FRAUD MAGNET!

Minimum Standards - S.E.C.U.R.I.T.Y.

Seller & Borrower Verification

ID: Obtain a valid government-issued color ID and closely scrutinize for authenticity.

Independently Verify Transaction with Property Owner: Confirm independently with the property owner in vacant land or absentee owner situations that the upcoming transaction is legitimate.

Escrow Protector

Independently Verify Payoff & Wire Transfer Instructions (WTI) with a Trusted Source: Beware of unsolicited payoff/WTI and compare for consistency. Beware of changes to routing & account numbers.

Encrypt Wire Communication: Encrypt emails containing WTI or Personal Information (PI).

Avoid Sensitive Terms in Email Subject Lines: (For example, a subject line using "Wire Instructions" is highly susceptible to spoofing and phishing attacks).

Track the Transaction: Keep track of transfers and monitor for any last-minute changes. Track receipt of disbursements (payoffs, insurance, seller proceeds).

Common Sense

Trust Your Instinct: Pause proceedings if there is a rejected wire, substituted unknown notary, or other irregularities. Be cautious of any last-minute changes, especially with vacant land, absentee owners, and foreign sellers.

Documents: Compare signor(s) locations on executed documents (deed/mortgage) with their ID document(s), and compare handwriting & signatures for similarities (witnesses, notary, grantor).

Utilize Secure Protocols

RON Service Providers: Use industry trusted and known RON platforms which incorporate KBA and other ID verifications.

Email Services Providers: Use secure email providers, avoiding public platform providers like Gmail, Yahoo, AOL, etc.

Cybersecurity Measures: Implement strict access controls.

Routine Training

Train Staff: Regularly update staff on fraud and anti-fraud techniques and encourage review of Fund education materials.

Practice Drills: Run drills and action plan rehearsals, including simulated test phishing emails to keep staff alert.

Incident Response Plan (IRP)

Incident Response Plan: Develop and maintain a strong plan with instructions, critical contacts including your bank's security officer, action items, and E&O carrier info.

Immediate Fraud Response: Inform outgoing and receiving banks immediately upon detecting fraud. Diligently work to recall wires.

Take Charge of the Closing

Trusted Sources: Control the closing process. Rely on trusted sources and known notaries.

RON: Use RON notary or require execution of documents with a known attorney or notary for signors who are not present and are unknown.

You

Stay updated on fraud trends and anti-fraud techniques.

Detect and Prevent Fraud: The responsibility ultimately lies with you. Everyone is counting on you to prevent fraud. You are in the best position to detect and thwart fraud.

Protect Yourself: These policies are essential to protect your business and livelihood.

Copyright © 2025 Attorneys' Title Fund Services, Inc. / **thefund.com**

The Fund® DON'T BE A FRAUD MAGNET!

Strongly Recommended - P.R.O.T.E.C.T.

Passwords
- Use strong passwords and change them frequently.
- Adopt ALTA's best practices where appropriate.

Records
- Secure records and purge Personal Information (PI).
- Transfer closed files with PI from internet-exposed servers to an external hard drive or other secured storage.

Operations
- Avoid personal email for work communications.
- Refrain from using open networks.
- Follow secure protocols to protect PI and other sensitive information.
- Regularly update your system to include all security patches by enabling automatic updates, using reliable antivirus software, keeping all software up-to-date, and backing up data to encrypted servers.
- Obtain and scrutinize a second valid government-issued ID.
- Consider sending a check instead of a wire but be aware of check washing risks.

Tools
- Use third-party vendors for wire transfer security, identity, and seller/borrower verification (e.g., CertifID, TLO Skip Tracing, Persona, Verisoul).
- Consider services that confirm bank account ownership.

Errors & Omissions Insurance
- Review and understand coverages and limitations of your E&O policy. Analyze to maximize protection for potential loss and actions taken as a closing agent.
- Ensure your office adheres to policy prerequisites and conditions for claims.
- Promptly review and comply with your E&O policy concerning notice obligations.

Cybersecurity Insurance
- Acquire cybersecurity insurance to cover matters excluded by E&O insurance.

Technology
- Implement Multifactor Authentication (MFA) across all accounts and devices.
- Utilize Positive Pay for escrow accounts.
- Use FaceTime or similar applications to secondarily verify ID photos with unknown seller/borrower on camera.

Copyright © 2025 Attorneys' Title Fund Services, Inc. / **thefund.com**

Alert

Alert - Imposter Fraud Variant

Fund Members should be on alert for the following variant of the Imposter Fraud Scheme. This appears to have been attempted, caught and prevented by at least one Fund Member who, during a recent large residential condominium transaction, investigated the imposter when each red flag observed was quickly dismissed by the imposter. The Member's insistence on not being rushed thwarted the criminal. However, recent significant claims have also been observed.

Each of these transactions shares the following fact pattern:

- Unencumbered high-value condominium unit in South Florida.
- Property originally owned by an absentee Foreign National (the person being impersonated).
- Shortly before the closing, the Imposter conveys the property from the individual's name to a newly formed LLC. The LLC bears the name of the Foreign National owner plus the words "Beach Investments, LLC."
- The Property Owner's Association provided the appraiser with access to the property based on an emailed request from the Imposter.
- The loans involve hard money lenders originated through a mortgage broker and are cash-out refinances.
- The closing agent is instructed to wire the loan proceeds to a Citizens Bank, N.A. account in the name of the Foreign National.
- The Imposter appears in person for closing and presents high-quality foreign identification credentials to the notaries.

Combating this type of fraud is becoming more difficult as the imposters become more sophisticated. Fund Members are the front line to prevent imposter fraud. Your diligence in determining the identity and the authority of the parties presenting themselves is what can eliminate this conduct and protect the parties, your firm, and Old Republic. The Fund has produced and will continue to produce materials to alert its Members to this issue and to provide guidance on how to limit this very real risk. Please consult previous Alerts, General Counsel Blog posts, Fund Concept articles and webinars.

Note also, The Fund has previously developed a Title Note to warn you to be on the lookout when you see a relatively recent conveyance in advance of your closing. Certain red flags may be present in the recent deed that indicate a possible forgery, fraud, coercion, or undue influence. See TN 10.03.09. The TN focuses on quitclaim deeds because that is what is generally used; however, these imposter fraud schemes very well may use a warranty deed, which bears some of the same red flags Members should be on the lookout for. Also, to help signal to you further diligence should be undertaken to confirm the validity of a recent transfer, Fund examiners are on the lookout for relatively recent deeds that may bear some of these red flags and will often include the following requirement:

> *Fund Member must determine through any reasonable means necessary that the quitclaim deed recorded in ___, Public Records of ___ County, Florida, is a legitimate conveyance of title involving no fraud or undue influence.*

Members should consider implementing additional safeguards such as:

1. Requiring the production of multiple forms of photo identification.
2. Requiring credential analysis through a vendor such as Intellicheck or CertifID.
3. Sending a letter to the mailing address listed for the owner on the property appraiser's website confirming you are closing a transaction on the property.
4. Recognize that requests to disburse proceeds to anyone other than the vested owner's bank account could be a red flag and may result in additional liability for you as the agent.

Please contact Fund Underwriting with any questions.

Trouble viewing? Click here for the web version.

The Fund, 6545 Corporate Centre Blvd., Orlando, FL 32822, USA
Copyright © 2025 Attorneys' Title Fund Services, Inc.

You are receiving this email as part of your Fund membership.

Preferences | Unsubscribe