Gallagher

The Misclassification That Is Costing Law Firms Millions

Wire Fraud Is Not a Cyber Claim: Why Law Firms Are Getting This Wrong

When a law firm falls victim to wire fraud, the instinct is often to categorize it as a cyber event. After all, the fraud often involves email, electronic communications or compromised credentials, which is the vocabulary of a cyber event. But that instinct, however understandable, is leading firms directly into a coverage gap that is growing more costly every year.

Wire fraud is not primarily a cyber claim. It is a crime claim. That distinction determines whether a loss is covered, which policy responds and whether the firm recovers at all.

Firms that have not examined this distinction closely may be carrying risk they do not fully understand.

Why Law Firms Are a Prime Target

Law firms operate at a uniquely exposed intersection. They manage large sums of client funds, execute high-value transactions under time pressure and communicate frequently with multiple external parties whose identities can be easily spoofed.

Common wire fraud scenarios include:

- **Business Email Compromise (BEC) targeting trust accounts.** A fraudster impersonates a client or transaction party and redirects wire instructions. Funds are sent in good faith and are unrecoverable by the time the fraud is identified.
- **Spoofed counterparty instructions.** An attorney receives what appears to be a routine update from opposing counsel or a title company. The request is convincing but fraudulent.
- **Internal authority impersonation.** A message appearing to come from firm leadership requests an urgent transfer, bypassing standard approval processes.

In each case, the loss results from a legitimate user authorizing a transfer based on false information, not from a system breach.

Why Cyber Policies Often Do Not Cover Wire Fraud

Cyber liability policies are designed to address unauthorized access, data breaches, ransomware and related response costs. They perform well within that scope.

However, they generally do not cover voluntary wire transfers, even when induced by fraud.

Most cyber policies include exclusions or sublimits for social engineering or funds transfer fraud because these events involve a human decision, not a system intrusion. From the policy's perspective, the transaction was authorized.

This is where the insurance gap emerges.

Crime policies are the appropriate vehicle for wire fraud coverage, typically through Computer Fraud and Funds Transfer Fraud insuring agreements. However, these policies can present challenges:

Computer Fraud may require that a computer be the direct cause of the loss, which can limit coverage when human authorization is involved.

Funds Transfer Fraud often requires that fraudulent instructions be sent directly to the financial institution, not to firm employees.

Social Engineering coverage, usually added by endorsement, is better aligned to these scenarios but often carries sublimits that are significantly lower than typical transaction values.

The result is a familiar outcome. A firm experiences a significant loss, holds both cyber and crime coverage, and still faces delays, disputes, or insufficient recovery.

Who Owns This Risk?

Wire fraud risk sits between IT, finance and operations. Without clear ownership, gaps emerge.

In many firms, accountability is diffused:

- IT views it as a financial controls issue.
- Finance expects stronger technical safeguards.
- Leadership assumes existing protocols are followed.

This lack of alignment creates three common issues:

1 **Siloed insurance decisions**	Cyber and crime policies are purchased independently, without a coordinated review of coverage gaps or sublimits.
2 **Inconsistent controls**	Verification protocols vary by practice group, increasing the likelihood of breakdowns.
3 **Misrouted claims**	Losses are often reported to cyber carriers first, delaying proper notice under crime policies.

What Firm Leadership Should Be Asking

Insurance

- Does our crime policy include social engineering coverage, and are the limits aligned with our transaction values?
- Have our cyber and crime policies been reviewed together against a realistic wire fraud scenario?
- Do key stakeholders understand reporting requirements and retentions?

Controls

- Do we have a consistent, firm-wide wire verification protocol?
- How are changes to instructions validated?
- Do we require voice verification using known contact information?

Claims readiness

- Who is responsible for responding to a wire fraud event?
- Are notice requirements clearly understood?
- Have we tested our response through an exercise?

Key Takeaways for Risk and Insurance

- **Reframe the exposure**. Wire fraud is a crime loss with cyber elements. This distinction should guide coverage strategy and claims response.
- **Review coverage with intent.** Evaluate how each policy responds to social engineering scenarios, including triggers, exclusions and sublimits.
- **Prioritize social engineering coverage.** Limits should reflect the size of the transactions your firm executes.
- **Strengthen internal controls.** Verification protocols, dual authorization, and staff training are critical and influence insurability.
- **Align operations and insurance.** Those authorizing wires and those managing claims should operate with the same understanding of risk and requirements.

A Word on the Stakes

Business Email Compromise remains one of the highest-loss categories in reported cybercrime, not because of technical complexity, but because of its effectiveness. These schemes rely on trust, urgency and familiarity.

Law firms, by the nature of their work, present all three.

Firms that manage this risk well are not only investing in technology. They are aligning coverage, strengthening controls and building consistent verification practices.

It starts with understanding the nature of the risk and ensuring the response matches it.

Connect with your Gallagher representative to review your current coverage and controls and identify any gaps before a wire fraud event puts them to the test.