Unified Financial Crimes Response

Cyber & Tech E&O Underwriting | January 2026

Executive Summary

The Problem

Our current response to Funds Transfer Fraud (FTF) is fragmented. When an Insured loses funds, they face a "definitions roulette" to determine if the loss is covered by Crime (Theft), Cyber (Hacking), or Professional Liability (Negligence). This hesitation causes latency, and in wire fraud, latency guarantees a total loss.

The Opportunity

We propose a **Unified Financial Crimes Overlay** that sits above all three lines. By shifting focus from "Liability Defense" to "Asset Recovery," we can:

- **Reduce Net Payouts:** Recovering the asset eliminates the claim
- **Increase Limits Safely:** Offer market-leading capacity ($1M+) conditional on speed
- **End Coverage Disputes:** If the money is recovered, the "Cyber vs. Crime" argument becomes moot

The Market Failure

Current policies force the Insured to navigate complex exclusionary language during a crisis.

Scenario	Commercial Crime	Cyber Liability	Professional Liability
The "Hack" *Hacker accesses bank portal*	COVERED Computer Fraud	MAYBE If Endorsed	EXCLUDED Not a professional error
The "Phish" *CFO tricked into wiring funds*	SUB-LIMITED Social Engineering	EXCLUDED No system breach	EXCLUDED Not a professional error
The "Trust Account" *Lawyer tricked with client funds*	DENIED 3rd Party Property	DENIED Not 1st party loss	GREY AREA Exclusion for Theft

The strategy: The gap is the product. We introduce a service layer that ignores *how* the money was lost and focuses entirely on getting it back.

The Mechanism: Conditional Limits

We trade capacity for speed. We can offer a higher sub-limit ($1M) because we only pay it if the Insured gives us a fighting chance to recover the funds.

DRAFT ENDORSEMENT CONCEPT

$100,000	**$1,000,000**
Base Sub-Limit ("Cold Loss" Tier)	Enhanced Sub-Limit ("Hot Loss" Tier)

CONDITIONS FOR ENHANCEMENT

The Enhanced Sub-Limit applies **only** to Loss reported to the Company's Financial Crimes Response Center within **72 hours** (or 5 days) of the initial transfer of funds.

Any Loss reported after this period shall be subject to the Base Sub-Limit, regardless of when the Insured discovered the Loss.

Why This Works

- **Operational Reality:** It ties coverage to the "Transaction Date," not the subjective "Discovery Date."
- **Risk Control:** We don't insure "negligence" (waiting 2 weeks); we insure "operational response" (acting fast).

The Vendor Ecosystem

To execute this, we need a specialist panel distinct from our General Breach Counsel.

1. The "Specialized Unit" Model (e.g., McDonald Hopkins)

Role: Operations & Banking Liaison

Differentiates "Wire Fraud Response" from general data privacy. Focuses purely on the financial kill chain.

2. The "Hybrid Intelligence" Model (e.g., Clark Hill)

Role: Technical Asset Tracking

Bridges the gap between legal counsel and forensic accounting. Uses intelligence specialists to track SWIFT flows.

3. The "Scale" Model (e.g., Mullen Coughlin)

Role: Volume & Benchmarking

High-volume handling of BEC (Business Email Compromise) with deep contacts at FBI field offices.

The Sales Tool: Battle Card

Marketing one-pager to be distributed with all Cyber, Crime, and PL quotes.

Financial Crimes Rapid Response Program

Turn Your Policy Into a Recovery Engine

Speed is the only currency that matters. In a Funds Transfer Fraud event, the window to recover stolen assets is less than 72 hours. Traditional insurance claims processes are too slow. We've replaced the "Claim Form" with the "Kill Chain."

Step 1: The First Mile (0-1 Hour)

- Call your bank immediately
- Demand the "Fraud Department"
- Request a "SWIFT Recall"

Step 2: The Second Mile (1-2 Hours)

Activate the Hotline: 1-800-XXX-XXXX

- < 72 Hours from Transfer: Unlocks your $1,000,000 Limit
- > 72 Hours from Transfer: Limits coverage to $100,000

Step 3: The Recovery

Our team will activate the FBI "Recovery Asset Team" (RAT) protocols to freeze funds before they leave the country.

Proof of Concept: A Tale of Two Wires

The Scenario: A paralegal at a Law Firm wires $2,000,000 of client money to a hacker on a Friday afternoon.

Feature	Path A: Siloed Approach (Current)	Path B: Unified Approach (Future)
First Action	Broker debates if it's a Crime or PL claim	Insured calls 24/7 Hotline immediately
Weekend Activity	Claims sits in a queue. Hackers move money.	Specialist activates Bank Kill Chain & FBI RAT
Monday Morning	Crime & PL carriers issue "Reservation of Rights" letters denying coverage	Specialist presents Indemnity Agreement to bank. Funds reversed.
Outcome	**$2.2M Net Loss** (Payout + Legal Fees)	**$15k Net Loss** (Vendor Fees Only)
Insured Sentiment	"Insurance is a scam."	"You saved our business."

Decision Required

Approval to form a cross-departmental Working Group (Cyber, Crime, Claims) to:

- Vet and select the "Wire Fraud Specialist" vendor
- Finalize the "Conditional Limits" endorsement wording
- Launch a Pilot Program in Q2