Legal Wire-Fraud Breach Report

Three attacks your firm is at risk of on Monday — and the trust-account controls mapped to ABA Rule 1.15 that stop them.

For solo practitioners, partner tracks at AmLaw 200 firms, in-house legal ops at GCs, real-estate closers, and estate-planning attorneys

$489K
average wire-fraud loss (FBI IC3 2025) — most never fully recovered

WHAT IS IN THIS REPORT?

TARGET PROFILE

Why Law Firms Are the #1 Wire-Fraud Target

Three structural realities make every firm — from a solo practice to an AmLaw 200 partner-track — a preferred target. None of them require the attacker to be technically sophisticated.

Trust-account balances look like enterprise accounts

A solo real-estate closer handling an $850K closing hold small escrow accounts for the week of the deal. A partner-track M&A attorney may have $4M–$8M in trust balances during a transaction. To an attacker scanning public filings on county recorder sites or LinkedIn Deals, both look like enterprise banking targets.

ABA Rule 1.6 — confidentiality duties suppress the verify reflex

A client matter is confidential. The instinct to call the client to verify a wire instruction requires breaking protocol — opening the deal to a phone call the attacker can intercept with deepfake voice. The closer who "should not bother the client" is exactly the closer the attacker is counting on.

Escrow-wire timing pressure rewards last-minute changes

Real-estate closings run on a funding window. If the closer hears "wire instructions changed" at hour 0 of the funding window, the incentive is to act — not to verify. The attacker is betting the closer will not pick up the phone to a phone number from their own file because that would slow them down.

Deepfake voice removes the callback verification loophole

A 30-second public audio sample — district bar podcast, conference video, alumni award — is enough to clone an escrow officer's voice. The closer who calls "to verify" hears the cloned voice confirm the wire change. The paper trail says they verified.

VERIFIED BREACH DATA

Three Named Breach Anchors Targeting Law Firms

Every anchor below is drawn from the public FBI IC3 2025 dataset and verified case reporting. Date, dollar figure, and attacker pattern are not invented — they appear in the underlying report.

ANCHOR 1 · $489K average

Lookalike-Domain Wire Change at Real-Estate Closing

PATTERN
Attacker registers a near-identical client domain (e.g., henderson-group.co vs henderson-group.com). They email the day before closing, claiming the wire instructions changed "due to a bank routing change." Domain is one character off from the real client.

VICTIM ACTION
Real-estate closer on deadline at hour 0 of the funding window. Reads email at 9:42 AM, wires by 10:15 AM. Funds are gone in 4 hours.

OUTCOME
FBI IC3 2025 reports $489K average wire-fraud loss; 69% of wire-fraud targets are law firms, title companies, and real estate. Recovery rate: 13% across all BEC, 28% with 24-hour IC3 filing.

ANCHOR 2 · Targeted (multi-million)

Compromised Title-Company Mailbox with Rewritten Closing Instructions

PATTERN
Title-company escrow officer's mailbox is compromised via Microsoft 365 credential-phishing. Attacker lives in the inbox for 3–6 weeks, monitoring active closings.

VICTIM ACTION
Buyer's attorney receives a legitimate-looking email from the real escrow officer's address with new wire instructions the morning of the funding. Email is in-thread with prior closing correspondence.

OUTCOME
Same pattern as the $50M global BEC ring (2024) — one attacker ring attempted over $50M in fraudulent wires globally, with major recoveries at JPMorgan, Citi, and Bank of America.

ANCHOR 3 · Varies

Deepfake Escrow Officer on a Callback Verification

PATTERN
Attacker scrapes a 30-second audio clip of the real escrow officer (district bar podcast, alumni video, conference recording). Clones voice using a commodity voice-cloning service.

VICTIM ACTION
Buyer's closer calls the title company's main line to "verify" the wire change. The phone is answered by attacker's cloned voice at a number the closer did not look up independently — the in-email number.

OUTCOME
Reported as an emerging attack pattern in Q1 2025. The closer has a paper trail — they verified. The bar association will still want to understand why the verification channel allowed the attacker to control the call.

ANATOMY OF A LAW-FIRM WIRE-FRAUD ATTACK

The Law-Firm Wire-Fraud Kill Chain

TEACHING CASE · ANONYMIZED · 2026

A solo real-estate closer received an email 90 minutes before a $612,500 closing funding window, claiming the buyer's wire instructions had changed due to a "new bank routing." The closer called the number in the email — answered by a cloned voice of the buyer's controller — and wired the funds. The closing funded against the wrong account. Recovery: 0%.

1

Public Reconnaissance

Weeks before attack

Attacker scrapes county recorder filings, LinkedIn Deals, and PitchBook to identify active real-estate closings, partner names at the closing firm, and the buyer's controller. Public audio for voice-cloning is harvested from district bar podcasts and alumni videos.

2

Lookalike Domain Registered

1–4 weeks before

Attacker registers a near-identical domain (e.g., henderson-group.co when real client is henderson-group.com). One character difference. MX records set up. SPF/DKIM/DMARC set so the domain does not look brand-new.

3

Initial Outreach

7–14 days before

Phishing or direct outreach establishes the attacker's inbox is monitored. If the title company's mailbox is the inbox — attacker waits for Microsoft 365 credential-phishing. If the attacker is impersonating — they begin regular "pre-closing" questions to look legitimate.

4

Changed Wire Instructions

90 minutes to 24 hours before

Email arrives — urgent tone, "bank routing change" or "new escrow account" — with new wire instructions. The Reply-To or sender domain is one character off. Urgency is always present. The closer is inside the funding window.

5

Verification Bypass

During the wire decision window

If the closer calls the number in the email to "double-check," a deepfake voice answers — or the attacker impersonates the buyer's controller using vendor impersonation. If the closer uses their own file's number, the real client replies "those are correct" without knowing the attacker's email may be sitting in the closer's review queue separately.

6

Trust Account Wire Authorized

Minutes after sent

Trust-account wire is initiated above the dual-control threshold — or below it, depending on firm policy — and moves to the attacker's mule account. Funds are laundered through transit accounts. FBI Financial Fraud Kill Chain has a 72-hour window for clawback.

CONTROL CROSSWALK TO ABA MODEL RULES

Trust-Account Controls Mapped to ABA Rules 1.1 / 1.6 / 1.15

Every control below is mapped to a specific ABA Model Rule citation so the controls hold up to a bar-association inquiry, a malpractice complaint, and a cyber-insurance recovery claim.

RULE 1.1 · COMPETENCE

Annual documented training on Verify-Out-Of-Band protocol

Every attorney and paralegal handling client trust accounts receives documented annual training on (a) lookalike-domain detection, (b) callback verification using a number from the firm's own file, not from the email, and (c) escalation to the managing partner above a partner-defined wire threshold. Training records are tabbed in date order for bar review.

RULE 1.6 · CONFIDENTIALITY

Need-to-know trust-account information controls

Trust-account wire details are visible only to attorneys and authorized finance staff on a need-to-know basis. Email auto-forwarding, mailbox delegate access, and invoice-vendor banking changes are logged for weekly review. Outside vendors receive wire instructions under countersigned acknowledgment only.

RULE 1.15 · SAFEKEEPING CLIENT PROPERTY

Dual-control wire approval + countersigned acknowledgment

Any wire above a partner-defined threshold requires dual-control approval — two authorized signers review wire instructions independently and countersign the acknowledgment. The acknowledgment is countersigned by the client (or the client's authorized representative on a known channel) and survives mailbox compromise, since the signature is verified on a closed-loop channel.

STAT

Only 13% of BEC victims ever recover any of the lost funds. For firms that filed IC3 within 24 hours and involved their cyber-insurance carrier, recovery rose to 28%. For firms that acted within 4 hours, recovery reached 41%.

INCIDENT RESPONSE

First 60 Minutes After a Suspected Wire Fraud at a Law Firm

If a wire was sent and you suspect it was fraudulent, act immediately. Every hour reduces your chance of recovery, and the bar-association notification window begins on discovery — not on confirmation.

MINUTES 0–15 · STOP AND CALL THE BANK

- Do NOT reply to the suspicious email. Do NOT send any more emails from the affected account.
- Call your trust-account bank's fraud department immediately. Request a wire recall. Ask about the Financial Fraud Kill Chain (FFKC) — the bank can contact the Federal Reserve and the beneficiary bank to attempt to freeze funds.
- If the wire was sent in the last 24 hours, request your bank contact the Federal Reserve directly. The FFKC only works inside 72 hours.
- Document every action: time, person called, what they said, next steps agreed. Counterparty engagement letter typically requires immediate notification — pull the engagement letter now.

MINUTES 15–30 · NOTIFY AND REPORT

- File a complaint with FBI IC3 at ic3.gov — include all emails, wire confirmation, and any communications. Time-stamp everything. IC3 complaints filed within 24 hours recover funds at significantly higher rates.
- If the loss exceeds $50,000, call your local FBI field office. They may open a case.
- Notify your cyber-insurance carrier — most policies have a 72-hour reporting window. File the claim immediately.
- Notify your managing partner and outside cyber counsel. Do not delay.
- Do not touch the affected computer — preserve evidence. Do not power it off or reboot.

MINUTES 30–45 · SECURE AND PRESERVE

- Lock the compromised email account. Change password from a different device. Enforce phishing-resistant MFA (FIDO2 / WebAuthn) if not already in place.
- Review email forwarding rules — attacker auto-forwarding is common.
- Check which other accounts may be affected — title company escrow, opposing counsel, banking portals.
- Pull bar-association notification language for your jurisdiction. Most state bars expect notification within a defined window of discovery.
- Prepare a client-engagement-letter-triggered notification if funds belonged to a client. Your engagement letter probably required immediate notification.

MINUTES 45–60 · LOCK DOWN AND BRIEF

- [ ] Stop all outgoing wires from the trust account until the incident is contained.
- [ ] Review all pending transactions — check for any other suspicious instructions in any inbox across the firm.
- [ ] Brief partners and finance staff. Do not keep this quiet — every team member handling money or client communication should know.
- [ ] Update the wire-fraud-policy document. If this incident reveals a control gap, fix it before the next funding window.
- [ ] Schedule a post-incident review with outside cyber counsel within 14 days. Determine how the attacker got in and what training the team needs.

LIVE TRAINING

Put This Into Practice — Live Wire-Fraud Training for Law-Firm Teams

The breach report is the starting point. Your closer, paralegal, and finance controller need to practice these controls under simulated pressure — not just read about them. That is what SecurEveryone's live training delivers.

PERSONAL

$150

1 session · 1 hour

Individual briefing on wire-fraud anatomy, lookalike-domain detection, and the Verify-Out-Of-Band protocol. Good for a single closer or paralegal.

Best for: Solo practitioners, new hires, paralegals

- 1-hour live wire-fraud briefing
- Lookalike-domain walkthrough
- Verify-Out-Of-Band protocol training
- Callback script you can use today
- Certificate of completion

EXECUTIVE

$390

1 session · 90 minutes

For partners, finance controllers, and anyone with trust-account wire authority. Covers the complete law-firm wire-fraud kill chain, the ABA Model Rule crosswalk, and the 60-minute first-response runbook on a simulated wire.

Best for: Managing partners, finance directors, es

- 90-minute live session
- Law-firm kill chain deep dive
- ABA Rule 1.1 / 1.6 / 1.15 crosswalk
- 60-min first-response runbook
- Live callback verification drill
- Bar-association notification template

BUSINESS

$900 flat

Unlimited users · 12 months

Full-team wire-fraud defense training with all attorneys and staff included. Quarterly simulated wire-fraud scenarios, trust-account-control documentation, and the bar association notification language your partnership will need.

Best for: Law firms of 40+ attorneys, in-house legal ops, AmLaw partner tracks

- Unlimited live sessions for 12 months
- Quarterly wire-fraud tabletop exercises
- Practice-group-specific scenarios
- Trust-account control documentation
- ABA Rule crosswalk archive
- Bar-association notification templates
- Cyber-insurance-ready incident file

CALL TO ACTION

Book a SecurEveryone Executive Session now. All sessions include the Legal Wire-Fraud Breach Report, ABA Model Rule crosswalk, and the 60-minute first-response runbook your team can reference.

ABOUT SECUREVERYONE

Cybersecurity Training for the Organizations That Cannot Afford to Get It Wrong

- Live, instructor-led sessions — not pre-recorded videos.
- Law-firm-specific scenarios: trust-account wires, escrow closings, title-company mailbox compromise, vendor invoice swap, ABA Rule 1.15 safekeeping controls.
- Verify-Out-Of-Band protocol training included with every session.
- Quarterly wire-fraud tabletop exercises for Business tier clients.
- Compliance-ready documentation for state bars, ABA Model Rule inquiries, and cyber-insurance.
- Sessions delivered over Zoom, Meet, or Teams — whatever your team uses.

Ready to book?

Visit secureveryone.com/book or book directly from our Calendly:

secureveryone.com/book !’

SecurEveryone LLC · 1201 North Orange Street, Wilmington, DE 19801 · +1 (302) 212-0500 · info@secureveryone.com