



SECURING YOUR LAW FIRM

Practice Law – Not Damage Control

ILLUSTRATIVE SAMPLE | FICTIONAL ORGANIZATION

Your Firm's Exposure Snapshot

examplelawgroup.example

No organization was scanned; this is a fictional example.

CONFIRMED | HIGH PRIORITY

Email that fakes your firm's address is not being blocked.

Your firm's email setting only watches for fake email sent in your firm's name. It does not tell Gmail, Outlook, and other email services to reject it.

WHAT IT COULD COST THE FIRM

A client gets an email that appears to come from your firm, telling them to wire settlement funds, a retainer, or closing money to a new account. They follow the false payment instructions, the money goes to a criminal, and the firm faces questions about its duty to safeguard client funds.

ALSO FOUND: 1 MORE ISSUE

TO CONFIRM Email services can't check whether email really came from your firm.

PRACTICAL CHECKS TO START WITH

1. Ask your email provider whether fake messages using your firm's address are rejected, not just monitored.
2. Confirm legitimate firm and vendor messages still reach clients before changing email policy.
3. Verify client payment changes through a second, known channel - not email alone.

Check your firm's status.

Request the Free Zero-Access Exposure Review™ to see which public signals apply to your domain. We verify a matching work email before the scan.

Request the Free Zero-Access Exposure Review™ >

Fictional example only. No real organization was scanned.