

## Coalition's Security Incident Response Team (SIRT) recovers \$150,000 for a policyholder

Fraudulent funds transfers is one of the most common claims we see amongst Coalition policyholders. Malicious actors can gain access to a company's corporate email systems through phishing attacks and spoofed emails, among other methods, and impersonate executives with a fraudulent request. Thankfully, Coalition is often able to help recover the funds — even after they're out the door.



### INDUSTRY: Law Firm

#### COMPANY

- Employees: 50-250
- Provide general legal services and title/real estate closing services
- Handles significant volume of large wire transfers

“



I wish I did not know how awesome it is to work with Coalition. I do not know what I would have done without you. On behalf of the entire company, I really appreciate it.

### CASE STUDY

We received a call that a client had lost \$200,000 in a social engineering incident. A hacker sent a spoofed email to their controller, impersonating the company's CFO, and the controller wired the funds to the bad actor. The company thought the funds were gone for good, but then they called Coalition.

Upon receiving the call, Coalition immediately began discussions with financial institutions and law enforcement. As a result of Coalition's urgency and relationships, \$150,000 of the \$200,000 was recovered within 24 hours of receiving the call. The money was returned to the client, and they were able to quickly get back to business. Their insurance policy with Coalition covered the remainder of the lost funds. Coalition's Security team also helped the company put two-factor authentication practices in place, to ensure a second person at the firm signed off on all significant wire transfers.

Unlike traditional insurance companies, Coalition has the relationships and know-how to recover funds even after they're out the door. For many policyholders, we're able to recover all of the funds lost -- helping them avoid a claim entirely!