CASE STUDY

# Environmental technology company duped in coordinated social engineering scam

**INDUSTRY**

Environmental Technology

**EMPLOYEES**

<100

**COVERAGES**

Funds Transfer Fraud

After receiving text alerts from their bank, an environmental technology company learned that someone was requesting to be added to their account. The company immediately picked up the phone and called the bank to deny access. Unfortunately, the number they dialed put them directly in touch with a threat actor posing as the bank to gain access to their account.

Meanwhile, a second threat actor was on the phone with their bank, impersonating a company employee. Working in tandem, the two threat actors manipulated the bank into sending a security code to the company for verification, which they then relayed to each other and successfully added themselves to the bank account to authorize transactions.

Over the course of two months, the threat actors initiated five fraudulent wires totaling nearly $500,000 in losses. That's when the company contacted Coalition's Claims hotline.

We began working on the case, but were unable to recover the fraudulent transfers due to the amount of time that had passed. The insured's Funds Transfer Fraud coverage[1] kicked in and covered the full loss amount. After the claim was adjudicated, the company was able to recover a portion of their fraudulently wired funds from the bank and reimbursed that portion of the claim.

Coalition brings together active monitoring, incident response, and comprehensive insurance to solve cyber risk. To learn more, visit coalitioninc.com.

[1] The claim scenarios described here are intended to show the types of situations that may result in claims. These scenarios should not be compared to any other claim. Whether or to what extent a particular loss is covered depends on the facts and circumstances of the loss, the terms and conditions of the policy as issued and applicable law.