CASE STUDY

Nonprofit Recovers Stolen Funds within an Hour of Reporting $1.55M Loss

INDUSTRY
Nonprofit

EVENT TYPE
Funds Transfer Fraud

REVENUE
$1-5M

EMPLOYEE COUNT
1-50

LOCATION
Texas

KEY COVERAGE
Breach Response

A community nonprofit suffered an email breach that led an employee to send $1.55 million to someone claiming to be a client. After realizing that the payment instructions were fraudulent and its email had been breached, the nonprofit reached out to Coalition.

Our claims team immediately requested the transaction information, which was provided within 15 minutes. The funds transfer fraud (FTF) was reported to our U.S. government agency partners to see if they could work with the banks to freeze the funds before they arrived in the fraudulent account. While on the phone with the nonprofit's executive director, Coalition received confirmation that all of the funds were frozen and would be safely returned to the nonprofit. Over the course of a single phone call, the nonprofit went from panic mode to a sense of relief, knowing that the funds would be returned — all within an hour of the fraud being reported.

Even though the funds were recovered, the nonprofit still needed to work through the business email compromise that made the fraudulent transfer possible, so they selected Coalition Incident Response (CIR)[1] to lead the digital forensics investigation. The compromise resulted from a phishing email, and CIR verified the threat actor was out of the environment by correlating the final dates of their access against the last password change times for the impacted accounts.

One key coverage helped this nonprofit navigate the claim after the funds were recovered: Breach Response. After the nonprofit paid its $5,000 self-insured retention, Breach Response covered the costs for breach counsel and CIR, which totaled nearly $12,000.

Once funds make it to a threat actor's bank account, the likelihood of banks or law enforcement recovering the funds decreases significantly.

Lesson Learned: Early Reporting Makes a Difference

Every minute counts when you're experiencing a cyber event. The sooner an event is reported to Coalition, the better. This is especially true in FTF matters. The first 48 hours are critical in trying to stop the funds from reaching the threat actor's account. Once funds make it to a threat actor's bank account, the likelihood of banks or law enforcement recovering the funds decreases significantly.

To learn more, visit coalitioninc.com.

[1] *Coalition Incident Response services provided through Coalition's affiliate are offered to policyholders as an option via our incident response firm panel.*