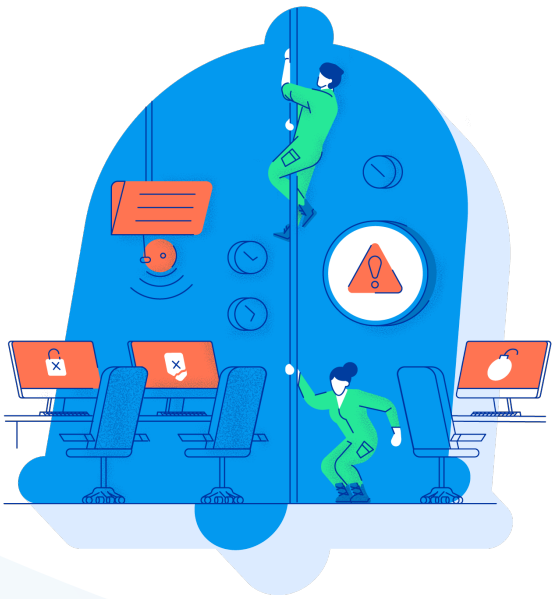
What is cybercrime and what does Coalition's policy cover?

Cybercrime – also referred to as funds transfer fraud (or FTF for short), invoice manipulation or social engineering – involves fraud where attackers manage to redirect funds before or during a transfer. This is typically accomplished through social engineering techniques, sometimes stemming from email spoofing or business email compromise.



Common attacks

Business email compromise/ email spoofing

Business email compromise involves an attacker gaining access to a legitimate email account and sending messages that appear to come from the account owner. Email spoofing is the creation of an email with a forged sender address. Criminals spoof emails in the hopes of duping the recipient (i.e., the victim) into thinking the email originated from someone or somewhere other than the intended source. In the context of funds transfer fraud, these techniques are used to spear phish, impersonating the email of a CEO/executive, vendor, or customer in an effort to trick the victim into wiring funds, or purchasing and share gift card PIN numbers.

Look-alike domains

Look-alike domains are domain names that closely resemble the domain name of a trusted website, for example by swapping letters around or substituting common characters. In this day and age, most of us are weary about clicking links that we don't trust, so look-alike domain names are designed to make it non-obvious that a lvink or message is coming from a malicious domain or sender. In an advance of a social engineering attack, it is common to see criminal actors registering domains similar to the victims to ultimately phish the victim or to perpetuate funds transfer fraud or business email compromise.

Domain spoofing

Email spoofing is the creation of an email with a forged sender address. Criminals spoof emails in the hopes of duping the recipient (i.e., the victim) into thinking the email originated from someone or somewhere other than the intended source. In the context of funds transfer fraud, it is a technique that is used to spear phish, impersonating the email of a CEO/ executive, vendor, or customer in an effort to trick the victim into wiring funds, or purchasing and share gift card PIN numbers.

What's covered?

Coalition's policy form covers lost funds for:

Funds Transfer Fraud

Theft of funds from an account of the Named Insured or Subsidiary due to electronic impersonation, including funds held in escrow.

Invoice Manipulation

Attacker uses the insured's system to redirect payment instructions and funds that a client or vendor of the insured owed and intended to pay to the insured

Funds Transfer Liability (added by endorsement)

Attacker uses the insured's system to send fraudulent payment instructions to a client of the insured for funds owed to a 3rd party.

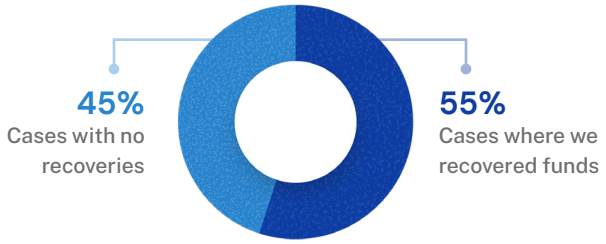
Coalition, Inc. · 1160 Battery Street, Suite 350, San Francisco, CA 94111 · join@coalitioninc.com

Social engineering by the numbers

The average funds transfer loss for one of Coalition's small business customers

$130,000

Coalition has recovered funds in 55% of all funds transfer fraud cases



Nonprofit hit with funds transfer loss

Case study

Industry: Nonprofit

Revenue: $10 - $50M

Employees: 1-25

A nonprofit organization providing child and family services grants to other nonprofits received a wire change instruction from a nonprofit partner. Only the email they received had been spoofed, and only appeared to be from the nonprofit partner. The spoofed email claimed that, due to COVID-19, funds sent to the partner could no longer be received by check, and instead should be sent by ACH transfer. Two days, and $1.3 million dollars later, the insured realized they'd been duped and phoned Coalition's claims and security incident response team (SIRT). Within 5 minutes, Coalition's SIRT went to work with law enforcement and the financial institutions involved to recover the stolen funds, successfully recovering all but $250 of the $1.3 million originally lost. Coalition SIRT is available to all policyholders at no cost, and is unique across the cyber insurance industry.

Don't just protect your network, protect your business

We offer a full suite of security apps including 24/7 security monitoring, automated threat and intelligence alerts, DDoS mitigation, security benchmarking, ransomware protection, employee training, patch reminders, and more — included with each policy at no additional cost.

Ready to protect your business? To learn more visit www.coalitioninc.com

Coalition, Inc. · 1160 Battery Street, Suite 350, San Francisco, CA 94111 · join@coalitioninc.com