

CLAIM CASE STUDY

Small Business – Construction

How Cowbell helped the policyholder
recover quickly and confidently

Who was affected:

Incident Type: Social Engineering

Revenue: \$850,000

Employee Count: 20



What happened?

The policyholder received an email that appeared to come from its regular parts supplier. The message stated that the supplier had changed its payment process and would now accept payment via wire transfer only.

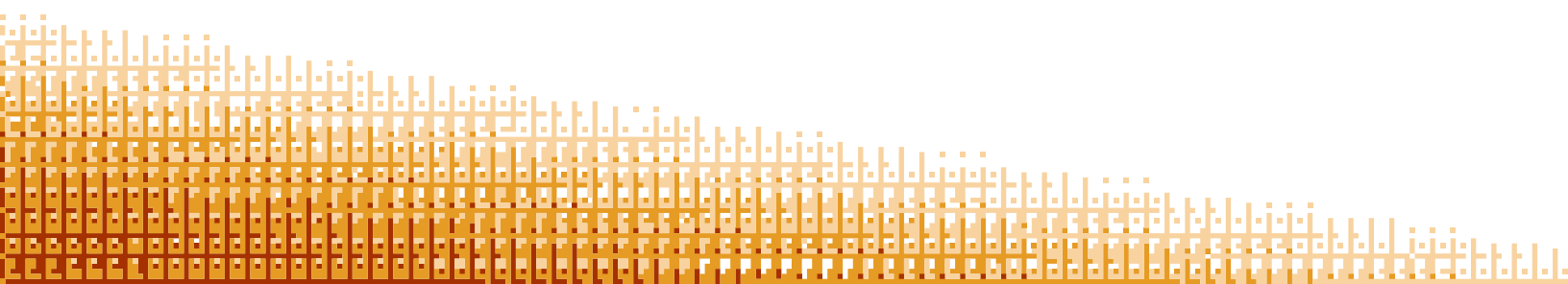
Following its internal verification procedure, the policyholder confirmed that the contact details and branding looked legitimate. Satisfied that the request was genuine, the company updated the payment instructions and processed a \$35,000 wire transfer that same day.

A few weeks later, the real supplier contacted the policyholder to ask about the unpaid invoice. Realizing the payment had been sent to a fraudulent account, the policyholder immediately contacted Cowbell to report the incident.

How Cowbell helped

Cowbell's claims team took immediate action, working closely with the policyholder to:

- Provide clear next steps, including contacting the issuing and receiving banks to recover funds.
- Coordinate breach counsel and forensic experts to confirm there was no broader compromise.
- Conduct a coverage review to confirm the policy's response.



Outcome

With Cowbell's quick response and coordination with trusted vendors, the policyholder's systems were confirmed secure. When the fraudulently transferred funds could not be recovered by the bank, Cowbell reimbursed the loss under the terms of the policy. The business has since strengthened its payment verification procedures to prevent future social engineering incidents.

Key takeaway

Social engineering scams are increasingly sophisticated and can deceive even cautious employees. Cowbell's fast response and expert guidance helped this construction company recover swiftly and strengthen its defenses against future fraud attempts.

Need cybersecurity support? Contact our team at cybersecurity@cowbellcyber.ai for tailored guidance from our experts.

Are you experiencing a cyber incident?

Report now! Call **(833) 633-8666** or email our claims team at claims@cowbellcyber.ai.

Cyber incidents don't just affect large enterprises. Small businesses are increasingly targeted by cybercriminals who know that many lack the dedicated security resources of larger organizations. Attacks like phishing and social engineering are often automated, making small businesses equally — if not more — vulnerable.

Cowbell: The Sound Approach to Risk

Cowbell delivers insurance that cuts through complexity and adapts as risks evolve. With streamlined quoting, expert guidance, and protection designed for the realities of today's threats, we make coverage easier to understand and more reliable when it matters most. Behind it all is the Hum—our constant, quiet vigilance—building stronger businesses, trusted partnerships, and the quiet confidence to keep moving forward.



This case study is provided for general informational purposes only and is illustrative in nature. The examples and descriptions included may not represent all possible scenarios or outcomes. Each incident and claim is unique, and actual results may vary. This document does not amend, extend, or form part of any insurance policy. Coverage, terms, limits, and availability may vary and are subject to underwriting approval. Actual coverage is determined solely by the specific terms, conditions, limitations, and exclusions of the issued policy. ©2025 Cowbell Cyber, Inc. All Rights Reserved. Cowbell Insurance Agency LLC, State Licenses: <https://cowbell.insure/state-licenses/>