COLLABRANCE®
A GREATAMERICA COMPANY

# TECH TOPIC

## Do You Know When Your Insurance Carrier Will – And Will Not – Pay Out?

Heed this cautionary tale: In 2022, a Minnesota-based technology solutions store sued its insurance provider, alleging the insurance provider owed more than was paid on a claim for nearly $600,000 in losses due to a successful business email compromise (BEC) attack. A Minnesota federal court dismissed the case, deeming the attack to have been the result of social engineering fraud rather than computer fraud – two separate, mutually exclusive policies under the tech provider's agreement with the insurance carrier, with very different coverage caps.

According to the court's dismissal filing, the insurance carrier defines computer fraud – which it covers up to $1M – as "intentional, unauthorized, and fraudulent entry or change of data directly into a computer system". The policy also states that entries or changes made by employees or authorized individuals based on fraudulent instructions is not covered. Social engineering fraud, on the other hand, is defined in the policy as "the intentional misleading of an employee or authorized person by impersonation". Those are two miniscule-seeming differences, but the financial impact is huge; the company's insurance policy only covers social engineering fraud up to $100,000.

Because the court found the tech provider's claim to fall squarely within their social engineering policy and not the computer fraud policy, the tech provider was only covered for a small fraction of the $600,000 in losses.

Not all insurance policies delineate between different types of fraud – but it's imperative you examine your contracts closely to find out.

The full summary of the case can be readhere:
https://www.theregister.com/2022/08/16/social_engineering_cyber_crime_insurance