Deceptive Transfer

A company’s most valuable asset, its employees, can inadvertently create risk

Deceptive transfer occurs when employees are unknowingly tricked into transferring company funds or other assets. Cyber thieves can use a variety of methods to obtain proprietary information including email phishing, social media and even traditional phone calls to gain information and deceptively transfer funds into an account under their control.

Claim Example

The CFO of ABC Manufacturing received an urgent email from his CEO regarding a large client, Illustrations, Inc. "Wire $95,137.21 to Illustrations, Inc. no later than 1:47 PM today. If we don’t make the cut-off time, we could lose them for good. Please contact accounting ASAP to have the wire transfer set up. Illustrations wire information is attached."

The CFO promptly contacted his accounting department and arranged the wire transfer. The accounting staff prepared the wire quickly and released it at 1:30 PM.

The CFO then called the CEO to let him know the urgent matter had been taken care of. The CEO had no idea what he was talking about - he hadn’t sent the email. Turns out his email had been hacked. Once they figured out they had been scammed, it was too late. Their bank had already released the $95,137.21.

How Does the Victor Policy Respond?

The Cybercrime Endorsement, an optional coverage in the Victor Cyber Protection Package, includes coverage for deceptive transfer fraud. If the policyholder falls victim to a deceptive transfer fraud scheme and is tricked into transferring their own funds from their account, this loss could be covered by the Victor Cyber Protection Package.

Visit victorinsuranceus.com/cyber for more information or contact a Cyber Protection Package underwriter at (301) 961-9800 or cyber.us@victorinsurance.com.