

▶ **Hanover Fidelity & Crime Advantage**

False Pretense Coverage

Are your clients protected against con jobs? Though hackers generate headlines, social engineering, or false pretense crime schemes, are increasingly common losses for businesses. The Ponemon Institute ranked it among the top 5 most costly cybercrimes.

In False Pretense crime schemes, a fraudster impersonates a trusted business partner, vendor, employee or client by phone, email, or text, and tricks the victim into voluntarily transferring funds or property to them.

Why your customers need False Pretense Coverage

With rapid innovations in technologies that enable cybercrimes, many businesses are vulnerable to these losses, which can be costly—and devastating—when a business assumes they will be covered by one of their policies, and they are not.

Commercial crime policies often do not cover false pretense crimes. Cyber insurance policies may only cover unauthorized access to systems and not resulting financial losses.

Hanover False Pretense coverage provides protection for the financial losses arising from the social engineering fraud: phishing, spear phishing, pretext, and impersonation, perpetuated by email, instant message, text, telephone or other electronic means.

Coverage Highlights

- Offered with standalone Hanover Fidelity & Crime Advantage or as part of Hanover's Private Company Advantage
- Limits up to \$100,000. Higher limits available on an individually underwritten basis

▶ Contact Us.

To learn more about how Hanover Fidelity & Crime can benefit your customers, contact Jennifer Moylan, Fidelity/Crime Manager, CORE Underwriting Center, 860-697-4338, jmoylan@hanover.com or visit hanover.com/agentsolutions

Could this happen to your clients?

- A CFO working remotely apparently sent an email request to the controller for a \$143,000 wire transfer to a trusted vendor, a routine procedure. After completing the transfer, they discovered a fraudster had spoofed the CFO's address, and had been conned.
- A fraudster created fake email addresses for a VP of Finance and one of their suppliers that were off by just one character, and not noticed by either party. After an email exchange through the fake addresses, the VP of Finances transferred a \$1,320,000 payment to the supplier account provided in the email, which turned out to be a fake account in China.

All products are underwritten by The Hanover Insurance Company or one of its insurance company subsidiaries or affiliates ("The Hanover"). Coverage may not be available in all jurisdictions and is subject to the company underwriting guidelines and the issued policy. This material is provided for informational purposes only and does not provide any coverage. For more information about The Hanover visit our website at www.hanover.com

©2015 The Hanover Insurance Group. All Rights Reserved.