Brown & Brown

PROPERTY & CASUALTY

Defending Your Business Against Deepfake Fraud

Authored by, Christopher Keegan and Jane Hahn

Deepfakes on social media platforms and those using email addresses and simulating voices are becoming increasingly common. For example, over $25 million was stolen from a large company in Hong Kong after an employee used deepfake simulations of their CFO and colleagues to receive payment information over Zoom[1]. This use of a deepfake indicates a rise in technologyand AI aiding in fraud attacks. Impersonation can cause a wide range of losses, many resulting in direct payment of funds to cybercriminals. In 2023, the Internet Crime Complaint Center (IC3) received 21,489 business email compromise (BEC) complaints, resulting in over $2.9 billion in adjusted losses[2].

Companies should think critically about utilizing methods to prevent fraudulent funds transfers that occur with information obtained through social engineering, information theft or deepfake technology.

How can you help protect your business?

Educate and Enlighten

- **Educate staff about deepfakes and BEC:** Stay informed about what deepfakes and BEC schemes criminals are employing and share this information with employees involved in the payment process.
- **Have treasury staff scrutinize content:** Teach employees who transfer funds to be skeptical of any unusual requests or instructions, especially if they involve financial transactions.

Verify Identity and Authenticity

- **Video and audio:** When participating in video conference calls or receiving audio messages requesting payments, verify the identity of participants. Confirm their legitimacy through other channels (official emails, phone calls to known people) for significant payments,
- **Supplier accounts**
  - » Confirm changes to bank details by phone from someone who knows the confirmer and using a previously provided contact number.
  - » Confirm changes to supplier bank details in writing to the supplier, only implementing changes after verification.
  - » Make a small first payment to a new supplier bank account and obtain confirmation of receipt
  - » Audits should be regularly completed by unconnected persons
- **Account changes:** Your customers, partners and payees should be instructed to follow the same process for changes advised for your accounts. Reiterate that any requests for changes, immediate action or lack of availability by phone or otherwise should be met with intense scrutiny.

1. A $25 Million Hong Kong Deepfake Scam on Zoom Shows New AI Risks - Bloomberg

2. 2023_IC3Report.pdf

Secure Your Systems

- **Securing funds transfer systems:** Aim to have funds transfer and banking systems in a separate secure physical location, logically segmented from the main network, accessible through separate hardened credentials, protected by multifactor authentication and, if available, strong privileged access management software. Take advantage of additional layers of authentication offered by financial institutions.
- **IT security best practices:** Limit credential theft by maintaining a strong information technology security posture, including communication platforms with end-to-end encryption, updated operating systems, frequent patching and training on phishing.

Develop Response Plan

- **Inform your organization and law enforcement:** If you encounter a scam, alert your company's IT or security team and report it to law enforcement or relevant authorities.
- **Inform insurers:** Report loss events to insurers as quickly as possible. The IC3 claims a success rate of more than 70% when recovering losses (freezing nearly $538 million of $758 million reported) involving fraudulent money transfers made to domestic accounts[3]. Speed is the key to preventing a loss.

Entities should avoid using standard email for wiring instructions or mentioning wire payments, as they are susceptible to infiltration exploits. Two-step verifications of any payments are critical when you cannot be certain of authenticity at first glance. For example, one phone call to the CFO at a known number would have prevented the $25 million loss in Hong Kong. Confirmation of instructions through an independent channel to a known individual at a known phone or contact point is now essential for large payments.

Available Insurance Coverages

Cyber

Cyber policies can cover a deepfake fraud, but only if they incorporate a social engineering provision alongside the other computer fraud provisions often incorporated in cyber policies. Many cyber policies do not include the loss of funds or social engineering extensions that must be requested. Narrower computer fraud and computer theft coverage often require a computer system breach. Most social engineering losses are implemented by an authorized system user; such coverages will not be broad enough. Social engineering coverage will be more extensive, triggered by the misrepresentation or fraudulent act that misleads an employee authorized to carry out financial transactions without restriction on how the payment is made.

3. 2023_IC3Report.pdf

Crime and Other Policies

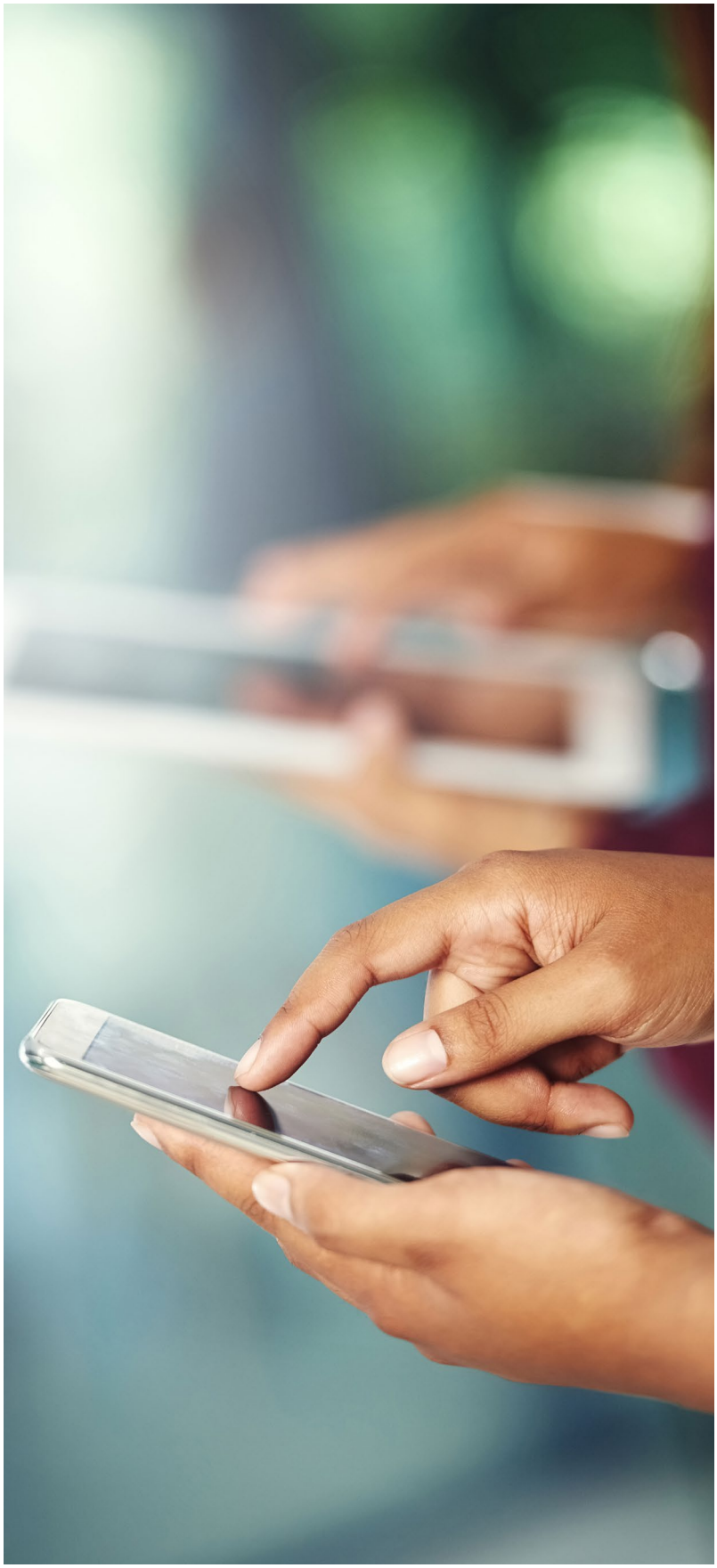
A comprehensive crime policy can cover monetary loss to an insured caused by a social engineering event; however, there is significant variation between insurers on the breadth and depth of the coverage. For example, many insurers limit coverage to claims where there has been "call-back verification."

A review of the social engineering insuring agreement should:

- Reference any electronic, written or digital instruction communicated to the financial institution or employee to transfer funds
- Require that, at minimum, the bad actor is claiming to be any director, officer, partner, member, sole proprietor, vendor, client, customer or governmental agency
- Look to expand verbal communication from bad actors utilizing AI to emulate any of the individuals through a deepfake as a means of entry.

While sublimits are common, many crime insurers are willing to write excess social engineering over primary sublimits at competitive rates. In addition, coordination with the cyber policy is imperative to determine which policy responds to a covered event as primary – crime is usually the better place. Most crime insurers have not embraced the expansion of social engineering to include AI deepfakes in their policies; thus, a careful review of the terms and conditions should be considered for broader language that contemplates AI deepfake exposures.

The pace of AI technology development will mean more sophisticated fraud in the coming years. Insurance markets can provide protection but will seek to have processes and procedures implemented. Entities should seek to align relevant insurance policies and ensure that language is sufficiently broad to cover intended events. Brown & Brown can help in this regard. Most importantly, companies should stay current with fraud methods and keep staff familiar with the most up-to-date controls.



How Brown & Brown Can Help

Connect with our Brown & Brown team to learn about our knowledge in your industry, how we build our risk mitigation strategies and how we can aid your business in building a cost-saving program.

Brown & Brown

Find Your Solution at BBrown.com