Deepfake Scammers Steal $25 Million From Company: 5 Ways You Can Avoid Being Victim to Latest AI Nightmare

Insights
2.09.24

A group of scammers recently used deepfake technology – now readily available to just about anyone – to trick a finance employee into paying them over $25 million of corporate funds. This might be one of the world's biggest AI-fueled heists, and it should lead your organization to immediately redouble your security efforts against this new nightmare scenario. What are the five things you can proactively do to protect your company and what are some steps you should take if you find yourself the victim of a deepfake scam?

How it Went Down

A Hong Kong finance employee at a multinational company thought something was suspicious when his chief financial officer – located in the UK – sent him an urgent email saying that they needed to discuss a secret business deal. In fact, the finance employee even suspected this might be a phishing expedition and proceeded with caution.

- But his fears disappeared when he joined a video call with the CFO and several other corporate executives. He recognized them all – their faces, their voices, their office backgrounds. They told him that the company was about to engage in a highly secretive business venture that required an immediate investment of capital, and that he was to lead the charge.
- Following the direction of the CFO and other corporate leaders, the finance employee initiated a series of 15 bank transfers to five different Hong Kong accounts totaling HK$200 million – or just over $25.6 million in U.S. dollars. The leaders almost certainly advised him to maintain the strictest discretion and not leak any information to his coworkers.
- About a week or so later, the finance employee checked with the company's home office to ask about the status of the secret deal. Except that there was no secret deal, and no one knew what he was talking about. That's when he realized he had been scammed, the victim of a sophisticated AI-fueled deepfake.
- "In the multi-person video conference, it turns out that everyone he saw was fake," said Hong Kong police official Baron Chan Shun-ching during a February 2 press briefing. The police did not release information about the identity of the company or the scammed employee given the pending nature of the criminal investigation.

What's a Deepfake?

What's a Deepfake?

Deepfakes are really, really good imitations. They are videos, audio, photos, text messages, and other forms of media created using AI that are extremely hard to differentiate from the real thing. Their aim is simple: to trick someone into thinking that something happened – or is happening – when it is actually untrue.

- In the Hong Kong case, the scammers used fabricated images of real individuals built from photos and videos that were easily obtainable online. They also convincingly replicated the voices using publicly available audio samples.
- Deepfakes have been in the news a lot lately. In just the past few weeks, we have heard stories about inappropriate deepfake videos of Taylor Swift and deepfake audio recordings purporting to be Joe Biden advising voters to stay home during the New Hampshire primary.
- What's scariest is that scammers can now use deep learning AI to improve their deepfakes. Everyone now has access to highly powerful modeling systems that can render incredibly convincing images, video, and audio.
- A recent report, in fact, indicated that advanced deepfake technology that makes it virtually impossible for people to distinguish fake videos from real will be available to everyone – even beginners – sometime this year.

No doubt this is not the last we're going to hear about deepfakes pervading our culture, our politics – and our workplaces – in 2024.

5 Considerations to Mitigate the Risk of Deepfakes

To guard against deepfakes, you should consider the following proactive measures, as first outlined by the FP AI Practice Group Chair Dave Walton and AI Team member Karen Odash in a November Insight:

1. **Offer Your Workers Deepfake Training:** Educate your employees about the existence and potential dangers of deepfakes. Start by showing them this Insight and describing what happened in Hong Kong. Explain how deepfakes work, their potential impact on the organization, and the importance of staying vigilant. This also involves fostering a culture of skepticism, similar to the way that employees are now on guard for phishing emails. Provide training about the ways to spot deepfakes (looking for blurry details, irregular lighting, unnatural eye or facial movements, mismatched audio, absence of emotion, etc.). As part of overall training, make sure your cybersecurity training is up to date and required for all employees.
2. **Develop Channels for Open Communication:** Employees must feel comfortable questioning the legitimacy of information and reporting any suspicious activity. Encourage them to speak up and promote a culture that supports open communication about questionable information and activity. Give employees examples of requests that are abnormal or outside the normal company procedures.

3. **Make Sure IT Adopts Robust Authentication Protocols:** Establish strong authentication measures for access to sensitive information, systems, and accounts. This may include multi-factor authentication, biometric verification, or other secure methods to minimize the risk of unauthorized access. Also, there must be failsafe measures for the requests involving financial and security issues. Assume that nefarious actors will use deepfakes to try to steal from your company. Implement multiple levels of approval before allowing certain actions to occur, such as transferring money above a certain threshold amount.
4. **Invest in New Threat-Detection Tools:** This is a developing area. Technology to protect against deepfakes has not kept up with the overall deepfake technology. But stay up to speed in this area and look for opportunities to invest in advanced technologies such as AI-powered deepfake detection tools as they become more robust. These might help identify and flag potential deepfakes.
5. **Review Your Policies:** Make sure your policies prohibit your employees from creating deepfakes involving company personnel and company proprietary information. There are very few legitimate businesses uses of deepfakes for most companies. In general, employees should not be allowed to use employer resources or data to create deepfakes.

3 Things to Do if Your Company is Victimized By a Deepfake

1. First, immediately contact your data security or artificial intelligence attorneys. Acting swiftly to protect data will help experts potentially find fingerprints that bad actors have left behind in a hurry after their scam worked. It is critical to engage counsel who have contacts with forensics experts and law enforcement to appropriately preserve and collect any information that could be used to trace the scammers. Acting quickly is important not just for the obvious reasons but also because electronic logs may only go back a certain number of days, and every day from the date of discovery is a day of lost data.
2. Second, resist the urge to do your own investigation. Well-intended searches of communications, e-mails, messages, and data entry could compromise the information addressed in point number one. Likewise, resist the urge to talk to others about the event until counsel is engaged and can protect and guide those discussions.
3. Third, work with your counsel to determine whether there is any required damage control. If you determine that protected or confidential information was accessed during the scam, you may be required to appropriately notify those affected. Your counsel can also help you contact your insurer and share appropriate information to determine if there is any coverage for the loss.

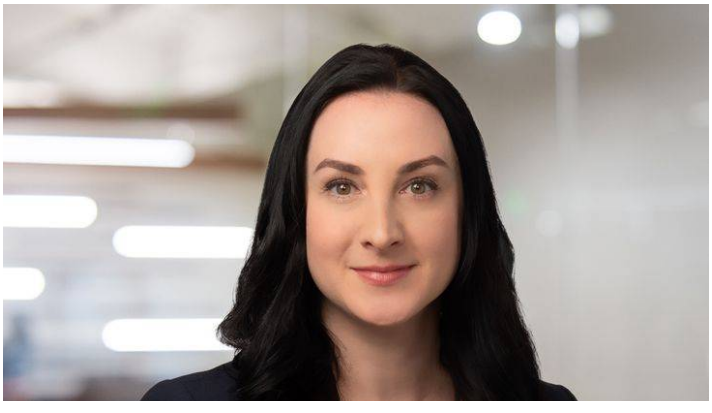
Conclusion

If you have questions, contact your Fisher Phillips attorney, the authors of this Insight, or any attorney in our Artificial Intelligence Practice Group. Make sure you subscribe to Fisher Phillips' Insight System to gather the most up-to-date information on AI and the workplace.

Related People

Wendy Hughes
Partner
610.230.6104
Email

Kelly Ahern
Associate
228.236.1764
Email



Marie Tedesco Scott
Partner
615.488.2904
Email

Service Focus

AI, Data, and Analytics

Counseling and Advice

Privacy and Cyber