KING & SPALDING

Financial Services

Providing Strategic Legal Guidance to the Global Financial Services Industry

OCTOBER 16, 2019

For more information,
contact:

Bill Gordon
+1 713 276 7373
+1 202 626 2944
bgordon@kslaw.com

John Horn
+1 404 572 2816
jhorn@kslaw.com

Thad Wilson
+1 404 572 4842
thadwilson@kslaw.com

King & Spalding

Atlanta
1180 Peachtree Street, NE
Atlanta, Georgia 30309-3521
Tel: +1 404 572 4600

Washington, D.C.
1700 Pennsylvania Avenue, NW
2nd Floor
Washington, D.C. 20006
Tel: +1 202 737 0500

Houston
1100 Louisiana Street
Houston, Texas 77002-5213
Tel: +1 713 751 3200

AI Driven "Deepfakes" Expose Holes in Corporate Compliance Programs: The Road to Recovery

Artificial intelligence ("AI") has made astounding advancements in recent years. Driven by incredible computing power, AI has the potential to change nearly every industry. AI is touted as having the potential to reduce disease outbreaks, detect never before seen objects, increase navigational accuracy and autonomous driving vehicles, and improve voice and facial recognition. Like most technological advancements, these breakthroughs present potentially great benefits. However, advancements in AI also present our clients with unprecedented risks in corporate compliance and risk management that demand immediate attention.

Particularly concerning are "deepfakes"—initially used to create phony photographs involving celebrities in compromising situations, the technology has graduated to realistic-looking or -sounding video and audio generated by robust computers and machine-learning software. "Deepfakes" can also be used to commit fraud and corporate theft.

Cybersecurity company Symantec[1] has reported that "deepfake" audio recently was used in three separate corporate attacks, where criminals played phony audio files during phone calls to cause the transfer of funds—basically, a new variation of the "business email compromise" schemes that have regained rampant popularity with cybercriminals across the world. The criminals are alleged to have culled samples from hours of speeches by the victim companies' CEOs during TED talks, earnings calls, and YouTube videos. "Deepfake" technology thus has the potential to cause immediate financial losses, adversely affect a company's financial performance, and give rise to many types of litigation, including lawsuits under various securities laws.

A recent real-world example highlights the potential dangers of "deepfakes." According to a recent report in the Wall Street Journal[2], a CEO of a U.K.-based energy firm was duped into wire transferring $243,000 into the account of criminals using AI to impersonate the voice of his boss, the CEO of the firm's German parent. The fake caller apparently used AI, in what is thought to be a first-of-its-kind crime, to impersonate the voice of the German CEO, including his unique accent and intonation. Because the UK CEO knew his boss's voice well, he was convinced it was a legitimate request and made the payment as requested. The "deepfake" impersonation was apparently well done—the criminals relied on it during three separate phone calls, although the third call tipped off the UK CEO enough to terminate all but one fraudulent transaction.

The fact that technology exists to allow criminals to pull off such a brazen theft is not shocking. Over the course of the past several decades, cyber-crimes have tracked many of the latest technological innovations, from blockchain, cryptocurrency, and AI-enabled password cracking. And relatively few companies have endeavored to adopt compliance programs and technologies to mitigate the risks and try to keep up with the more sophisticated criminal and nation-state actors.

However, many companies have not yet invested in the latest cybersecurity tools that can detect "deepfakes" or are unaware of such technologies, particularly live spoofed voices and video. Indeed, the fact that the technology to detect "deepfake" voice and audio spoofing is lagging makes it even more likely that video-conferences and audio-verification systems will be susceptible to similar spoofs and thefts.

Many banks and tax professionals use voice recognition, or voice biometrics, to confirm the identity of their customers. Countless numbers of corporate entities allow audio approvals, sometimes with voice biometrics, for payments within certain thresholds. Companies assume voice biometrics make identification faster and more secure. But with AI-aided "deepfake" technology now available to spoof voice biometrics, one should question whether this form of identification is secure and/or a best practice.

Advancements in AI thus necessitate immediate action to build and/or update corporate compliance programs to effectively deal with the impending threats from these technologies. Traditional approval methods may no longer be sufficient to guard against sophisticated AI attacks using "deepfake" technologies. We recommend seeking counsel experienced with these issues to ensure that your compliance program is up to the task—and technology.

Corporate compliance is just one area where "deepfake" technology can adversely impact your businesses. In forthcoming alerts, we will discuss other potential adverse consequences our clients may experience as the result of "deepfake" technologies.

ABOUT KING & SPALDING

Celebrating more than 130 years of service, King & Spalding is an international law firm that represents a broad array of clients, including half of the Fortune Global 100, with 1,100 lawyers in 21 offices in the United States, Europe, the Middle East and Asia. The firm has handled matters in over 160 countries on six continents and is consistently recognized for the results it obtains, uncompromising commitment to quality, and dedication to understanding the business and culture of its clients.

This alert provides a general summary of recent legal developments. It is not intended to be and should not be relied upon as legal advice. In some jurisdictions, this may be considered "Attorney Advertising."

ABU DHABI
ATLANTA
AUSTIN
BRUSSELS
CHARLOTTE
CHICAGO
DUBAI
FRANKFURT
GENEVA
HOUSTON
LONDON
LOS ANGELES
MOSCOW
NEW YORK
PARIS
RIYADH
SAN FRANCISCO
SILICON VALLEY
SINGAPORE
TOKYO
WASHINGTON, D.C.

[1] https://www.fastcompany.com/90379001/criminals-are-using-deepfakes-to-impersonate-ceos
[2] https://www.wsj.com/articles/fraudsters-use-ai-to-mimic-ceos-voice-in-unusual-cybercrime-case-11567157402