King & Spalding

Financial Services

Providing Strategic Legal Guidance to the Global Financial Services Industry

NOVEMBER 5, 2019

For more information, contact:

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

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

Aaron Lipson
+1 404 572 2447
alipson@kslaw.com

Brian Thavarajah
+1 202 626 5520
bthavarajah@kslaw.com

King & Spalding

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

Houston
1100 Louisiana Street
Suite 4000
Houston, Texas 77002-5213
Tel: +1 713 751 3200

"Deepfakes" Pose Significant Market Risks for Public Companies: How Will You Respond?

As we highlighted in our recent alert, "deepfakes" and related artificial intelligence technology pose substantial corporate compliance risks for financial institutions and companies alike. Proactive updates to compliance programs and technology together with vigilance can help protect against theft attempts and related schemes by cybercriminals.

For public companies and their officers and directors, however, the nefarious use of "deepfakes" presents potentially greater legal and financial challenges because of possible illegal attempts at market manipulation. Many public company directors and officers speak frequently in investor calls, media interviews, industry conferences and community events—usually leaving behind a trail of recorded video and audio. Consequently, these individuals are actively creating source materials allowing them to become the subject of a "deepfake." Bad actors may well use now freely available technologies to mine libraries of publicly available audiovisual records to create "deepfakes" that mimic statements by public company directors and officers.

The adverse effects of the use of a "deepfake" in this context could be considerable for a company and its shareholders. Not only could it trigger an investigation by the SEC, the FBI or other law enforcement agencies, but it could also result in shareholder lawsuits and fiduciary duty litigation. The following simple scenario highlights some of the challenges such a "deepfake" might raise.

It is not hard to imagine a video clip showing two chief executive officers shaking hands and congratulating themselves and their companies on the future they will share together, as they publicly disclose for the first time an agreed-to tender offer. As the video clip makes its way across social media platforms, financial news aggregators, and even websites apparently connected with the issuers, the share price of the offeree

skyrockets up 40% to just below the announced tender price. Normally these events are cause for celebration for the two issuers.

But in this case, no tender offer actually exists. A criminal enterprise has crafted a “deepfake” video by utilizing a treasure trove of public statements and recordings available on investor relations websites, corporate social media, and throughout the internet. Shortly before going live, the criminal enterprise invested in deep, out-of-the-money call options for the tender target, and perfectly timed its exit with the strike price having been reached. By the time the two public companies have responded, exchange circuit-breakers have been tripped and confusion and a lack of confidence in each issuer’s information results in the share prices falling below recent trading levels. Consequently, these public companies face an onslaught of adverse media requests and investigative activity from the SEC, FINRA, and likely criminal law enforcement, too. Existing shareholders are likely to suffer harm, and potential shareholder derivative lawsuits may even follow.

Though somewhat fantastical, the age of “deepfake” market manipulation is likely right around the corner. Market manipulations require the public dissemination of information—often false, positive information—to succeed. And there is analogous SEC precedent resulting from market manipulation schemes that is instructive.

Recent SEC actions have centered around the exploitation of the SEC’s EDGAR website to file fake tender offer notices for the purpose of artificially inflating the share price of publicly-traded companies and, consequently, benefitting previously-held trading positions by the perpetrators. Organized market manipulation rings are oftentimes willing to “invest” large sums to send spam email blasts, commission fake analyst reports, paper a message-board with touts, mail glossy hardcopy materials, or bankroll a boiler room.

The move to “deepfake” technology by more sophisticated manipulation rings—with the potential for a greater positive market “bang” with a much smaller promotional cost—is likely a question of when and not if. The ability to combat these fakes by corporate victims and regulators will be challenging. For one, “deepfakes” of public company executives could gain much broader dissemination among investors and in the press than a regulatory filing, especially when dealing with exciting, or even embarrassing (in an effort to drive down the price to support short activity), statements or conduct. Additionally, depending on the sophistication of a “deepfake,” companies may need time, and possibly the assistance of outside experts, to confirm that the released content does not reflect authentic remarks or conduct of an executive. Those steps could lead to a greater lag before the company can make subsequent corrective disclosures, thereby potentially expanding the period of stock price manipulation. Additionally, for those companies whose Twitter, Facebook, or corporate website are susceptible to being hacked, market manipulators are likely to look to those channels as a preferred means of distribution.

As illustrated by the example, “deepfakes” have the potential to create substantial issues for public companies and their directors and officers, including investigations and litigation. Accordingly, public companies would be well served to work with their legal and public relations advisors to revise their crisis management plans to address potential scenarios involving “deepfakes.” In a forthcoming alert, we will discuss other potential adverse consequences our clients, including public companies, may experience as the result of criminal and nefarious use 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.

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

[1] SEC Lit. Rel. No. 24204, July 17, 2018 (action alleging use of a fake tender offer filing to manipulate the price of Fitbit shares*); SEC v. PTG Capital Partners LTD, et. al.*, 15-CV-04290, (S.D.N.Y.) (June 4, 2015) (action alleging use of a fake tender offer filing to manipulate the price of Avon shares).