King & Spalding

Financial Services

Providing Strategic Legal Guidance to the Global Financial Services Industry

DECEMBER 16, 2019

For more information, contact:

Zack Harmon
+1 202 626 5594
zharmon@kslaw.com

Sumon Dantiki
+1 202 626 5591
sdantiki@kslaw.com

Brendon Walsh
+1 202 626 9267
bwalsh@kslaw.com

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

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

King & Spalding

Washington, D.C.
1700 Pennsylvania Avenue, NW
Washington, D.C. 20006-4707
Tel: +1 202 737 0500

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

Deepfakes, Artificial Intelligence, and Corporate Espionage

This is the third alert in our series on the risks to corporations, including financial services firms, posed by "deepfakes"—a type of technology, powered by artificial intelligence and machine learning, that can be used to create increasingly realistic, but false, audio and video. As discussed in our previous alerts, "deepfakes" have already successfully provided cybercriminals with novel ways to commit corporate fraud, generating new challenges for corporate compliance programs. Criminal enterprises can also build on earlier schemes and use deep fakes to illegally manipulate public markets, highlighting the need for companies to consider such deepfake scenarios in crisis management planning. As deepfake technology becomes simultaneously more sophisticated and widely available, malign actors will be interested in using deepfakes to do much more than commit traditional cybercrimes: nation-states are also keen to leverage this technology to commit corporate espionage, affect competitors or the commercial ecosystem, or otherwise benefit their governments or domestic companies.

Over the past few years, there has been a landmark uptick in state-sponsored corporate espionage. Since 2015, the Office of the Director of National Intelligence has reported that the cost of Chinese intellectual property and trade secret theft alone reaches into the hundreds of billions per year. FBI Director Wray similarly noted earlier this year that the Bureau has over a 1,000 open cases of attempted theft of U.S. intellectual property, across a range of industries and spanning its offices around the country.

Foreign governments have used nearly every possible tactic to gain access and commit such economic espionage, ranging from classic human influence techniques to sophisticated digital attacks—and everything in between. Deepfakes are fast becoming another vector to enable access and commit a variety of malicious acts. Indeed, McAfee Labs earlier this month predicted that in 2020 less skilled actors would gain greater access to more effective deepfake technology. As we previously discussed, criminals have already used these techniques this year to successfully commit fraud. Press reports from earlier this year also suggest that foreign

spies are beginning to use deepfakes to enable their espionage efforts through enhanced false social media personas.

Ultimately, foreign nation-states, criminals, and even business competitors, could use deep fakes against a corporate target in several ways, including to:

- Steal money, commit financial fraud, or enable cyberattacks like ransomware;
- Facilitate destructive malware attacks, particularly against industries in critical infrastructure, such as energy, defense contractors, or life sciences;
- Steal PII or other sensitive data either for criminal or foreign intelligence purposes;
- Gain access and steal crown jewel IP, sensitive technologies, and trade secrets;
- Disrupt business operations, for either ideological or commercial reasons;
- Assist in securing the support of key business constituencies, such as customer or supplier relationships;
- Create false “evidence” to affect legal or regulatory proceedings;
- Perpetrate disinformation campaigns targeting particular companies;
- Manipulate market conditions;
- Manufacture a damaging public relations crisis, such as tainted products.

It is only a matter of time until adversaries make more widespread use of deepfakes. In an industry forecast released this month, the credit-reporting company Experian identified deepfakes as a top data breach trend for 2020, predicting that they would be used to “disrupt the operations of large commercial enterprises, and potentially create geo-political confusion among nation states, in addition to disruption in financial markets.”

Against this dynamic threat landscape, corporations need to take a holistic, forward-leaning approach that accounts for AI-enabled attempts to target them with technologies like deepfakes. A successful strategy should, at a minimum, examine and update existing threat awareness capabilities, cybersecurity measures, training and compliance programs, tabletop exercises, crisis management planning, and resilience protocols.

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	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.