Session II

Focus China:
Great Rewards, Great Risk

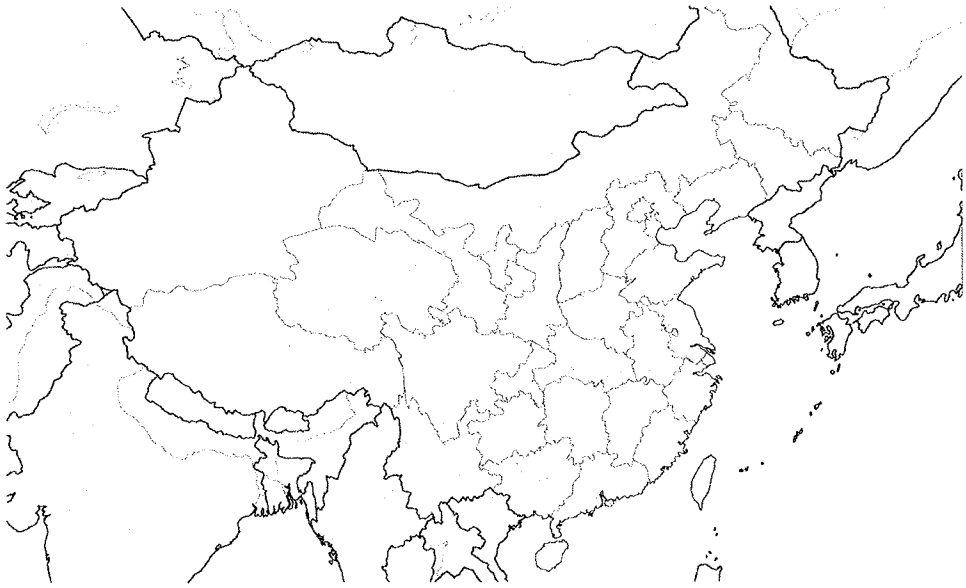
- PowerPoint
- *The China Conundrum: Balancing Risk and Reward*, Compliance Week, By Joe Mont (January 17, 2018) (reprinted with permission)
  Available at: https://www.complianceweek.com/news/news-article/the-china-conundrum-balancing-risk-and-reward#.W0ZVM02ovcs
- *Implications of FCPA on Doing Business in China*, By Catherine X. Pan-Giordano, Lei Li (July 11, 2018)
- *U.S. Citizens' Legal Exposure Related To Foreign Commercial Bribery*, By Beth Forsythe & J Jackson
- *China's Commercial Bribery Law, A Summary of Amendments Effective January 1, 2018*, By J Jackson
- 2017 China Law LEXIS 1236 (reprinted with permission)

DORSEY always ahead

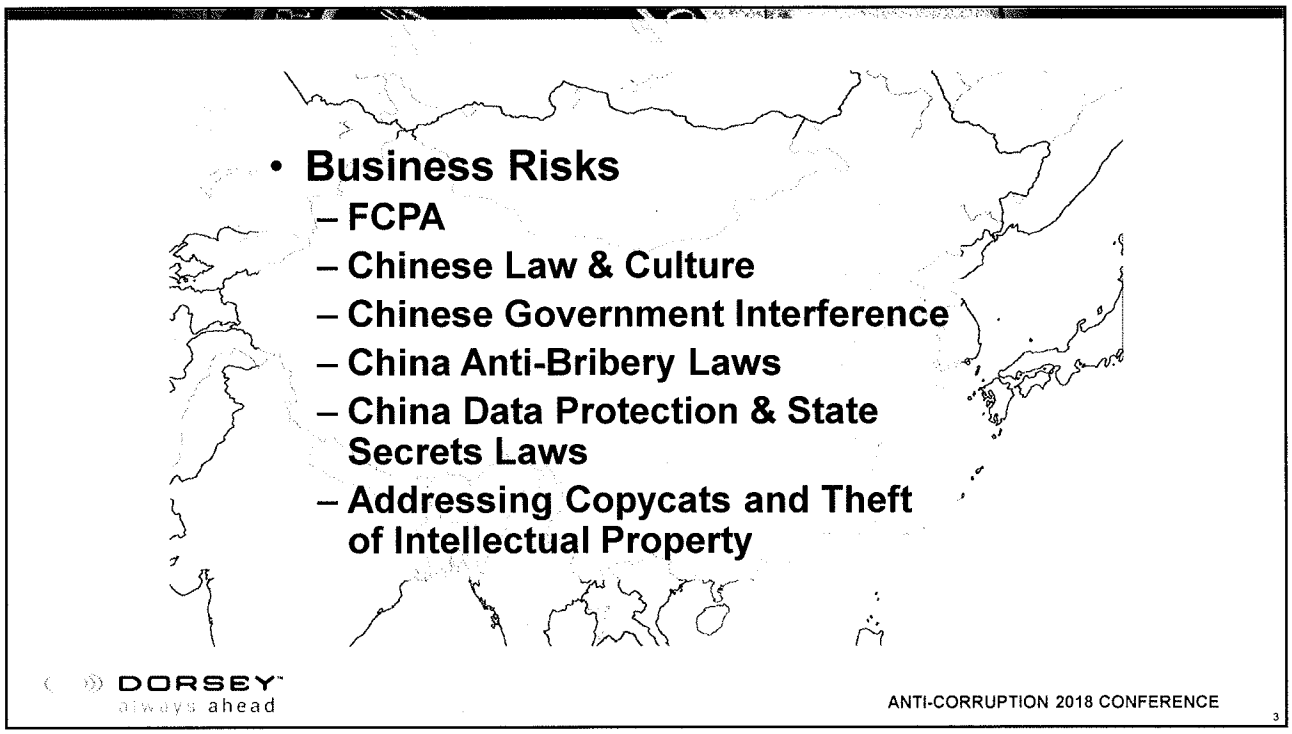
Focus China: Great Rewards, Great Risk

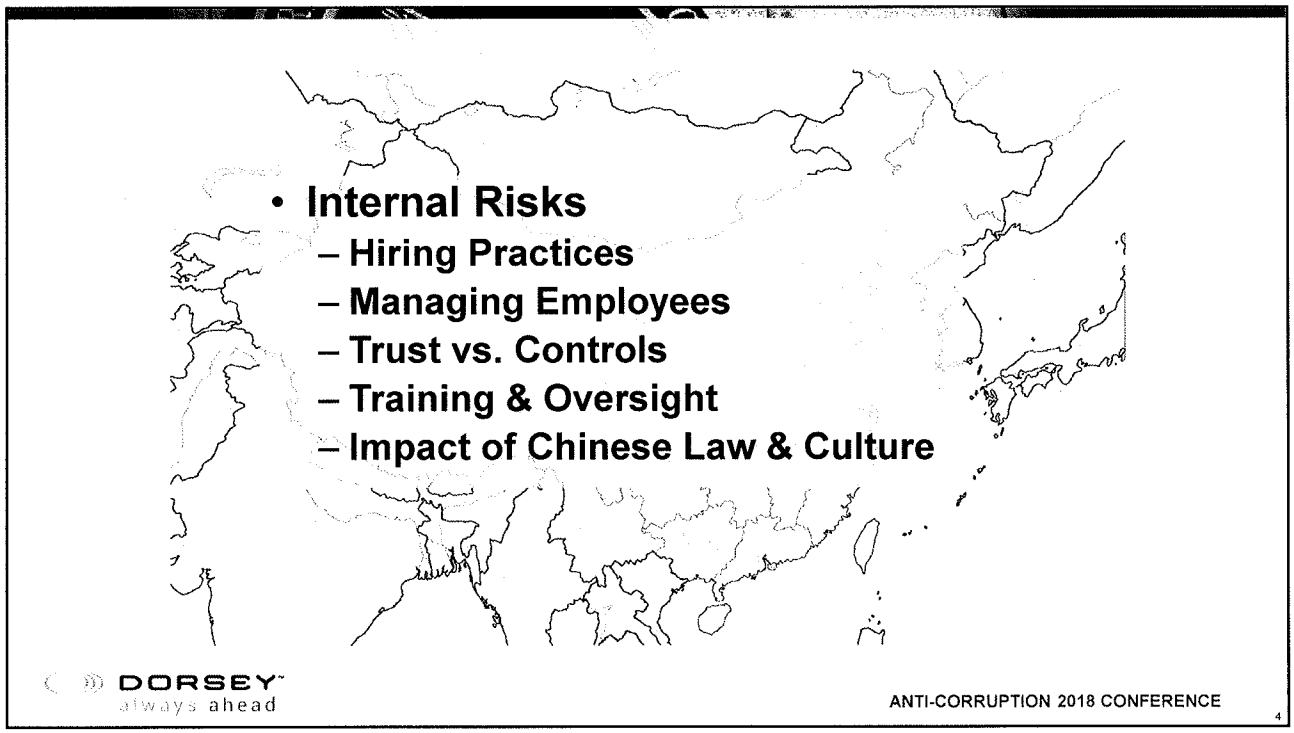
Michael J. Hoff, Tennant Company
Francisco Santamaria, Sinotau Pharmaceuticals
Catherine Pan-Giordano, Dorsey & Whitney LLP
J Jackson, Dorsey & Whitney LLP

1



DORSEY always ahead


• Business Risks
– FCPA
– Chinese Law & Culture
– Chinese Government Interference
– China Anti-Bribery Laws
– China Data Protection & State Secrets Laws
– Addressing Copycats and Theft of Intellectual Property
DORSEY
always ahead
ANTI-CORRUPTION 2018 CONFERENCE
3


• Internal Risks
– Hiring Practices
– Managing Employees
– Trust vs. Controls
– Training & Oversight
– Impact of Chinese Law & Culture
DORSEY
always ahead
ANTI-CORRUPTION 2018 CONFERENCE
4

Questions?

The China conundrum: balancing risk and reward

China is both highly prized and under-penetrated by U.S. companies. Recent deterrents, including tough trade talk by the Trump Administration and confusing new cyber-security laws, may keep things that way.

On the trade front, Presidential intervention in cross-border mergers has traditionally been a rarity. The current administration shows no signs, however, of following that tradition and sitting on the sidelines.

Under the Defense Production Act, the President is authorized to suspend or prohibit certain acquisitions that result in foreign control of a U.S. business if he or she concludes there is credible evidence that the foreign interest exercising control might take action that threatens to impair national security.

On Jan. 10, MoneyGram and Ant Financial Services Group mutually agreed to terminate their planned merger due to the inability of the companies to obtain the required approval for the transaction from the Committee on Foreign Investment in the United States (CFIUS). The rejection came despite "extensive efforts to address the Committee's concerns," they said.

MoneyGram is a global provider of money transfer services. Ant Financial Services Group, an affiliate of China-based Alibaba, "is focused on serving small and micro enterprises, as well as individuals.

On April 16, 2017, MoneyGram and Ant Financial had entered into an amended merger agreement under which Ant Financial would acquire all the outstanding shares of MoneyGram for $18.00 per share in cash.

Reprinted with permission © 2018 Compliance Week.

"The geopolitical environment has changed considerably since we first announced the proposed transaction with Ant Financial nearly a year ago," Alex Holmes, CEO of MoneyGram, said in a statement. "Despite our best efforts to work cooperatively with the U.S. government, it has now become clear that CFIUS will not approve this merger."

In September, with another example of the White House flexing its trade muscles, it utilized a CFIUS review to block the sale of Lattice Semiconductor to a consortium of Chinese investment funds that had agreed to buy it for $1.3 billion.

"The national security risk posed by the transaction relates to, among other things, the potential transfer of intellectual property to the foreign acquirer, the Chinese government's role in supporting this transaction, the importance of semiconductor supply chain integrity to the U.S. government, and the use of Lattice products by the U.S. government," the executive order scuttling the deal said.

With the White House already inclined to block Chinese business deals, proposed legislation may give it even more ammunition.

In November, U.S. Senators John Cornyn (R-Texas), Dianne Feinstein (D-Calif.), and Sen. Richard Burr (R-N.C.), introduced the Foreign Investment Risk Review Modernization Act. Its goal: to modernize and strengthen the process by which the Committee on Foreign Investment in the United States reviews acquisitions, mergers, and other foreign investments in the United States for national security risks.

Specifically, the Foreign Investment Risk Review Modernization Act would:

- Expand the CFIUS jurisdiction to include certain joint ventures, minority position investments, and real estate transactions near military

bases or other sensitive national security facilities.

- Update the Committee's definition of "critical technologies" to include emerging technologies that could be essential for maintaining the U.S. technological advantage over countries that pose threats, such as China.
- Allow foreign investors to submit "light filings" to CFIUS for certain types of transactions.
- Add new national security factors for CFIUS to consider in its analyses.

The bill would also authorize CFIUS to exempt certain otherwise covered transactions if all foreign investors are from a country that meets certain criteria, such as being a U.S. treaty ally and having a mutual investment security arrangement.

Predictions are afoot that, if passed, the bill would make Presidential merger reviews and rejections far more commonplace.

> ***"We are deeply concerned that current and pending security-related rules will effectively erect trade barriers along national boundaries that effectively bar participation in your market and affect companies across industry sectors that rely on information technology goods and services to conduct business."***
>
> *The U.S.-China Business Council*

Also in the works is the Defending U.S. Government Communications Act,

introduced by Rep. Mike Conaway (R-Texas), which would prohibit the U.S. government from purchasing or leasing telecommunications equipment and/or services from Chinese tech companies Huawei, ZTE, or any subsidiaries or affiliates.

"Chinese commercial technology is a vehicle for the Chinese government to spy on United States federal agencies, posing a severe national security threat," Conaway said. "Allowing Huawei, ZTE, and other related entities access to U.S. government communications would be inviting Chinese surveillance into all aspects of our lives."

U.S. lawmakers are reportedly working behind the scenes to urge wireless carriers, in particular AT&T, to sever commercial ties to Huawei.

Legislators also, reportedly, are fighting plans by China Mobile, the world's largest mobile phone operator, to enter the U.S. marketplace.

China, intentionally or not, is also doing its part to create cross-border trade obstacles, notably with tough new cyber-security rules.

New laws went into effect June 1, provisions on matters such as the storing of data in China and security reviews of network equipment.

China says "critical information infrastructure" companies include those with computer-network operations in telecommunications, energy, transportation, information services, and finance. Foreign business groups say the definition is vague and too broad.

While many companies continue to fret uncertainties in the law and sweat its details, others quickly fell in line after the June 1 enactment, lest they fall in disfavor with the Chinese government. Apple announced plans to store all cloud data for Chinese customers with a government-owned company to

comply with the new rules.

Apple also stopped selling virtual private network apps that might enable Chinese citizens to bypass censored Websites. Similarly, Microsoft released a new version of its operating system: Windows 10 China Government Edition, a partnership with China Electronics Technology Group.

The law is also causing enforcement troubles for U.S. companies. Earlier this month, Chinese regulators suspended Marriott International's Chinese Website when an online questionnaire for its rewards program inadvertently categorized Chinese territories (Macau, Taiwan, and Tibet) as separate countries.

The faux pas was also a violation of the new cyber-security law. It prohibits any online activity that "undermines the country's sovereignty and territorial integrity."

Critics of China's cyber-security law include the U.S.-China Business Council.

The cyber-security law primarily applies to the construction, operation, maintenance, and usage of networks, as well as network security supervision and management within the mainland territory.

The overall intent, the law states, is "to ensure network security, to safeguard cyber-space sovereignty, national security, and the societal public interest," but critics, such as the U.S.-China Business Council see things differently.

"We are deeply concerned that current and pending security-related rules will effectively erect trade barriers along national boundaries that effectively bar participation in your market and affect companies across industry sectors that rely on information technology goods and services to conduct business," the Council wrote in a recent open letter.

Included in the law is a data localization requirement. It requires that personal information and other "important data" gathered and produced by "critical information infrastructure" (CII) operators must be stored on servers physically located within mainland China.

This, critics say, could pose challenges for multinational companies needing transfer data across borders in their business operations. "Personal information" broadly, and perhaps ambiguously refers to information, recorded electronically or through other means, that taken alone or together with other information is sufficient to identify a natural person's identity, including, but not limited to, full name, birth dates, identification numbers, address, and telephone number.

CII operators found in violation of the data localization provision will be sanctioned with a warning, or worse, the confiscation of unlawful gains, Website shutdown, revocation of relevant operations permits, or a hefty fine.

The law also imposes numerous data protection measures on network owners, managers, and network service providers. Among the demands: maintaining the confidentiality of user information they collect; making data privacy notices publicly available, explicitly stating the purposes, means, and scope for collecting or using information; adopting technical measures to ensure the security of personal information and prevent against loss, destruction, or leaks; and, in the event of a data security breach, taking immediate remedial action and promptly notifying users and relevant authorities.

The law stipulates that network operators shall not provide an individual's personal information to others without the individual's consent or illegally sell an individual's personal data; gather personal information unrelated to the services they provide; or disclose, tamper with, or destroy personal

information that is gathered.

Those last requirements, building blocks for other cyber-security regimes, are especially similar to the European Union's controversial General Data Protection Regulation.

Another stipulation: Network security products and services procured by CII operators that may impact national security must pass a cyber-security review by an expert panel.

"CSL will present an unprecedented challenge for international businesses with operations in China," law firm Reed Smith said in a recent client advisory on the matter. "The path to CSL compliance is not straightforward. The Chinese legislative and enforcement style creates confusion and misunderstandings, and sometimes false hopes for Western companies."

Xiaoyan Zhang, counsel at Reed Smith, offers a three-step plan for compliance: conduct a CSL compliance-risks assessment with a focus on content monitoring, IT procurement, and cross-border data transfer; conduct in-depth data due-diligence for new or existing mission-critical business operations in China; and conduct a comprehensive data audit to operations in China.

"CSL compliance is not an equivalent to compliance in China because there are a dozen other laws in the pipeline, in addition to other laws that are already established," Zhang warned. "If you somehow reach compliance in China, which seems impossible right now, focus on best practices regarding security risks, business continuity, and increasing consumer confidence."

Issues to scrutinize include procurement, outsourcing, privacy policies, privacy and security procedures, and cross-border data transfers.

"How much investment are you willing to put in to strengthen your IT and data collection practices in china?" Zhang asks. Not only does the training needed for employees and vendors take time, "you cannot go to your favorite vendor, one you have been using for the past several years."

"You need to go through the government authority to find IT equipment," she says.

"Before you collect data, have you actually obtained consent from the user, in addition to just giving them notice?" Zhang asks, warning that compliance policies must be followed in practice, and "translated, localized, and customized to local practice."

Other advice: Conduct a tailored assessment for mission-critical business.

"That includes existing business and plans once you push into China," Zhang says. "That is for obvious reasons. You don't want to invest money and energy in some future business only to find out later that you cannot, or should not, under CSL or other laws."

Order a Reprint

DORSEY
DORSEY & WHITNEY LLP

MEMORANDUM

FROM: Catherine X. Pan-Giordano, Lei Li, Dorsey & Whitney LLP

Re: **Implications of FCPA on Doing Business in China**

DATE: July 11, 2018

CURRENT CASES

In June, 2018, Credit Suisse Hong Kong Ltd. agreed to pay a $47 million penalty to the Department of Justice (the "DOJ") to end an investigation concerning potential violations of the Foreign Corrupt Practices Act ("FCPA") related to its hiring practices in the Asia Pacific region. Credit Suisse Group AG first disclosed that the DOJ and the Securities and Exchange Commission (the "SEC") was investigating whether Credit Suisse hired referrals from government agencies and other state-owned entities in exchange for investment banking business and/or regulatory approvals in February this year. This is not the first FCPA-related investigation of a company's hiring practices in Asia. In 2016, JPMorgan Chase paid $264 million in penalties to the DOJ, the SEC, and the Federal Reserve for awarding jobs to relatives and friends of Chinese government officials to win banking deals. Other banks that disclosed FCPA-related investigations based on hiring practices include Citigroup Inc.,[1] Barclays PLC,[2] Deutsche Bank,[3] HSBC Holdings plc,[4] and Goldman Sachs Group, Inc.[5] Nor are the "Sons and Daughters" inquiries confined to financial services companies. In 2016, mobile chipmaker Qualcomm Inc. paid the SEC $7.5 million to settle FCPA offenses for hiring relatives of Chinese government officials.

On April 23, 2018, The Dun & Bradstreet Corporation reached a $9 million resolution with the SEC and the DOJ over allegations that Dun & Bradstreet violated the FCPA when its two Chinese subsidiaries used third-party agents to make unlawful payments to obtain data vital to Dun & Bradstreet's business in China between 2006 and 2012. A core component of Dun & Bradstreet's business model, including its credit reporting business, includes access to business data. The two subsidiaries, Shanghai Huaxia Dun & Bradstreet Business Information Consulting

---

[1] Citi Says U.S. Regulators Are Investigating Its Foreign Hiring Practices, February 24, 2017 (available at https://www.bloomberg.com/news/articles/2017-02-24/citi-says-u-s-regulators-probing-its-foreign-hiring-practices).
[2] Barclays Falls Under SEC Spotlight for Asian Hiring, March 1, 2016 (available at https://www.wsj.com/articles/barclays-falls-under-sec-spotlight-for-asian-hiring-1456826347).
[3] Regulators investigate Deutsche Bank in China 'princeling' probe, June 5, 2014 (available at https://uk.reuters.com/article/uk-deutsche-bank-princelings/regulators-investigate-deutsche-bank-in-china-princeling-probe-idUKKBN0EG2BT20140605).
[4] HSBC probed by SEC over Asia hiring practices, February 22, 2016 (available at https://www.ft.com/content/d070ed3a-d917-11e5-a72f-1e7744c66818).
[5] US Accelerates Pursuit Of Companies For FCPA Violations, December 23, 2016 (available at https://www.forbes.com/sites/erikakelton/2016/12/23/us-accelerates-pursuit-of-companies-for-fcpa-violations/#4964dec050b0).

Co., Limited and Shanghai Roadway D&B Marketing Services Co., Ltd. ("Roadway DB"), paid government officials, including employees of China's State Administration of Industry and Commerce, other agencies, and state-owned entities, to obtain proprietary data for Dun & Bradstreet's global commercial database. Roadway DB's practices first caught the public eye when a television news program featured a Roadway DB sales executive stating that Roadway DB created a database with information on over 150 million Chinese citizens, access to which Roadway DB sold for marketing purposes on March 15, 2012. The same day, local police raided the Roadway offices in Shanghai. Dun & Bradstreet suspended and then shut down Roadway DB's operations shortly after the raid. In September 2012, Roadway DB and five employees were subsequently convicted of illegally obtaining private information of Chinese citizens by the Shanghai District Prosecutor. Subsequently, in January 2013, Roadway DB and the five individuals were convicted and Roadway DB was required to pay an approximately $160,000 criminal fine.

These cases again highlight the special risks associated with corruption and bribery present in conducting business operations in the People's Republic of China ("PRC").These risks are further amplified when the operations deal with PRC state-owned entities.

BACKGROUND AND SUMMARY OF CONCLUSIONS

Congress enacted the FCPA in 1977 to deter corporate bribery of foreign officials.[6] The FCPA contains two major parts. First, it prohibits U.S. citizens and certain foreign companies and individuals from bribing foreign officials to obtain or maintain business. Second, the FCPA requires companies with securities listed on a U.S. exchange to develop and maintain books and records that accurately reflect the transactions of the corporation and to devise and maintain adequate systems of internal accounting controls. The DOJ is responsible for all criminal enforcement of the FCPA as well as civil enforcement of the anti-bribery provisions applicable to domestic concerns and foreign companies and nationals. The SEC has jurisdiction over civil enforcement of the anti-bribery and books and records provisions applicable to issuers of securities.

This memorandum summarizes the key provisions of the FCPA and surveys the current state of federal enforcement actions including those affecting corporate entities doing business in the PRC. In recent years, the SEC and the DOJ have substantially stepped up efforts to investigate and prosecute suspected violations of the FCPA. These efforts have been buoyed by increased resources provided by Congress and a renewed interest in corporate malfeasance sparked by the Enron debacle. Aggressive FCPA enforcement activities have been particularly apparent in the context of the PRC, where payments to "foreign officials" are often necessary to secure business and where the distinction between purely private entities and government officials is blurred. Companies facing criminal indictment for FCPA violations have shown little appetite for challenging federal prosecutors, opting instead to secure agreements with federal investigators. These agreements often result in the payment of fines and the establishment of internal auditing controls under deferred prosecution agreements. With the federal enforcement

[6] Foreign Corrupt Practices Act of 1977, Pub.L.No. 94-23, 91 Stat. 1494 (codified as amended at 15 U.S.C. 78m, 78dd-1 to 78d-3, 78-ff).

efforts on the dramatic rise, companies have taken a particular interest in DOJ policies affecting business interests in the PRC.

SUMMARY OF FCPA PROVISIONS

Anti-Bribery Provisions

In broad terms, the anti-bribery provisions of the FCPA make it unlawful for a U.S. person, a U.S. company as well as foreign companies that meet the requirements of the statute from making payments to a "foreign official" for the purpose of obtaining or retaining business for or with, or directing business to any person.[7] It also applies to third parties who assist in furtherance of FCPA prohibitions.[8] The statutory elements necessary to demonstrate a violation of the FCPA are drafted broadly, thereby giving the Department of Justice wide discretion in enforcing its provisions. The following summarizes the key provisions of the anti-bribery portion of the statute.

Covered Persons and Entities

The FCPA potentially applies to a myriad of persons and entities including any individual, firm, officer, director, employee, or agent of a firm and any stockholder acting on behalf of a firm.[9] Individuals and firms may also fall within the statute's purview if they authorize or assist someone else to violate the anti-bribery provisions or if they conspire to violate those provisions.[10] The applicability of the FCPA's prohibitions depends on whether the violator is an "issuer," a "domestic concern," or a foreign national or business.

- An "issuer" includes any corporation that has issued securities registered in the U.S. or who is required to file periodic reports with the SEC.[11]

- A "domestic concern" is defined as "any individual who is a citizen, national, or resident of the United States, or any corporation, partnership, association, joint-stock company, business trust, unincorporated organization, or sole proprietorship which has its principal place of business in the United States, or which is organized under the laws of a State of the United States or a territory, possession, or commonwealth of the United States."[7]

- In 1998, Congress expanded the scope of the FCPA to include territorial jurisdiction over foreign companies and nationals.[12] A foreign company or person is now subject to the FCPA if it causes, directly or through agents, an act in furtherance of corrupt payments within the U.S.[13]

With respect to federal jurisdictional requirements, issuers and domestic concerns are liable if they initiate an act in furtherance of a corrupt payment to a foreign official using the U.S.

---

[7] 15 U.S.C. §§ 78dd-1 *et seq.*

[8] 15 U.S.C. § 78dd-3.

[9] *See* 15 U.S.C. § 78dd-2(h) (defining "domestic concern").

[10] 15 U.S.C. § 78dd-3(a).

[11] 15 U.S.C. § 78dd-1(a).

[12] P.L. 105-366, International Anti-Bribery and Fair Competition Act of 1998 (Nov. 10, 1998; 112 Stat. 3302).

[13] 15 U.S.C. § 78dd-3.

mails or other means or instrumentalities of interstate commerce.[14] Such means or instrumentalities include telephone calls, internet, facsimile transmissions, wire transfers, and interstate or international travel.[15] In addition, issuers and domestic concerns may be held liable for taking steps that facilitate the making of a corrupt payment outside the U.S.[16] DOJ has interpreted this language broadly subjecting U.S. companies to liability for corrupt payments authorized by employees or agents operating outside the U.S.

For foreign companies, there is no requirement that the act prohibited by the statute make use of the U.S. mails or other means or instrumentalities of interstate commerce. Under section 78dd-3, foreign corporations or nationals may be held liable for any act that furthers the prohibited payment as long as the actual payment takes place within the boundaries of the U.S.[17] For example, a foreign company may be held liable if it initiates a corrupt payment that, at some point, moves through the U.S. banking system. In addition, U.S. parent corporations and their employees and agents may be held liable for the acts of foreign subsidiaries where they authorized, directed, or controlled the activity in question.[18] DOJ, in its enforcement actions, has interpreted this section of the statute broadly with little interference by the courts.

Payment or Offer to Pay

Under the FCPA, covered persons and entities are prohibited from paying, offering, or promising to pay money or anything of value.[19] In other words, the act to influence a business decision need not succeed, but the mere offer or promise of a corrupt payment is enough to constitute a violation of the statute. In addition, the person making or authorizing the payment must have a corrupt purpose.[20] Specifically, the statute prohibits any payment intended to influence "any act or decision of such foreign official in his official capacity, inducing such foreign official to do or omit to do any act in violation of the lawful duty of such official, or securing any improper advantage," or to induce a "foreign official to use his influence with a foreign government or instrumentality thereof" to improperly affect or influence any act or decision.[21]

Recipient of Payment or Offer to Pay

FCPA violations extend to corrupt payments made to a foreign official, a foreign political party or party official, or any candidate for foreign political office.[18] The statute defines "foreign official" broadly to include "any officer or employee of a foreign government or any department, agency or instrumentality thereof, or of a public international organization, or any person acting in an official capacity for or on behalf of any such government or department, agency, or instrumentality, or for or on behalf of any such public international organization."[22] The broad scope of this statutory definition has proven particularly troublesome for companies doing

---

[14] 15 U.S.C. §§ 78dd-1(a) and 78dd-2(a).

[15] *See* 15 U.S.C. §§ 78dd-2(h)(5); *see also* Department of Justice, *Lay-Person's Guide to FCPA* (available at http://www.usdoj.gov/criminal/fraud/docs/dojdocb.html).

[16] 15 U.S.C. §§ 78dd-1(a) and 78dd-3(a).

[17] 15 U.S.C. §§ 78dd-3(a).

[18] U.S.C. §§ 78dd-1(a), 78dd-2(a), and 78dd-3(a).

[19] *Id.*

[20] *Id.*

[21] *Id.*

[22] 15 U.S.C. §§ 78dd-1(f)(1), 78dd-2(h)(2), and 78dd-3(f)(2).

business in the PRC where it can be a challenge to differentiate government and party officials from business partners not connected to the government. The FCPA, however, includes certain exceptions, such as payments used to facilitate "routine governmental action," discussed in more detail below.[23]

Business Purpose

The FCPA prohibits payments made in order to assist a company in obtaining or retaining business for or with, or directing business to, any person.[24] The Department of Justice interprets "obtaining or retaining business" to encompass more than the mere award or renewal of a contract.[22] It should be noted that the business to be obtained or retained does not need to be with a foreign government or an instrumentality of a foreign government.[25]

Third Party Payments

The FCPA prohibits payments made through third parties. The statute makes it unlawful to pay a third party, while knowing that all or a portion of the payment will go directly or indirectly to a foreign official.[26] The term "knowing" includes awareness of the conduct or result, and conscious disregard or deliberate ignorance of the action's repercussions.[27] Otherwise, the elements necessary to prove a violation of the FCPA applicable to third parties are identical to those that apply to domestic concerns or issuers.

Permissible Payments

There is an exception to the anti-bribery prohibition for payments made to facilitate or expedite performance of "routine governmental action."[28] Under the FCPA, "routine governmental action" includes obtaining permits, licenses, or other official documents; processing governmental papers, such as visas and work orders; providing police protection, mail pick-up and delivery; providing phone service, power and water supply, loading and unloading cargo, or protecting perishable products; and scheduling inspections associated with contract performance or transit of goods across country.[29] "Routine governmental action" does not include any decision by a foreign official to award new business or to continue business with a particular party.

Affirmative Defenses

A person charged with a violation of the FCPA's anti-bribery provisions may raise as an affirmative defense that the payment was lawful under the written laws of the foreign country or

---

[23] 15 U.S.C. §§ 78dd-1(b), 78dd-2(b), and 78dd-3(b).

[24] 15 U.S.C. §§ 78dd-1(a)(2), 78dd-2(a)(2), and 78dd-3(a)(2). Department of Justice, *Lay-Person's Guide to FCPA* (available at http://www.usdoj.gov/criminal/fraud/docs/dojdocb.html).

[25] 15 U.S.C. §§ 78dd-1(a)(2), 78dd-2(a)(2), and 78dd-3(a)(2).

[26] *Id.*

[27] 15 U.S.C. §§ 78dd-1(f)(2), 78dd-2(h)(3), and 78dd-3(f)(3).

[28] 15 U.S.C. §§ 78dd-1(b), 78dd-2(b), and 78dd-3(b).

[29] 15 U.S.C. §§ 78dd-1(f)(1), 78dd-2(h)(2), and 78dd-3(f)(2).

that the funds were spent to demonstrate product performance or to fulfill a contractual obligation.[30]

Record-Keeping and Internal Control Provisions

The record keeping and internal control provisions of the FCPA are designed to supplement and facilitate detection of the FCPA's anti-bribery provisions. The statute applies only to "issuers," companies whose securities are registered with the SEC or who are required to file periodic reports with the SEC; however, other companies may voluntarily implement similar record keeping and internal control policies as a good practice. The FCPA requires issuers to "make and keep books, records, and accounts which, in reasonable detail, accurately and fairly reflect the transactions and dispositions of the assets."[31] It also requires issuers to install a system of internal accounting controls sufficient to provide reasonable assurances that:

(1) transactions are executed in accordance with management's general or specific authorization;

(2) transactions are recorded as necessary;

(3) access to assets is permitted only in accordance with management's general or specific authorization; and

(4) the recorded accountability is compared with the existing assets at reasonable intervals and appropriate action is taken with respect to any differences.[32]

Compliance with the FCPA's disclosure provisions can be onerous, because the statute requires more than the disclosures mandated by securities laws such as financial statements and executive compensation information. In addition, there is no requirement that violations be intentional or that violations be "material."[33] The record-keeping and internal control provisions of the FCPA are primarily regulated and enforced by the SEC, although the DOJ can bring criminal charges for "knowing" violations of the statute.[34]

Penalties

Individuals who commit willful violations of the FCPA anti-bribery provisions may be fined by up to $100,000 and/or imprisoned for up to five years.[35] Individuals who violate the FCPA accounting provisions are subject to fines of up to $5,000,000 and prison terms of up to 20 years.[36] Corporations may be fined up to $2,500,000 per violation of the statute's accounting provisions and $2,000,000 per violation of the FCPA's anti-bribery provisions.[37] The penalties apply regardless of whether the company is an "issuer," a "domestic concern" or a foreign entity. While

---

[30] 15 U.S.C. §§ 78dd-1(c), 78dd-2(c), and 78dd-3(c).
[31] 15 U.S.C. § 78m.
[32] 15 U.S.C. § 78m(b)(2).
[33] 15 U.S.C. § 78m(b)(5).
[34] 15 U.S.C. § 78m(a).
[35] 15 U.S.C. § 78dd-2(g)(2)(A); 78dd-3(e)(2)(A); 78ff(c)(2)(A).
[36] 15 U.S.C. § 78ff(a).
[37] 15 U.S.C. § 78ff(a); 78dd-2(g)(1)(A).

DOJ has exclusive jurisdiction to prosecute criminal violations of the FCPA, both the DOJ and the SEC may obtain injunctive relief to prevent bribery and recordkeeping violations of the FCPA.

RECENT DEVELOPMENTS AND CURRENT ISSUES

In recent years, the SEC and the DOJ have dramatically increased their FCPA enforcement activities. The courts have posed few barriers to federal prosecutions of suspected wrongdoers and Congress has expanded rather than limited the authority of the DOJ and SEC to prosecute potential violations. With few limits, federal investigators have utilized their wide discretion under the statute to aggressively pursue suspected bribery under the FCPA.

Companies and individuals threatened with an FCPA indictment are increasingly negotiating agreements with the DOJ and the SEC to avoid costly and lengthy prosecutions.

Congressional Action

Since 1977, Congress has retained the FCPA's basic structure including its three primary components: the anti-bribery provisions, the accounting standards, and the reporting requirements. In 1988, Congress amended the FCPA in response to criticisms that the original act did not provide clear guidance on liability for potential violations, and that the statute placed U.S. companies at a disadvantage in the global marketplace.[38] The 1988 amendments added two affirmative defenses to FCPA violations and directed the President to urge U.S. trading partners to enact anti-corruption statutes similar to the FCPA to ensure a level playing field for U.S. companies doing business abroad. These efforts led to the adoption of the Convention on Combating Bribery of Foreign Public Officials in International Business Transactions ("OECD Convention") signed by member countries of the Organization for Economic Cooperation and Development ("OECD") in 1997. [39][40]

Congress further amended the FCPA in 1998 to conform with the provisions of the OECD Convention and extend the reach of the FCPA to include foreign companies and individuals.[41] In addition, Congress expanded the FCPA's scope to include payments made to secure "any improper advantage" and to include officials of public international organizations within the definition of "public official." The amendments also granted DOJ jurisdiction over the acts of U.S. businesses and nationals in furtherance of unlawful payments that take place wholly outside the United States. Since 1998, no substantive legislative changes have been made to the FCPA. The focus for companies doing business abroad has been squarely on the DOJ's and the SEC's interpretation of the statute.

Increased Federal Enforcement

Since 1998, the DOJ and the SEC have significantly increased the number of investigators assigned to FCPA investigations. In 2007, 16 new cases were filed, twice as many as in 2006. And between 2006 and 2008, 30 cases were filed, more than all the cases filed by the SEC in the

---

[38] Added by the Omnibus Trade and Competitiveness Act of 1988 (Pub. L. No. 100-418, 102 Stat. 1107 (1988)).

[39] Convention on Combating Bribery of Foreign Public Officials in International Business Transactions Dec. 18, 1997,

[40] I.L.M. 1

[41] The International Anti-Bribery and Fair Competition Act of 1998 (Pub. L. No. 105-366, 112 Stat. 3302 (1998)).

28 years of the statute.[42] The trend of increased enforcement has continued since 2008. In 2008, 43 cases were filed by the SEC and the DOJ. [43] In 2010, 74 cases were filed, the most enforcement actions in the 33-year history of the statute.[44] In 2016, 53 cased were filed, trailing only the year of 2010 for the most enforcement actions in the 39-year history of the statute.[45] In addition to the notable increase in enforcement, the costs required to resolve these inquires have increased significantly. In 2007, Baker Hughes, Inc. and its subsidiary, Baker Hughes Services International Inc., paid a then record sum of $44 million to resolve its FCPA investigations; a mere 5 years later, that figure is dwarfed by the $1.6 billion paid by Siemens A.G. In 2008, the $579 million paid by Kellogg Brown & Root LLC. In 2009, the $400 million paid by BAE System PLC and many more.[41] In 2016, the $519 million paid by Teva Pharmaceutical Industries Ltd, the $795 million paid by VimpelCom, and the $957 million paid by Braskem S.A. Federal investigators have also been successful in marshalling resources from different federal agencies including the FBI and the SEC as well as receiving international cooperation. For example, the SEC and the DOJ usually conduct parallel investigations simultaneously filing criminal and civil complaints. In addition, cooperation between foreign countries and U.S. investigators is on the rise, and civil suits arising from FCPA violations are being filed with more frequency. Given the aggressiveness of federal investigators and the costs of litigation and/or penalties imposed by the statute, it is often in the best interest of the company to settle all claims early in the investigation. Most companies under FCPA investigation have entered non-prosecution and deferred prosecution agreements to avoid lengthy and costly trials and to receive reduced penalties.

DOJ Opinion Letters

For companies concerned about potentially violating the FCPA, the DOJ has established a review process by which any U.S. company or national may request a DOJ opinion letter outlining its enforcement intentions under the anti-bribery provisions of the FCPA regarding a specific business transaction.[46] The procedures are not available for inquiries regarding the FCPA's record-keeping provisions. Under these procedures, the Attorney General must issue an opinion in response to a specific inquiry from a person or firm within thirty days of the request. If the DOJ issues an opinion stating that the conduct conforms with current enforcement policy, the conduct is entitled to a presumption, in any subsequent enforcement action, of conformity with the FCPA.[47] The opinion are purely case specific have no binding or authoritative effect on other business conduct. However, these opinion letters can serve to gauge trends in DOJ's interpretation of the FCPA.

Judicial Interpretation

The courts have, by and large, declined to limit the scope of federal investigations under the FCPA. There have been no significant challenges to the constitutionality of DOJ's broad powers under the FCPA to prosecute non-U.S. persons and companies who have, through minimal contacts in the U.S., fallen within the scope of the FCPA's purview. Prosecution of such

---

[42] China's Tricky Terrain on the Foreign Corrupt Practices Act, The Wall Street Journal, China Journal, June 10, 2008 (available at http://blogs.wsj.com/chinajournal/2008/06/10/chinas-tricky-terrain-on-the-foreign-corrupt-practices-act/).

[43] 2016 Year-End FCPA Update, January 19, 2017 (available at https://corpgov.law.harvard.edu/2017/01/19/2016-year-end-fcpa-update/).

[44] *Id.*

[45] *Id.*

[46] Details on the opinion procedure may be found at 28 CFR Part 80.

[47] Copies opinion letters are available on the DOJ's website at http://www.usdoj.gov/criminal/fraud/fcpa/opinion/.

companies with tangential and limited contacts to bribes effectuated in the U.S. could raise due process concerns, but have yet to be challenged.

In the most notable challenge to the broad powers conferred by the FCPA, the Fifth Circuit Court Appeals expanded the scope of the statute's reach. In *United States v. Kay*, defendants David Kay and Douglas Murphy were prosecuted for making payments to Haitian customs officials to reduce duties and taxes on the importation of rice into Haiti. In a 2004 opinion, the Fifth Circuit held that payments made to "obtain and retain business" under the statute includes payments to reduce customs and taxes.[48] Reading the statute broadly, the court found that the "obtain and retain business" prong is satisfied as long as there is a general nexus between the payment and some gain achieved by the company.[49] The case was remanded and found its way back to the Fifth Circuit which again rejected the defendants' appeal. This time, the Fifth Circuit held that DOJ did not need to prove that the defendants knew their conduct violated the FCPA under the "willful" prong of the statute.[50] The court found that it was sufficient to show that the defendants were aware that their conduct was generally unlawful.[51] Lower courts have generally followed suit and refused to provide a more narrow interpretation the FCPA.

DOJ and SEC Guidance

In late 2012, the DOJ and the SEC jointly published a booklet titled *A Resource Guide to the U.S. Foreign Corrupt Practices Act* ("Guide") on the interpretation and implementation of the FCPA. The Guide comes after the demand for clarification of key statutory terms of the FCPA, a procedures defense, and a safe harbor from successor liability. In regards to successor liability, a key element of the Guide aims to reassure companies that "the DOJ and the SEC have only taken action against successor companies in limited circumstances, generally in cases involving egregious and sustained violations or where the successor company directly participated in the violations or failed to stop the misconduct from continuing after the acquisition."[52] Specifically, if the acquiring company can demonstrate an adequate level of due diligence and promptly report any violations to the government, then the government will likely hold the predecessor or target company, and not the acquirer, liable. The Guide is a comprehensive review of the FCPA analyzing the pertinent statutory provisions, current case law and positions reflected in settlements. Instead of the clarification demanded by the business organizations, the Guide offers a road map to building a compliance system that is cost effective and reflects the current trend of enforcement. For each business with sales, distribution, and services contracts in the PRC, this Guide serves as a necessary starting point in an effort to comply with FCPA regulations.

Self-Disclosure Pilot Program

On November 29, 2017, the DOJ announced that it has implemented a permanent, revised version of the FCPA Pilot Program (the "New Pilot Program"). The FCPA Pilot Program was implemented by the DOJ in April 2016, which was initially set to run for one year and was later temporarily extended. The program encourages companies to self-report suspected bribery,

---

[48] United States v. Kay, 359 F.3d 738, 756 (5th Cir. 2004).

[49] *Id.*

[50] United States v. Kay, No. 05-20604, 2007 WL 3088140 (5th Cir. Oct. 24, 2007).

[51] *Id.*

[52] *FCPA Resource Guide* at 28.

cooperate with the government's subsequent investigation, and implement remediation measures. The New Pilot Program builds on and formalizes the FCPA Pilot Program.

In remarks announcing the New Pilot Program at the 34th International Conference on the FCPA, Deputy Attorney General Rosenstein stated that it "provide[s] transparency about the benefits available if [disclosing companies] satisfy the requirements. We want corporate officers and board members to better understand the costs and benefits of cooperation. The policy therefore specifies what we mean by voluntary disclosure, full cooperation, and timely and appropriate remediation."[53]

The New Pilot Program, which has been incorporated into the U.S. Attorney's Manual, offers increased incentives to companies to self-report suspected bribery. To qualify for benefits under the New Pilot Program, companies must (1) voluntarily self-disclose the potential violation; (2) fully cooperate with the government's subsequent investigation; and (3) timely and appropriately remediate identified issues. In addition, the company must pay disgorgement, forfeiture, and/or restitution resulting from the violation. If the company satisfies these requirements, there is a presumption that the company will receive a declination.[54]

The DOJ has disclosed that 30 companies have participated in the FCPA Pilot Program since its launch.[55] Participants are eligible for incentives, including a reduction in applicable financial penalties and avoiding the appointment of a corporate monitor. A number of companies that self-reported received declination letters with the payment of disgorgement, confirming that the DOJ had declined to pursue penalties despite evidence of FCPA violations.[56]

THE PERILS OF DOING BUSINESS IN CHINA

Conducting business in the PRC may present special risks under the FCPA, because many businesses in the PRC are either state-owned or state-controlled. Thus, employees of PRC businesses and industries may often be considered foreign officials for purposes of the FCPA. In addition, notwithstanding PRC laws prohibiting bribery, corruption is still widely recognized as an essential way of doing business in the PRC.

The pitfalls of doing business in China have taken center stage in a number of FCPA enforcement actions. More than 40% of the 53 FCPA enforcement actions brought in 2016 involved allegations of FCPA misconduct in China.[57] China is one of the most frequent situses of FCPA violations.[58]

---

[53] Deputy Attorney General Rosenstein Delivers Remarks at the 34th International Conference on the Foreign Corrupt Practices Act, November 29, 2017 (available at https://www.justice.gov/opa/speech/deputy-attorney-general-rosenstein-delivers-remarks-34th-international-conference-foreign).
[54] DOJ Issues New Policy Encouraging Self-Reporting FCPA Violations, December 7, 2017(available at https://www.lexology.com/library/detail.aspx?g=848ed831-5d70-48c2-9e00-99184c3e4897).
[55] DOJ Enhances And Makes Permanent FCPA Self-Disclosure Pilot Program, December 1, 2017 (available at https://www.lexology.com/library/detail.aspx?g=c85eae61-a4c0-4557-8b5f-66c5b5e63662).
[56] *Id.*
[57] 2016 Year-End FCPA Update, January 19, 2017 (available at https://corpgov.law.harvard.edu/2017/01/19/2016-year-end-fcpa-update/).
[58] *Id.*

In 2005, U.S. officials charged DPC Tianjin Co. Ltd., a Chinese subsidiary of the U.S. company Diagnostic Products Corporation, with violating the FCPA in connection with the payment of approximately $1.6 million in bribes to physicians and laboratory personnel employed by government-owned hospitals in the PRC.[59] In exchange for the payments, hospital doctors and employees agreed to purchase DPC Tianjin products. DPC Tianjin agreed to plead guilty in exchange for adopting internal compliance measures, and cooperating with ongoing criminal and SEC civil investigations. DPC Tianjin also agreed to pay a criminal penalty of $2 million. Simultaneously with the criminal charge, the SEC filed an FCPA enforcement proceeding against DPC Tianjin's parent company, DPC. The SEC ordered the company to cease and desist from violating the anti-bribery, internal controls and books and records provisions of the FCPA and to pay approximately $2.8 million in compensatory fines.

In December 2007, the French company Alcatel Lucent was fined $2.5 million ($1 million in penalties to DOJ and $1.5 in civil penalties to the SEC) as part of a deferred prosecution agreement for bribes Lucent employees paid to Chinese officials before Alcatel took over the company.60 The SEC complaint charged Lucent with spending over $10 million for approximately 1,000 Chinese officials, all employees of Chinese state-controlled telecommunications enterprises. The enterprises where entities to which Lucent was seeking to sell its equipment. The payments came in the form of trips to the U.S. ostensibly to inspect Lucent factories and train Chinese officials in using the equipment. However, the SEC claimed that little work took place with Chinese officials spending most of their time visiting tourist destinations such Disney World and the Grand Canyon.

In connection with the Beijing Olympics in 2008, the DOJ and the SEC stepped up their efforts to crack down on FCPA violations in the PRC. On June 5, 2008, the DOJ announced that it agreed to a non-prosecution agreement with Faro Technologies, Inc., a company registered with the SEC that specializes in computer measurement devices and software.[61] According to the DOJ Press Release, Faro began direct sales in the PRC through a subsidiary, Faro China, in 2003. Between 2004 and 2005, the DOJ charged that "a Faro employee authorized other Faro employees to make corrupt payments, termed 'referral fees' within Faro, directly to employees of state-owned or state-controlled in China to secure business for Faro." Faro was also charged under the FCPA books and records provisions for "inaccurately describing the bribe payments as referral fees." Rather than face prosecution, Faro agreed to pay a $1.1 million penalty, $1.85 million in disgorgement fees, and to implement future internal controls in compliance with the FCPA.

On June 3, 2008, AGA Medical Corp., a privately held U.S. medical device manufacturer, agreed to pay $2 million in criminal penalties to avoid prosecution under the FCPA.[62] The DOJ alleged that AGA employees made corrupt payments to doctors in China who were employed by government-owned hospitals and caused those payments to be made through AGA's local

---

[59] Press Release, Department of Justice, DPC (Tianjin) Ltd. Charged with Violating the Foreign Corrupt Practices Act (May 20, 2005).

[60] Press Release, Department of Justice, Lucent Technologies Inc. Agrees to Pay $1 Million Fine to Resolve FCPA Violations (December 21, 2007).

[61] Press Release, Department of Justice, Faro Technologies Inc. Agrees to Pay $1.1 Million Penalty and Enter Non Prosecution Agreement for FCPA Violations (June 5, 2008).

[62] Press Release, Department of Justice, AGA Medical Corporation Agrees to Pay $2 Million Penalty and Enter Deferred Prosecution Agreement for FCPA Violations (June 3, 2008).

Chinese distributor. The Chinese doctors, in exchange for the payments, directed the government-owned hospitals to purchase AGA's products rather than those of the company's competitors. In addition, AGA officials were charged with making payments to third parties to influence the approval of patents pending before PRC authorities.

In December 2012, Eli Lilly, an Indianapolis-based pharmaceutical company, reached a $29 million settlement with the SEC related to allegations that subsidiaries of the company in Russia, Brazil, China, and Poland made improper payments to foreign government officials in order to obtain business contracts. Specifically, Eli Lilly's Chinese subsidiary falsified expense reports to provide jewelry, cash, and other gifts to government employed physicians.

On August 7, 2012, as part of the then pharmaceutical industry wide sweep, Pfizer also settled with the SEC for $45 million. The SEC allegations against Pfizer were very similar to the ones levied against Eli Lilly. The company was alleged to have provided recreational and entertainment activities to reward doctors' product sales and prescriptions. Additionally, Pfizer created a number of "point programs" that rewarded doctors with points in accordance with the quantity of Pfizer products prescribed by the doctors. The accumulated points would then be redeemed for gifts such as cell phones, tea sets and others.

On February 28, 2013, Keyuan Petrochemicals Inc., a China-based firm, and its former CFO, Aichun Li, jointly settled FCPA books and records and internal controls offenses with the SEC. Keyuan paid civil penalties of $1 million.[63] It is thought to be the first FCPA-related enforcement action ever taken against a China-based company. The SEC alleged that from 2008 to 2011, Keyuan maintained an off-books account into which it channeled approximately $1 million that was used, in part, to fund gifts to Chinese government officials, including officials from the local environmental, port, police, and fire departments. The gifts, which were typically given around the Chinese New Year, ranged from household goods (such as beddings and linens) to "red envelope" gifts, in which cash was directly gifted to the officials.

On May 15, 2013, Dejun 'David' Zou and Jianping 'Amy' Qiu, husband-and-wife executives of China-based Rino International Corporation, agreed to settle the SEC charges by paying penalties of $100,000 and $150,000 respectively and disgorging $3.5 million into a related class action settlement for FCPA books and records violations.[64] They're barred for 10 years from serving as officers or directors of any company publicly traded in the U.S. the SEC alleged that Rino maintained two conflicting sets of financial records — one set of books for filings in China and another set of books for filings in the U.S. The U.S. books that formed the basis for Rino's SEC filings contained false contracts and portrayed sales revenues of approximately $491 million.

On December 15, 2014, Bruker Corporation, a Billerica, Mass.-based global manufacturer of scientific instruments, agreed to pay $2.4 million to settle the SEC charges that it violated the FCPA by providing non-business related travel and improper payments to various Chinese government officials in an effort to win business.[65] The SEC said Bruker "lacked sufficient internal controls to prevent and detect approximately $230,000 in improper payments out of its China-

---

[63] Securities and Exchange Commission v. Keyuan Petrochemicals, Inc. and Aichun Li, Civil Action No. 13-cv-00263 (D.D.C.) , February 28, 2013 (available at https://www.sec.gov/litigation/litreleases/2013/lr22627.htm).
[64] Securities and Exchange Commission v. RINO International Corporation, Dejun 'David' Zou, and Jianping 'Amy' Qiu, Civil Action No. 1:13-cv-00711, May 15, 2013 (available at https://www.sec.gov/litigation/litreleases/2013/lr22699.htm).
[65] SEC Enforcement Actions: FCPA Cases (available at https://www.sec.gov/spotlight/fcpa/fcpa-cases.shtml).

based offices that falsely recorded them in books and records as legitimate business and marketing expenses."

On December 17, 2014, Avon Products Inc., a global beauty products company, and its China subsidiary agreed to pay $135 million to settle the SEC charges and a parallel criminal case, relating to violation of the FCPA by failing to put controls in place to detect and prevent payments and gifts to Chinese government officials from a subsidiary.[66] One Avon's China subsidiary pleaded guilty in federal court in Manhattan to one count of conspiring to violate the FCPA. The Chinese subsidiary made $8 million worth of payments in cash, gifts, travel, and entertainment to various Chinese officials. Avon needed their approval for direct selling in China. In March 2006, Avon became one of the first companies to receive a direct selling license. Avon management learned in late 2005 of potential FCPA problems in China. It didn't start a full-blown internal investigation until 2008, after its CEO received a letter from a whistleblower in China.

On July 28, 2015, Mead Johnson Nutrition, an infant formula manufacturer, agreed to pay $12 million to settle SEC charges that it violated the FCPA when its Chinese subsidiary made improper payments to health care professionals to recommend the company's product to new and expectant mothers. [67] The SEC investigation found that employees used "distributor allowances" to fund the bribes in China, the practice of which was stopped in 2013. "Although the funds contractually belonged to the distributors, employees exercised some control over how the money was spent and provided specific guidance to distributors on how to use the funds," the SEC said.[68]

On October 5, 2015, Bristol-Myers Squibb, a New York-based pharmaceutical company, agreed to pay more than $14 million to settle SEC charges that it violated the FCPA when employees of its China-based joint venture made improper payments and provided other benefits to health care providers at state-owned and state-controlled hospitals in exchange for prescription sales. [69] The SEC alleged that BMS China sales representatives tried to win and increase business by giving health care providers cash, jewelry and other gifts, meals, travel, entertainment, and sponsorships for conferences and meetings between 2009 and 2014.

On February 4, 2016, SciClone Pharmaceuticals, a California-based pharmaceutical firm, agreed to pay $12 million to settle SEC charges that it violated the FCPA when its subsidiaries increased sales by making improper payments to health care professionals employed at state health institutions in China.[70] The SEC alleged that SciClone's China employees pumped up sales for five years by making improper payments to professionals employed at state health institutions in China. They gave money, gifts, travel, golf games, and lavish hospitality to China customers and decision makers.

On February 16, 2016, PTC Inc., a Massachusetts-based tech company, and its two Chinese subsidiaries agreed to pay more than $28 million to settle FCPA cases involving bribery

---

[66] *Id.*
[67] SEC Charges Mead Johnson Nutrition With FCPA Violations, July 28, 2015 (available at https://www.sec.gov/news/pressrelease/2015-154.html).
[68] *Id.*
[69] SEC Charges Bristol-Myers Squibb With FCPA Violations, October 5, 2015 (available at https://www.sec.gov/news/pressrelease/2015-229.html).
[70] SciClone Charged With FCPA Violations, February 4, 2016 (available at https://www.sec.gov/litigation/admin/2016/34-77058-s.pdf).

of Chinese government officials by arranging travels to the U.S. to win business.[71] In addition, Yu Kai Yuan, a former employee at PTC's China subsidiaries, resolved FCPA offenses on February 16, 2016 through the SEC's first deferred prosecution agreement with an individual in an FCPA case. The SEC deferred FCPA civil charges for three years "as a result of significant cooperation". Yuan, 47, a Chinese citizen, lives in Shanghai.

On March 1, 2016, Qualcomm agreed to pay $7.5 million to settle charges that it violated the FCPA when it hired relatives of Chinese officials deciding whether to select company's products.[72] According to the SEC's administrative order, Qualcomm offered and provided full-time employment and paid internships to foreign officials' family members internally referred to as "must place" or "special" hires in order to try to obtain or retain business in China. One official asked Qualcomm employees to find an internship for her daughter studying in the U.S. and the company obliged, acknowledging in internal communications that her parents "gave us great help for Q.C. new business development."[73]

On March 23, 2016, Novartis AG, a Swiss-based pharmaceutical company, agreed to pay $25 million to settle charges that it violated the FCPA when its China-based subsidiaries engaged in pay-to-prescribe schemes to increase sales. [74] The SEC alleged that Novartis' two China-based subsidiaries bribed doctors and others to prescribe its drugs. Novartis improperly recorded the payments as travel and entertainment, conferences, lecture fees, marketing events, educational seminars, and medical studies.

On April 7, 2016, Las Vegas Sands, casino and resort company, agreed to pay $9 million to settle charges that it failed to properly authorize or document millions of dollars in payments to a consultant facilitating business activities in China. [75] According to the DOJ, certain Sands executives knowingly and willfully failed to implement a system of internal accounting controls to adequately ensure the legitimacy of payments to a business consultant who assisted Sands in promoting its brand in the PRC, and to prevent the false recording of those payments in its books and records. The SEC said Sands spent more than $62 million on the China consultant. The consultant acted as an intermediary to hide the company's role in buying a basketball team and a building in China.

On July 11, 2016, Johnson Controls, a Wisconsin-based temperature control systems manufacturer, agreed to pay more than $14 million to settle charges that its Chinese subsidiary used sham vendors to make improper payments to employees of Chinese government-owned shipyards and other officials to win business.[76] The SEC alleged that it violated the books and records and internal accounting controls provisions of the FCPA.

On September 30, 2016, GlaxoSmithKline, a UK-based pharmaceutical company, agreed to pay a $20 million penalty to settle charges that it violated the FCPA when its China-based subsidiaries engaged in pay-to-prescribe schemes to increase sales. [77] The FCPA offenses

---

[71] Tech Company Bribed Chinese Officials, February 16, 2016 (available at https://www.sec.gov/news/pressrelease/2016-29.html).
[72] Qualcomm Hired Relatives of Chinese Officials to Obtain Business, March 1, 2016 (available at https://www.sec.gov/news/pressrelease/2016-36.html).
[73] *Id.*
[74] SEC Enforcement Actions: FCPA Cases (available at https://www.sec.gov/spotlight/fcpa/fcpa-cases.shtml).
[75] *Id.*
[76] *Id.*
[77] *Id.*

spanned at least 2010 to 2013 and involved gifts, improper travel and entertainment with no or little educational purpose, shopping excursions, family and home visits, and cash. The costs associated with these payments were recorded in GSK's books and records as legitimate expenses, such as medical association sponsorships, employee expenses, conferences, speaker fees, and marketing costs. In addition, China authorities accused GSK of paying nearly $500 million in bribes to health officials and doctors to boost sales. [78] China's Ministry of Public Security said in 2013 that GSK had used 700 travel agents to deliver the illegal payments since 2007. In September 2014, a court in Changsha, China fined GSK $490 million following a conviction for bribery. GSK's former head of China operations, Mark Reilly, was given a three-year prison sentence that was suspended. Mark Reilly was deported. Other China nationals working as GSK executives were sentenced to between two and four years in prison.

Conclusion

With increasing enforcement by the SEC and DOJ, an increase in the cost to remedy the investigations, and the special pitfalls, it is important to consider FCPA compliance prior to engaging in business activities in China. As part of the preparation process, an interested company should follow the Guide and conduct a thorough investigation for possible FCPA violations and have an adequate compliance system in place. The complex make-up of state-owned enterprises and the government system in China further complicate the FCPA compliance procedures, thus increasing the risk involved in the deals. Cases like the "Sons and Daughters" hiring, pharmaceutical industry operations, and the Alcatel Lucent successor liability, highlight some of the financial implications of FCPA violations in China and further cement the need for a solid compliance program.

[78] China Fines GlaxoSmithKline Nearly $500 Million in Bribery Case, September 19, 2014 (available at https://www.nytimes.com/2014/09/20/business/international/gsk-china-fines.html).

DORSEY
always ahead

U.S. CITIZENS' LEGAL EXPOSURE RELATED TO FOREIGN COMMERCIAL BRIBERY

By Beth Forsythe and J Jackson

This memorandum addresses United States laws under which the U.S. citizens may be prosecuted for (1) authorizing kickbacks during in-person meetings in China (or elsewhere); and (2) authorizing kickbacks during telephone calls while the U.S. citizens were in the United States.

I. Analysis

A. Scenario 1: U.S. Citizens Authorize Bribery While in China

1. Travel Act

In 1961, then Attorney General Robert F. Kennedy submitted the bill that became the Travel Act as part of his legislative program designed to aid local law enforcement authorities in their efforts to combat organized crime.

A Travel Act charge is often included with an FCPA charge. However, the Travel Act differs from the FCPA in several ways. Unlike conduct under the FCPA, the unlawful activity itself is not what leads to violating the Travel Act. Rather, violating the Travel Act stems from the use of communications and travel facilities to perform the unlawful activity, which is defined as bribery of foreign officials, commercial bribery of private individuals, or other unlawful activities as defined in the act, including among others, extortion and certified financial crimes.

The Travel Act's definition of "unlawful activity" includes bribery conducted "in violation of the laws of the state." If a state has a law criminalizing commercial bribery, including bribery between private parties, any act violating that state law would be an "unlawful activity" and would subject the actor to prosecution under the Travel Act.

The elements of a Travel Act violation include: (1) travel in interstate or foreign commerce or use of the mail or any facility in interstate or foreign commerce (including the telephone), (2) with intent to promote, manage, establish, or facilitate the promotion, management, establishment, or carrying on of any unlawful activity, followed by (3) performance of or an attempt to perform an act of promotion, management, establishment, carrying on, or facilitation of the unlawful activity. 18 U.S.C. § 1952(a). "Unlawful activity" is defined in the Travel Act, and includes "extortion, bribery, or arson in violation of the laws of the State in which committed or of the United States." 18 U.S.C. § 1952(b). The potential unlawful activity is commercial bribery in violation of the state law. *United States v. Perrin*, 44 U.S. 37, 50 (1979) ("Congress intended 'bribery . . . in violation of the laws of the State in which committed' to encompass conduct in violation of state commercial bribery statutes.")

The Travel Act does not itself prohibit commercial bribery. Rather, it is a stand-alone offense that prohibits the use of foreign travel, cross-border communications or wire transfers to promote or facilitate bribery. 18. U.S.C. § 1952.

The purpose of the Travel Act, as recognized by the United States Supreme Court, "was aimed primarily at . . . persons who reside in one State while operating or managing illegal activities located in another." *Rewis v. United States*, 401 U.S. 808, 811 (1971). As

federal law enforcement has explained: "if a company pays kickbacks to an employee of a private company who is not a foreign official, such private-to-private bribery could possibly be charged under the Travel Act." DOJ and SEC, *A Resource Guide to the U.S. Foreign Corrupt Practices Act*, 48 (2012) ("FCPA Guide").

(a) Elements of a Travel Act Violation

(i) Foreign Travel or Facility in Interstate or Foreign Commerce

If U.S. citizens were in the United States when they set into motion the authorization of the kickbacks, including by leaving from the United States and traveling to China with intent to authorize the kickbacks, a U.S. court is likely to find there is a territorial nexus to the United States sufficient to give a U.S. court jurisdiction over the matter.

The Supreme Court generally has taken a broad view of the jurisdiction of criminal statutes such as the Travel Act, which are "not logically dependent on their locality for the government's jurisdiction, but are enacted because of the right of the government to defend itself against obstruction, or fraud wherever perpetrated, especially if committed by its own citizens, officers, or agents." *United States v. Bowman*, 260 U.S. 94, 98 (1922). Lower courts likewise have taken a broad view of the jurisdiction of the Travel Act, concluding that it reaches conduct overseas. *See United States v. Carson et al.*, No. 8:09-CR-00077, Order on Mot. to Dismiss at 8–10 (C.D. Cal. Sept. 20, 2011), ECF No. 440 ["*Carson* Mot. to Dismiss"]; *United States v. Viktor Kozeny, et al.*, No. 05-CR-518-SAS (S.D.N.Y. 2005) (jury instructed that "[a] facility in interstate commerce is any vehicle or instrument that crosses state lines, or boundaries between a state and foreign country, in the course of commerce," including phone calls, faxes, email, or wire transfers).

To establish jurisdiction under the Travel Act, "foreign travel" includes travel from the United States to China. This definition also appears to encompass a multi-stop trip from the United States that includes the stop in China. *See United States v. Weingarten*, 632 F.3d 60, 71 (2d Cir. 2011). In *Weingarten*, the court found there was no jurisdiction to prosecute activities committed while travelling *wholly* between two foreign countries and with no territorial nexus to the United States. *Id.* However, the Second Circuit clarified that:

> We do not suggest of course, that the mere presence of an intermediate stop outside the United States on a multi-legged journey undertaken for unlawful purposes will immunize a defendant from prosecution . . . . **An offender violates the law when he embarks on travel with the requisite illicit purpose, and mere stops along the way do not deprive travel of its territorial nexus to the United States.**

Id. (emphasis added).

(ii) Intent to Promote Any Unlawful Activity

The language of the statute indicates that to violate the Act, the actor must have the *intent* to "promote, manage, establish, carry on, or facilitate the promotion . . . of any unlawful activity" at the time he or she uses the facilities of or travels in interstate commerce. This would mean that if the U.S. citizens boarded the plane to China intending to authorize payment of a bribe or kickback, they would have the requisite intent. In contrast, if they flew to China solely with the intention of conducting business meetings, and only developed the

intention to authorize bribes while in China, such travel may not violate the Travel Act.

The government may prove intent through circumstantial evidence. For example, the government may use the authorization of kickbacks on the trip as circumstantial proof that one purpose of the trip was to authorize the kickbacks. In addition, the government may use evidence of other similar trips by the U.S. citizens and the U.S. citizens' education, training, business experience, or other characteristics, to support an inference that the U.S. citizens intended to authorize the kickbacks when they made the trip. *See United States v. Abadie*, 879 F.2d 1260, 1266 (5th Cir. 1989) (inference of intent may be based on pattern of similar trips).

Intent is a jury issue. The government may charge a Travel Act offense and simply state that when the defendant engaged in international travel, he intended to promote an unlawful activity. Not until trial will the defendant have an opportunity to argue that he engaged in the travel without the intent to promote kickbacks. *See United States v. Welch*, 327 F.3d 1081, 1097 (10th Cir. 2003) (court accepts allegations in indictment as true and allows defendant to argue lack of intent at trial).

(iii) "Unlawful Activity"—Violation of State Commercial Bribery Laws

The Travel Act specifically defines "unlawful activity" to include bribery in violation of state or federal law. 18 U.S.C § 1952(b)(2). The United States does not have a federal law that prohibits commercial bribery, so in this factual scenario, the "unlawful activity" would have to be commercial bribery in violation of a state law.[1]

Not every state has a commercial bribery statute, but most do. Lexis-Nexis provides a 50 state survey of state commercial bribery statutes, which survey includes Iowa,[2] Minnesota,[3] Nebraska,[4] New Jersey,[5] New York,[6] and North Carolina.[7] In deciding under which state law to charge the unlawful activity, the government typically looks to the corporation's principal place of business. If multiple states are involved—for example, if the company's principal place of business is in one state, but the individual who violated the Travel act lives and works in another state and travels to a foreign country from yet another state—this provides prosecutors the ability to "forum shop" to find a state law that most closely fits the government's theory of the case.

Commercial bribery statutes differ by state, but most prohibit substantially the same behavior. For example, the language of the Iowa commercial bribery statute, broadly prohibits bribery and kickbacks, and does not limit the prohibition to bribery that takes place in Iowa:

---

[1] "The predicate offense, *i.e.*, the 'unlawful activity,' in a Travel Act prosecution serves only to define the accused's conduct. The Travel Act proscribes not the unlawful activity per se, but the use of interstate facilities with the requisite intent to promote such unlawful activity." *Welch*, 327 F.3d at 1092 (citations omitted).
[2] Iowa Code § 722.10, subd. 2.
[3] Minn. Stat. § 609.86
[4] R.R.S. Neb. § 28-613.
[5] N.J.S.A. 2C:21-10.
[6] N.Y.C.P.L. § 180.00.
[7] N.C. Gen. Stat. § 14-353.

> It is unlawful for a person to offer or deliver directly or indirectly for the personal benefit of an employee acting on behalf of the employee's employer in a business transaction or course of transactions with the person a gratuity in consideration of an act or omission which the person has reason to know is in conflict with the employment relation and duties of the employee to the employer. . . .

Iowa Code Ann. § 722.10, subd. 2.[8] This prohibition on indirect offers or payments appears on its face to prohibit the authorization of a bribe or kickback, and it is not limited to offers or payments made within Iowa. A court interpreting California's commercial bribery statute, which is very similar to Iowa's and Minnesota's, concluded that "California's commercial bribery statute applies even if the bribery transaction is consummated outside of California." *Carson* Mot. to Dismiss at 6 (finding that Travel Act violation adequately alleged that offense was complete the moment defendants used a channel of foreign commerce to allegedly offer a "corrupt payment" to an employee and then paid the employee).

In *Carson*, the court denied the defendants' motion to dismiss violations of the Travel Act based on California's commercial bribery statute, which is similar to Iowa's and Minnesota's.[9] *Carson* Mot. to Dismiss at 10. The court stated that California would have jurisdiction over the offense if the defendant met the other elements of the Travel Act and completed a preparatory act in California that amounted to more than a *de minimis* act toward eventual completion of the offense, even where several of the underlying alleged bribes consisted of wire payments from a foreign bank account to another foreign country. *Id.* at 11. In concluding that only a *de minimis* act in furtherance of the bribe occur in California, the Court referred to California's criminal jurisdictional statute, Cal. Penal Code § 778a(a), which states that California has jurisdiction over any crime even if only partially executed in California. Iowa's (Iowa Code § 803.1) and Minnesota's (Minn. Stat. § 609.025) criminal jurisdictional statutes, are at least as broad as California's and may not even require that a preparatory act amounting to more than a *de minimis* act occur in Iowa.

In most Travel Act cases, the "unlawful activity" in violation of state law typically had a stronger connection to the state than merely boarding a flight out of the state. Usually the government has charged substantive violations of the Travel Act based on activity like wire transfers originating from a state, email or fax communication while in a state, or telephone

---

[8] Minnesota's commercial bribery statute, Minn. Stat. § 609.86, is similar:

Subd. 2.**Acts constituting.**

Whoever does any of the following, when not consistent with usually accepted business practices, is guilty of commercial bribery and may be sentenced as provided in subdivision 3:

(1) corruptly offers, gives, or agrees to give, directly or indirectly, any benefit, consideration, compensation, or reward to any employee, agent or fiduciary of a person with the intent to influence the person's performance of duties as an employee, agent, or fiduciary in relation to the person's employer's or principal's business; or

(2) being an employee, agent or fiduciary of a person, corruptly requests, receives or agrees to receive, directly or indirectly, from another person any benefit, consideration, compensation, or reward with the understanding or agreement to be influenced in the performance of duties as an employee, agent, or fiduciary in relation to the employer's or principal's business.

[9] Cal. Penal Code § 641.3(a): "Any employee who solicits, accepts or agrees to accept money or anything of value from a person other than his or her employer, other than in trust for the employer, corruptly and without the knowledge or consent of the employer, in return for using or agreeing to use his or her position for the benefit of that other person, and any person who offers or gives an employee money or anything of value under those circumstances, is guilty of commercial bribery."

calls from one state to another state or foreign jurisdiction. Nevertheless, travel from one state to another state or country to authorize or facilitate activity prohibited by the state of departure may support a Travel Act prosecution. *See United States v. Jones*, 642 F.2d 909 (5th Cir. 1981) (trip from Oklahoma to Texas to cash wagering checks in "facilitation" of ongoing gambling enterprise met jurisdictional requirements of Travel Act).

(iv) Subsequent Act to Promote or Facilitate Unlawful Activity

Following an act of travel with intent to facilitate unlawful activity, a defendant must engage in some subsequent act that actually facilitates or promotes, or attempts to facilitate or promote, the unlawful activity. 18 U.S.C. § 1952.

This element is met even without actual payment of a bribe. To violate the Travel Act a defendant's mere *attempt* to commit bribery is sufficient. *See* 18 U.S.C. § 1952(a). In the *United States v. Kozeny* case, the court instructed the jury that the Travel Act requires proof that the defendant used a facility of commerce "for the purpose of facilitating the unlawful activity," but that proof of a "completed bribery scheme" was unnecessary. The court stated that "[a]ll that is required is proof that the person agreed to use interstate channels in order to facilitate the crime. ..." Jury Instruction, *United States. v. Viktor Kozeny, et al.*, No. 05-CR-518-SAS (S.D.N.Y. filed May 12, 2005). In *Control Components*, the court stated that the Travel Act "offense was complete the moment Defendants used a channel of foreign commerce allegedly to offer a 'corrupt payment' to an employee and thereafter effectuated [or attempted] a payment to that employee." Jury Instructions, *United States v. Control Components, Inc.*, No. 09-CR-162-JVS (C.D. Cal. filed Jul. 22, 2009).

In this factual scenario, a U.S. citizen's authorization of kickbacks once in China satisfies this element. *See, e.g., United States v. Johns*, 755 F. Supp. 130 (E.D. Pa. 1991) (overt act committed after interstate travel was deposit of check reflecting proceeds from unlawful activity).

Some courts may determine that a violation of state bribery law will not lie where the only overt act that occurred in the state was arranging for and taking the flight to China; however, previous Travel Act jurisprudence suggests that such actions may be sufficient to bring a Travel Act case. A motivated United States prosecutor may look for ways to fit the facts into this or some other law, including by charging conspiracy or attempt to violate the Travel Act or another federal law.

(b) Penalties

Each violation of the Travel Act may be punished by imposition of a fine of the greater of $250,000 (for an individual, $500,000 for a company) or twice the gross gain from the offense, and/or a term of imprisonment up to 5 years. 18 U.S.C. § 1952(a)(3)(A); 18 U.S.C. § 3571 (fines).

(c) Connection with State Whose Commercial Bribery Statute is Being Used

The connection between foreign commercial bribery and a state's interest in prosecuting such activity is important, and many cases could be prosecuted by federal or state prosecutors. Typically, a federal prosecutor in a state such as Iowa will focus on prosecution of crimes in which their state has a particular interest, but that is not necessarily

the case in Travel Act prosecution. In Travel Act cases, a state's particular interest may have little to do with the government's decision to investigate and prosecute. In *Control Components*, for example, the case involved a violation of California's commercial bribery statutes, but the majority of government investigators and attorneys were based in Washington, D.C.

It is also conceivable that prosecutors in the state where the company is headquartered could prosecute this case as a state commercial bribery case, even if the federal prosecutors were not interested in the possible Travel Act charge.

(d) No *De Minimis* Exception for Travel Act Violation under Federal Law or Relevant State Statutes

There is no *de minimis* exception or threshold amount of corrupt payment required for the Travel Act to apply. A prosecutor would always look to the applicable state law to determine if there is a threshold amount. State commercial bribery statutes typically contain no threshold amount; rather, they use terms like "any gift or gratuity whatever," "any benefit," or "a gratuity." Minn. Stat. § 609.86; N.C. Gen. Stat. § 14-353; R.R.S. Neb. § 28-613(1); Iowa Code § 722.10, subd. 2.

In reality, the DOJ typically prosecutes cases involving bribes of significant amounts. In *United States v. Nguyen*, for example, Nexus Technologies was charged with conspiring with its employees to pay Vietnamese officials $250,000 in bribes in exchange for major equipment and technology contracts. Superseding Indictment, *United States v. Nam Quoc Nguyen et al.*, No. 08-CR-522-TJS (E.D. Pa. 2008), ECF No. 106. In *Control Components*, the company paid millions of dollars in bribes to officials at state-owned businesses abroad and to private sector employees. Plea Agreement, *United States v. Control Components, Inc.*, No. 09-CR-162-JVS (C.D. Cal. 2009), ECF No. 7.

(e) Both the Company and Individuals May Be Prosecuted

The United States Department of Justice ("DOJ") may bring a Travel Act prosecution against a company, its employees, or both. For example, Nexus Technologies was charged with conspiracy, violations of the Foreign Corrupt Practices Act ("FCPA"), violations of the Travel Act in connection with bribery, and money laundering for conspiring with its employees to pay Vietnamese officials $250,000 in bribes in exchange for major equipment and technology contracts. Superseding Indictment, *United States v. Nam Quoc Nguyen, et al.*, No. 08-CR-522- TJS (E.D. Pa. 2008), ECF No. 106. The individual employee defendants pleaded guilty and received sentences ranging from sixteen months' imprisonment to two years' probation. The company also pleaded guilty to the charges against it.

In another prominent case, the government alleged in 2009 that from 1998 through 2007 Control Components, Inc. paid millions of dollars in bribes to numerous officers and employees of state-owned and privately-owned customers around the world, including China, Korea, Malaysia, and the United Arab Emirates, to obtain or retain business. *United States v. Control Components, Inc.*, No. 09-CR-162-JVS (C.D. Cal. filed Jul. 22, 2009). The company pleaded guilty to both Travel Act and FCPA charges and agreed to pay a criminal fine of $18.2 million and to serve three years of organizational probation. During the probationary period, the company was prohibited from committing further violations of any law, required to continue to cooperate with the government in its ongoing investigation into the company, and required to self-report any violation of any law. In addition, the company was required to retain an independent compliance monitor for three years and to implement

an anti-bribery compliance program. The former executives who allegedly approved, negotiated or made the purported payments were also indicted and pleaded guilty. *See, e.g.*, Plea Agreement, *United States v. Carson*, No. 8:09-cr-00077-JVS (C.D. Cal. Filed 2009), ECF No. 695 (former executive); Plea Agreement, *United States v. Control Components, Inc.*, No. 09-CR-162-JVS (C.D. Cal. 2009), ECF No. 7 (company).

2. Conspiracy to Violate the Travel Act

Federal prosecutors typically bring charges of conspiracy to violate the Travel Act in conjunction with charges of substantive violations of the Travel Act. *See, e.g., United States v. Arruda*, 715 F.2d 671, 682 (1st Cir. 1983) ("Travel is not incidental if it is an important link in the interchange among defendants." (Quotation omitted.))

The elements of conspiracy are (1) an agreement to achieve an unlawful objective (for example, the Travel Act violation; mail, wire, or honest services fraud), (2) knowing and voluntary participation in the agreement, and (3) the commission of an overt act in furtherance of the agreement. *United States v. Esquenazi*, 752 F.3d 912, 934 (11th Cir. 2014). The overt act taken in furtherance of the conspiracy need not be a crime. *United States v. Kozeny*, 667 F.3d 122, 132 (2d Cir. 2011) (citing *Braverman v. United States*, 317 U.S. 49, 53, 63 S. Ct. 99, 87 L. Ed. 23, 1942 C.B. 319 (1942) ("The overt act, without proof of which a charge of conspiracy cannot be submitted to the jury, may be that of only a single one of the conspirators and need not be itself a crime.")).

Depending on the state statute involved, a jury may find that U.S. citizens conspired to violate the Travel Act if, for example, they agreed to bribe a Chinese business person to obtain a contract and later one of the U.S. citizens boarded a plane to China with the intention of meeting the Chinese citizen and bribing him.

3. Potential Tax Consequences

Bribe expenses are not deductible as business expenses; false deductions on tax returns could lead to civil, administrative, or criminal tax liability. A company or individual that violates the Travel Act may also violate U.S. tax law, which explicitly prohibits tax deductions for bribes, such as false sales "commissions" deductions intended to conceal corrupt payments. 26 U.S.C § 162(c); *see, e.g.*, Plea Agreement, *United States v. Smith*, No. 07-cr-69 (C.D. Cal. 2009), ECF No. 89. The Internal Revenue Service-Criminal Investigation Unit has been involved in several bribery investigations involving tax violations. *FCPA Guide*, at 49.

B. Scenario 2: Phone Calls from United States to China (or elsewhere) to Authorize Bribery

1. Travel Act

Unlike Scenario 1, all jurisdictional requirements of the Travel Act are satisfied in this scenario, in which the U.S. citizens participate in telephone calls from the United States to China and during those conversations authorize the payment of kickbacks in China. *See Carson* Mot. to Dismiss at 4-5, 14-15 (denying motion to dismiss Counts 12 and 14 of indictment, which charged wire transfers from Sweden to China and Sweden to Latvia, respectively, because "Defendants allegedly set in motion the corrupt payments from California," which established a "'territorial nexus' to the United States") (citing *Pasquantino v. United States*, 544 U.S. 349, 353 (2005) (offense was complete the moment the scheme was executed inside the United States)).

As long as the calls were made from a state with a commercial bribery statute, the assumed facts of this scenario will substantiate a Travel Act violation.

2. Mail and Wire Fraud

Besides the possible enforcement instruments discussed above, the government also may use the federal mail and wire fraud statutes, 18 U.S.C. §§ 1341 and 1343, to combat private foreign bribery.

The elements of mail and wire fraud are (1) knowing participation in a scheme or artifice to defraud and (2) the use of the mails or wires in carrying out such a scheme or artifice. 18 U.S.C. §§ 1341, 1343. Courts generally have interpreted the mail and wire fraud statutes broadly, with "fraud" being interpreted to encompass actions inconsistent with moral uprightness, fundamental honesty, fair play, and right dealing. Penalties of the mail and wire fraud statutes include up to twenty years in prison and fines.

In *United States v. SSI International Far East*, the company pled guilty to wire fraud charges in connection with bribes paid to managers of both private and government-owned companies as part of a "scheme and artifice to obtain property by means of materially false and fraudulent pretense . . . ." Plea Agreement, No. 06-CR-398 (D. Or. Filed Oct. 10, 2006). The wire fraud charges were based on allegations that the funds for the "commissions" were paid via wire transfers from the United States. *See also Welch*, 327 F.3d at 1103-04 (reversing dismissal of wire fraud and mail fraud counts based on international wire transfers originating from Utah).

II. Compliance

Companies should consider how to address the Travel Act in their compliance program and trainings. First, although company training materials often focus on defining who qualifies as a "foreign official" and explaining that definition to employees around the world, training materials should be expanded to include an explanation of the Travel Act, where no foreign official is required. Companies should emphasize that bribes paid to private parties through travel or use of the mail in interstate or foreign commerce can implicate the Travel Act and are, therefore, also prohibited.

Second, companies should implement internal controls and anti-corruption policies designed to detect instances of commercial bribery, as well as bribes paid to foreign officials. Companies should consider whether their policies provide for a distinction between gifts, travel, and entertainment provided to a foreign official versus a private official and whether adequate due diligence is being conducted on third parties regardless of whether they are retained for government or private contracts. The FCPA's accounting provisions apply regardless of whether the accounting violation relates to a bribe to a government official or a private party. Companies, therefore, should monitor payments made to private companies as they would monitor payments made to government entities.

DORSEY
always ahead

CHINA'S COMMERCIAL BRIBERY LAW
A Summary of Amendments Effective January 1, 2018
By J Jackson

On November 4, 2017, the Standing Committee of the National People's Congress adopted amendments to China's Anti-Unfair Competition Law. The Amendments became effective on January 1, 2018 (the "2018 AUCL"). The Congress had enacted the AUCL in 1993 to encourage and protect fair competition among businesses in a then-expanding Chinese economy. Two initial drafts, circulated in 2016 and 2017, had preceded the final version—the 2018 AUCL.[1]

The 2018 AUCL updated several provisions of the Original Law. Businesses operating in China should take specific note of the changes addressed below.

Describes Three Categories of Commercial Bribery Recipients

The 2018 AUCL describes three types of bribery recipients. They are

- "any employee of the counterparty in a transaction;"
- "any entities or individuals entrusted by the transaction counterparty in a transaction to handle relevant affairs;"
- "any other entity or individual that is to take advantage of powers or influence to influence a transaction."

2018 AUCL at Article 7.

The 2018 AUCL considers government entities, private entities, and individuals to be potential commercial bribery targets. However, the 2018 AUCL does not include transaction counterparties among the categories of bribe recipients. Companies should not provide benefits to transaction counterparties to obtain business opportunities or competitive advantages, except for accurately recorded discounts.

The 2018 AUCL allows discounts and commissions between transaction counterparties: "A business operator may expressly give a discount to the counterparty or pay a commission to the middleman of a transaction in the course of transaction activities. Where a business operator gives a discount to the transaction counterparty

---

[1] A copy of the 2018 AUCL is attached.

or pays a commission to the middleman, it shall truthfully enter it in his account books. A business operator that accepts such discount or commission shall also enter it into its account books." 2018 AUCL at Article 7, second ¶. Under this provision, business operators may pay or accept discounts or commissions in a transaction, provided those arrangements are transparent and are clearly and accurately recorded.

Defines Commercial Bribery

Article 7 of the 2018 AUCL defines commercial bribery to mean the "offering [of] money or goods or by any other means . . . in order to seek a transaction opportunity or competitive advantage."

Creates Vicarious Liability

The original AUCL was silent on whether vicarious liability—finding an employer liable for misconduct committed by its employees—applied to commercial bribery acts. Article 7 of the 2018 AUCL provides that bribery by employees "shall be deemed an act of the business operator itself . . .."

However, the 2018 AUCL creates an exception where vicarious liability does not attach if it is "otherwise proven by the business operator with evidence that such bribery is not related to efforts of seeking a transaction opportunity or competitive advantage for the business operator." The burden of proof would remain on the business operator.

Describes the Investigative Processes that May Be Used by Administrations of Industry & Commerce ("AICs")

The 2018 AUCL expands enforcement agencies' investigation powers. However, the 2018 AUCL also imposes more processes and procedures on these agencies. The investigation procedures that AICs may use during investigations of potential commercial bribery violations include (a) entering business premises to conduct inspections; (b) questioning business operators and other related entities and individuals, and requiring them to explain the matter under investigation and to provide evidentiary materials or related information; (c) accessing or copying related evidentiary materials; (d) sealing and/or detaining property related to suspected unfair competition; and (e) inquiring about bank accounts of business operators suspected of unfair competition. 2018 AUCL at Article 13.

Increases Administrative Penalties

The 2018 AUCL increases administrative penalties to RMB 10,000 – RMB 3,000,000. 2018 AUCL at Article 19. Plus, if a business operator commits a "serious" act of bribery, that operator will have its business license revoked. *Id.* The 2018 AUCL

emphasizes that administrative penalties can be imposed on wrongdoers whether or not a crime has been committed. 2018 AUCL at Article 31.

Administrative penalties may be mitigated. 2018 AUCL at Article 25. The 2018 AUCL allows business operators with minor violations to mitigate administrative penalties by proactively eliminating or reducing the harms that the violations caused. Although the provision does not specify the extent of harm that should be eliminated or reduced, it provides business operators with an avenue to mitigate their exposure to penalties.

2017 China Law LEXIS 1236

Reporter
2017 China Law LEXIS 1236 *

Title: Anti-Unfair Competition Law of the People's Republic of China (Revised in 2017)

Document Number: 3168615

Article Number: Order of the President of the People's Republic of China No. 77

Topic: Market Competition Law

Effective: Effective

Promulgator: Standing Committee of the National People's Congress

Promulgation Date: 11-04-2017

Effective Date: 01-01-2018

Effect Area: [*1] NATIONAL

Source: China Online

Update: replacement

Anti-Unfair Competition Law of the People's Republic of China (Revised in 2017)

Order of the President of the People's Republic of China No. 77

November 4, 2017

The revisions to the Anti-Unfair Competition Law of the People's Republic of China were adopted at the 30th Session of the Standing Committee of the 12th National People's Congress on November 4, 2017. The revised Anti-Unfair Competition Law of the People's Republic of China is hereby promulgated and shall come into force as of January 1, 2018.

Xi Jinping, President of the People's Republic of China

Anti-Unfair Competition Law of the People's Republic of China

Used with permission © 2018 LexisNexis

(Adopted at the Third Session of the Standing Committee of the Eighth National People's Congress on September 2, 1993, and revised at the 30th Session of the Standing Committee of the 12th National People's Congress on November 4, 2017.)

Table of Contents

Chapter I General Provisions

Article 1 This Law is formulated with a view [*2] to promoting the healthy development of the socialist market economy, encouraging and protecting fair competition, preventing acts of unfair competition, and protecting the legitimate rights and interests of business operators and consumers.

Article 2 While carrying out production or business activities, a business operator shall follow the principles of voluntariness, equality, fairness, and good faith, abide by laws and observe business ethics.

For the purpose of this Law, unfair competition refers to any business operator's act of participating in the production and operation activities in violation of the provisions herein to disrupt the competition order in the market and infringe the legitimate rights and interests of other business operators or consumers.

For the purpose of this Law, a business operator refers to a natural or legal person or any other unincorporated association engaged in the manufacturing or trading of commodities or the provision of services ("commodities" referred to hereinafter include services).

Article 3 People's governments at various levels shall take measures to prevent acts of unfair competition and create a favorable environment and conditions [*3] for fair competition.

The State Council shall establish an anti-unfair competition work coordination mechanism, study and decide on major anti-unfair competition policies, and coordinate and deal with major issues to maintain the competition order.

Article 4 The department responsible for administration for industry and commerce under a people's government at or above the county level shall investigate and deal with acts of unfair competition. Where laws or administrative regulations provide that such acts shall be investigated and handled by another department, those provisions shall apply.

Article 5 The State encourages, supports and protects all organizations and individuals in the exercise of social supervision over unfair competition acts.

State organs and their staff members shall not support or cover up any unfair competition conduct.

Industry organizations shall strengthen industry self-discipline, guide and regulate their members to compete according to the law, and maintain the competition order in the market.

Chapter II Unfair Competition Acts

Article 6 A business operator shall not perform any of the following confusing acts that will enable people to mistake [*4] its products for another business's products or believe certain relations exist between its products and any business's products,

1. unauthorized use of a mark that is identical or similar to the name, packaging or decoration of another business's commodity, which has influence to a certain extent,

2. unauthorized use of another business's corporate name (including its shortened name, trade name, etc.), the name of a social group (including its shortened name, etc.), or the name of an individual (including his or her pen name, stage name, translated name, etc.), which has influence to a certain extent;
3. unauthorized use of the main domain name, website name or webpage, which has influence to a certain extent; and
4. other confusing acts that are sufficient to enable people to mistake its products for another business's products or believe certain relations exist between its products and any business's products.

Article 7 A business operator shall not resort to bribery, by offering money or goods or by any other means, to any of the following entities or individuals, in order to seek a transaction opportunity or competitive advantage,

1. any employee of the counterparty in a [*5] transaction;
2. any entity or individual entrusted by the counterparty in a transaction to handle relevant affairs; or
3. any other entity or individual that is to take advantage of powers or influence to influence a transaction.

A business operator may expressly give a discount to the counterparty or pay a commission to the middleman of a transaction in the course of transaction activities. Where a business operator gives a discount to the transaction counterparty or pays a commission to the middleman, it shall truthfully enter it in his account books. A business operator that accepts such discount or commission shall also enter it into its account books.

The act of an employee of a business operator bribing any other individual shall be deemed an act of the business operator itself, unless otherwise proven by the business operator with evidence that such act is not related to efforts in seeking a transaction opportunity or competitive advantage.

Article 8 A business operator shall not conduct commercial promotions for the performance, function, quality, sales status, user evaluation, honor received concerning its products in a false or misleading manner, attempting to cheat or [*6] mislead consumers.

A business operator shall not assist another business operator with its commercial promotions in a false or misleading manner by way of organizing false transactions or by other means.

Article 9 A business operator shall not engage in any of the following infringements of commercial secrets:
1. obtaining an obligee's commercial secrets by theft, bribery, intimidation or other improper means;
2. disclosing, using, or allowing others to use an obligee's commercial secrets obtained by the means mentioned in the preceding paragraph; or
3. disclosing, using or allowing others to use an obligee's commercial secrets in violation of an agreement or the obligee's requirements on keeping such commercial secrets confidential.

Where a third party knows or should know of the fact that an employee or former employee of the right owner of commercial secrets or any other entity or individual conducts any of the illegal acts specified in the preceding paragraph, but still accepts, publishes, uses or allows any other to use such secrets, such practice shall be deemed as infringement of commercial secrets.

For the purpose of this Law, commercial secrets refer to any technical information [*7] or operational information which is not known to the public and has commercial value, and for which its obligee has adopted measures to ensure its confidentiality.

Article 10 The prize-attached sale activities of a business operator shall not involve the following situations:
1. making sales with prizes attached without expressly specifying the prize types, terms for collecting prizes, the amounts of cash or the goods as prizes, or other related information that will affect the collection of prizes;
2. making sales with prizes attached in a fraudulent manner by falsely claiming the existence of prizes or intentionally causing internally-chosen persons to win the prizes; and
3. making sales with prizes attached in the form of a lucky draw where the amount of the highest prize exceeds CNY50, 000.

Article 11 A business operator shall not fabricate or disseminate any false information or misleading information to injure the credit standing of its rival or the reputation of its rival's commodities.

Article 12 A business operator that makes use of the network to engage in production and business activities shall abide by all the provisions herein.

It shall not perform any of the following [*8] acts that impede or disrupt the normal operation of network products or services legally provided by other business operators, by taking advantage of technical means to influence users' choices or otherwise,
1. inserting a link into a network product or service legally provided by another operator to compel a destination jump without the approval of such operator;
2. misleading, deceiving or compelling users into modifying, closing, or uninstalling a network product or service legally provided by another business operator;
3. implementing in bad faith an incompatibility with a network product or service legally provided by another business operator; or
4. any other act that impedes or disrupts the normal operation of network products or services legally provided by another business operator.

Chapter III Investigations into Suspected Unfair Competition Acts

Article 13 The supervision and inspection authorities may adopt any of the following measures to investigate suspected unfair competition conduct,
1. accessing the business premises involved in a suspected unfair competition act for inspection;

2. questioning the business operator under investigation, any interested party, or [*9] any other related entity or individual, and requiring them to explain relevant situations or provide other materials in relation to the investigated act;
3. inquiring into and copying the contracts and agreements, account books, vouchers, documents, records, business correspondence and other materials related to a suspected unfair competition act;
4. sealing up and/or detaining the property involved in a suspected unfair competition act; and
5. inquiring into the bank account of a business operator that is suspected of an unfair competition act.
Before any measure specified in the preceding paragraph is adopted, a written report shall be submitted to the principal of the supervision and inspection authority for his or her approval. Where the measure specified in Item 4 or Item 5 of the preceding paragraph is to be adopted, a written report shall be submitted to the principal of the supervision and inspection authority under the people's government at or above the level of a city with district division for his or her approval.

The supervision and inspection authorities shall abide by the Administrative Coercion Law of the People's Republic of China and other applicable laws and administrative [*10] regulations while looking into suspected unfair competition acts, and disclose the investigation and handling results to the public in a timely manner.

Article 14 The business operators subject to investigation, interested parties, and other related entities or individuals, shall truthfully provide the relevant materials or information when the supervision and inspection authorities are investigating suspected unfair competition conduct.

Article 15 The supervision and inspection authorities and their staff members shall keep confidential any commercial secrets known to them during the investigations.

Article 16 Any entity or individual shall have the right to report any suspected unfair competition acts to the supervision and inspection authority. The supervision and inspection authority shall promptly deal with such reports according to the law upon receipt of these reports.

The supervision and inspection authorities shall make available to the public the phone numbers, mailing addresses or email addresses for such reports and keep the identities of informants confidential. For real-name informants who present evidence for their claims, the supervision and inspection authorities [*11] shall inform them of the handling results.

Chapter IV Legal Liability

Article 17 A business operator that violates this Law and thus causes damage to others shall bear civil liability for such damage in accordance with the law.
A business operator whose lawful rights and interests are infringed by an unfair competition act may file a lawsuit with a people's court.

The amount of compensation for damage caused by any unfair competition act to a business operator shall be determined depending on the actual losses suffered by such operator as a result of the infringement; where it is truly difficult to work out the actual losses, such amount shall be determined in accordance with the benefits obtained by the infringer from the infringement. The amount of compensation shall also include the reasonable expenses paid by the damaged business operator to stop the infringement.

Where a business operator violates the provisions stipulated in Article 6 or Article 9 herein, and it is truly difficult to determine the actual losses suffered by the obligee as a result of the infringement or the benefits obtained by the infringer from the infringement, the people's court shall award the obligee [*12] less than CNY3 million in damages, depending on the seriousness of the infringement.

Article 18 Where a business operator violates Article 6 herein by performing any confusing act, the supervision and inspection authority shall order it to cease the offense, and confiscate its illicit commodities. If the illicit turnover exceeds CNY50, 000, it shall be fined up to five times the illicit turnover. If there is no illicit turnover or the illicit turnover is less than CNY50, 000, it shall be fined up to CNY250, 000; where the circumstance is serious, it business license shall be revoked.
Where a corporate name registered under a business operator violates the provisions of Article 6 herein, the business operator shall go through formalities to change its registered corporate name promptly. Prior to the change of the corporate name, the original corporate registration authority shall use the unified social credit code in lieu of its corporate name.

Article 19 Where a business operator bribes any other party in violation of Article 7 herein, the supervision and inspection authority shall confiscate its illegal gains, and impose on it a fine of between CNY100,000 and CNY3 million. Where [*13] the circumstance is serious, its business license shall be revoked.

Article 20 Where a business operator violates the provisions of Article 8 herein to conduct commercial promotions for its commodities in a false or misleading manner, or assists other business operators with commercial promotions in a false or misleading manner by way of organizing false transactions or by other means, the supervision and inspection authority shall order the business operator to cease its violations and impose on it a fine of between CNY200, 000 and CNY1 million; where the circumstance is serious, it shall be fined between CNY1 million and CNY2 million, and its business license may be revoked.
Where a business operator's violation of Article 8 herein constitutes the releasing of a false advertisement, it shall be punished according to the Advertising Law of the People's Republic of China.

Article 21 Where a business operator infringes any commercial secret in violation of Article 9 herein, the supervision and inspection authority shall order it to cease the illegal act and impose on it a fine of between CNY100, 000 and CNY500, 000; where the circumstance is serious, the fine shall be between CNY500, [*14] 000 and CNY3 million.

Article 22 Where a business operator makes a prize-attached sale in violation of Article 10 herein, the supervision and inspection authority shall order it to cease the illegal act and impose on it a fine of between CNY50, 000 and CNY500, 000.

Article 23 Where a business operator causes injury to the credit standing of its rivals or the reputation of its rivals' commodities in violation of Article 11 herein, the supervision and inspection authority shall order it to cease the illegal act and eliminate any bad influences, and impose on it a fine of between CNY100, 000 and CNY500, 000; where the circumstance is serious, the fine shall be between CNY500, 000 and CNY3 million.

Article 24 Where a business operator impedes or disrupts the normal operation of network products or services legally provided by another business operator, in violation of Article 12 herein, the supervision and inspection authority shall order it to cease the illegal act and impose on it a fine of between CNY100, 000 and CNY500, 000; where the circumstance is serious, the fine shall be between CNY500, 000 and CNY3 million.

Article 25 Where a business operator performs any unfair competition [*15] act in violation of the provisions herein, and if such operator proactively eliminates or relieves the harmful consequence of its illegal act, it shall be subject to a lighter or mitigated administrative penalty; if the illegal act is considered as a minor violation and is corrected in a timely manner without leading to any harmful consequence, it may not be subject to an administrative penalty.

Article 26 Where a business operator is subject to the administrative penalty for performing an unfair competition act in violation of this Law, the supervision and inspection authority shall enter such penalty in its credit record and publicly disclose the same in accordance with the relevant laws or administrative regulations.

Article 27 Where a business operator shall bear civil liability, administrative liability and criminal liability as a result of its violation of the provisions herein, but its property is not sufficient to cover all the damages, the civil liability shall take precedence.

Article 28 Where a party obstructs the efforts of the supervision and inspection authority to fulfill its duties according to this Law, refusing or impeding the investigations, the supervision [*16] and inspection authority shall order it to make corrections, and impose a fine of up to CNY5, 000 if the party is an individual, or a fine of up to CNY50, 000 if the party is an entity, and the public security organ may impose a public security punishment according to the law.

Article 29 Where the party concerned disagrees with the decision made by the supervision and inspection authority, it may apply for administrative reconsideration or file an administrative lawsuit.

Article 30 Where any staff member of a supervision and inspection authority abuses powers, neglects duties, commits malpractices or reveals any commercial secrets known during the investigations, such staff member shall be subject to punishment in accordance with the law.

Article 31 Where any violation of this Law constitutes a crime, there shall be an investigation for criminal liability.

Chapter V Supplementary Provisions

Article 32 This Law shall come into force as of January 1, 2018.

Load Date: January 22, 2018

LexisNexis China Law Database
©2018 LexisNexis China, a division of Reed Elsevier Information Technology (Beijing) Co., Ltd. All Rights Reserved

End of Document