By **Guy David Singer** and **Joshua C Foster**

Navigating the Foreign Corrupt Practices Act in the IP context

Although IP business practices have not been a traditional area of Foreign Corrupt Practices Act enforcement, a number of the high-risk areas apply in the IP context. Counsel should thus take care to establish procedures to mitigate such risks

As the US government has ramped up its enforcement of the Foreign Corrupt Practices Act (FCPA) over the past decade, the focus has largely remained on several key risk areas, such as third-party sales agents, distributors or local partners that maintain relationships with key foreign officials. However, one critical business component for many companies has remained relatively under the radar in terms of FCPA enforcement actions – IP acquisition and enforcement. Companies should not, however, assume that business practices with respect to their IP holdings are immune to the reach of the FCPA. For companies with IP holdings that constitute an important, if not critical, aspect of the business, threats to IP activities must be taken very seriously.

Several aspects of IP practices have significant overlap with the traditional areas of FCPA enforcement and these business practices could be ripe for future investigations. Companies need to be cognisant of these risks and take the appropriate measures to mitigate the risk, particularly as companies continue to expand their global footprint and operations and IP holdings take on increased importance in such growth. Moreover, many countries in which companies are seeking to expand present significant anti-corruption risks – most notably China, where IP issues already present significant challenges. This article provides an overview of the FCPA, the risks that companies face with respect to their IP activities and measures to mitigate such risk.

Overview of the FCPA

The US Department of Justice (DOJ) and the US Securities and Exchange Commission (SEC) enforce the FCPA, which creates civil and criminal liability for both individuals and companies. The FCPA contains two key provisions: the anti-bribery provisions and the internal controls provisions.

Anti-bribery provisions

The anti-bribery provisions prohibit direct and indirect corrupt payments to foreign officials for the purpose of obtaining or retaining business. The anti-bribery provisions apply to US companies and individuals, and other "issuers" under US securities laws (see 15 USC § 78dd-1, *et seq*). The basic elements of an FCPA anti-bribery violation are:

- an offer, gift, payment, promise to pay or authorisation of the payment;
- of money or anything of value;
- to a foreign government official;
- with corrupt intent;
- to assist in obtaining a business advantage, obtaining or retaining business, or directing business to any person (*id*).

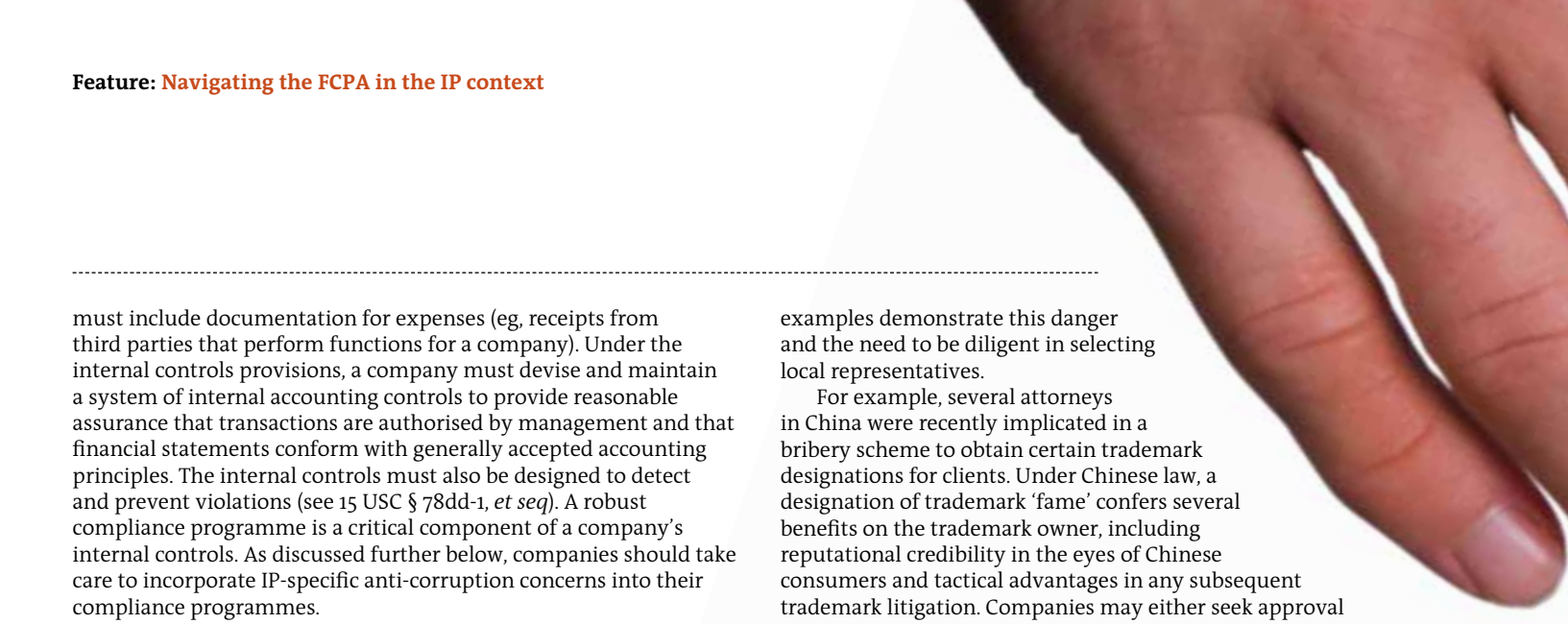
These provisions have been interpreted broadly by the SEC and DOJ. For example, 'anything of value' has been interpreted to include money, travel upgrades, meals, entertainment, gifts, charitable contributions or in-kinds services (see the DOJ's Resource Guide to the Foreign Corrupt Practices Act). Payment need not be made to constitute a violation; rather, the mere promise of an improper payment is sufficient to trigger FCPA liability. Similarly, the definition of 'foreign government official' has been interpreted broadly to include any employee of a non-US government (eg, state, national, municipal), department or agency of a non-US government, state-owned or controlled company, or any foreign political party or official, or candidate for political office (*id*).

The FCPA contains one important exception to the general prohibition against payments made to foreign officials for the purpose of obtaining or retaining business: facilitating payments. Facilitating payments are small amounts paid to a foreign official to induce that or another official to perform or expedite a routine, non-discretionary act that he or she is required to perform in the course of his or her ordinary duties (see 15 USC § 78dd-1, *et seq*).

Because this exception is narrow and difficult to satisfy, many companies explicitly prohibit the use of facilitating payments. Moreover, the UK Bribery Act – the United Kingdom's legislative counterpart to the FCPA – does not contain a facilitating payments exception. Accordingly, although such payments may be exempt from liability in the United States, they may subject companies to liability in the United Kingdom.

Accounting provisions

The accounting provisions of the FCPA contain two parts: the books and records provision and the internal controls provision. Under the books and records provision, a company must maintain books, records and accounts in reasonable detail to accurately reflect the transactions and dispositions of assets, and the records



must include documentation for expenses (eg, receipts from third parties that perform functions for a company). Under the internal controls provisions, a company must devise and maintain a system of internal accounting controls to provide reasonable assurance that transactions are authorised by management and that financial statements conform with generally accepted accounting principles. The internal controls must also be designed to detect and prevent violations (see 15 USC § 78dd-1, *et seq*). A robust compliance programme is a critical component of a company's internal controls. As discussed further below, companies should take care to incorporate IP-specific anti-corruption concerns into their compliance programmes.

Penalties and fines

The FCPA carries stiff penalties for criminal violations. Under the anti-bribery provisions, companies face up to a $2 million fine per violation and individuals face up to five years of prison and $250,000 in fines per violation. Under the accounting provisions, companies face up to a $25 million fine per violation, and individuals face up to 20 years in prison and up to $2 million in fines. Both the DOJ and the SEC may impose a $10,000 per violation civil fine on individuals and companies, and the SEC may also impose additional civil penalties of $5,000 to $100,000 for individuals, $50,000 to $500,000 for companies, or alternatively a civil penalty equal to the gross pecuniary gain to an individual or company arising from the violation. These fines and penalties can add up quickly and, in large cases, easily reach hundreds of millions of dollars (not including the extensive legal fees associated with the investigations).

Other non-monetary penalties for FCPA violations may include the imposition of a corporate monitor, reputational damage, debarment from government contracts and programmes, costs associated with internal investigations and private causes of action brought for monetary damages under federal and state laws. Moreover, internal investigations into FCPA allegations or concerns can be expensive, time consuming and disruptive to regular business operations.

IP risk areas

At first glance, it may seem as though a company's business practices with respect to its IP holdings would involve little to no risk of FCPA exposure, particularly given the relative lack of previous FCPA enforcement actions involving IP practices. However, several critical risk areas could leave a company open to FCPA exposure if not adequately addressed.

Third-party agents

The use of third-party agents has historically been a ripe area for FCPA liability. In many of their most high-profile investigations, the DOJ and SEC have focused on third-party agents (eg, sales agents, travel agents) as facilitators and/or providers of illicit payments. This will undoubtedly continue to be a significant focus going forward, as companies are often forced to rely upon third parties for business activities in foreign countries.

Nearly every company with active IP portfolios in foreign countries engages third-party agents for a variety of tasks. The most obvious example is the engagement of local legal counsel to handle IP prosecution matters with local, state and national government agencies charged with IP registration. Local counsel are often also integral in providing monitoring services and advice with respect to IP policing. Although one might not typically think of local attorneys as a third-party FCPA risk area, local counsel are often in the best position to understand local customs and/or systemic weaknesses that may be exploited through illicit payments. Several recent examples demonstrate this danger and the need to be diligent in selecting local representatives.

For example, several attorneys in China were recently implicated in a bribery scheme to obtain certain trademark designations for clients. Under Chinese law, a designation of trademark 'fame' confers several benefits on the trademark owner, including reputational credibility in the eyes of Chinese consumers and tactical advantages in any subsequent trademark litigation. Companies may either seek approval from local and national trademark authorities – a process which may take several years – or seek a well-known trademark designation through the Chinese judiciary during the course of a trademark infringement litigation.

It was recently reported that a number of companies and their attorneys had exploited the ability to seek a judicial designation by filing fake trademark infringement lawsuits. The attorneys accomplished this by hiring fake defendants to sue and by bribing judges to rule in their favour. The scheme was discovered when a Taiwanese soy milk manufacturer's trademark suffered as a result of a fake litigation and subsequently notified the authorities. One Chinese attorney, Zheng Lifang, confessed to receiving over Rmb1 million, some of which he used to bribe Chinese judges. To date, at least six judges and three attorneys have been arrested on similar charges (see Caixan Online, "Fake Lawsuits Behind China's 'Famous' Brands"). Although it is unclear whether these arrests are a result of a local government's efforts or a larger effort to root out corruption, China's President Xi Jinping has made rooting out corruption a major initiative of his new government. Other recent Chinese government crackdowns on corruption suggest the possibility that similar conduct could result in additional arrests. Although it does not appear that any US-based companies were involved in this specific case, companies should nonetheless be cautious in selecting local representatives as a result.

Other third parties can present a similar FCPA risk. In 2008, AGA Medical Corporation agreed to pay a $2 million settlement in connection with illegal payments to Chinese officials to issue several patents between 2000 and 2002. AGA allegedly agreed to make the illicit payments to a local distributor, which would in turn make illicit payments to Chinese officials at the State Intellectual Property Office in order to have the patents approved. At least one high-ranking AGA employee in the United States was aware of the illicit payments (see DOJ press release, "AGA Medical Corporation Agrees to Pay $2 Million Penalty and Enter Deferred Prosecution Agreement for FCPA Violations"). Undoubtedly, these corruption risks are not limited to China. A simple Google search reveals, for example, extensive speculation of corruption concerns with various other countries' IP regulators, most notably India.

Customs interactions

Another area that presents significant FCPA risk is a company's interactions with customs officials as part of its IP enforcement practice. Certain issues, such as expedited clearance or clearance of goods without the appropriate paperwork, have been especially problematic for companies and the area has become a high-profile focus for the DOJ and SEC.

In the IP context, companies may routinely interface with local customs officials as part of their anti-counterfeiting practice, either directly or through third-party agents. It is common for companies to encourage customs officials to inspect and seize counterfeit goods

at the border as part of its anti-counterfeiting programme, and such interactions pose corruption risks.

This is particularly significant in countries with historically poor records for anti-counterfeiting enforcement efforts, most notably China. In such circumstances, companies and their agents may be forced to choose between making potentially illicit payments to induce Customs to disallow counterfeit goods or allowing the counterfeit goods into the market. Although there is nothing improper with fostering and maintaining a close relationship with customs officials, care must be taken not to improperly incentivise the officials to act on the company's behalf. Although there have been no official enforcement actions to date based on a company's anti-counterfeiting activities, the government's extensive history of focusing on customs activities in this context suggest that it is an area ripe for future enforcement.

IP due diligence

Another anti-corruption risk area that has recently made headlines is due diligence. Nearly every merger and acquisition involves at least some level of IP due diligence, including the use of private investigators. Although the due diligence process may seem straightforward and risk free, a recent arrest in China illustrates the care that one must take when operating in opaque business environments.

Although it is not entirely clear what the exact conduct entailed, the *New York Times* recently reported on the arrest of two private investigators who were accused of illegally acquiring private personal information, and the jailing of several other 'business researchers' on similar charges (see Jane Perlez, "In China, the Dangers of Due Diligence"). The article noted that in China, even corporate documentation may be difficult to obtain. As another example of the difficult business environment, the article also highlighted the recent arrest of a Canadian investigator who conducted diligence on a Chinese company and prepared a negative report about the target company (*id*). One anonymous US lawyer was quoted in the article as saying that his firm works with investigators, but "don't want to know where they get the information" (*id*).

IP due diligence is typically wrapped up within the larger due diligence efforts for any acquisition, and the anti-corruption risks in this scenario are not only germane to the IP aspect of diligence. However, the recent arrests reflect the prospective dangers for seemingly ordinary business activities in high-risk countries. This environment can place companies in a difficult position, having to choose between absorbing the risks of conducting thorough due diligence and proceeding with less robust diligence.

Companies and their agents may be forced to choose between making potentially illicit payments to induce Customs to disallow counterfeit goods or allowing the counterfeit goods into the market

Practical tips to reduce FCPA risk

Given the critical nature that IP holdings may play in a company's business, it is easy to see how both informed and uninformed employees may be coaxed into making poor decisions in an effort to maximise IP value. Although companies cannot completely eliminate FCPA risks in their IP activities, a number of measures serve to mitigate the potential risk.

Effective third-party due diligence

With the rise of FCPA enforcement and focus on third parties, it has become increasingly critical that companies conduct thorough due diligence on all third parties that may interact with foreign officials on the company's behalf, including on attorneys providing legal services in foreign countries. The methods and reach of the due diligence may vary from third party to third party and from country to country. At a minimum, however, the due diligence should consider:

- the company's history with the third party;
- its reputation within the industry and country;
- its prior legal issues within the country;
- its prior experience with anti-corruption concerns and/or issues;
- its own anti-corruption policies and procedures; and
- the names and positions of all personnel that will interact with foreign officials on the company's behalf.

Depending on the volume of work that the third party will handle and the extent of the anticipated interactions with foreign officials, companies may wish to conduct additional diligence, including the engagement of an investigative firm to uncover other issues or irregularities.

"With the rise of FCPA enforcement and focus on third parties, it has become increasingly critical that companies conduct thorough due diligence on all third parties that may interact with foreign officials on the company's behalf, including on attorneys providing legal services in foreign countries"

Anti-corruption language and audit rights

Third-party due diligence does not end once the third party has been engaged. Rather, companies should institute internal controls designed to keep tabs on third-party activities, including requiring third parties to provide detailed narratives of any interactions with foreign officials on the their behalf and requiring annual certifications that third parties are in compliance with US anti-corruption laws. Even if the likelihood of third parties admitting to violations in these documents is slim, ongoing diligence efforts are a positive story to tell in the event that a company ends up defending itself before the DOJ and/or SEC.

Companies should also insist that audit rights be included in the agreement, where appropriate. Whether a company opts to exercise these audit rights will depend on the volume of work conducted by the third party and the time and budget available to the company. However, in the event that a red flag is raised, audit rights can be an effective tool to uncover the facts.

Robust compliance programme

In this era of extensive FCPA enforcement, it is increasingly critical for companies to have a robust compliance programme in place covering all aspects of its business. In fact, the DOJ and SEC are increasingly requesting information concerning companies' compliance programmes during the course of official investigations.

Although the outlines of compliance programmes are not likely to originate from the IP business practice, companies should ensure that existing compliance programmes explicitly consider and address the unique circumstances raised by IP portfolio management. For example, companies should implement a system of controls that requires detailed invoices and receipts with accompanying explanations for all payments to foreign officials, such as customs employees, prior to payment. Companies should also take care to examine closely all invoices from third parties, including local legal counsel, and escalate any irregularities to the appropriate internal personnel.

Anti-corruption training

As part of a company's compliance programme, and arguably the most important step that a company can take, companies should provide anti-corruption training to both domestic and foreign employees.

The employees who manage the day-to-day aspects of a business are also the individuals who are most likely to identify potential issues or concerns. Training should be tailored to the specific circumstances and challenges presented by each specific business sector, and should identify anti-corruption red flags, including:

- excessive commissions to third parties;
- unreasonably large discounts to distributors;
- vaguely described services in third-party agreements;
- close relationships with foreign officials;
- irregularities in invoicing or payment processing; and
- requests for expediting fees.

The training programme should clearly identify the options available to individual employees when red flags are identified and how to escalate concerns to the appropriate personnel.

Although IP business practices have not been a traditional area of FCPA enforcement, a number of the high-risk areas that have traditionally been a focus by the DOJ and SEC also apply in the IP context. As IP holdings become increasingly large and critical business components, companies should take great care to ensure that employees are aware of the corruption risks inherent in their industry and establish procedures to mitigate such risks. WTR

Guy David Singer is a partner and **Joshua C Foster** managing associate at Orrick
gsinger@orrick.com
jfoster@orrick.com