As the International Criminal Court (“ICC”) Review Conference in Kampala, Uganda approaches, the United States is making huge strides towards acceptance. Beginning May 31 and continuing through June 11, 2010, the Review Conference to the Rome Statute (governing the ICC) will be meeting to consider any amendments to the statute and to review the performance of the Court over the past decade. This will be the first ever, and perhaps only, review conference for the Rome Statute. Over the past three years, beginning with a resolution proposed by the International Criminal Law Committee in 2007 and eventually adopted by the American Bar Association (“ABA”) House of Delegates (“HOD”) in 2008, the Section of International Law has been preparing diligently to attend this conference and to encourage the attendance and positive participation by the United States in the conference. Following the adoption of the resolution by the HOD, a task force was appointed by the Section Chair to

---

1 Judge Don Shaver is a Co-Chair of the International Criminal Law Committee.
develop strategy to involve the United States in the conference. That task force has enjoyed considerable success in dealing with the Obama Administration.

Working quietly behind the scenes over the past year, Task Force Co-Chairs Jeff Golden and David Crane have separately or together met with various government and international officials, including the U.S. and U.N. Legal Advisors on ICC Policy, the President of the Assembly of States Parties (“ASP”) – the governing body for the Court, the Chair of the ASP committee charged with formulating a definition of the crime of “aggression” (to be considered at the conference), and a number of U.S. Senators.

In November 2009, the Co-Chairs attended the ASP General Meeting in The Hague and were greatly impressed and heartened by the level of participation and acceptance demonstrated by the U.S. delegation, led by Ambassador-at-large for War Crimes Issues Stephen Rapp and State Department Legal Advisor Harold Koh. “Our government has now made the decision that Americans will return to engagement at the ICC,” Rapp stated at an earlier press conference. This major delegation included officials from the State Department, White House, Department of Defense, and others. Ambassador Rapp addressed the Assembly at the morning session, expressing broad support for the work of the ICC in an effort to dispel years of distrust and suspicion of the ICC expressed by the United States, and Mr. Koh addressed U.S. concerns relating to suggested definitions of the crime of “aggression” in the afternoon session. Ambassador Rapp expressed the United States’ “strong willingness” to participate in the Kampala conference. Mr. Koh agreed that the United States has a “keen interest in—and much to contribute to—the success of the cases before the ICC.” Both were well received by the Assembly. Following the conference, the Co-Chairs met with Ambassador Rapp and Mr. Koh in a two-hour private session, presenting the ABA SIL position and offering assistance in preparing the U.S. government position for the upcoming Review Conference.

Four members of the Task Force will be attending the Review Conference in Kampala. In the meantime, the Task Force will continue to coordinate with senior members of the U.S. government, the Council on Foreign Relations, and other NGOs that will be attending, including the American NGO Coalition for the ICC (AMICC) and the American Society of International Law (ASIL) Task Force at a high level meeting at the Tillar House in Washington, DC on May 14.

* * *

---


Corporate Criminal Liability and Enforcing Respect for Human Rights

Elise Groulx⁶ & L.H. (Lew) Diggs⁷

I. Companies Have a Responsibility to Respect Human Rights

For years, many business corporations considered that they were not responsible for enforcing human rights, arguing that this was the exclusive responsibility of states. The duty of business, they argued, was limited to compliance with legislation, regulations and court rulings that state organs issue to enforce human rights.

Today, there is a growing international consensus that private actors, including business corporations, have a “responsibility to respect” human rights. This responsibility is generally presented as being anchored in a general business duty to respect the rule of law but as also extending to a growing body of international, voluntary and treaty-based standards. Corporations increasingly recognize the need to implement and promote these standards in order to earn their so-called social licenses to operate. This responsibility applies with special force in countries that may lack legal enforcement powers, or where states themselves commit human rights abuses.

The consensus on the “corporate responsibility to respect” has emerged from 4 years of work (2005-2009) by John Ruggie, the United Nations special representative on business and human rights. His 2008 report articulates a policy framework comprising three core principles that links business responsibility to the other complementary principles: the “state duty to protect against human rights abuse” and “greater access to remedies” by victims. That report won broad support from member states sitting on the UN Human Rights Council. The Council gave Ruggie an extended mandate, to 2011, with instructions to make recommendations regarding enforcement and the so-called “operationalization” of human rights in the business world.

---

⁶ Elise Groulx (elisegroulx@citenet.net), Solicitor & Barrister, President of the International Criminal Defence Attorneys Association (ICDA), and Founding President of the International Criminal Bar (ICB), is a practising criminal defence attorney in Canada and a leader of international NGOs operating in the field of international criminal justice. In recent years, she has been advising corporations and organizations in Europe and Canada on international criminal law issues, including the legal liability of corporations for participation in international crimes committed in conflict zones. She has completed a two-year research project on the issue of “business complicity” in war crimes and formulated a due-diligence framework for use by a major multinational corporation in assessing investments in conflict-prone countries. She began speaking on the issue at an IBA conference in 2003 and led the preparation of a policy paper on corporate complicity under Canadian criminal law submitted by the ICDA to the International Commission of Jurists (ICJ) in Geneva in 2006. She recently joined as an international consultant a UK Chamber in London: www.perrenbuildings.com.

⁷ L.H. Diggs (lhdiggs@citenet.net), Management and Strategy Consultant, is a management consultant who co-led the research project on “business complicity” in war crimes and a due-diligence process enabling multinational corporations to assess investments in conflict-prone countries. His varied career spans wire service news reporting, corporate public affairs, book writing and strategic planning. He has written business books with an IT consulting house and provided senior consulting support to an NGO, an international development contractor, and various financial institutions.
Significantly, Ruggie has refused to give business a short list of rights of special concern to the private sector arguing that “business can affect virtually all internationally recognized rights” given the wide variety of economic activities around the world. The specific rights of concern to states, companies and victims will clearly vary from one case to the next.

II. Enforcement Is a Big Challenge

The primary challenge in most fields of human rights is not to articulate the rights in charters, declarations and treaties—the there are already several dozen of these legal instruments on the books of the UN system. Nor is the challenge to win general commitments in principle to respect human rights and the rule of law. The really difficult “trial by fire” in most fields of human rights is the effective enforcement of human rights standards that states, corporations and other stakeholders have made multiple commitments to respect. This is as true in the political sphere as in the business world.

In this regard, Ruggie argues that the primary problem is “governance gaps created by globalization.” In his key 2008 report, he defines these as gaps “between the scope and impact of economic forces and actors, and the capacity of societies to manage their adverse consequences. These governance gaps provide the permissive environment for wrongful acts by companies of all kinds without adequate sanctioning or reparation.”

Ruggie faces a jungle of policy options regarding enforcement, and a lot of debate about the issue. The options, developed over a number of decades, include the following:

- Self-regulation by individual companies
- Voluntary industry codes
- Soft law & multi-stakeholder initiatives
- Ombudsmen
- Criminal & civil law
- Disclosure requirements in securities law for public companies
- Legislation on environment, labour rights, human rights, etc.
- Treaties on these subjects

There is often a broad consensus on the substance of human rights. It is the issue of enforcement methods that generates heated debate between business leaders and their critics in the NGO world. The debate often degenerates into an exchange of sweeping arguments about the value of binding legislation versus self-regulation by business.

These discussions often produce more heat than light, as Ruggie the pragmatist has pointed out on several occasions. He and other experts point out that, in fact, enforcement of

---

9 Examples include the Voluntary Principles on Security and Human Rights, Extractives Industry Transparency Initiative, OECD Guidelines on Multinational Corporations.
human rights is rarely an “either/or” issue. The main challenge is to find the best combination of enforcement instruments for a specific right or family of rights.\textsuperscript{11}

If the punishment must fit the crime, it is equally true that the enforcement instrument must match the right. When to use carrots or sticks? Voluntary codes or legislated minimum standards? Soft law or hard law? These questions need to be answered in order to move forward in the field of business and human rights.

\section*{III. Enforcement Is Becoming Robust for Large-Scale Violations of Human Rights}

There is one field of human rights where the governance gap is being rapidly closed by the international community of nations and where the debate on enforcement methods is largely complete. This is the field of massive human rights violations occurring in wars, civil conflicts and insurgencies. These violations are defined as major international crimes in various “hard law” instruments. They are defined, in fact, as war crimes, crimes against humanity and genocide—essentially the same crimes judged by Nuremberg tribunals in 1945-47.

Not surprisingly, given the gravity of the crimes, there is a broad political consensus that strong international legal standards are required and that “big sticks” are required to ensure enforcement. The consensus is reinforced by a recounting of the sad history of massive war crimes and genocides—often officially sanctioned and later minimized or denied—that marked the 20th century. And it leads to serious statements of intent to “end impunity” for the leaders who organize major international crimes.

The “big sticks” have been created in the form of both new international courts and extensions of the jurisdictions of national prosecutors, investigating magistrates and superior courts.

An obvious example is the creation in the 1993-2008 period of a half-dozen UN ad hoc courts and special courts, including those for the former Yugoslavia, Rwanda, Sierra Leone, Cambodia and Lebanon.

Another dramatic example is, of course, the International Criminal Court and its treaty, called the Rome Statute. The Rome Statute creates an international Office of the Prosecutor within the ICC. Less well known is the fact that it also empowers national prosecutors and courts in about 110 states parties to enforce the Rome Statute using a form of universal jurisdiction. Canada has already started with two prosecutions of Rwandese citizens arrested in Canada (one completed and one recently launched) and Germany has recently followed with the arrests of two Rwandese living in Germany and alleged to lead a militia committing atrocities in the eastern Congo.


In Europe, national prosecutions have also been launched (and in some cases completed) against business officials and companies alleged to have supported violence by repressive regimes in various ways—from joint ventures in major natural resource projects to purchases of conflict timber, illicit arms imports and UN sanctions busting. In these actions, the courts of the Netherlands, Belgium, France, and Spain have been asked to exercise a form of universal jurisdiction against executives or companies located in their jurisdictions but alleged to have participated in war crimes committed in other countries.

In the United States, the federal government has so far refused to ratify the Rome Statute while generally supporting the UN ad hoc tribunals. At the same time, the U.S. court system and strong tort law tradition have combined to become an incubator of civil law innovations aimed at seeking redress for victims of war crimes and a variety of other serious crimes such as torture.

Most notably, the U.S. federal court system has been used to launch about 40 tort actions against companies alleged to have supported the commission of major international crimes by repressive regimes in Africa, Asia and Latin America. The Supreme Court has confirmed the jurisdiction of federal district courts to hear such actions using extraterritorial authority to apply international standards of justice under the Alien Torts Claims Act (“ATCA”) and other federal statutes. While the precise legal standards to determine liability are still subject to debate, the jurisdiction to hear such cases is now established, creating another avenue besides criminal justice for victims’ groups to seek redress against companies that are alleged to act as “accomplices” in human rights abuse.

Based on the U.S. experience, victims’ groups have launched various civil and criminal actions in European courts. There are also legislative proposals to create a sweeping European version of ATCA to be used by victims of environmental and human rights violations in any country to launch actions against European-based companies.

There are still gaps in jurisdiction and the ICC is still in its early days. Nevertheless, robust enforcement instruments are being developed in this field of human rights at a rapid pace.

In the debate on human rights and business, corporate leaders often plead for a focus on self-regulation and “soft law” standards. That plea does not apply in the field of international criminal law. The only issue is how, and in which circumstances, that body of law applies to business executives and companies.

IV. Applications to Business

The primary aim of the ICC and international criminal justice is to “end impunity” for the leaders who organize large-scale violence against civilians. For the most part, those leaders are political and military figures. But the net of liability is expansive—and it has been cast wide enough to catch those who plan, support or contribute to conflict. In certain cases, that group can certainly include business executives.
There are clear precedents. The main ones are the prosecutions at Nuremberg of Nazi Industrialists, most notably the management teams of major German companies such as Krupp (arms) and IG Farben (chemicals) for their role in supporting the Nazi war machine. Many senior and mid-level executives were convicted, mainly for participating in (even encouraging) various Nazi schemes for property confiscation and forced labour regimes in occupied Europe.

At Nuremberg, the business leaders were not found be lead actors—in fact, they were generally acquitted of charges that they participated with the Nazi leadership in planning to wage an aggressive war. But they were clearly identified, and punished, for playing the role of supporting actors.

This pattern also emerged in more recent prosecutions in the Netherlands. One led to the conviction of a businessman charged with selling the components of chemical weapons to Saddam Hussein whose regime used them to commit acts of genocide. The other case ended in the acquittal (on appeal) of a top business associate of Charles Taylor, charged with complicity in war crimes and UN sanctions busting.

One point is illustrated clearly by these cases: the fact that business executives are not lead actors does not make them immune from prosecution. Nor are their organizations in any way immune from investigation and public challenge about their roles in armed conflict and, worse, ethnic cleansing.

To understand the emerging legal risks, directors and officers of companies operating in conflict zones need to understand two fundamental legal concepts: (i) substantive crimes; and (ii) modes of participation, or various ways in which supporting actors can be held liable for committing a crime.

V. Substantive Crimes: “Pillage and Plunder” Are Economic War Crimes

The traditional English expression “pillage and plunder” refers to the ways in which armies used to live off the land. In the 20th century, and even before, these methods were clearly branded by various international conventions as war crimes. Many are also crimes against humanity and now recognized as methods of ethnic cleansing (genocide).

Consider the fictional example of a rogue army battalion (or militia) that operates a mine, takes over some plots of land for their families and illegally “taxes” peasants for money and food in a war zone. This is a common occurrence in resource wars documented by UN and the ICC in Africa. The following crimes are commonly committed in such situations:

- Property confiscation
- Forced migration
- Forced labour, enslavement & child labour
- Recruiting child soldiers
- Rape and killing of civilians as a method of enforcing co-operation in the above schemes
These actions often have significant economic motivations. In poor countries, systematic violence against civilians is used as an instrument of competition for scarce agricultural land, natural resources, labour and sources of revenue.

Corporations operating in conflict zones are also significant economic actors. They must, of course, ensure that their own employees do not become involved in such crimes—and, moreover, that their policies and training programs do not show implied tolerance or tacit encouragement of such conduct. In conflict zones they may also need to develop special training programs to ensure that managers and employees (even directors) take specific steps to respect and implement International Criminal Law and International Humanitarian Law.

All these responsibilities apply to the corporation’s operations and employee conduct “inside the fence.”

VI. Modes of Participation: Extending the Net of Liability

But there is more. Corporations and executives can also be held liable for contributing to crimes perpetrated by other actors. These crimes are committed largely or wholly “outside the fence” of company operations and hierarchies. In particular, as noted earlier, executives can be prosecuted and sued as “supporting actors” in a conflict. The Rome Statute and international case law define many “modes of participation” that are designed to catch supporting actors and facilitators of violence.

What are those modes of participation? In judging complex war crimes cases, the international criminal courts have developed a variety of concepts such as “common planning” and “joint criminal enterprise” to hold leaders and their associates responsible for their roles in large-scale conflict. They have also adapted traditional notions of “command responsibility” and “aiding and abetting” for this purpose.

In total, we believe there are about 25 modes of participation grouped into three families that have been used by the international courts. They create what we call an extended “net of liability” designed to catch larger groups of associates that can include business executives.

To understand how the net can be used by the prosecution to capture a business leader, consider a scenario where an international company owns and operates the mine that is taken over by the militia. The militia leader insists that royalty payments be diverted by the company to the offshore bank account managed by the so-called political wing of the organization (operating like a sort of shadow state). Even worse, he orders company engineers to build roads that facilitate its military operations, and regularly requisitions trucks and drivers to conduct such operations.

These arrangements can be construed as making the company a business partner of the militia that contributes to the violence. The company officials may argue that they were coerced by the militia into co-operating—but this can be hard to prove and raises complex legal issues. How convincing does the story sound? To a judge, a jury, a journalist, or a casual Web browser?
The legal question remains complex. Does the company’s decision to co-operate (even under duress) amount to indirect participation in the war crimes committed by the militia? Does the company have a legal duty to pursue (or at least explore) alternative courses of action? Does it have a related duty to prepare for such eventualities when operating in a conflict zone?

The legal answers are not yet clear since there have been relatively few prosecutions of business executives since Nuremberg. Even though precise legal standards of conduct remain to be developed, however, it is possible to offer a few practical rules of thumb to business leaders:

- “It is always important to manage your own business conduct, ensuring legal compliance and respect for the role of law. But this is not easy in a conflict zone.”
- “When there is a risk of conflict, you must look outside your own organization to manage your business relationships with organizations that may engage in questionable conduct.”
- “You need not only to manage the people working inside your fence and but also relationships with people and organizations operating outside your fence.”

The situation is complex. The risk of conflict in a country appears to void traditional working assumptions about conducting “business as usual” and respect for the “rule of law.” Most likely, it creates additional legal obligations for business corporations.

**VII. Summary**

To summarize, business leaders need to confront squarely the emerging realities of the so-called corporate responsibility to respect human rights. These realities include:

1. The emergence of enforcement methods as a key issue in the global debate on human rights and business;
2. The broad international consensus that “big sticks” are required to prosecute perpetrators of serious human rights abuses such as war crimes and crimes against humanity;
3. The risk that business executives and corporations can be held liable for many types of direct and indirect participation in violence against civilian populations that is committed by armed groups.
4. The need to manage external business relationships with other organizations, not just internal business conduct, when operating in conflict zones.

***
When Does an ADR Program Give U.S. Authorities FCPA Jurisdiction over a Foreign Issuer?

Patrick O. Hunnius¹² & Michael H. Huneke¹³

I. Introduction

U.S. enforcement authorities’ current focus on the Foreign Corrupt Practices Act (“FCPA”) has received widespread media coverage. In addition to criminal enforcement of the FCPA’s anti-bribery and accounting provisions, civil enforcement of the FCPA’s accounting provisions has become a potent weapon in FCPA enforcement. Appreciation of the civil enforcement risks appropriately places the concept of “FCPA risk” in the broader context of securities compliance risk, because the FCPA is an amendment to, and borrows terms and elements from, the Securities Exchange Act of 1934 (“Exchange Act”). For example, assessing whether or not a foreign private issuer’s American Depositary Receipts (“ADRs”) trigger U.S. enforcement authorities’ FCPA jurisdiction—thereby exposing the ADRs’ issuer to potential fines, costly compliance measures, loss of sources of business revenue, and reputational harm—requires familiarity with numerous U.S. securities laws, the SEC’s rulemaking interpreting those laws, and the effect of such laws and rules in the context of the FCPA’s jurisdictional hooks. Foreign private issuers will likely not find warnings regarding FCPA risks in financial literature promoting ADRs and Global Depositary Receipts (“GDRs”) programs, and issuers need to consider such risks carefully before setting up an ADR program.

This article will first provide an overview of the current ADR programs available to foreign private issuers, including the reporting and registration requirements that U.S. law, as administered through SEC rules, imposes on each. Next, this article will review how certain ADR programs can trigger U.S. FCPA jurisdiction over foreign private issuers and will illustrate how differences between two foreign private issuers’ ADR programs appear to have affected the resolution of recent, high-profile investigations into potential FCPA violations.

II. ADR Programs and the Reporting and Registration Requirements for Each

A. General Information

The SEC defines an ADR as “a negotiable instrument that represents an ownership interest in a specified number of securities, which the securities holder has deposited with a designated bank depositary.”¹⁴ ADRs are subject to both registration and reporting requirements.

Pursuant to Section 5 of the Securities Act of 1933 (“Securities Act”), issuers must register any securities before trading or transferring the securities in any way that affects U.S.

¹² Patrick O. Hunnius is a partner at White & Case LLP in Los Angeles. He defends clients in a wide array of securities litigation and enforcement matters, including SEC and DOJ inquiries concerning Foreign Corrupt Practices Act compliance. Prior to joining White & Case, Mr. Hunnius was an SEC enforcement attorney.
¹³ Michael H. Huneke is an associate at White & Case LLP in Washington, DC.
¹⁴ Exemption from Registration under Section 12(g) of the Securities Exchange Act of 1934 for Foreign Private Issuers; Final Rule, 73 Fed. Reg. 52,751, 52,752 n.14 (Sept. 10, 2008).
Issuers of deposited securities represented by ADRs register the ADRs on a Form F-6 (or another form that provides the information required by Form F-6).

Such issuers must also file reports under either Exchange Act Section 13(a) (if the ADRs trade on a U.S. exchange) or Exchange Act Section 15(d) (if the SEC determines that the public interest or protection of investors require reports related to the ADRs), unless such issuers are excepted from those reporting requirements under Exchange Act Rule 12g3-2(b) (discussed below). The Securities Act registration is separate and independent from Exchange Act registration under Exchange Act Section 12 for securities that trade on U.S. exchanges. Although the practical effect—filing registrations or reports—is the same, whether the Exchange Act also requires registration has important implications for the scope of FCPA jurisdiction.

JPMorgan established the first ADR program in 1927; however, the use of ADRs did not become widespread until two decades ago. Currently, the use of ADRs for raising capital or investor awareness is near ubiquitous. According to a 2005 report by JPMorgan:

- More than 2,100 companies from more than 80 non-U.S. countries have used ADR programs;
- 500 ADR programs are listed on U.S. exchanges;
- Depositary receipts (including both ADRs and GDRs representing ownership of non-U.S. shares) “account for 16% of the entire US equity market”;
- As of March 2006, the value of Depositary receipt programs was USD 527 billion, approximately 99% of which were at four depositary banks: Bank of New York, JPMorgan, Citibank, and Deutsche Bank.

There are several types of ADRs, each with different purposes and reporting and registration requirements under U.S. law.

**B. Level I ADRs**

A “Level I” ADR program consists of ADRs representing an ownership interest in existing foreign shares that a foreign private issuer issues and cancels in the issuer’s home market. Such home market shares are subject to the home market’s accounting and disclosure

---

16 See 17 C.F.R. § 239.36; Form F-6, Registration Statement under the Securities Act of 1933 for Depositary Shares Evidenced by American Depositary Receipts, General Instruction I.B.
17 See Exchange Act Rule 12g3-2(d) (codified at 17 C.F.R. § 240.12g3-2(d)).
19 Id. at 3.
20 Id.
21 Id.
22 Id. at 17.
23 Id. at 9-10.
standards, but the ADRs in a Level I program are not new capital in the U.S. Level I ADRs do not trade, and are not listed, on a U.S. exchange; instead, they trade over-the-counter through the NASDAQ’s “Pink Sheets” program.

According to JPMorgan, the practical advantages to a Level I program are that it is simple, is cheap to establish, and imposes minimal regulatory obligations on the issuer. The disadvantages are that Level I programs, being limited to retail investors over-the-counter, does not significantly raise the issuer’s profile with other investors. Additionally, because these ADRs do not trade on a U.S. exchange, Level I ADRs are less liquid than other ADR programs in which ADRs do trade on a U.S. exchange.

SEC Exchange Act Rule 12g3-2(b) excuses from Exchange Act Section 12’s registration requirements ADRs that represent ownership in securities that primarily trade on a foreign market and for which an issuer has published in English and promulgated through the Internet (or other generally available electronic medium) the same disclosures that home market regulators require, and whose issuer does not have any reporting requirements for any class of securities under either Section 13(a) (due to listing equity securities on a U.S. exchange) or Section 15(d) (due to the SEC’s exercise of discretion to require reports) of the Exchange Act. Separately, the SEC has excluded securities of any class issued by any foreign issuer and held by less than 300 persons in the U.S. from Exchange Act Section 12’s reporting requirements.

If an issuer of Level I ADRs does not have any securities listed on a U.S. exchange or fewer than 300 persons hold the security in the U.S., then Section 13(a) does not require such an issuer to file reports. The SEC has declined to exercise its discretionary authority to require reports under Section 15(d) for Level I ADRs: SEC Exchange Act Rule 15d-3 excuses from Section 15(d)’s reporting requirements “Depositary Shares registered on Form F-6” pursuant to the Securities Act, provided that the ADRs do not trigger any other SEC registration requirement. Level I ADRs, therefore, do not trigger Exchange Act registration or reporting if the Level I ADR program meets the above criteria.

Foreign issuers may also offer Level I ADRs through a Rule 144A placement to qualified institutional buyers. Securities Act Rule 144A provides a limited exception to Section 5’s registration requirement for securities traded or transferred in any manner that affects U.S. interstate commerce. Securities Act Section 4 provides a safe harbor from Section 5’s

---

24 Id. at 9.
25 Id. at 9-10.
26 See id. at 9-10, 14-15.
27 Id.
28 Rule 12g3-2(b)(1) (codified at 17 C.F.R. § 240.12g3-2(b)(1)); see Exemption from Registration under Section 12(g) of the Securities Exchange Act of 1934 for Foreign Private Issuers; Final Rule, 73 Fed. Reg. 52,751, 52,757 (Sept. 10, 2008) (explaining the SEC’s consideration of the reporting requirement in Rule 12g3-2(b)).
29 Rule 12g3-2(a).
30 Rule 15d-3 (codified at 17 C.F.R. § 240.15d-3).
31 17 C.F.R. § 230.144A.
prohibition for “transactions by an issuer not involving any public offering.”32 Rule 144A Level I ADR placements avoid any Exchange Act reporting or registration requirement due to the nature of the underlying Level I ADRs and, because Rule 144A placements are also not subject to Securities Act registration requirements, a Rule 144A Level I ADR program “is the quickest, easiest, and most cost-effective way [for foreign issuers] to raise capital in the United States.”33

An example of a Level I ADR program is the facility representing ownership interests in shares of BAE Systems plc. BAE Systems’ ADRs trade under the symbol BAESY on the Pink Sheets market.34 Although BAE Systems’ was reportedly the subject of an investigation by U.S. enforcement authorities for violations of the FCPA, the U.S. DOJ’s criminal investigation resulted only in BAE Systems’ guilty plea to one count of criminal conspiracy to impede the lawful government functions of the U.S., to make false statements, and to violate arms export laws.35 BAE Systems, however, did receive a $400 million criminal fine.36 Although the SEC reportedly also investigated BAE Systems,37 the SEC has not brought an enforcement action against BAE Systems.38

C. Level II and Level III ADRs

Level II and Level III ADR programs list on a U.S. exchange, which triggers Exchange Act registration and reporting requirements (in addition to the Securities Act registration on Form F-6). Level II ADRs are similar to Level I ADRs in that they represent ownership over deposited shares in the issuer’s home market; the only difference is that the Level II ADRs also trade on a U.S. exchange.39 A Level III ADR program begins through a public offering of new shares.40

According to JPMorgan, the advantages of a Level II or Level III program are that the ADRs achieve a higher visibility among U.S. investors because analysts and the media may cover the ADRs and the ADRs may be promoted and advertised in the U.S.41 This increased exposure generates trading volume and, as a result, Level II or Level III ADRs have greater

34 See, e.g., BAE Systems plc, Registration Statement under the Securities Act of 1933 for American Depositary Shares Evidenced by American Depositary Receipts (Form F-6EF) (May 1, 2003), http://www.otcmarkets.com/pink/quote/quote.jsp?symbol=BAESY&amp;3BtabValue=2 (last visited Apr. 19, 2010).
37 James Boxell, Brooke Masters, & Stephanie Kirchgaessnerin, BAE Faces Threat of Fines in US Probe, Financial Times, June 27, 2007 (“The US Securities and Exchange Commission is also investigating BAE for possible violations of the books and records provisions of the Foreign Corrupt Practices Act, said two people familiar with the matter. . . . BAE said it had not been notified of an SEC inquiry.”).
40 Id.
41 Id.
potential liquidity than Level I ADRs. Issuers may also use Level II or Level III ADRs for employee incentive programs and for mergers and acquisitions.

Level II and Level III ADRs trigger registration and reporting requirements under the Exchange Act and the Securities Act. By virtue of their listing on a U.S. Exchange, these ADRs cannot qualify for Rule 12g3-2(b)’s exception to Exchange Act registration and reporting requirements. Issuers of Level II and Level III ADRs must:

- Register the ADRs under Securities Act Section 2 on Form F-6 (or equivalent) and, for Level III ADRs only, register the new securities underlying the ADRs under Securities Act Section 2 on Form F-1;
- Register the ADRs under Exchange Act Section 12 on Form 20-F (requiring financial disclosures and reconciliation with U.S. GAAP);
- File annual reports under Exchange Act Section 13(a) on Form 20-F; and
- File Exchange Act Section 13(a) interim reports on Form 6-K, as necessary, for information made public, filed with home market regulators, or provided to shareholders in-between regular reports.

An example of a Level II or Level III ADR program is that of Siemens AG. In 2008, U.S. enforcement authorities asserted FCPA jurisdiction over Siemens AG because Siemens’ ADRs traded on the New York Stock Exchange. Siemens received a fine from the U.S. DOJ of $450 million for criminal FCPA violations, and Siemens settled a related civil enforcement action with the U.S. SEC, without admitting or denying the SEC’s allegations, by agreeing to disgorge $350 million in wrongful profits.

III. ADRs and FCPA Jurisdiction

The FCPA contains two broad sets of prohibitions: the “anti-bribery provisions” and the “accounting provisions.” Although there are several grounds for U.S. FCPA jurisdiction over non-U.S. organizations, the jurisdictional basis relevant to this article is that both provisions apply to non-U.S. companies that, inter alia, qualify as “issuers” under the FCPA because they

---

42 Id.
43 See supra note 16.
44 Level III ADR issuers may use Form 8-A for the initial registration of the ADRs under Section 12, but must file annual reports on Form 20-F thereafter. See Rule 12d1-2 (codified at 17 C.F.R. § 240.12d1-2).
45 See 17 C.F.R. §§ 240.13a-16, 249.306.
either (1) must register securities with the SEC under Section 12 of the Securities Exchange Act of 1934, or (2) must file reports under Section 15(d) of the same act.\(^49\)

Exposure to the U.S. FCPA exposes foreign issuers to the risk of criminal and civil penalties that U.S. enforcement authorities can obtain for violations. Corporations can face criminal fines of up to $25 million for a violation of the FCPA’s accounting provisions and a maximum of $2 million for a violation of the FCPA’s anti-bribery provisions.\(^50\) Individuals can be imprisoned for not more than 20 years and fined up to $5 million for a violation of the accounting provisions, as well as face imprisonment for up to five years and fines of up to $250,000 (under the Alternative Fines Act) for a violation of the anti-bribery provisions.\(^51\) Civil penalties can run up to $500,000 for corporations and $100,000 for individuals, as well as disgorgement of any ill-gotten gains.\(^52\)

Because Level I ADRs do not trigger Exchange Act registration or reporting, foreign issuers whose securities underlie these ADRs do not expose themselves to FCPA jurisdiction. Conversely, because Level II and Level III ADRs trigger Section 12 registration, they subject the foreign issuer to U.S. enforcement authorities’ FCPA jurisdiction. The contrast between the outcome of the recent U.S. investigations of BAE Systems and Siemens AG, where only the former had a Level I ADR program, illustrates the potential magnitude of the increased legal and financial risks under Level II or Level III ADR programs.

Many financial institutions promote ADRs without reference to the ADRs’ potential to expose the foreign issuer to FCPA liability,\(^53\) even though the scope of liability, described above, can quickly outpace the benefits from such ADR programs. All foreign issuers who are considering implementing an ADR program or already have an ADR program ought to evaluate carefully whether such programs trigger FCPA jurisdiction and, if so, whether they can effectively manage FCPA risk through appropriate compliance programs to ensure that FCPA-related fines and penalties, or even compliance costs, do not offset the benefits of an ADR program.

\* * *

\(^{49}\) 15 U.S.C. § 78dd-1(a); see Pub. L. 73-291, § 12, 48 Stat. 892 (codified, as amended, at 15 U.S.C. § 78l); id. at § 15(d) (codified, as amended, at 15 U.S.C. § 78o(d)). In addition to a foreign issuer’s status as an “issuer,” the anti-bribery provisions require U.S. authorities to establish that a foreign issuer—or any officer, director, employee, or agent of the issuer—used U.S. mails or other means or instrumentalities of U.S. interstate commerce (including, for example, e-mail travelling across U.S. wires) in furtherance of the promise or payment prohibited by the FCPA. 15 U.S.C. § 78dd-1(a).

\(^{50}\) 15 U.S.C. §§ 78ff(a), 78ff(c)(1)(A).


Victims of murder, torture and other war crimes in foreign countries have few avenues for civil recovery because, in part, plaintiffs have difficulty determining which court has jurisdiction over individuals responsible for the alleged conduct. While the U.S. Foreign Sovereign Immunities Act (“FSIA”) clearly provides U.S. federal courts with jurisdiction over foreign sovereigns in certain situations, whether that statute also provides courts with jurisdiction over individual government officials has confounded courts. On March 3, 2010, the U.S. Supreme Court heard arguments in *Samantar v. Yousuf*, which involved the interplay of head-of-state immunity and the FSIA, focusing on whether the statute provides immunity to individual government officials or only provides immunity for foreign states, state agencies, and other state organizations, such as state-run corporations. The Supreme Court’s decision in the case will affect the ability of future plaintiffs to seek civil recovery in U.S. federal courts against individual government officials, including for alleged acts of torture, extrajudicial killing and other war crimes. This article discusses the development of head-of-state immunity law and the current split among U.S. federal courts of appeals at issue in *Samantar*.

**I. The Origin of Head-of-State Immunity Law in the United States**

In 1812, the U.S. Supreme Court provided the seminal discussion of head-of-state immunity in *Schooner Exchange v. McFaddon*. In *Schooner Exchange*, the French government had seized a merchant ship from American citizens while the ship was in Europe and converted it into a French naval vessel. Later, the American citizens spotted the ship in the Philadelphia harbor and brought suit in U.S. federal court, requesting that the ship be attached and returned to them. The Supreme Court held that individuals, acting under the direction of the French sovereign, were immune from U.S. jurisdiction. Chief Justice Marshall stated that a head of state and foreign ministers enjoyed immunity when travelling abroad because “[a] foreign sovereign is not understood as intending to subject himself to a jurisdiction incompatible with his dignity, and the dignity of his nation, and it is to avoid this subjection.”

---

54 Paul E. Sumilas is an associate at White & Case LLP in Washington, DC.
55 Although commonly referred to as “head-of-state immunity,” the common law immunity provided by the doctrine generally covered a number of high-ranking government officials, including the “head of state[,] . . . head of government[,] . . . foreign minister[,] . . . [or] any other public minister, official or agent of the state with respect to acts performed in his official capacity if the effect of exercising jurisdiction would be to enforce a rule of law against the state.” Restatement (Second) of Foreign Relations Law of the United States § 66 (1965).
56 11 U.S. (7 Cranch) 116 (1812).
57 *Id.* at 117-18.
58 *Id.*
59 *Id.* at 137.
II. The Restrictive Theory of Sovereign Immunity in the United States: From the Tate Letter to the FSIA

After Schooner Exchange, U.S. federal courts generally provided foreign sovereigns and heads of state, including other government officials, with absolute immunity. However, as the global economy grew, international law developed a restrictive sovereign immunity based on the recognition that sovereign states were acting as parties in commercial transactions with private parties. In 1952, Jack Tate, Acting Legal Advisor for the U.S. Secretary of State, issued guidelines outlining the application of this restrictive immunity in the United States (“Tate Letter”). The letter noted that other countries were beginning to recognize a “newer or restrictive theory of sovereign immunity [pursuant to which] the immunity of a sovereign is recognized with regard to sovereign or public acts (jure imperii) of a state, but not with respect to private acts (jure gestionis).”60 The Tate Letter justified the policy change by stating:

[T]he granting of sovereign immunity to foreign governments in the courts of the United States is most inconsistent with the action of the Government of the United States in subjecting itself to suit in these same courts in both contract and tort and with its long established policy of not claiming immunity in foreign jurisdictions for its merchant vessels. Finally, the Department feels that the widespread and increasing practice on the part of governments of engaging in commercial activities makes necessary a practice which will enable persons doing business with them to have their rights determined in the courts. For these reasons it will hereafter be the Department’s policy to follow the restrictive theory of sovereign immunity in the consideration of requests of foreign governments for a grant of sovereign immunity.61

After the issuance of the Tate Letter, individual government officials seeking the same immunity generally provided to foreign sovereigns would request a written “Suggestion of Immunity” from the U.S. State Department. Such a suggestion was considered binding on U.S. courts and left private parties with few options.

In 1976, Congress codified this restrictive theory of sovereign immunity in the FSIA. The FSIA states, among other things, that a foreign state, and an “agency or instrumentality” of the foreign state, is immune from jurisdiction in U.S. courts except under certain circumstances.62 An “agency or instrumentality” of the foreign state includes:

60 Letter from Jack B. Tate, Acting Legal Advisor, U.S. Dep’t of State, to Philip B. Perlman, Acting Att’y Gen., U.S. Dep’t of Justice (May 19, 1952).
61 Id.
Any entity (1) which is a separate legal person, corporate or otherwise, and (2) which is an organ of a foreign state or political subdivision thereof, or a majority of whose shares or other ownership interest is owned by a foreign state or political subdivision thereof, and (3) which is neither a citizen of a State of the United States as defined in section 1332(c) and (e) of this title, nor created under the laws of any third country.63

The FSIA clearly covers foreign states and sets forth specific and detailed exemptions when such immunity will not be granted. However, whether the immunity granted in the FSIA extends to individual government officials acting on behalf of a foreign state has been a more contentious issue.

III. Application of the FSIA to Individual Government Officials

The majority of U.S. federal courts to have considered the issue find that an individual government official falls within the ambit of the FSIA by treating such an official as an “agency or instrumentality of a foreign state” as long as that individual was “acting in his official capacity.”64 As the D.C. Circuit has explained, although the statute itself does not expressly “discuss the liability or role of natural persons, whether governmental officials or private citizens[,] . . . reason dictates that the sovereign immunity granted in the FSIA does extend to natural persons acting as agents of the sovereign, because FSIA immunity is based not on the identity of the person or entity so much as the nature of the act for which the person or entity is claiming immunity.”65 As a result, individual government officials sued for tortious conduct committed while acting in their official capacities as government officials generally have been able to avoid jurisdiction in U.S. federal courts by relying on the FSIA.66

64 El-Fadl v. Central Bank of Jordan, 75 F.3d 668, 671 (D.C. Cir. 1995); Globalindex v. Mkapa, 290 F. Supp. 2d 108, 110 (D.D.C. 2003) (“[I]t is well settled that individuals who act in their official capacities on behalf of a foreign sovereign are considered agencies or instrumentalities of a foreign state.”); see also In re Terrorist Attacks on Sept. 11, 2001, 538 F.3d 71, 85 (2d Cir. 2008); Keller v. Cent. Bank of Nigeria, 277 F.3d 811, 815-16 (6th Cir. 2002); Byrd v. Corporacion Forestal y Industrial de Olancho, 182 F.3d 380, 388-89 (5th Cir. 1999); Chuidan v. Philippine Nat’l Bank, 912 F.2d 1095, 1101 (9th Cir. 1990).
65 First Am. Corp. v. Al-Nahyan, 948 F. Supp. 1107, 1120 (D.C. Cir. 1996); see also Leutwyler v. Office of Her Majesty Queen Rania Al-Abdullah, 184 F. Supp. 2d 277, 286-87 (S.D.N.Y. 2001) (“Although [28 U.S.C.] § 1605(b) does not specifically refer to natural persons, it has been generally recognized that individuals employed by a foreign state’s agencies or instrumentalities are deemed ‘foreign states’ when they are sued for actions undertaken within the scope of their official capacities.”).
66 The Second, Fifth, Sixth, Ninth and D.C. Circuits have applied the FSIA to individuals and granted immunity to government officials for acts undertaken on behalf of the foreign state. See In re Terrorist Attacks on Sept. 11, 2001, 538 F.3d 71, 85 (2d Cir. 2008); Belhas v. Ya’Alon, 515 F.3d 1279, 1284 (D.C. Cir. 2008); Keller v. Cent. Bank of Nig., 277 F.3d 811, 815-16 (6th Cir. 2002); Byrd v. Corporacion Forestal y Industrial de Olancho, 182 F.3d 380, 388-89 (5th Cir. 1999); Chuidan v. Phil. Nat’l Bank, 912 F.2d 1095, 1101 (9th Cir. 1990).
IV. The Minority View and Samantar

Alternatively, the Fourth and Seventh Circuits have affirmatively rejected this reading of the FSIA. The Supreme Court granted certiorari in Samantar v. Yousef to review the application of the FSIA to individual government officials acting on behalf of foreign states.

In Samantar, a number of expatriate Somalis sued Mohamed Ali Samantar, a former official in the Somali dictatorship run by Mohamed Siad Barre that collapsed in 1991. The plaintiffs alleged that Samantar, who had served as the First Vice President, Minister of Defense, and Prime Minister in the Barre government, was directly responsible for torture, extrajudicial killings and other war crimes in Somalia during the Barre regime. After the Barre government collapsed, Samantar left Somalia and eventually moved to the United States.

The plaintiffs brought suit in the Eastern District of Virginia under the Alien Tort Statute (“ATS”) and the Torture Victim Protection Act (“TVPA”). The district court stayed proceedings to allow the State Department time to determine whether it would issue a Statement of Interest regarding Samantar’s assertion of sovereign immunity. After the U.S. government failed to intervene, the district court concluded that Samantar acted within his role as a government official and qualified as an “agency or instrumentality” under the FSIA. The district court upheld Samantar’s assertion of immunity. After noting that the majority of circuits that have faced the issue had concluded that the FSIA does grant sovereign immunity to individual officials, the Fourth Circuit reversed, concluding that the intent of the FSIA was to protect “a political body or corporate entity,” not an individual official, from suit.

---

67 See Yousef v. Samantar, 552 F.3d 371, 381 (4th Cir. 2009) (determining that the FSIA did not apply to a former Somali government official) cert. granted, 130 S. Ct. 49 (2009); Enahoro v. Abubakar, 408 F.3d 877, 881-82 (7th Cir. 2005) (asserting that the FSIA language and statutory history should be interpreted to exclude individual officials from its protection).
68 Also at issue in Samantar is whether the FSIA applies to current government officials or also to former officials. The defendant in the case was no longer a government official at the time suit was brought.
70 Id. at *2. At the time of the suit, Samantar was living in Fairfax, Virginia.
71 The ATS grants federal district courts jurisdiction “of any civil action by an alien for a tort only, committed in violation of the law of nations or a treaty of the United States.” 28 U.S.C. § 1350. The TVPA states that “[a]n individual who, under actual or apparent authority, or color of law, of any foreign nation . . . subjects an individual to torture [or] . . . subjects an individual to extrajudicial killing,” is liable in a civil action. Pub. L. No. 102-256, § 2(a), 106 Stat. 73 (1991).
73 Id. at *13-14.
74 Id. at *14-15.
75 Yousef v. Samantar, 552 F.3d 371, 375-76 (4th Cir. 2009).
76 Id. at 380-81.
Both sides of the case fundamentally agree that the FSIA fails to clearly state whether Congress intended the statute to shield individual government officials from U.S. jurisdiction. Samantar argued that the two main purposes of the FSIA, “to promote comity and ensure reciprocal treatment of U.S. interests abroad,” could only be served by providing government officials with the same sovereign immunity provided to foreign states. In addition, pre-FSIA common law concerning head-of-state immunity supported such an interpretation of the statute. Seeking to avoid application of the FSIA, the Somali expatriates focused on the text of the statute itself, which fails to mention “individuals,” and argued for judicial restraint when interpreting its plain language.

V. Conclusion

The Supreme Court’s decision in Samantar will likely provide a framework for how federal courts should approach civil actions against foreign officials. A decision to uphold the Fourth Circuit’s determination that the FSIA does not provide immunity for individual government officials could generate a number of new suits against such individuals. During the course of an active oral argument held on March 3, 2010, the justices noted the confusing and overlapping aspects of the FSIA, ATS and TVPA, and the apparent dissonance between providing immunity for a foreign state under the FSIA but not for the individual officials who actually committed the acts in their official capacity. The justices also seemed skeptical of the government’s position that the Executive Branch should have discretion in these cases, which appeared to reinstate the pre-FSIA reliance on Suggestions of Immunity from the State Department. The decision in Samantar, which is expected to be issued in the coming weeks, should provide clarity regarding the FSIA and the extent to which private citizens may be able to seek civil recovery from foreign government officials in U.S. federal courts for tortuous conduct.

* * *

The United Kingdom’s Bribery Act of 2010

Daniel Bork & Jacqueline Kort

On April 9, 2010, the United Kingdom passed into law the Bribery Act of 2010 (“Act”), the result of a decade long effort to consolidate and enhance the legal regime to combat corrupt transactions between private individuals, corporations, and foreign public officials, in both the

---

77 See Brief of Petitioner at 22, Samantar v. Yousuf, No. 08-1555 (U.S. Nov. 30, 2009) (“the statute does not expressly mention individuals . . .”); Brief for the Respondents at 14, Samantar v. Yousuf, No. 08-1555 (U.S. Jan. 20, 2009) (“None of these definitions [in FSIA] even arguably encompasses an individual ministerial officer.”).

78 Id. at 16-17.

79 Id. at 26-30.

80 Brief for the Respondents at 12-15, 53-58. The Supreme Court also asked the government to file a brief stating its position. In an amicus brief supporting affirmance, the government contended that decisions about whether individual officials should be immune from suit should be determined by the Executive Branch, not the FSIA. Brief for the United States as Amicus Curiae Supporting Affirmance at 6, Samantar v. Yousuf, No. 08-1555 (U.S. Jan. 27, 2010).

81 Daniel Bork and Jacqueline Kort are associates at White & Case LLP in Washington, D.C.
U.K. and elsewhere. The Act raises important compliance issues for both individuals and corporations alike. A number of recent high-profile prosecutions by the U.K. Serious Fraud Office (“SFO”) involving international bribery underscore the SFO’s stated intention to combat corruption aggressively, often in cooperation with other national authorities.

I. Background

Prior to the enactment of the Act, the U.K. was criticized for its piecemeal common law and statutory approach to combating corruption,82 which was seen as inadequate.83 As early as 1998, the U.K. Law Commission recommended reform of the existing laws; however, reform proposals failed to receive necessary support.84 In response to a 2008 OECD “Working Group on Bribery” review identifying fundamental weaknesses in the U.K. anti-bribery laws and the U.K.’s falling position in Transparency International’s Corruption Perception Index, the government redoubled its efforts to enact a comprehensive anti-bribery law. The draft bribery bill was first published on March 25, 2009. After a period of intense debate and review, the U.K. Bribery Bill received royal assent on April 9, 2010.

Although formally enacted, the effective date of the Act is not yet determined. The Secretary of State will set a date on which the Act will take effect.85 It is anticipated that the Act will be enforced in stages between June and October 2010. Importantly, the portion of the Act creating an offense for failure to prevent bribery will not take effect before the government provides additional guidance on the nature of adequate procedures to prevent corruption that, if extant in an organization, could serve as a defense to the new offense.86

II. Highlights of the Bribery Act

The Act creates four separate offenses: two “general” offenses, an offense addressing bribery of foreign officials, and a fourth offense focusing on commercial organizations’ failure to prevent bribery. Unlike the U.S. Foreign Corrupt Practices Act (“FCPA”), the Act also reaches commercial bribery and in this sense, is a broader anti-corruption tool than the FCPA. The Act has a broad jurisdictional reach that allows U.K. officials to prosecute illicit conduct well beyond the borders of the United Kingdom. The Act also authorizes stiff civil and criminal penalties for violations of the new bribery-related offenses.

A. General Bribery Offenses

The first general offense proscribes offering, promising, or giving a bribe to another person to induce improper performance of a “relevant function or activity.”87 The second

---

84 Id.
85 Bribery Act, 2010, c. 23, s. 19(1).
86 Id., c. 23, s. 9(1).
87 Id., c. 23, s. 1.
general offense prohibits requesting, agreeing to receive, and actually receiving a bribe.\footnote{Id., c. 23, s. 2.} For purposes of the two general offenses described in the Act, any “financial or other advantage” may constitute a bribe.\footnote{See id., c. 23, s. 1, 2.} For a violation to occur, the bribe must be linked to the “improper performance of a relevant function or activity.”\footnote{Id.} The Act broadly defines “relevant function or activity” so that a wide variety of conduct in the normal course of employment and business transactions may be covered by the Act if affected by a bribe.\footnote{See id., c. 23, s. 3.} The general offenses cover conduct committed in the U.K. and conduct outside of the U.K. by a person with “a close connection with the United Kingdom.”\footnote{Id.} These general offenses cover both commercial bribery and bribery of domestic U.K. public officials.

\section*{B. Bribery of a Foreign Official}

Bribery of a foreign public official is covered by a specific offense in the new Act. For purposes of the Act, “foreign official” broadly includes any type of “legislative, administrative or judicial position” as well as officials and agents of “public international organisations.”\footnote{Id., c. 23, s. 6(5)(c).} To commit an offense under this section, the bribe must be made with the intent to influence the official in his or her “capacity as a foreign public official” and with the intent to obtain or retain business or “an advantage in the conduct of business.”\footnote{Id., c. 23, s. 6(2).} Unlike the FCPA, but consistent with the OECD Convention, the U.K. Act does not contain an exception for so-called “facilitation payments” made to foreign public official to expedite the performance of non-discretionary functions.\footnote{See 15 U.S.C. § 78dd-1(b).} This offense also covers conduct carried out in the U.K. and conduct outside of the U.K. by any person with “a close connection with the United Kingdom.”\footnote{Id., c. 23, s. 12.} The Act lists nine categories of a “close connection” that permit jurisdiction, including British citizens, individuals ordinarily residing in the U.K., and “a body incorporated under the law of any part of the United Kingdom.”\footnote{Id., c. 23, s. 12(4).}

\section*{C. Failure of Commercial Organizations to Prevent Bribery}

The fourth offense created by the Act imposes strict liability on a commercial organization for illegal bribery by a person “associated” with the organization.\footnote{Id., c. 23, s. 7.} Liability under this provision may attach if the associated person “is, or would be, guilty” of paying or promising a bribe to a foreign official or another person.\footnote{Id., c. 23, s. 3.} The Act requires that an “associated person” perform “services for or on behalf of” a commercial organization, which may include
employees, agents, and subsidiaries. The underlying bribe by the “associated person” must have been offered, promised, or paid with the intention of “obtain[ing] or retain[ing] business” or a business related advantage for the commercial organization. Bribery by any “associated person” may form the basis for liability under this provision, regardless of the person’s connection to the U.K.

The Act establishes four categories of “relevant commercial organizations” that can be held liable under this provision. Among others, an organization incorporated under the law of the U.K., even if it conducts no business there, is covered. Organizations not incorporated in the U.K., but that carry “on a business, or part of a business, in any part of the U.K.” are also covered. The liability of a commercial organization may be established without any proof that the “associated person” (e.g., an employee, agent, or subsidiary) was directed to make the bribe payment by others at the organization and “irrespective of whether the acts or omissions . . . take place in the United Kingdom or elsewhere.”

“Adequate Procedures” Defense. The Act creates an affirmative defense for a commercial organization to this offense if the organization can prove that it “had in place adequate procedures designed to prevent persons associated with [the commercial organization]” from paying bribes. The organization will have to establish by a preponderance of the evidence that “adequate procedures” were in place at the time of the relevant conduct. Although the Act does not define “adequate procedures,” in July, 2009, the SFO issued preliminary guidance addressing the issue. Before the Act becomes effective, the government will issue additional guidance.

Because the Act covers commercial bribery and the FCPA does not, companies that already have FCPA compliance programs should review them to ensure that they cover commercial bribery and comport with whatever additional guidance emerges from U.K. authorities. Companies without anti-corruption compliance programs have even stronger incentive now to adopt them.

99 Id., c. 23, s. 8.
100 Id., c. 23, s. 7(1).
101 Id., c. 23, s. 7(3).
102 Id., c. 23, s. 7(5).
103 Id.
104 Id., c. 23, s. 12(5).
105 Id., c. 23, s. 7(2).
108 See Bribery Act, 2010, c. 23, s. 9.
D. Penalties

Under the penalty provision of the Act, an individual found guilty of a general bribery offense or bribing a foreign official faces up to ten years imprisonment per offense and unlimited fines. An organization found guilty of any of the offenses, including failure to prevent bribery by an associated person, is subject to unlimited fines.

III. Heightened Enforcement Efforts of SFO

Even prior to the passage of the Act, the SFO revamped itself, hired additional personnel, and announced its intention to enforce more aggressively and consistently the U.K. anti-corruption laws. Recent enforcement actions in several high-profile cases demonstrate the SFO’s renewed emphasis on anti-corruption enforcement, including cooperating with the U.S. Department of Justice (“DOJ”) and other national enforcement agencies.

A. New Enforcement Regime

In July 2009, the SFO set out guidance for corporations on approaching the SFO. The enforcement guidance highlights two main components to the SFO’s approach. First, patterned largely on DOJ practices, the SFO encourages corporations to self-report potential corrupt payments through a “carrot and stick” approach. The SFO guidelines explain that when a corporation self-reports and cooperates sufficiently, the SFO will generally pursue civil penalties rather than criminal penalties. Civil penalties are significantly more favorable, among other reasons, because they do not result in mandatory debarment for public contracts under Article 45 of the EU Public Sector Procurement Directive of 2004. Alternatively, if a party identifies an issue and fails to self-report, the SFO will be more likely to pursue criminal prosecution and related remedies.

---

109 Id., c. 23, s. 11(1).
110 Id., c. 23, s. 11(2), (3).
113 Id. at 2.
114 Id. at 8.
Second, the SFO has developed an opinion release procedure, which closely parallels the U.S. practice. Under this approach, a corporation facing a potential future violation can approach the SFO with the specific fact-pattern for guidance on whether enforcement action would be taken against the corporation. The SFO has indicated that this procedure is particularly relevant for issues arising in the merger and acquisition context. The contours of the procedure will undoubtedly develop through use.

B. Recent High-Profile Enforcement Actions

BAE Systems

On February 5, 2010, BAE Systems plc (“BAE Systems”) announced plans of a £30 million settlement with the SFO. BAE Systems stated in its News Release that “the Company will plead guilty to one charge of breach of duty to keep accounting records in relation to payments made to a former marketing adviser in Tanzania.” In a February speech, SFO Director Alderman stated that there are three lessons from the outcome of the BAE Systems case. First, the settlement was the result of the joint efforts of the DOJ and the SFO. Second, Alderman stressed that global settlements can be achieved despite differences in the U.K. and U.S. legal systems. Third, “SFO will continue to pursue cases when we think it right to do so but that we are always open to appropriate solutions.” BAE also settled related charges with the DOJ.

Innospec

In February, the SFO charged Innospec Limited, the U.K. subsidiary of Innospec, Inc., a Delaware-based chemical manufacturer, with bribing employees of a state-owned refinery in Indonesia and other Indonesian officials. In addition, both the DOJ and SEC also filed charges against the U.S. parent company. On March 18, 2010, Innospec Limited pleaded guilty to “conspiracy to corrupt contrary to s. 1 of the Criminal Law Act 1977,” and was fined US$ 12.7 million. The U.K. authorities were first alerted to potential corruption in 2005 by the

115 Id. at 6-7.
117 Id.
118 Id.
119 Id.
120 Id.
124 Id. ¶ 47.
DOJ and Office of Foreign Asset Control (“OFAC”) at the U.S. Treasury Department, which were investigating Innospec’s involvement in the U.N. Oil for Food Program. The SFO began formal investigation of the company in May 2008. The DOJ and SFO worked in tandem to investigate the misconduct and negotiate a settlement with Innospec. This case exemplifies how national enforcement agencies can cooperate in reaching a negotiated global resolution for misconduct that violates the laws and regulations of more than one state.

Alstom

On March 24, 2010, three U.K.-based executives of Alstom, a French engineering company which develops transportation and energy infrastructure world-wide, were arrested in an ongoing SFO investigation. The company’s U.K. president, finance director, and legal director were arrested on suspicions of “bribery and corruption, conspiracy to pay bribes, money laundering and false accounting.” All three men were released without charges. It is suspected that Alstom’s subsidiaries in the U.K. bribed foreign officials to win overseas contracts. In another example of international cooperation, the SFO worked closely with Switzerland’s Office of the Attorney General and federal police during its investigation.

The SFO’s recent stepped up anticorruption enforcement activity is likely to continue and expand under the new Bribery Act, which enhances the U.K.’s anticorruption regime.

ABA INTERNATIONAL LAW SECTION CONFERENCES

From November 2-6, 2010, the ABA International Law Section will hold their Fall Meeting at the Westin Paris in Paris, France. Participants can register on-line, through the ABA International Law Section website at http://www.abanet.org/intlaw/home.html.

* * *

MONTHLY COMMITTEE CALLS

The International Criminal Law Committee will continue holding monthly telephone conference calls with committee members on the last Tuesday of each month (unless otherwise noted). Calls will occur at 6:00 PM EST. The remaining schedule for 2010 is as follows: May 25, June 29, July 27, August 31, September 28, October 26, and November 30.

* * *

125 id. ¶ 5.
128 id.
ABA INTERNATIONAL CRIMINAL LAW COMMITTEE
CALENDAR OF EVENTS

Israel Bar Association Annual Conference
Date: May 30, 2010 – June 2, 2010
Location: Isrotel Royal Beach Hotel, Eliat, Israel
Format: Live/In-Person

Live from Kampala: A Report from the International Criminal Court Review Conference
Date: June 3 & 11, 2010
Format: Live/Teleconference

5th Annual Fordham Law School Conference on International Arbitration and Mediation
Date: June 14-15, 2010
Location: Fordham Law School, New York, New York
Format: Live/In-Person

Inter-American Bar Association XLV1th Conference
Date: June 15-19, 2010
Location: Rio de Janeiro, Brazil
Format: Live/In-Person

Joint ABA International/German Bar Association International Section Conference:
“Transatlantic Deals & Disputes: How to Avoid Shipwrecks in U.S.-German Business”
Date: June 20-21, 2010
Location: Frankfurft, Germany
Format: Live/In-Person

2010 Section Leadership Retreat
Date: August 4-5, 2010
Location: Claremont Hotel Club & Spa, Berkeley, California
Format: Live/In-Person

2010 ABA Annual Meeting
Date: August 6-9, 2010
Location: JW Marriott Union Square, San Francisco, California
Format: Live/In-Person

48th Annual AIJA Congress
Date: August 24-28, 2010
Location: Charleston Place Hotel, Charleston, South Carolina
Format: Live/In-Person
Korean Bar Association Annual Grand Meeting  
Date: August 30, 2010  
Location: Grand Intercontinental Seoul, Seoul, Korea  
Format: Live/In-Person

ABA International Commercial Dispute Resolution Conference  
Date: September 2010  
Location: Moscow, Russia  
Format: Live/In-Person

11th Annual Live from the SEC  
Date: October 14, 2010  
Location: Washington, DC  
Format: Live/In-Person

2010 Fall Meeting  
Date: November 2-6, 2010  
Location: The Westin Paris, Paris, France  
Format: Live/In-Person

To view current and future Criminal Law Committee events, please see our website at http://www.abanet.org/intlaw/calendar/home.html.