DEBEVOISE & PLIMPTON LLP

FCPA Update

April 2012 ■ Vol. 3, No. 9

Les Difficultés in Conducting FCPA Third Party Due Diligence in France

Companies that operate both in the United States and in European Union Member States, such as France, often must grapple with tensions between FCPA compliance and enforcement of European Union and local country data privacy protections. Because of the particularly stringent data privacy laws in France and the active enforcement of these laws, this article focuses on the challenges faced by companies that operate in both the United States and France in conducting FCPA due diligence on business partners in France. As compliance officers are probably well aware, conducting adequate background diligence on potential third parties in France while respecting France's strict data privacy laws can be a difficult path to navigate.

In recent years, the Department of Justice ("DOJ") and Securities and Exchange Commission ("SEC") increasingly have enforced the FCPA's prohibition on corrupt third party payments.[1] Assistant Attorney General Lanny A. Breuer has made clear that "[t]he use of intermediaries to pay bribes will not escape prosecution under the FCPA."[2]

To mitigate FCPA liability for corrupt payments by third parties, companies are expected to conduct due diligence prior to entering into relationships with business partners. As discussed below, adequate third party due diligence necessarily involves collecting and documenting personal information concerning potential third parties.

At the same time, in recent years the French data protection authority, *la Commission nationale de l'informatique et des libertés* ("CNIL"), has increased its oversight and enforcement of French laws that protect individuals' right to data privacy. In 2010, the last year for which data is available, the CNIL conducted 308 inspections of companies to ensure compliance with data privacy laws, a 14% increase over the previous year.[3] The CNIL planned to conduct 400 inspections in 2011, with particular emphasis on ensuring

CONTINUED ON PAGE 2

1. *See, e.g.*, DOJ Press Rel. 11-629, Tenaris S.A. Agrees to Pay $3.5 Million Criminal Penalty to Resolve Violations of the Foreign Corrupt Practices Act (May 17, 2011), http://www.justice.gov/opa/pr/2011/May/11-crm-629.html; SEC Press Rel. 2011-112, Tenaris to Pay $5.4 Million in SEC's First-Ever Deferred Prosecution Agreement (May 17, 2011), http://www.sec.gov/news/press/2011/2011-112.htm.
2. DOJ Press Rel. 09-1220, Former Willbros International Consultant Pleads Guilty to $6 Million Foreign Bribery Scheme (Nov. 12, 2009), http://www.justice.gov/opa/pr/2009/November/09-crm-1220.html.
3. Commission nationale de l'informatique et des libertés, "31e Rapport d'Activité 2010," at 13, 20 (Nov. 16, 2011), http://www.cnil.fr/fileadmin/documents/La_CNIL/publications/CNIL_rapport_annuel_%202010.pdf (official English translation unavailable).

Click here for previous issues of FCPA Update

Also in this issue:

If there are additional individuals within your organization who would like to receive FCPA Update, please reply to ssmichaels@debevoise.com or pferenz@debevoise.com.

Third Party Due Diligence ■ Continued from page 1

that French and U.S. companies that engage in international data transfers respect the privacy rights of French citizens.[4]

Companies that operate in the United States and France, therefore, are faced with two seemingly incompatible requirements: third party FCPA due diligence, on the one hand, and protecting a third party's right to data privacy, on the other hand. In addressing these issues, this article will (1) provide an overview of the FCPA and French anti-bribery legislation concerning third party payments; (2) review relevant European Union and French data privacy laws; and (3) outline factors that companies may wish to consider in implementing programs to address both third party due diligence and data privacy requirements.

FCPA Third Party Due Diligence Requirements

The FCPA prohibits companies and individuals subject to the FCPA from making payments to third parties while "knowing" that all or a portion of such payments will be passed on to foreign officials in order to obtain or retain business, or secure an improper advantage.[5] The DOJ and SEC have taken the position that the term "knowing" includes conscious disregard or willful blindness of "red flags" that would alert a reasonable person to the risk that a third party may make corrupt payments to foreign officials.[6] The FCPA itself contains an express definition of "knowing" that reflects a congressional determination that willful blindness or conscious avoidance constitutes knowledge.[7]

The DOJ and SEC have made clear that, either as part of an issuer's obligations under the 1934 Securities Exchange Act's mandate to implement internal controls reasonably designed to prevent FCPA anti-bribery violations, or simply as a matter of good compliance (a key factor in how the government evaluates any violations that may arise), companies subject to the FCPA are expected to conduct third party due diligence prior to entering into business relationships in order to reduce the risk of corrupt payments by third parties.[8] The DOJ suggests that such due diligence includes, among other things, verifying whether a potential third party is qualified for the relevant position, determining whether the third party has personal or professional ties to foreign governments or

CONTINUED ON PAGE 3

4. Commission nationale de l'informatique et des libertés, "Programme des contrôles 2011: une ambition reáffirmée, des compétences élargies" (Apr. 26, 2011), http://www.cnil.fr/la-cnil/actu-cnil/article/article/programme-des-controles-2011-une-ambition-reaffirmee-des-competences-elargies/?tx_ttnews%5BbackPid%5D=2&cHash=91ae300acd (official English translation unavailable).
5. 15 U.S.C. §§ 78dd-1(a)(3), 78dd-2(a)(3), 78dd-3(a)(3).
6. *See, e.g.*, Dep't of Justice & Dep't of Commerce, "Lay Person's Guide" to the Foreign Corrupt Practices Act, at 4, http://www.justice.gov/criminal/fraud/fcpa/docs/lay-persons-guide.pdf (hereinafter "Lay Person's FCPA Guide").
7. *See* 15 U.S.C. §§ 78dd-1(f)(2), 78dd-2(h)(3), 78dd-3(f)(3).
8. *See, e.g.*, Lay Person's FCPA Guide, note 6, *supra*.
9. *Id.* Note that, although outside the specific scope of this article, acquiring companies are expected to evaluate a target company's practices with respect to third party due diligence in order to enhance the target's FCPA due diligence program, as necessary, and to mitigate the risk of corrupt third party payments for which the acquiring company may be held liable. Similar issues arise in connection with the formation of joint ventures.

FCPA Update

FCPA Update is a publication of Debevoise & Plimpton LLP

919 Third Avenue
New York, New York 10022
+1 212 909 6000
www.debevoise.com

Washington, D.C.
+1 202 383 8000

Moscow
+7 495 956 3858

London
+44 20 7786 9000

Hong Kong
+852 2160 9800

Paris
+33 1 40 73 12 12

Shanghai
+86 21 5047 1800

Frankfurt
+49 69 2097 5000

Paul R. Berger
Co-Editor-in-Chief
+1 202 383 8090
prberger@debevoise.com

Bruce E. Yannett
Co-Editor-in-Chief
+1 212 909 6495
beyannett@debevoise.com

Sean Hecker
Associate Editor
+1 212 909 6052
shecker@debevoise.com

Steven S. Michaels
Managing Editor
+1 212 909 7265
ssmichaels@debevoise.com

David M. Fuhr
Deputy Managing Editor
+1 202 383 8153
dmfuhr@debevoise.com

Erin W. Sheehy
Deputy Managing Editor
+1 202 383 8035
ewsheehy@debevoise.com

Noelle Duarte Grohmann
Assistant Editor
+1 212 909 6551
ndgrohmann@debevoise.com

Amanda M. Bartlett
Assistant Editor
+1 212 909 6950
ambartlett@debevoise.com

Elizabeth A. Kostrzewa
Assistant Editor
+1 212 909 6853
eakostrzewa@debevoise.com

Please address inquiries regarding topics covered in this publication to the editors.

Please note: The URLs in *FCPA Update* are provided with hyperlinks so as to enable readers to gain easy access to cited materials.

Third Party Due Diligence ■ Continued from page 2

government officials, and assessing the third party's reputation with the U.S. Embassy or Consulate and with business associates.[9]

The DOJ also recommends that companies be aware of "red flags" raised during the due diligence process or while negotiating business relationships with third parties.[10] Such "red flags" may include the history and risk of corruption in the relevant foreign country, unusual payment patterns or financial arrangements, unusually high commissions, and a lack of transparency in expenses and accounting records.[11] Best practice suggests that companies follow up on any "red flags" with further investigation and proceed with the business relationship only if red flags can be resolved to an appropriate level of comfort.

Best practice further suggests that companies document and retain the results of any third party due diligence for a sufficient period to enable companies to respond to DOJ and SEC inquiries and to defend themselves as needed. Given the statute of limitations for FCPA violations, many companies utilize a retention period of between five and ten years.[12] The DOJ has further indicated that it would view favorably a U.S. company's retaining due diligence documentation in the United States.[13]

In practice, implementing FCPA due diligence standards often requires that companies obtain, document, and retain information that may be considered "personal data" under European Union and French data privacy law[14] concerning potential third parties who are natural persons; the directors, principals and other employees of a third party that is a legal entity; and foreign officials who are closely related to these natural persons. Best practice suggests that this personal information include any government or political party affiliations, prior criminal conduct, and financial information. Companies often employ a number of investigative tools to obtain this information, including detailed FCPA due diligence questionnaires to be completed by potential third parties and private investigation firms to conduct additional on-the-ground due diligence.

> "In practice, implementing FCPA due diligence standards often requires that companies obtain, document, and retain information that may be considered 'personal data' under European Union and French data privacy law."

French Anti-Bribery Legislation

In addition to the FCPA, companies that operate both in the United States and France are subject to French anti-bribery legislation. Similar to the FCPA, French anti-bribery legislation prohibits corrupt payments to public officials, directly or indirectly through third parties, as well as the solicitation and acceptance of corrupt payments by public officials, directly or indirectly through third parties.[15]

CONTINUED ON PAGE 4

10. *Id.*

11. *Id.*

12. Federal law imposes a five-year limitations period on DOJ actions and SEC enforcement actions seeking civil penalties. *See* 18 U.S.C. § 3282 (DOJ); 28 U.S.C. § 2462 (SEC). The statute of limitations may be extended beyond five years for DOJ actions involving foreign evidence, 18 U.S.C. § 3292; and for DOJ and SEC actions alleging scheme liability under the "continuing violation doctrine," *see, e.g.*, *Nat'l R.R. Passenger Corp. v. Morgan*, 536 U.S. 101, 114–15 (2002). SEC enforcement actions seeking equitable remedies are not subject to a limitations period and are time-limited only by the equitable doctrine of laches. *See Johnson v. SEC*, 87 F.3d 484, 491 (D.C. Cir. 1996) (section 2462's limitations period does not apply where "the effect of the SEC's action is to restore the *status quo ante*, such as through a proceeding for restitution or disgorgement of ill-gotten profits"); *SEC v. Kelly*, 663 F. Supp. 2d 276, 287 (S.D.N.Y. 2009) (section 2462's limitations period does not apply to SEC actions seeking "permanent injunctive relief, disgorgement, or an officer and director bar").

13. *See* DOJ Opinion Procedure Rel. 08-01, at 12 (Jan. 15, 2008), http://www.justice.gov/criminal/fraud/fcpa/opinion/2008/0801.pdf (citing as a factor in its determination not to take enforcement action that "the Requestor conducted and documented reasonable due diligence . . . with attention to both FCPA risks and compliance with local laws and regulations, and will maintain such documentation in the United States"). Note that the transfer of due diligence documentation collected in France to the United States, as well as the retention of such documentation in the United States, raise a number of issues under European Union and French data privacy laws that are outside the scope of this article. *See, e.g.*, French Law No. 78-17 on Information Technology, Data Files and Civil Liberties, Jan. 6, 1978, arts. 68–70, http://www.cnil.fr/fileadmin/documents/en/Act78-17VA.pdf (hereinafter "French Data Protection Act") (the CNIL generally must authorize transfers of personal data from France to the United States, subject to limited exceptions); French Law No. 68-678, July 26, 1968, *amended by* Law No. 80-538, July 16, 1980, arts. 1, 1-*bis*, http://legifrance.gouv.fr/jopdf/common/jo_pdf.jsp?numJO=0&dateJO=19800717&numTexte=&pageDebut=01799&pageFin= (official English translation unavailable) (commonly known as the "French Blocking Statute," prohibiting French individuals and entities from communicating certain categories of information to foreign public officials that would be harmful to France's interests, and further prohibiting requesting, investigating or communicating such information for use in foreign judicial or administrative proceedings).

14. For a definition of "personal data" under European Union and French data privacy law, *see infra* Part III.A. and note 21.

15. *See* French Penal Code, arts. 435-1, 435-2, 435-3, 435-4. Violations committed by natural persons are punishable by ten years' imprisonment and a fine of €150,000. *Id.* arts. 435-1, 435-2, 435-3, 435-4. Violations committed by legal persons are punishable by a fine of five times the applicable fine for natural persons, or €750,000. *Id.* arts. 131-38, 435-6.

Third Party Due Diligence ■ Continued from page 3

In enacting this anti-bribery legislation, France incorporated the terms of several international anti-bribery initiatives, including the Organization for Economic Cooperation and Development's Convention on Combating Bribery of Foreign Public Officials in International Business Transactions ("OECD Anti-Bribery Convention").[16] Of particular significance to companies operating in France, the OECD recommends that, in complying with its Anti-Bribery Convention (which was incorporated into French law), companies should implement ethics and compliance programs that would be applicable to third parties and that would include conducting "properly documented risk-based due diligence" with respect to the hiring and regular oversight of third parties.[17]

European Union and French Data Privacy Protections

Despite the similarities between U.S. and French anti-bribery legislation's prohibition of corrupt third party payments, as well as the OECD's recommendations concerning third party due diligence, companies that operate both in the United States and France are faced with tensions between the expectations regarding FCPA third party due diligence and legislation enacted and enforced in the European Union and France to protect a natural person's right to privacy in his or her personal data.

A. European Union Data Privacy Protections

An individual's right to protection of personal data is considered to be a fundamental right in the European Union.[18] The centerpiece of European Union legislation on personal data protection is Directive 95/46/EC of the European Parliament and Council ("E.U. Data Privacy Directive" or the "Directive").[19] The Directive was enacted to protect individuals' fundamental right to privacy with respect to the processing of personal data, and to guarantee the free flow of personal data among E.U. Member States.[20] The "processing" of "personal data" includes the collection, recording, organization, storage, use, disclosure by transmission, or dissemination of any information that could be used to directly or indirectly identify an individual or the individual's habits or tastes.[21] The Directive applies to the processing of personal data by any person whose activities are governed by European Community law, including situations in which a person in a third country uses processing means located in the European Union.[22]

As such, the Directive sets forth principles and standards that Member States must implement in regulating the processing of personal data within their jurisdiction. These principles include fairness, proportionality, consent, and transparency.[23] The Directive also establishes "special categories" of particularly sensitive data, which must not be processed except under specified circumstances.[24]

CONTINUED ON PAGE 5

16. *See id.* arts. 435-3, 435-4. The OECD Anti-Bribery Convention required parties to implement measures to criminalize the intentional giving or offering of any undue pecuniary gain to a foreign public official, whether directly or through intermediaries, to obtain or retain business or other improper advantage in the conduct of international business. OECD Anti-Bribery Convention, art. 1, Dec. 17, 1997, http://www.oecd.org/dataoecd/4/18/38028044.pdf.

17. *See* Organization for Economic Cooperation and Development, "Good Practice Guidance on Internal Controls, Ethics, and Compliance," Annex II to the Recommendation of the Council for Further Combating Bribery of Foreign Public Officials in International Business Transactions, § A(6)(i) (Nov. 26, 2009), http://www.oecd.org/dataoecd/5/51/44884389.pdf.

18. *See, e.g.*, Charter of Fundamental Rights of the European Union, Oct. 2, 2000, *amended by* Treaty of Lisbon, Dec. 13, 2007, art. 8(1), http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2010:083:0389:0403:EN:PDF ("Everyone has the right to the protection of personal data concerning him or her.").

19. Directive 95/46/EC of the European Parliament and of the Council of the European Union, Oct. 24, 1995, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:1995:281:0031:0050:EN:PDF. In January 2012, the European Commission released a proposed regulation that would repeal the E.U. Data Privacy Directive and would update the Directive's data protection principles. *See* Proposal for a Regulation of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, Jan. 25, 2012, http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf (hereinafter "E.C. Data Privacy Proposal").

20. E.U. Data Privacy Directive, note 19, *supra*, art. 1.

21. *Id.* art. 2(a), (b). "Personal data" may include reference to an identification number or factors specific to an individual's physical, psychological, mental, economic, cultural, or social identity, including the individual's name, photograph, email address, and bank details. *See id.* art. 2(a); Commission nationale de l'informatique et des libertés, "Personal Data," http://www.cnil.fr/english/the-cnil/personal-data/.

22. E.U. Data Privacy Directive, note 19, *supra*, ¶¶ 12, 20.

23. *Id.* arts. 3, 6, 7(a), 8(2)(a), 10, 11, 12, 14.

24. *Id.* art. 8.

Third Party Due Diligence ■ Continued from page 4

B. French Data Privacy Protections

1. The French Data Protection Act

French Law No. 78-17 on Information Technology, Data Files and Civil Liberties (the "French Data Protection Act") incorporates, and enhances, many of the E.U. Data Privacy Directive's protective principles.[25] The French Data Protection Act applies to the processing of personal data if the data controller carries out its activity on French territory; or if the data controller, although not established on French territory or in another E.U. Member State, uses processing means located in French territory.[28]

> "The French Data Protection Act also specifies that the processing of 'special categories' of personal data, including data revealing racial or ethnic origin and political opinions, is prohibited except under specified circumstances."

The French Data Protection Act sets forth the conditions under which personal data must be processed in France. In particular, processing may be performed only if the personal data, among other factors, is: (1) "obtained and processed fairly and lawfully;" (2) obtained for "specified, explicit and legitimate purposes;" (3) limited in scope to personal data that is "adequate, relevant and not excessive" in relation to the purposes for which the data is obtained; and (4) "stored in a form that allows the identification of the data subjects for a period no longer than is necessary for the purposes for which [the data] are obtained and processed."[27]

The French Data Protection Act also specifies that the processing of "special categories" of personal data, including data revealing racial or ethnic origin and political opinions, is prohibited except under specified circumstances.[28] In addition, the processing of personal data relating to offenses and convictions may be conducted only by certain entities, including courts, public authorities and legal entities that manage public services.[29]

The French Data Protection Act further specifies that data subjects must be informed of certain details concerning the personal data to be processed and generally must "consent" to the processing of personal data.[30] The term "consent" is not defined in the French Data Protection Act; however, the E.U. Data Privacy Directive specifies that "the data subject's consent" means "any freely given specific and informed indication of his wishes by which the data subject signifies his agreement" to the processing of personal data.[31] Building upon the Directive's definition, E.U. Member States and advisory bodies have promulgated additional requirements and guidance concerning the elements of valid consent.[32] Given the complexity of this framework, counsel knowledgeable in European Union and French data privacy laws should be consulted prior to obtaining consent with respect to data processing.

2. The CNIL

The French Data Protection Act created a French data protection authority, the CNIL, to inform data subjects and controllers of their rights and duties, and to enforce French data privacy laws.[33] The CNIL, therefore, must be notified

CONTINUED ON PAGE 6

25. *See generally* French Data Protection Act, note 13, *supra*.
26. *Id.* art. 5.
27. *Id.* art. 6.
28. *Id.* art. 8.
29. *Id.* art. 9.
30. *Id.* arts. 7, 32. For example, in March 2011, the CNIL imposed a fine of €100,000 on Google Inc. for having engaged in the "unfair collection" of personal data. The CNIL concluded that, in connection with Google's Street View program in France, Google had collected data transmitted by individuals' Wi-Fi networks without their knowledge and had recorded personal data, including passwords, login details, and email exchanges that revealed sensitive information. *See* Commission nationale de l'informatique et des libertés, "Google Street View: CNIL pronounces a fine of 100,000 Euros" (Mar. 21, 2011), http://www.cnil.fr/english/news-and-events/news/article/google-street-view-cnil-pronounces-a-fine-of-100000-euros/#.
31. *See* E.U. Data Privacy Directive, note 19, *supra*, art. 2(h).
32. *See, e.g.*, Article 29 Data Protection Working Party, "Opinion 15/2011 on the Definition of Consent," at 11–21 (July 13, 2011), http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2011/wp187_en.pdf (clarifying that, under the E.U. Data Privacy Directive, consent should be, among other requirements, based upon an affirmative act and should "refer clearly and precisely to the scope and the consequences of the data processing").
33. French Data Protection Act, note 13, *supra*, art. 11.

Third Party Due Diligence ■ Continued from page 5

of any automatic processing of personal data.[34] The CNIL also must authorize any processing, whether automatic or not, of "special categories" of personal data, as well as data relating to offenses or convictions.[35]

3. Sanctions for Data Privacy Violations

The French Data Protection Act empowers the CNIL to impose fines in cases of non-compliance with French data privacy laws and provides for criminal penalties as set forth in the French Penal Code.[36]

The CNIL may impose fines if a data controller fails to comply with a warning and formal notice from the CNIL.[37] In such cases, the CNIL may impose a fine of up to €150,000 for a first violation.[38] For a second violation within five years from the date of the first penalty, the CNIL may impose a fine of up to €300,000 on natural persons, or a fine of 5% of gross revenue for the latest financial year, up to €300,000, on legal persons.[39]

The French Data Protection Act further provides for criminal penalties, as set forth in France's Penal Code.[40] In particular, France's Penal Code prohibits the following acts: (1) processing of personal data, including through negligence, without respecting the formalities required by statute;[41] (2) collecting personal data by fraudulent, unfair or unlawful means;[42] (3) recording or preserving in a "computerized memory" "special categories" of personal data or name-bearing information relating to offenses and convictions without the express agreement of the persons concerned;[43] and (4) retaining personal data beyond the length of time specified by statute, in the request for authorization or notice sent to the CNIL, or in the preliminary declaration sent to the CNIL.[44]

Each of the above violations by natural persons is punishable by five years' imprisonment and a fine of €300,000.[45] Violations committed by legal persons are punishable by a fine of five times the applicable fine for natural persons, or €1,500,000.[46]

Reconciling the Tension between Third Party Due Diligence and Data Privacy

Companies that must comply with the FCPA and other international anti-bribery legislation by conducting due diligence on third parties in France are therefore faced with competing obligations under European Union and French data privacy laws intended to protect the data privacy rights of individuals associated with these third parties.[47]

Common FCPA due diligence practices, such as employing private investigation firms to conduct discrete due diligence on individuals, often without their knowledge or consent, may violate data privacy laws.[48] In addition, information essential to FCPA due diligence, such as political affiliations and criminal convictions, may qualify as "special categories" of personal data that may not be collected by private companies operating in France under most circumstances.[49] Furthermore, the scope of information gathered, and

CONTINUED ON PAGE 7

34. *Id.* arts. 11, 22.
35. *Id.* art. 25.
36. *Id.* arts. 17, 45, 50.
37. *Id.* art. 45.
38. *Id.* art. 47.
39. *Id.*
40. *Id.* art. 50.
41. French Penal Code, art. 226-16.
42. *Id.* art. 226-18.
43. *Id.* arts. 226-19, 226-23.
44. *Id.* art. 226-20.
45. *Id.* arts. 226-16, 226-18, 226-19, 226-20.
46. *Id.* arts. 131-38, 226-24.
47. Although European Union and French data privacy laws do not protect the rights of legal entities, adequate due diligence on third party entities for U.S. law purposes would include investigation into key individuals associated with those entities.
48. *See* French Data Protection Act, note 13, *supra*, arts. 7, 11, 22, 32.
49. *See id.* arts. 8, 9, 25.

Third Party Due Diligence ■ Continued from page 6

the documentation and storage of such information by companies for up to 10 years, may be deemed excessive under data privacy laws.[50]

As in-house counsel and compliance officers at many multinational firms know, these tensions are not easily resolved. Striking the right balance between FCPA compliance obligations and French legal requirements must be achieved on a company-by-company basis, ideally with the assistance of counsel knowledgeable about both the FCPA and French and European Union data protection regimes. Considerations that should be taken into account include notice provided to third parties, the types of sources used in performing third party diligence, how questions are crafted in questionnaires completed by third parties, how information is recorded in diligence documentation, how information is transferred outside of France, and the length and method of storage of due diligence documentation. Some companies may decide to seek authorization from the CNIL for their specific third party compliance practices.

Companies may find that implementing FCPA third party due diligence programs that comply in good faith with conflicting data privacy obligations necessitates compromise approaches that may prevent these programs from complying with best practice standards. Companies that have adopted such compromise approaches to third party due diligence programs have typically incorporated data protection measures, including: (1) limiting due diligence searches on individuals to public sources; (2) omitting individual names and identifying information when reporting negative information discovered during diligence on legal entities using proprietary sources and private investigation firms; (3) carefully wording sensitive questions on FCPA due diligence questionnaires; and (4) limiting access to due diligence results to small, relevant groups. Although FCPA third party due diligence programs that incorporate data protection measures such as these generally would be viewed as appropriate, these "compromise" programs may not meet best practice standards with which leading firms aspire to comply in other parts of the world. Adding to the tension in this arena, it remains unclear whether the CNIL would authorize or at least refuse to prosecute the implementation of such "compromise" due diligence programs in France.

> "Striking the right balance between FCPA compliance obligations and French legal requirements must be achieved on a company-by-company basis, ideally with the assistance of counsel knowledgeable about both the FCPA and French and European Union data protection regimes."

Given the challenges faced by multinational companies in complying with these competing obligations, it is clear that cross-border cooperation between U.S. and French authorities to resolve these tensions would be highly beneficial.[51] Several international bodies, including the OECD and the European Commission, have recommended that Member countries develop effective international mechanisms to facilitate cooperation with foreign authorities in the enforcement of data privacy laws.[52] Thus far, these recommendations have focused on ensuring cross-border enforcement of such laws.

However, effective cross-border enforcement necessarily involves cooperating with foreign authorities to resolve conflicts with foreign laws and policies that would hinder the enforcement of data privacy laws. Cooperation between, and guidance from, U.S. and French authorities, therefore, would enable companies to better comply with both

CONTINUED ON PAGE 8

50. *See id.* art. 6.

51. Cooperation between U.S. and foreign authorities in light of such tensions is not unheard of. In 2006, U.S. and E.U. authorities engaged in discussions concerning tensions between the whistleblower provisions of the Sarbanes-Oxley Act of 2002 and the E.U. Data Privacy Directive. Companies subject to both requirements, therefore, may turn to these discussions for guidance in resolving these tensions. *See* Letter from Peter Schaar, Chairman, Article 29 Data Protection Working Party, to Christopher Cox, Chairman, SEC (Feb. 16, 2006); Letter from Ethiopis Tafara, Director, Office of Int'l Affairs, SEC, to Peter Schaar, Chairman, Article 29 Data Protection Working Party (June 8, 2006); Letter from Peter Schaar, Chairman, Article 29 Data Protection Working Party, to Ethiopis Tafara, Director, Office of Int'l Affairs, SEC (July 3, 2006); Letter from Ethiopis Tafara, Director, Office of Int'l Affairs, SEC, to Peter Schaar, Chairman, Article 29 Data Protection Working Party (Sept. 29, 2006) (letters on file with authors).

52. *See, e.g.*, Organization for Economic Cooperation and Development, "Recommendation on Cross-border Co-operation in the Enforcement of Laws Protecting Privacy" (June 12, 2007), http://www.oecd.org/dataoecd/43/28/38770483.pdf; E.C. Data Privacy Proposal, note 19, *supra*, art. 45 (incorporating the OECD's recommendations).

Third Party Due Diligence ■ Continued from page 7

FCPA third party due diligence and data privacy standards in good faith and in accordance with best practice. Absent such cooperation and guidance from regulators on both sides of the Atlantic, companies that operate in both the United States and France need to be aware of, and strive to implement programs to resolve, these tensions in the nevertheless unsatisfactory and uncertain legal environment that presently exists.

Paul R. Berger
Frederick T. Davis
Erin W. Sheehy
Margot Laporte

Paul R. Berger is a partner and Erin W. Sheehy and Margot Laporte are associates in the firm's Washington, D.C. office. Frederick T. Davis is a partner in the firm's Paris office. They are members of the Litigation Department and White Collar Litigation Practice Group. The authors may be reached at prberger@debevoise.com, ftdavis@debevoise.com, ewsheehy@debevoise.com, and mlaporte@debevoise.com. Full contact details for each author are available at www.debevoise.com.

The Tax Man Cometh: Recurring FCPA-Related Issues Under the U.S. Internal Revenue Code[1]

The fact that FCPA violations carry the risk of significant U.S. tax law consequences is important throughout the year. Indeed, the tax consequence of FCPA violations is an issue U.S. law enforcement personnel are highlighting, as indicated by case filings and appearances by representatives of the Internal Revenue Service ("IRS") at FCPA conferences.[2]

Prosecution of tax violations connected to FCPA issues is nothing new, with the list of corporate and individual matters including *United States v. Titan Corp.*, *United States v. Liebo*, and *United States v. Green*, among others.[3] Potential tax liabilities can increase the costs of non-compliance with the FCPA's substantive standards and accounting provisions, and complicate corporate and individual FCPA settlement discussions. It has long been the case that that non-prosecution agreements and deferred prosecution agreements entered into by the U.S. Department of Justice ("DOJ") of FCPA matters leave open the possibility of further criminal or civil tax prosecutions.[4]

In the following sections, we address (1) issues arising under section 162 of the Internal Revenue Code of 1986, as amended ("Code"), which bars the deduction of payments that violate the anti-bribery provisions of the FCPA, and (2) the tax treatment of payments to the U.S. government and others in connection with resolution of allegations of FCPA violations.

Non-Deductibility of Illegal Payments and the FCPA

Since the Tax Equity and Fiscal Responsibility Act of 1982 ("TEFRA"), U.S. tax law has specifically barred

CONTINUED ON PAGE 9

1. This article provides summary information only and is not intended as legal advice. Readers should seek specific legal advice before taking any action with respect to the matters discussed herein. This article was not intended or written to be used, and it cannot be used by any taxpayer, for the purpose of avoiding penalties that may be imposed on the taxpayer under U.S. Federal tax law.

2. At the January 2012 "FCPA Boot Camp" hosted by the American Conference Institute in Houston, Texas, Clarissa M. Balmaseda, a Special Agent in Charge of IRS Criminal Investigation in the Northern District of California, signaled the IRS's newfound willingness to step into the FCPA arena. American Conference Institute, "FCPA Boot Camp" at 4 (Jan. 2012) (on file with author). Another IRS representative is slated to speak at the American Conference Institute's FCPA conference for the pharmaceutical, medical device and life sciences industry in May 2012. *See* American Conference Institute, "FCPA & Anti-Corruption for the Life Sciences" (May 2012) (on file with author).

3. *See, e.g.*, *United States v. Titan Corp.*, No. 05-CR-314-BEN, Information at 42-46 (S.D. Cal. 2005); *United States v. Liebo*, 923 F.2d 1308, 1310 n.1 (8th Cir. 1991); *United States v. Green*, No. 08-CR-59(B)-GW, Second Superseding Indictment at 30 (C.D. Cal. Mar. 11, 2009); *see also* Morgan R. Hirst & Elizabeth H. Jenkins, Adding Insult to Injury: Tax Consequences of FCPA Violations, *Tax Notes*, 1074–75 (June 6, 2011).

4. For the most recent language utilized by the DOJ, *see, e.g.*, *United States v. Smith & Nephew, Inc.*, No. 12-CR-00030, Deferred Prosecution Agreement at 5 (D.D.C. Feb. 1, 2012); *United States v. Marubeni Corp.*, No. 12-CR-022, Deferred Prosecution Agreement at 7 (S.D. Tex. Jan. 17, 2012); *In re Aon Corp*, Non-Prosecution Agreement at 2 (Dec. 20, 2011); *In re Deutsche Telekom, AG*, Non-Prosecution Agreement at 1 (E.D. Va. Dec. 29, 2011); *see also* Hirst & Jenkins, note 3, *supra* at 1076.

The Tax Man Cometh ■ Continued from page 8

deduction of bribe payments made illegal under the FCPA:[5]

> No deduction shall be allowed under subsection [162](a) for any payment made, directly or indirectly, to an official or employee of any government, or of any agency or instrumentality of any government, if the payment constitutes an illegal bribe or kickback or, if the payment is to an official or employee of a foreign government, the payment is unlawful under the Foreign Corrupt Practices Act of 1977. The burden of proof in respect of the issue, for the purposes of this paragraph, as to whether a payment constitutes an illegal bribe or kickback (or is unlawful under the Foreign Corrupt Practices Act of 1977) shall be upon the Secretary to the same extent as he bears the burden of proof under section 7454 (concerning the burden of proof when the issue relates to fraud).

If a taxpayer has admitted making payments that violate the anti-bribery provisions of the FCPA, amendments to earlier-filed returns may need to be filed,[7] raising issues of potential civil penalties and interest.[8] Depending on the circumstances, a corporation or corporate employee who helped prepare the flawed tax returns while aware of the underlying corrupt payments involved could also face criminal liability. At a minimum, in-house tax, finance, accounting, and legal and compliance personnel face the task of weighing the relevant evidence in the face of uncertainty before making determinations of deductibility, and, at a broader level, of instituting internal controls to assure compliance with FCPA-related tax regulations.

"If a taxpayer has admitted making payments that violate the anti-bribery provisions of the FCPA, amendments to earlier-filed returns may need to be filed,7 raising issues of potential civil penalties and interest."

These tax issues can affect a broad range of U.S. taxpayers, including U.S. corporations,[9] U.S. shareholders of controlled foreign corporations, partnerships and individuals.

A. Civil Penalties

Civil penalties for improper deductions of payments that violate the FCPA's anti-bribery provisions can range from accuracy related-penalties to fraudulent filing penalties. Section 6662 of the Code establishes an accuracy-related penalty of twenty percent of an underpayment of tax that is attributable to various errors and omissions,[10] including negligence, disregard of IRS rules or regulations, or substantial understatement of income tax.[11]

CONTINUED ON PAGE 10

5. Pub. L. No. 97-248, § 288, 96 Stat. 324 at 571 (1982). Congress's efforts to deal with the tax implications of foreign bribery date at least as far back as the Technical Amendments Act of 1958, Pub. L. No. 85-866, 72 Stat. 1606 at 1608 (1958), which amended section 162(c) of the Internal Revenue Code of 1954 to prohibit the deduction of any expenses "made, directly or indirectly, to an official or employee of a foreign country, and if the making of the payment would be unlawful under the laws of the United States if such laws were applicable to such payment and to such official or employee." *Id.* Even as of 1958, the IRS had long taken the view that "when bribes or improper payments are made to officials of foreign countries, such expenditures usually are not considered to be 'ordinary and necessary' business expenses," except in cases in which "the foreign government itself demand[ed] or acquiesce[d] in the payment," as "legal recourse [was] not available to the taxpayer in the operation of his business." S. Rep. No. 85-1983, at 16 (1958). In 1982 – after the FCPA had been on the books for nearly half a decade – TEFRA eliminated the hypothetical test for deductibility of bribes of foreign officials, generating "a single standard of legality for payments to foreign government personnel . . . for both the Foreign Corrupt Practices Act and the Internal Revenue Code." S. Rep. No. 97-494, at 164.

6. 26 U.S.C. § 162(c)(1). Whether commercial bribe payments are deductible for federal income tax purposes implicates Code provisions concerning the tax treatment of payments that violate the federal (and state) laws used to prosecute the making of such payments, *see* Code § 162(c)(2); Tax Reform Act of 1969, Pub. L. No. 91-172, § 902(b), 83 Stat. 487, 710 (1969); S. Rep. No. 91-552, at 275 (1969); Revenue Act of 1971, Pub. L. 92-178, § 310(a), 85 Stat. 497, 525 (1971); S. Rep. No. 92-437, at 72–73 (1971). Those laws include, among others, the federal Travel Act. *See* Paul R. Berger, Bruce E. Yannett, and David M. Fuhr, "The Use of the Travel Act to Prosecute Foreign Commercial Bribery: A Review of the Denial of the Defense Motion in *United States v. Carson*," *FCPA Update*, Vol. 3, No. 3 (Oct. 2011), http://www.debevoise.com/newseventspubs/publications/detail.aspx?id=64730281-500e-48e2-85ca-630f30a991ee.

7. Generally a business may deduct any expenses that are "ordinary and necessary," *id.* § 162(a), but if a payment was once characterized as an "ordinary and necessary" expense, but later revealed as an illegal bribe, a company may need to amend its previous years returns to forego the deduction to the extent of the value of the bribe.

8. *Id.* § 6601(a) ("If any amount of tax imposed by this title . . . is not paid on or before the last date prescribed for payment, interest on such amount at the underpayment rate . . . shall be paid for the period from such last date to the date paid.").

9. The controlled foreign corporation ("CFC") rules are an anti-deferral regime that, among other things, subject certain direct and indirect U.S shareholders of a CFC to U.S. federal income tax on their proportionate share of the so-called "subpart F income" of the CFC, even if the CFC does not make distributions to its shareholders. *Id.* § 951(a). Subpart F income includes "the sum of the amounts of any illegal bribes, kickbacks, or other payments (within the meaning of section 162(c)) paid by or on behalf of the corporation during the taxable year" which would be unlawful under the FCPA. *Id.* § 952(a). As a result, a U.S. shareholder in a CFC may be subject to current U.S. tax on the amount of any illegal FCPA payment made by the CFC even if the CFC has not made any distributions to its shareholders.

10. *Id.* § 6662(a).

11. *Id.* § 6662(b)(1).

The Tax Man Cometh ■ Continued from page 9

Section 6663(a) imposes penalties on fraudulent filings. It provides that "[i]f any part of any underpayment of tax required to be shown on a return is due to fraud, there shall be added to the tax an amount equal to 75 percent of the portion of the underpayment which is attributable to fraud."[12] For section 6663(a) to apply, the government must show by clear and convincing evidence[13] that the underpayment of taxes was due to fraud.[14] "The fraud determination turns on whether the taxpayer had an actual, specific intent to evade a tax owed."[15] A taxpayer's fraudulent intent can be demonstrated indirectly via evidence of "badges of fraud," which include: (1) understating income, (2) maintaining inadequate records, (3) implausible or inconsistent explanations of behavior, (4) concealment of income or assets, (5) failing to cooperate with tax authorities, (6) engaging in illegal activities, (7) intent to mislead which may be inferred from a pattern of conduct, (8) lack of credibility of taxpayer's testimony, (9) filing false documents, (10) failing to file tax returns, and (11) dealing in cash.[16]

The statute of limitations provides very little, if any, refuge in fraud penalty proceedings. Generally a tax must be assessed by the IRS "within 3 years after the return was filed."[17] Once assessed, the IRS has ten years to seek to collect the tax by administrative means or institute a suit for collection or judgment.[18] Section 6501 of the Code, however, provides that "[i]n the case of a false or fraudulent return with the intent to evade tax, the tax may be assessed, or a proceeding in court for collection of such tax may be begun without assessment, at any time."[19] Indeed, in 1995 the Tax Court held that the IRS properly assessed tax, penalty, and interest for fraudulent returns filed from twenty-four to thirty years earlier, *i.e.*, those filed in the period including tax years 1964 to 1970.[20]

B. Criminal Penalties

Deducting or attempting to deduct an illegal payment may also give rise to a variety of potential criminal charges.[21] Section 7201 of the Code, for example, prohibits any person from willfully attempting to evade or defeat tax or the payment thereof.[22] Similarly, section 7206(1) prohibits any person from willfully making "any return, statement, or other document, which contains or is verified by a written declaration that it is made under the penalties of perjury, and which he does not believe to be true and correct as to every material matter,"[23] while section 7206(2) criminalizes the willful aid or assistance in preparing a return, affidavit or claim "which is fraudulent or is false as to any material matter."[24] Section 7207 punishes any person's willful disclosure "to the Secretary any list, return, account, statement, or other document known by him to be fraudulent or to be false as to any material matter."[25]

CONTINUED ON PAGE 11

12. *Id.* § 6663(a).
13. The 1958 legislation addressing the deductibility of foreign bribes imposed on the taxpayer the burden to show entitlement to a deduction. *See generally INDOPCO, Inc. v. Comm'r,* 503 U.S. 79, 84 (1992) (noting the "familiar rule that an income tax deduction is a matter of legislative grace and that the burden of clearly showing the right to the claimed deduction is on the taxpayer") (internal citations and quotations omitted). The Tax Reform Act of 1969 shifted to the IRS the burden of showing by clear and convincing evidence in bribery-related disallowance proceedings that the deduction was not available. *See* Pub. L. No. 91-172, Section 902, 83 Stat. at 710.
14. *Gagliardi v. United States*, 81 Fed. Cl. 772, 774, 785 (Ct. Cl. 2008); *Cole v. Comm'r*, 637 F.3d 767, 780 (7th Cir. 2011); *Petzoldt v. Comm'r*, 92 T.C. 661, 699 (T.C. 1989).
15. *Cole*, 637 F.3d at 780 (quotations omitted).
16. *Aston v. Comm'r*, 2003 WL 21000282, at *4 (T.C. May 2, 2003) (citing *Spies v. United States*, 31 U.S. 492, 499 (1943)); *see also Bradford v. Comm'r*, 796 F.2d 303, 307 (9th Cir. 1986) (similar); *Cole*, 637 F.3d at 780 (similar). *See also Badaracco v. Comm'r*, 464 U.S. 386, 394 (1984) ("[A] taxpayer who submits a fraudulent return does not purge the fraud by subsequent voluntary disclosure").
17. 26 U.S.C. § 6501(a).
18. *Id.* § 6502(a).
19. *Id.* § 6501(c)(1).
20. *See Levitt v. Comm'r*, 70 T.C.M. (CCH) 851, at *27 (T.C. 1995) (also imposing the special fifty percent penalty provided by 26 U.S.C. § 6653(2)).
21. *See* 26 U.S.C. §§ 7201–12.
22. *Id.* § 7201.
23. *Id.* § 7206(1).
24. *Id.* § 7206(2). This conduct is criminal, irrespective of whether the taxpaying entity or individual had knowledge of the fraud *Id.*
25. *Id.* § 7207.

The Tax Man Cometh ■ Continued from page 10

Of particular import for corporate officers, "[a]ny person" is not limited to a taxpayer, but includes "an officer or employee of a corporation, or a member or employee of a partnership."[26]

Criminal tax violations, of course, are subject to the requirement that the government prove the elements of the offense beyond a reasonable doubt. Moreover, a successful prosecution requires proof of "willful" misconduct by the defendant.[27] The U.S. Supreme Court has held that, by including this term, Congress departed from "[t]he general rule that ignorance of the law or mistake of law is no defense to criminal prosecution . . . ."[28] The government must prove "that the law imposed a duty on the defendant, that the defendant knew of this duty, and that he voluntarily and intentionally violated that duty."[29] To prove the second element, the government must "negat[e] a defendant's claim of ignorance of the law or a claim that because of a misunderstanding of the law, he had a good faith belief that he was not violating any of the provisions of the tax laws."[30] It is not sufficient on this front that the defendant's belief is unreasonable.[31]

"Criminal tax violations, of course, are subject to the requirement that the government prove the elements of the offense beyond a reasonable doubt. Moreover, a successful prosecution requires proof of 'willful' misconduct by the defendant."

Section 6531 governs the statute of limitations with respect to criminal tax violations, generally establishing that "[n]o person shall be prosecuted, tried, or punished for any of the various offenses arising under the internal revenue laws unless the indictment is found or the information instituted within 3 years next after the commission of the offense."[32] This section, however, also includes exceptions for which the applicable statute of limitations can be six years.[33]

Finally, criminal tax proceedings against a corporation for fraud or willful misconduct, like prosecutions under the FCPA itself, raise potential questions relating to the "collective knowledge" doctrine,[34] under which "[a] corporation is considered to have acquired the collective knowledge of its employees and is held responsible for their failure to act accordingly."[35] The doctrine remains controversial, and its application in the

CONTINUED ON PAGE 12

---

26. *Id.* § 7343.
27. *See United States v. Bishop*, 412 U.S. 346, 360–61 (1973) (meaning of "willful").
28. *Cheek v. United States*, 498 U.S. 192, 199–200 (1992).
29. *Id.* at 201; *see also Bishop*, 412 U.S. at 360.
30. *Cheek*, 498 U.S. at 202.
31. *Id.*
32. 26 U.S.C. § 6531.
33. *Id.* Section 6531 mandates a six year statute of limitations "for offenses described in sections 7206(1) and 7207 (relating to false statements and fraudulent documents)" as well as for the offenses "described in section 7212(a) [and] 7214(a)[.]" *Id.* § 6531(5)–(7). Section 6531 also establishes a six year limitation period for offenses in other sections, but by describing the misconduct rather than by explicit reference to the section. For example, section 6531(2) establishes a six year statute of limitation for section 7201 by providing that "the period of limitation shall be 6 years . . . for the offense of willfully attempting in any manner to evade or defeat any tax or the payment thereof." *Id.* § 6531(2); *cf. id.* § 7201 (criminalizing the willful attempt "to evade or defeat any tax imposed by this title or the payment thereof"). Other sections for which 6531 establishes a six year statute by describing misconduct rather than by explicit reference include sections 7202 (willfully failing to pay any tax), 7203 (willful failure to file return), and 7206(2) (willfully aiding or assisting preparation false or fraudulent returns). *See id.* § 6531(2)-(4). Finally, a six year statute of limitations also applies to the prohibition on conspiracy to evade taxes, which is codified not in the Code but rather at 18 U.S.C. § 371. *See id.* § 6531(8).
34. In *N.Y. Cent. R.R. & Hudson River R.R. Co v. United States*, the U.S. Supreme Court held that a corporation could be criminally prosecuted for the misconduct of its agents acting within their scope of employment. 212 U.S. 481 (1909). This remains the law. *See United States v. Koppers Co., Inc.*, 652 F.2d 290, 298 (2d Cir. 1981); *United States v. Halpin*, 145 F.R.D. 447, 449 (N.D. Ohio 1992). The collective knowledge doctrine expands this rule by enabling a corporation to be held criminally liable even when no single employee engaged in covered misconduct with the required knowledge, or, depending on the court applying the doctrine, *mens rea*. *United States v. Bank of New England*, 821 F.2d 844, 856 (1st Cir. 1987).
35. *Bank of New England*, 821 F.2d at 856.

The Tax Man Cometh ■ Continued from page 11

criminal tax context is a largely untested question.[36]

> "The steps related to tax compliance should be coordinated with the company's response to information it has learned about any FCPA violation itself, including the decision whether to self-report through an amended tax filing or otherwise."

C. Tax-Related Responses to Illegal Payments Under the FCPA

If a company determines that an underlying improper payment was made to a foreign official under the FCPA, it should not deduct the payment. If the payment already has been deducted, quickly learning who knew of the improper nature of the payment, and when, should guide in-house counsel in determining the extent to which the corporation could be liable. In-house counsel should consider the applicable statute of limitations, including whether potential conspiracy charges or other factors might toll or extend the limitations period or otherwise affect legal exposure, as well as mitigating and aggravating factors regarding the primary FCPA violation and tax issues.

The steps related to tax compliance should be coordinated with the company's response to information it has learned about any FCPA violation itself, including the decision whether to self-report through an amended tax filing or otherwise.[37] Every case will be different, however, and in house counsel and corporate compliance officers would do well to confer with both experienced tax counsel and experienced FCPA counsel to determine a corporation's exposure and next steps.

Deductibility of Payments to the Government to Resolve FCPA Matters

Deductibility of payments to government entities to resolve FCPA allegations and investigations will generally turn on whether the payments are penal or compensatory in nature. Section 162(f) of the Code provides that "[n]o deduction shall be allowed . . . for any fine or similar penalty paid to a government for the violation of any law."[38] For purposes of this section, penalties include any amounts paid in settlement of actual or potential liability for a civil or criminal fine or penalty.[39]

Payments to settle claims of restitution and disgorgement raise issues under these regulations. Because compensatory and remedial payments are deductible,[40] the deductibility of restitution and disgorgement payments will therefore turn

CONTINUED ON PAGE 13

---

36. In *United States v. Science Applications Int'l Corp*, 626 F.3d 1257, 1274-76 (D.C. Cir. 2010), for example, the D.C. Circuit expressed strong doubts about the collective knowledge doctrine, noting that "we are dubious of the legal soundness of the 'collective intent' theory, under which, as we explained, a corporation's specific intent to defraud can be inferred if the company's public statements contradict the accumulated 'collective knowledge' of the corporation's employees." (quotation marks omitted)). *See also Southland Sec. Corp. v. INSpire Ins. Solutions, Inc.,* 365 F.3d 353, 366 (5th Cir. 2004); *Nordstrom, Inc. v. Chubb & Son, Inc.*, 54 F.3d 1424, 1435 (9th Cir. 1995). Some commentators question the doctrine's applicability to specific intent crimes, *see* Sarah Kelly-Kilgore & Emily M. Smith, *Corporate Criminal Liability*, 48 Am. Crim. L. Rev. 421, 431–32 (2011), while others conclude that "when courts have aggregated knowledge, they invariably have done so as a technique in response to willful blindness to inculpatory knowledge." Thomas A. Hagemann & Joseph Grinstein, *Mythology of Aggregate Corporate Knowledge: A Deconstruction*, 65 Geo. Wash. L. Rev. 210, 236–37 (1997). District courts outside of the First Circuit have also confined *Bank of New England* to its facts. *See, e.g.*, *United States v. Walthers*, 779 F. Supp. 2d 735, 738 (N.D. Ill. 2011). One state court has flatly disagreed with the First Circuit and broadly held that "a corporation acts with a given mental state in a criminal context only if at least one employee who acts (or fails to act) possesses the requisite mental state at the time of the act (or failure to act)." *Commonwealth v. Life Care Ctrs. of Am.*, 926 N.E.2d 206, 212 (Mass. 2010). *But see State v. Zeta Chi Fraternity*, 696 A.2d 530 (N.H. 1997). Although the U.S. Supreme Court has cited *Bank of New England*, it has never opined on the collective knowledge doctrine, let alone its application to tax cases. *Staub v. Proctor Hosp.,* 131 S. Ct. 1186, 1192 (2011); *Ratzlaf v. United States*, 510 U.S. 135, 141 (1994).

37. There is some question whether a taxpayer is legally obliged to file an amended return. *See* 26 C.F.R. § 1.162-21 ("If a taxpayer ascertains that an item should have been included in gross income in a prior taxable year, he *should*, if within the period of limitation, file an amended return and pay any additional tax due." (emphasis added)); *see also Badaracco v. Comm'r*, 464 U.S. 386, 393 (1984) ("[T]he Internal Revenue Code does not explicitly provide either for a taxpayer's filing, or for the Commissioner's acceptance, of an amended return."). Irrespective of its legal obligation, however, a taxpayer may wish to amend an incorrect return to avoid or stanch potential interest charges and penalties on the original return, or for a host of non-tax reasons.

38. 26 U.S.C. § 162(f).

39. The U.S. Treasury Regulations define "fine or similar penalty" as an amount:
(i) Paid pursuant to conviction or a plea of guilty or nolo contendere for a crime (felony or misdemeanor) in a criminal proceeding;
(ii) Paid as a civil penalty imposed by Federal, State, or local law . . . ;
(iii) Paid in settlement of the taxpayer's actual or potential liability for a fine or penalty (civil or criminal).
26 C.F.R. § 1.162-21 (2012); *Hawronsky v. Comm'r*, 105 T.C. 94, at *97 (T.C. 1995).

40. 26 C.F.R. § 1.162-21(b)(2). ("Compensatory damages . . . paid to a government do not constitute a fine or penalty.").

The Tax Man Cometh ■ Continued from page 12

on whether they can be characterized as compensatory or remedial, rather than penal in nature.[41] If the penalty is "imposed for purposes of enforcing the law and as punishment for the violation thereof,"[42] the payment is not deductible. Remedial payments, in contrast, are "'imposed to encourage prompt compliance with the law, or as a remedial measure to compensate another party for expense incurred as a result of the violation.'"[43] The specific purpose of the payment is relevant,[44] and a court will also consider whether the payment was made to the government or a third party.[45] Finally a court may consider "whether allowing the deductions severely frustrate[s] a sharply defined national policy or thwart[s] a State policy."[46]

These are fact-sensitive inquiries. If a specific payment is made in consideration of the government's forbearance from seeking a potential criminal penalty, courts generally conclude that the payment was punitive.[47] Indeed, FCPA settlements with the DOJ typically bar deduction of a payment made by the settling corporation.[48] Recent U.S. Securities and Exchange Commission FCPA resolutions have contained similar language prohibiting settling companies from deducting the penalty components of the dispositions, leaving the tax status of the disgorgement component unaddressed.[49]

Conclusion

In an era of economic challenges that have put a spotlight on tax compliance, in house counsel, financial and accounting departments, as well as corporate compliance personnel would do well to keep tax issues associated with FCPA compliance on the front burner. The importance of the issues warrants diligence in implementing compliance programs and swift, effective action when addressing specific evidence of misconduct.

Peter F.G. Schuur
Bruce E. Yannett
Steven S. Michaels
John T. Pierpont

Peter F.G. Schuur is a partner in the New York office and a member of the firm's Tax Department. Bruce E. Yannett is a partner, Steven S. Michaels is a counsel, and John T. Pierpont is an associate in the firm's New York office; they are members of the Litigation Department and White Collar Litigation Practice Group. The authors may be reached at pfgschuur@debevoise.com, beyannett@debevoise.com, ssmichaels@debevoise.com, and jtpierpont@debevoise.com. Full contact details for each author are available at www.debevoise.com.

---

41. *Cavaretta v. Comm'r*, No. 24823-07, 2010 WL 23331 at *4 (T.C. 2010).

42. *Fresenius Med. Care Holdings, Inc. v. United States*, No. 08 Civ. 12118, 2010 WL 2595541, at *4 (D. Mass. June 24, 2010). *See also Talley Indus. Inc. v. Comm'r*, 116 F.3d 382, 385 (9th Cir. 1997) (quoting *S. Pac. Transp. Co. v. Comm'r*, 75 T.C. 497, 652–53 (T.C. 1980)); *True v. United States*, 894 F.2d 1197, 1204 (10th Cir. 1990).

43. *Fresenius*, 2011 WL 2595541, at *4 (quoting *S. Pac. Transp. Co*, 75 T.C. at 652–53).

44. *See Stephens v. Comm'r*, 905 F.2d 667, 672–73 (2d Cir. 1990) (examining why a restitution payment was made to determine if it was punitive); *see also* R.W. Wood, "Tax Deductions for Damage Payments: What, Me Worry?" *Tax Notes* (Jan. 16, 2006).

45. *Stephens*, 905 F.2d at 673. This factor is not, however, dispositive. *See Kraft v. United States*, 991 F.2d 292, 298-99 (6th Cir. 1993) (restitution held to be nondeductible because it arose out of criminal proceedings).

46. *Bailey v. United States*, No. 122-77, 1997 WL 759654, at *40 (Fed. Cl. Sept. 30, 1997).

47. *See Allied Signal, Inc. v. Comm'r*, T.C. Memo 1992-204, 1992 WL 67399 (T.C. 1992), *aff'd* 54 F.3d 767 (3d Cir. 1995). *But see Spitz v. United States*, 432 F. Supp. 148 (E.D. Wis. 1977) (allowing a deduction despite criminal sentence being conditioned on making restitution).

48. *See United States v. Smith & Nephew, Inc.*, No.12-CR-00030, Deferred Prosecution Agreement at 5 (D.D.C. Feb. 1, 2012); *United States v. Tyson Foods, Inc.*, No. 11-CR-037, Deferred Prosecution Agreement at 5 (Feb. 4, 2011). *But cf. Jenkins v. Comm'r*, 72 T.C.M (CCH) 1470, at *4 (T.C. 1996) ("some payments, although labeled 'penalties,' remain deductible if imposed to encourage prompt compliance with a requirement of the law, or as a remedial measure to compensate another party.").

49. *See, e.g.*, *In re Tenaris*, Deferred Prosecution Agreement at 7 (May 17, 2011); *SEC v. IBM Corp.*, No. 11-cv-0563, Consent of Defendant International Business Machine Corp. at 3 (D.D.C. Apr. 5, 2011). The tax court may split payments, determining that they are in part punitive and in part compensatory for federal tax purposes. *Barnes v. Comm'r*, T.C. Memo. 1997-25, 1997 WL 12138 at *5 (Jan. 15, 1997).

UK FSA's Review of Anti-Bribery and Corruption Systems and Control at Investment Banks

The United Kingdom's Financial Services Authority ("FSA"), which is responsible for regulating the financial services industry in the United Kingdom, last month issued a review addressing anti-bribery and corruption systems at investment banks (the "Review").[1] Although the Review, as described below, was critical of the investment banks' systems in a number of respects, the FSA has provided valuable pointers for all financial firms—not just investment banks.

Publication of the Review follows a public notice by the FSA to all firms subject to its authority that they need to institute adequate internal controls reasonably designed to prevent bribery.[2]

The Review followed a fact-finding mission in which the FSA visited 15 investment banks, including some of the world's largest, to determine whether the investment banks were complying with existing anti-bribery and corruption ("ABC") legislation and FSA rules and principles. Though only investment banks were visited, the FSA said that its findings and recommendations applied to financial firms in general.

Overall, the FSA was disappointed; it stated that investment banks had been "too slow and reactive in managing bribery and corruption risks,"[3] and that a number of firms had "significant work to do to get an adequate ABC control framework in place."[4] Many investment banks claimed to have "zero tolerance" bribery policies, but there was generally little substance behind such statements.[5]

The Review highlighted some specific inadequacies, including the following:

- Senior management and directors were not being given enough ABC management information to take responsibility for the mitigation of bribery and corruption risk.[6]
- Few firms had policies ensuring that gifts and entertainment expenses were reasonable.[7]
- Firms were not carrying out proper bribery and corruption risk assessments and none of them had taken action in response to the FSA's review of insurance brokers' ABC controls and the fines levied on brokers Aon Limited and Willis Limited.[8]
- Firms' dealings with intermediaries were inadequate, particularly in the areas of due diligence and continued review.[9]
- Nearly half the firms reviewed did not have adequate ABC risk assessment in place.[10]
- The majority of firms had not considered how to monitor the effectiveness of their ABC controls.[11]
- Firms' understanding of bribery and corruption was often limited.[12]

However, the Review also pointed out some examples of good practice[13] which

CONTINUED ON PAGE 15

1. *See* U.K. FSA, "Anti-Bribery and Corruption Systems and Controls in Investment Banks" (Mar. 2012), http://www.fsa.gov.uk/static/pubs/other/anti-bribery-investment-banks.pdf (hereinafter, "Review").
2. *See* U.K. FSA, "The FSA and the Bribery Act," *Financial Crime Newsletter*, No. 15 (Sept. 2011) (hereinafter "FSA Newsletter No. 15"), http://www.fsa.gov.uk/pubs/newsletters/fc_newsletter15.pdf; *see also* Karolos Seeger and Matthew H. Getz, "The U.K. FSA Reminds Financial Services Firms of Anti-Corruption Compliance Obligations," *FCPA Update*, Vol. 3, No. 2 (Sept. 2011), http://www.debevoise.com/newseventspubs/publications/detail.aspx?id=ccf8c29f-9f86-47ac-95f5-05c65c607046.
3. Review at § 1.3(4).
4. *Id.* at § 1.3(5).
5. *Id.* at § 1.3(4).
6. *Id.* at § 1.2(3)(c), 3.1(24-33).
7. *Id.* at §§ 1.2(3)(g), 3.6(96-99).
8. *Id.* at §§ 1.2(3)(f), 3.2.2 (43-46, 56).
9. *Id.* at § 3.4(69, 81-92).
10. *Id.* at §§ 1.2(3)(b); 3.2.
11. *Id.* at § 1.2(3)(d).
12. *Id.* at § 1.2(3)(e).
13. *Id.* at § 4.

UK FSA's Review ■ Continued from page 14

should assist all financial firms, especially when considered in tandem with the FSA publication "Financial Crime: A Guide for Firms," which sets out the FSA's expectations in some detail.[14] Some key examples of good practice include:

- A gap analysis of existing ABC procedures against applicable legislation, regulations and guidance, and the implementation of enhancements as necessary to close any significant gaps that were identified.[15]
- Inclusion of ABC-specific clauses and appropriate protections in contracts with third parties.[16]
- Processes for filtering and analyzing the provision and receipt of gifts and hospitality by employee, client and type of hospitality.[17]
- Processes to identify unusual or unauthorized gift and hospitality and deviations from approval limits.[18]
- Enhanced vetting for staff in roles with higher bribery and corruption risk (including checks of credit records, criminal records, financial sanctions lists and commercially available intelligence databases).[19]
- Measures to allow staff to raise concerns anonymously, with adequate levels of protection, and clear communication of these measures to staff.[20]

Following these good practices would help firms comply with the FSA's principles and system and control rules. In addition, following such practices should also help firms comply with the U.K. Bribery Act. Under Section 7(2) of the Bribery Act, it is a defense against a charge of the corporate offense of failing to prevent bribery that a firm has "adequate procedures" in place to prevent bribery. Though the FSA does not prosecute violations of the Act, it is most unlikely that a financial firm following the FSA's own precepts would not be found to have adequate procedures.

> "[T]hose firms that fall short are well-advised to act swiftly to improve their systems: The FSA stated that a number of the firms sampled might face regulatory action in relation to their compliance with the FSA's systems and controls rules."

But those firms that fall short are well-advised to act swiftly to improve their systems: The FSA stated that a number of the firms sampled might face regulatory action in relation to their compliance with the FSA's systems and controls rules.[21] The FSA has the power to levy fines, publicly censure firms and obtain injunctions against firms, and has not been shy to use its power.[22]

Karolos Seeger
Matthew H. Getz
Warren Balakrishnan

Karolos Seeger is a partner and Matthew H. Getz is an associate in the firm's London Office. They are members of the Litigation Department and White Collar Litigation Practice Group. Warren Balakrishnan is a trainee solicitor in the firm's London office and a member of the Corporate Department. The authors may be reached at kseeger@debevoise.com, mgetz@debevoise.com, and wbalakrishnan@debevoise.com. Full contact details for each author are available at www.debevoise.com.

14. U.K. FSA, "Financial Crime; a guide for firms" (June 22, 2011), http://www.fsa.gov.uk/library/policy/cp/2011/11_12.shtml.
15. *See* Review at § 3.3(55).
16. *Id.* at § 3.3(52).
17. *Id.* at § 3.6.7.
18. *Id.*
19. *Id.* at § 3.7(121).
20. *Id.* at § 3.10.1(147).
21. *Id.* at § 1.3(5).
22. *See, e.g.*, U.K. FSA Final Notice to Coutts & Company, No. 122287 (Mar 23, 2012), http://www.fsa.gov.uk/static/pubs/final/coutts-mar12.pdf (imposing financial penalty of £8.75 million for breach of the FSA's management and control Principles for Business).

Recent and Upcoming Speaking Engagements

April 25, 2012
Paul R. Berger
"Enforcement Developments"
Global Capital Markets and the U.S. Securities Laws 2012: Raising Capital in an Evolving Regulatory Environment
PLI
New York
Conference information: http://www.pli.edu/Content/Seminar/Global_Capital_Markets_the_U_S_Securities/_/N-4kZ1z1337n?Npp=1&ID=143096

April 25, 2012
Philip Rohlik
AML Event
Gaming Law and Money Laundering / Corruption in Asia
Website: http://www.cch.com.hk

May 4, 2012
Paul R. Berger
"Country Developments--China"
Foreign Corrupt Practices Act and International Anti-Corruption Developments 2012
PLI
New York
Conference information: http://www.pli.edu/Content/Seminar/Global_Capital_Markets_the_U_S_Securities/_/N-4kZ1z1337n?Npp=1&ID=143096

May 8–9, 2012
Paul R. Berger
"FCPA, Corporate Governance and Personal Liability: How to Deal with Audit Committees, Board of Directors and Corporate Officers when FCPA Issues Arise"
Sixth National Conference on the FCPA and Anti-Corruption for the Life Sciences Industry
American Conference Institute
New York
Conference information: http://americanconference.com/2012/709/fcpa-and-anti-corruption-for-the-life-sciences-industry/overview

June 4–6, 2012
Frederick T. Davis
Matthew H. Getz
"Global Anti-Corruption Enforcement Efforts"
Certificate in Healthcare Compliance Ethics & Regulation
Seton Hall Law and SciencesPo.
Conference information: http://www.sciences-po.fr/spf/conferences/certificat_healthcare.php

June 7, 2012
Philip Rohlik
Asia Discovery Exchange 2012
Proactive Legal Management - Dialogue - Transforming reactive to proactive eDiscovery benefits business and litigation outcomes.
Website: http://www.asiaediscovery.com/

June 26–27, 2012
Bruce E. Yannett
"What the Latest Cases Reveal About the US DOJ and SEC Enforcement Priorities"
Karolos Seeger
"Optimising Compliance: How Leading Companies are Enhancing their Compliance Programmes One Year After the Implementation of the UK Bribery Act"
6th Annual European Forum on Anti-Corruption
C5
London
Conference information: http://www.c5-online.com/2012/683/anti-corruption-london/overview

Recent Publication

Michael B. Mukasey
James C. Dunlop*
Criminal Law & Procedure
"Can Someone Please Turn on the Lights? Bringing Transparency to the Foreign Corrupt Practices Act"
For more information:
http://www.fed-soc.org/
** Mr. Dunlop is an attorney with Jones Day.*