DEBEVOISE & PLIMPTON LLP

International Corporate Investigations and Defense Group

ICID Review

Winter 2009/2010 ■ Volume 1, Number 1

Internal investigations: comparative overview and trends

IN THE US

I. Internal investigations in the US

Corporate internal investigations in the United States trace their roots to the mid-1970s, when, as part of the fallout from the Watergate scandal and disclosures of widespread misuse of corporate funds, bribery and fraud, the US Congress passed the Foreign Corrupt Practices Act (*FCPA*) in 1977.[1] Nine years later, in 1986, Congress passed the Money Laundering Control Act to further stem the tide of corrupt corporate activity. In 2002, the Sarbanes-Oxley Act (*SOX*) went into effect in response to the numerous high-profile corporate scandals around the time.

Continues on page 3 click here

IN THE UK

I. Internal investigations in the UK

Corporate internal investigations are historically less common in the United Kingdom than in the United States. This is a result of both the absence of legislation calling for such investigations but, also, of an approach to enforcement by the UK regulators and prosecutors which – unlike the approach of their US counterparts – did not, until recently, incentivise companies to self-investigate and self-report. There are now clear signs that both the legislative landscape and the approach to enforcement have changed and will continue to change very significantly.

Continues on page 8 click here

IN FRANCE

I. Internal investigations in France

This article presents key points to consider if a criminal investigation in France, or with possible ties to France, has been, or may be, launched. The attitude towards, and experience with, internal investigations in France differs greatly from that in the United States. In France, prosecuting authorities will carry out their own investigation regardless of whether the company under scrutiny conducts an investigation of its own.

Continues on page 14 click here

IN GERMANY

I. Internal investigations in Germany

Internal investigations of German companies have taken place in recent years, notwithstanding the fact that there is no obligation under German law for a company to conduct an internal investigation.[1] Indeed, German constitutional law requires prosecutors to conduct their own criminal investigations, irrespective of whether the company decides to perform an internal investigation itself.

Continues on page 18 click here

Introduction

by Mary Jo White
Lord Goldsmith QC
Bruce E. Yannett

Welcome to the first issue of our firm's International Corporate Investigations and Defense (ICID) Review. Produced by our global team of leading practitioners, the ICID Review will focus on the field of regulation, white collar crime, internal investigations and defense in our four key ICID jurisdictions: the US, the UK, France and Germany.

In each issue, we will take a single hot topic, such as prosecutorial stances, leniency through cooperation, etc., and consider it in relation to the above four countries. This country-by-country analysis will enable readers to compare directly the approaches of US and European authorities and the respective legal frameworks – essential in an environment

CONTINUED ON PAGE 2

Upcoming Events

(Click on event for more details)

January 13, 2010 – New York
The Year Just Passed and the One to Come: Staying Ahead of the FCPA

January 19, 2010 – Zurich
Internal Investigations in Switzerland

Introduction Continued from page 1

in which prosecutions are becoming more and more global in their reach and regulators are increasingly active and learning from each other. Here, in this introductory issue, we start off by giving you an overview of the principal laws and approaches in each country as they relate to regulatory and internal investigations, only briefly touching on the topics that will be explored in greater depth in later editions.

In addition, the ICID Review will provide a round-up of news and developments in the field, which will include links to our recently launched US "FCPA Update" and our periodic international client updates, as well as to events and publications of significance in this realm, again on a country-by-country basis in our four key ICID jurisdictions.

We know that the international world of regulation is changing fast and we want to help keep you, our clients and friends, apace with its developments. We hope you enjoy the ICID Review and that it proves useful to you. Please let us know if there are specific topics of interest that you would like to see covered in future issues. ■

Mary Jo White, Chair of the Litigation Department, previously served as the US Attorney for the Southern District of New York.

Lord Goldsmith, European Chair of Litigation, served as the UK's Attorney General from 2001-2007.

Bruce Yannett, former federal prosecutor, is Co-Chair of the White Collar Practice Group.

International Corporate Investigations and Defense (ICID) Group Partner/Counsel Members

New York
+1 212 909 6000

Andrew J. Ceresney
ajceresney@debevoise.com

Matthew E. Fishbein
mefishbein@debevoise.com

Mark P. Goodman
mpgoodman@debevoise.com

Sean Hecker
shecker@debevoise.com

James E. Johnson
jejohnson@debevoise.com

Michael B. Mukasey

Mary Jo White
mjwhite@debevoise.com

Bruce E. Yannett
beyannett@debevoise.com

Steven S. Michaels
ssmichaels@debevoise.com

Nicola C. Port
ncport@debevoise.com

Washington, D.C.
+1 202 383 8000

Paul R. Berger
prberger@debevoise.com

W. Neil Eggleston
wneggleston@debevoise.com

Colby A. Smith
casmith@debevoise.com

Jonathan R. Tuttle
jrtuttle@debevoise.com

Frankfurt
+49 69 2097 5000

Marcia L. MacHarg
mlmacharg@debevoise.com

Dr. Thomas Schürrle
tschuerrle@debevoise.com

London
+44 20 7786 9000

Lord Goldsmith QC
phgoldsmith@debevoise.com

Peter J. Rees QC
prees@debevoise.com

Karolos Seeger
kseeger@debevoise.com

Paris
+33 1 40 73 12 12

Frederick T. Davis
ftdavis@debevoise.com

Antoine F. Kirry
akirry@debevoise.com

Michael M. Ostrove
mmostrove@debevoise.com

The *ICID Review* is a publication of

Debevoise & Plimpton LLP

www.debevoise.com

Editor-in-Chief

Nicola C. Port
ncport@debevoise.com

Please address inquiries regarding topics covered in this publication to the editor or any other member of the Practice Group.

IN THE US Continued from page 1

Corporations conduct internal investigations to respond to allegations of financial malfeasance, to ensure compliance with anti-bribery and anti-fraud laws, to improve their internal controls systems, and to reduce potential penalties by demonstrating cooperation with regulatory investigations. The number of internal investigations spiked in the first half of this decade as a result of highly-publicized corporate scandals and stricter requirements and standards under SOX. Internal investigations have become even more commonplace over the past five years as the Securities and Exchange Commission (*SEC*) and the Department of Justice (*DOJ*) have embraced the FCPA as a tool for battling international bribery.

II. US laws that could trigger an investigation

Internal investigations tend to originate from a number of common sources, including: (1) allegations by company whistleblowers,[2] (2) results from internal or external audits,[3] or (3) evidence of wrongdoing identified by regulatory agencies,[4] the news media, or members of the company's board of directors.[5]

The following statutes may be implicated by allegations of corporate wrongdoing:

- **Foreign Corrupt Practices Act (*FCPA*):** The FCPA makes it unlawful to make or to promise a payment or to confer a benefit corruptly to a foreign official for the purpose of obtaining, retaining, or directing business to or for any person. Subject to varying jurisdictional requirements, this so-called anti-bribery provision applies to foreign and US issuers of securities, US companies and citizens, and any associated employees and representatives, as well as to any company or person violating the provision while in the territory of the US. The FCPA also contains accounting provisions that regulate an issuer's books-and-records and internal controls.[6]

The DOJ is responsible for all criminal enforcement of the FCPA and for civil enforcement of the anti-bribery provisions with respect to non-issuers and public companies. The SEC is responsible for civil enforcement of the FCPA with respect to public issuers. FCPA violations can result in significant fines and penalties: a company can be fined up to $2 million per criminal violation of the anti-bribery provisions, and an individual can be fined up to $250,000 per violation and/or 5 years imprisonment. Additionally, criminal violations of the books and records provisions can result in fines for companies up to $25 million and fines for individuals of up to $5 million and/or 20 years imprisonment.

CONTINUED ON PAGE 4

Links to related information:

FCPA Update

- August 2009 (click here)
- September 2009 (click here)
- October 2009 (click here)
- November 2009 (click here)

---

1 http://www.usdoj.gov/criminal/fraud/docs/dojdocb.html.

2 See Section V. Whistleblower Protection and Leniency for Cooperation, *supra*.

3 Title III of the Private Securities Litigation Reform Act of 1995 amends the Securities Exchange Act of 1934 by adding Section 10A, "Audit Requirements" (15 USC 78j-1), which requires that each independent audit of an issuer under the Exchange Act include: "Procedures designed to provide reasonable assurance of detecting illegal acts that would have a direct and material affect on the determination of financial statements amounts."

Under Section 10A, when an auditor detects or is notified by the company of information indicating that an illegal act has or may have occurred, the company may then be compelled by the auditor to conduct an independent investigation under the oversight of the Audit Committee. Additionally, if the auditor is not satisfied that the company has taken "timely and appropriate remedial action" to address any illegal acts discovered, the auditor may not be able to issue an opinion on the company's financial statements and may be required to resign from the engagement and/or notifiy the SEC of the matter.

4 See Section VI. Recent Regulatory Developments in the US, *supra*.

5 Under American corporate law, the fiduciary duties of officers and directors, including the duty of care, the duty of obedience, and the duty of loyalty, require that they make a reasonable effort to uncover all relevant information when notified of suspicious activity involving the above statutes or any other laws. Officers and directors must make an inquiry that an ordinarily prudent person would make under similar circumstances, which usually involves conducting an internal investigation. Officers and directors who do not address suspicious activity brought to their attention may become personally liable for breach of their fiduciary duties.

6 Although they lay dormant for many years, recently FCPA enforcement actions and penalties have skyrocketed and show few signs of declining. In 2004, there were only five combined FCPA enforcement actions filed by the DOJ and the SEC. In 2008, the number of FCPA enforcement actions peaked at 38, and the following year slightly dropped to 32. Correspondingly, there has also been a trend toward increased enforcement actions against individuals and greater financial penalties for corporate defendants. In 2008, 26 individuals were charged with new FCPA offenses, settled old enforcement actions, or had charges amended, reinstated, or affirmed in rehearings or on appeal. The total amount of FCPA penalties assessed in 2008 was over $516 million. The total amount of FCPA penalties in the first quarter of 2009 alone was greater than $400 million.

IN THE US Continued from page 3

- **Money Laundering Control Act:** In 1986, Congress passed the Money Laundering Control Act, which proscribes knowingly engaging in a financial transaction with the proceeds of an unlawful activity. The Act also applies extraterritorially by granting jurisdiction over foreign persons and institutions that commit an offense under the statute, if (i) the offense was committed while they were in the US; or (ii) the person or institution maintained a bank account at a financial institution in the US.

  Changes to this law were recently made through the Fraud Enforcement and Recovery Act of 2009 (*FERA*). FERA was designed to countermand a recent Supreme Court decision[7] that had effectively rendered unprofitable money laundering schemes not prosecutable by limiting the scope of the statute to the "profits" of crimes, rather than to their gross receipts. FERA manifests Congress's intent for the statute to cover all proceeds of illegal activity, including gross receipts, rather than just profits.

  The Money Laundering Control Act is enforced by the DOJ; there are many other anti-money laundering provisions that are also enforced by the SEC.[8] Violations of the Act may result in fines of up to the greater of $500,000 or twice the value of the illegal transaction, and/or prison sentences of up to 20 years.

- **Sarbanes-Oxley Act of 2002 (*SOX*):** SOX was passed in 2002 in the wake of various corporate scandals, establishing new accountability standards for public US companies and their executives. Section 302 requires Chief Executive Officers and Chief Financial Officers personally to certify and to assume responsibility for their company's financial statements and accounting. Section 304 addresses the forfeiture of certain bonuses and profits paid to executives at companies that are forced to restate financials due to material non-compliance with federal securities laws. This section can be used to disgorge bonuses or other performance-based compensation.

  All publicly traded companies in the US are subject to SOX requirements. Pursuant to the statute, the Public Company Accounting Oversight Board has the obligation and authority to send US audit inspectors to certain foreign audit firms to enforce the new accounting standards. SOX, thus effectively, has global reach – foreign companies that are publicly traded in the US must comply with the minimum audit standards established in the US, even if they are audited by foreign audit firms.

  SOX provisions are enforced by either the SEC or the DOJ, depending on the nature of the violation. Penalties for non-compliance vary depending on the individual provision but can amount to fines up to $1 million and prison sentences of not more than 20 years.

- **Sanctions imposed by the Office of Foreign Assets Control of the US Department of the Treasury (*OFAC*):** OFAC administers and enforces a set of economic and trade sanctions against, among others: (i) certain foreign countries and regimes (such as Cuba, Sudan, Iran, and North Korea); and (ii) designated individuals and entities believed to sponsor terrorism, to pose threats to US foreign policy, national security, or economy, or to engage in international narcotics trafficking.

  All US citizens or residents must comply with OFAC sanctions, regardless of where they are located around the world. OFAC sanctions also apply to US-based companies and, in certain situations, non-US subsidiaries of US companies. Failure to comply with OFAC sanctions may have significant adverse consequences under both US civil and criminal laws, including fines and imprisonment.

III. US enforcement authorities

The following enforcement authorities are charged with enforcing the laws specified above:

- **US Securities and Exchange Commission (*SEC*):** The Division of Enforcement is primarily responsible for executing the SEC's law enforcement function by launching investigations of securities law violations and bringing civil actions in federal court or before an administrative law judge.[9] When an investigation is commenced, the SEC gathers facts through voluntary cooperation (witness interviews and document production). Should the SEC commence a formal investigation, then the SEC may compel witnesses by subpoena to testify or to produce

CONTINUED ON PAGE 5

7 *United States v. Santos*, 128 S. Ct. 2020 (2008).

8 See "Anti-Money Laundering (AML) Source Tool for Broker-Dealers," *available at* http://www.sec.gov/about/offices/ocie/amlsourcetool.htm.

9 *Id.*

IN THE US Continued from page 4

records. Once a formal order of investigation is issued, the SEC may compel witnesses by subpoena to testify or to produce records. In most cases, the SEC and the party charged will settle the matter without trial.

- **US Department of Justice (*DOJ*):** The Fraud Section of the DOJ investigates and prosecutes alleged criminal violations of white collar laws. The DOJ frequently coordinates interagency and multi-district investigations within the US, as well as international enforcement efforts. Like the SEC, the DOJ can issue subpoenas and it encourages self-reporting and cooperation by companies and individuals.
- **Office of Foreign Assets Control of the US Department of the Treasury (*OFAC*):** OFAC acts under Presidential national emergency powers, as well as authority granted by specific legislation, to enforce sanctions by imposing controls on transactions and freezing assets under US jurisdiction.[10] Many of the sanctions are based on mandates from the United Nations and other international entities and involve close international cooperation.[11]

IV. Conducting an internal investigation in the US

A. Data protection in the US

Unlike the European Union, the US does not have a national comprehensive data protection regime, but instead follows a "sectoral" approach consisting of self-regulation, legislation, and state-level laws.[12] US employees do not benefit from the same kind of personal data protection as employees in EU countries. For example, emails sent on a company server are the property of the company, and employees typically have no expectation of privacy.

By comparison, the EU Data Protection Directive, implemented by each EU member state, is one of the toughest sets of data protection regulations in the world. It only allows for the transfer of personal data to a third country if that third country provides an "adequate" level of data protection.[13] Although the US does not meet the standard of "adequate" level of data protection imposed by the European Union, an agreement exists whereby US companies may qualify for a "safe harbor" exception to the EU Data Protection Directive by independently meeting the data protection standards required in Europe.[14] This safe harbor has allowed those qualifying companies with offices in both the US and Europe to transfer personal data, including data required for internal investigations and litigation, within the law.[15]

Companies subject to regulatory investigations should also consider the Freedom of Information Act (*FOIA*) when faced with US government requests for documents. Because FOIA requires federal agencies to comply with public requests for information, documents handed over to the government may become public unless confidentiality is specifically requested and particular privileges apply.

B. Employment law

Labor and employment laws do not play the same role in the US as in European countries. Private employment in the US is generally "at will," meaning that employees can be hired or fired at any time without cause, subject to a limited set of federal anti-discrimination laws (pertaining to age, sex, color, religion, national origin and disability) and potentially broader state laws.

During internal investigations, US employees can generally be interviewed by company counsel without the assistance of a lawyer.

C. Attorney-client privilege

The attorney-client privilege is designed to promote open, honest, and complete communication between a client and lawyer. The privilege applies to individual clients and institutional clients and exists only with respect to communications to, from, or with an attorney for the purpose of requesting or receiving legal advice.

The attorney-client privilege is not absolute – if the substance of the communication is disclosed to a third party, the privilege may be broken. This is relevant in the context of internal investigations because company counsel may decide to conduct interviews of company employees who are technically considered third parties. In 1981, the US Supreme Court carved out an exception to this rule in *Upjohn Company v. United States*, holding that the attorney-client privilege may be maintained between a counsel and a company-client even when the counsel communicates with company employees.[16]

CONTINUED ON PAGE 6

10 http://www.treas.gov/offices/enforcement/ofac/mission.shtml.

11 *Id.*

12 "European Union Safe Harbor Overview," *available at* http://www.export.gov/safeharbor/eu/eg_main_018476.asp.

13 *Id.*

14 *Id.*

15 *Id.*

16 *Upjohn Company v. United States*, 449 US 383, 386-396 (1981).

IN THE US Continued from page 5

It is vital, however, that before communicating with any employee, company counsel provide an explicit warning that the counsel does not represent the employee personally.[17] This disclaimer is very important, because if the employee reasonably believes that the company counsel's representation extends to him or her, the attorney-client privilege may attach to the employee, who may unilaterally block disclosure of privileged communications to US regulators or other third parties.

The US and Europe have different privilege rules governing the circumstances under which data may be turned over to the government or another third party. The attorney-client privilege is broader in the US than in many EU States; moreover, different rules may apply for outside counsel and in-house counsel. When a European company is subject to a government investigation in the US, it is therefore vital to ensure that any applicable privileges are not accidentally waived when complying with the government's requests for documents and information.

V. Whistleblower protection and leniency for cooperation

A. Protection of whistleblowers vis-à-vis company

In the US, voluntary disclosure of alleged legal violations is encouraged through federal whistleblower protection laws. Pursuant to Section 301 of SOX, audit committees of public companies are required to establish procedures for the "receipt, retention, and treatment of complaints" obtained by the companies regarding accounting, internal controls, and auditing. Furthermore, each audit committee has the authority to retain independent counsel or other advisors as needed. Many public companies have implemented hotline systems or other means by which employees can express anonymous concerns; responsibility for responding to major complaints has frequently been delegated to outside legal counsel or other independent counsel.

Section 806 of SOX provides a civil right of action for employees of publicly traded companies who face retaliation for providing information about, or participating in investigations relating to, alleged violations of securities laws on the part of their employers.[18]

SOX whistleblower provisions apply to all publicly traded companies subject to the registration or reporting requirements of the Securities Exchange Act of 1934, including foreign corporations.[19] The same protections also apply to private companies that are agents or contractors of publicly traded companies.

In addition, several SEC whistleblower policy changes have recently been enacted or proposed:

- President Obama's Financial Regulatory Reform Plan includes a proposal for a revised whistleblower protection program that would allow the SEC to compensate tipsters with money and immunity. Currently, such incentives for whistleblowing are only available for SEC insider trading cases.
- In March 2009, SEC Chairman Mary Schapiro announced that the SEC had enlisted the services of a federally funded research and development center to begin a comprehensive review of the SEC's whistleblower program, including the procedures the SEC uses to evaluate and act upon tips, complaints, and referrals.[20]
- The McCaskill Amendment to the American Recovery and Reinvestment Act (the $787 billion stimulus bill passed by the US Congress in 2009), provides additional whistleblower protections to employees of private companies that receive funding from the stimulus bill. Pursuant to the amendment, employees raising concerns about waste or mismanagement of stimulus funds are protected from retaliation and are provided with the right to jury trials, compensatory damages, and investigations by the Inspector General.

B. Leniency from authorities through cooperation

Companies and individuals can benefit from cooperation with US regulatory agencies, with the expectation that they will receive a lighter sentence or lesser fine. In criminal cases, the plea bargain is a prosecutorial tool that has become well-established and widely used in the United States.[21] In return for the defendant's

CONTINUED ON PAGE 7

17 This disclaimer has come to be known as the "Upjohn warning."

18 Since Congress passed SOX in 2002, over 1,000 corporate employees have filed complaints under the law with the US Department of Labor (*DOL*), which investigates and adjudicates whistleblower claims. Although the DOL has dismissed the majority of these cases, a significant number have resulted in settlements between whistleblowers and companies.

19 Although SOX (which clearly has international reach) provides comprehensive whistleblower protection, US courts have been divided as to whether those provisions extend to foreign national workers employed by the overseas subsidiaries of US companies. *See Carnero v. Boston Scientific Corp.*, 433 F.3d 1 (1st Cir. 2006), cf., O'Mahony v. Accenture Ltd., No. 07-7906 (S.D.N.Y. Feb. 5, 2008).

20 SEC Press Release, March 5, 2009, *available at* http://www.sec.gov/news/press/2009/2009-44.htm.

21 By contrast, American-style plea bargains have not been widely used throughout most of Europe until very recently. See ICID Review articles for France, Germany, and the United Kingdom.

IN THE US Continued from page 6

waiver of his constitutional right to trial, the defendant pleads guilty and may expect reduced punishment.

Plea bargains and settlements of companies and individuals in the context of internal investigations may take the shape, *inter alia*, of deferred prosecution agreements, non-prosecution agreements, or witness assurance letters. In the case of deferred- or non-prosecution agreements, the DOJ will postpone or forego prosecution. The DOJ and SEC may also require actions ranging from an injunction on certain activities to fines or disgorgement of profits to a period of independent monitoring and continued cooperation with the investigation.[22]

The SEC Division of Enforcement recently encouraged the wider use of witness assurance letters. Section 3.3.5.3.1. of the SEC Enforcement Manual authorizes the SEC staff to "provide a witness with a letter assuring him or her that the SEC does not intend to bring an enforcement action against him or her or an associated entity. In return, the witness agrees to provide testimony and documents and information."[23] Such witness assurance letters must be expressly approved by the Commission, but are another sign that the SEC has become more keen to cooperate with individuals.

VI. Recent regulatory developments in the US

A number of recent developments have sought to increase the powers of regulators, or to make them more effective:

- On February 20, 2009, the SEC adopted a rule to adjust for inflation the maximum civil monetary penalty amounts for various acts it administers. This new rule will increase the maximum amount of potential civil penalties assessed under the FCPA, as well as every other law enforced by the SEC, and will bring companies under greater pressure to strengthen their compliance programs.
- In February 2009, Chairman Schapiro announced the end of a two-year-old pilot program that required SEC staff to obtain pre-approved settlement ranges from the Commission before engaging in settlement negotiations in cases that involved civil monetary penalties as a sanction for securities fraud. It is widely believed that this pilot program suppressed both the number of settlements and the average amount of each settlement. In the first quarter of 2009, since the end of the pilot program, the average SEC settlement has already skyrocketed past last year's average.
- Chairman Schapiro recently implemented a plan to expedite formal orders of investigation, which authorize the SEC staff to issue subpoenas. Under the new SEC policy, only one Commissioner is required to authorize a formal order, whereas previously the entire Commission had to vote on the issuance of formal orders. This policy change will likely lead to an increase in the number of investigations advanced beyond the initial preliminary stages.
- On August 5, 2009, SEC Division of Enforcement Director Robert Khuzami gave a speech announcing several major initiatives of the enforcement division, including the following:[24]
  - *Specialization* – The SEC will create national units dedicated to particular highly specialized and complex areas of securities law. The specialized units, to be headed by unit chiefs, will include: (i) the Asset Management Unit; (ii) the Market Abuse Unit; (iii) Structured and New Products; (iv) Foreign Corrupt Practices Act; and (v) Municipal Securities and Public Pensions.
  - *Fostering cooperation by individuals* – The SEC will increase its incentives to individuals to cooperate with the agency, including use of immunity and rewards for whistleblowers.
- FERA has appropriated additional funds for the fighting of securities, mortgage and other financial institution frauds, as well as frauds against federal assistance and relief programs. Budget funding for the DOJ, SEC, and FBI will increase as a result. ■

---

22 The threat of criminal prosecution and incentives for voluntary cooperation have proven effective tools in the fight against corporate fraud. Mark Mendelsohn, the Deputy Chief of the Fraud Section in the DOJ's Criminal Division, stated at a conference in November 2009 that the DOJ had, at that time, 130 open FCPA investigations. Approximately 25% of those matters were initiated through voluntary disclosure, which has been promoted by the US Sentencing Commission as a factor for decreased punishment, by the DOJ's *Thompson* and *McNulty* memoranda as a factor in the decision to prosecute, and by the SEC's *Seaboard Report* as a criterion in the decision to bring an enforcement action.

23 US Securities and Exchange Commission Division of Enforcement, *Enforcement Manual*, October 6, 2008, *available at* http://www.sec.gov/divisions/enforce/enforcementmanual.pdf.

24 Robert Khuzami, "Remarks Before the New York City Bar: My First 100 Days as Director of Enforcement," August 5, 2009, *available at* http://www.sec.gov/news/speech/2009/spch080509rk.htm.

IN THE UK Continued from page 1

This is particularly so in the field of anti-corruption, where an increase in corporate internal investigations can be expected. It is of particular note, in this context, that Richard Alderman, Director of the Serious Fraud Office (*SFO*), the lead agency responsible for investigating and prosecuting cases of serious fraud and corruption, recently stated:

> *"What I want to see in suitable cases is corporates identifying a corruption issue and then bringing in their advisers to conduct a rigorous investigation. At some point in this process (and views vary as to when) I want the corporate to engage us about a suitable resolution."*[1]

His remarks are indicative of the SFO's new "carrot and stick" approach, where tougher enforcement actions will be complemented by a culture in which self-investigating and self-reporting corruption is very seriously encouraged. Similar pronouncements forecasting a more robust approach have been made by the Financial Services Authority (*FSA*), the United Kingdom's financial services regulator. Both the SFO and the FSA have already increased their staff by 20-30%, which included the hiring of a well-known criminal QC by the SFO and the former Director of the Fraud Prosecution Service (a division of the Crown Prosecution Service) by the FSA. The SFO has set up a separate work unit for its anti-corruption efforts (the Anti-Corruption Domain), to which it is dedicating significant resources and which it expects to increase to a staff of 100. New laws already enacted and future laws that are planned will give the authorities more powers and are likely to make for a fundamental change in the approach to, and practice of, corporate internal investigations in the UK.

II. UK laws that could trigger an investigation

Allegations of corporate wrongdoing that trigger internal investigations can stem from a wide variety of sources, but commonly include: (i) tip-offs from company whistleblowers; (ii) a company's self-reporting to the regulator;[2] (iii) a Suspicious Activity Report made to the Serious Organized Crime Agency (*SOCA*) by either the company or a third party,[3] or (iv) the findings of an internal or external audit.

- The UK has four different laws relating to the prosecution of corruption, in addition to the common law offense of bribery: the Public Bodies Corrupt Practices Act 1889, the Prevention of Corruption Act 1906, the Prevention of Corruption Act 1916, and the Anti-Terrorism, Crime and Security Act 2001. The 1889, 1906 and 1916 Acts together apply both to public bribery but also to bribery in the private sphere. Unlike US corrupt practices laws, the UK bribery offenses are broadly based on an agency concept, the relevant test being the corrupt giving or agreeing to give consideration to an agent (or conversely, the receiving or agreeing to receive such consideration by the agent) as an inducement or reward for doing or omitting to do any act in relation to his principal's affairs.
- Section 108 of the Anti-Terrorism, Crime and Security Act 2001 seeks to give effect to the UK's obligations

Links to related information:

Client Updates:

- UK Serious Fraud Office Releases Guidelines on Self-Reporting of Overseas Corruption (Click here)
- The Draft Bribery Bill (Click here)

Speeches:

- Lecture given by Richard Alderman at Debevoise's First Annual ICID Lecture (Click here)
- Address given by Lord Goldsmith QC at The 27th Cambridge International Symposium on Economic Crime (Click here)

1 Richard Alderman, "Talking Corruption with the SFO", October 20, 2009, Debevoise & Plimpton LLP's First Annual ICID Lecture. *Available at*: http://www.sfo.gov.uk/about-us/our-views/speeches/speeches-2009/talking-corruption-with-the-sfo.aspx.

2 Although there is no explicit duty of directors to investigate suspicions of wrongdoing, the directors' duties of care, skill and diligence and of promoting the success of the corporation would require that a director investigate such allegations and, if necessary, report them to the appropriate regulator.

3 Such suspicious transaction reports are required by the market abuse regime and the anti-money laundering regime, amongst others.

IN THE UK Continued from page 8

under the OECD Convention on Combating Bribery of Foreign Public Officials in International Business Transactions to criminalise the bribery of foreign public officials. The 2001 Act applies equally to public and private bribery. It provides that if a UK national (or a body incorporated under UK law) performs any act outside the UK which would, if performed in the UK, be a corruption offense, then that person is liable in exactly the same way as if the offense had been committed within the UK. Until its enactment in 2001, the UK bribery laws did not have extraterritorial application.

- Suspicions of the commission of any of the money laundering offenses set out in the Proceeds of Crime Act 2002.
- Allegations of market abuse contrary to sections 118 or 397 of the Financial Services and Markets Act, or other allegations of breaches of the financial regulatory regime, such as the FSA's Principles for Businesses.
- Allegations of breaches of European Union and UK competition law, such as the Competition Act 1998 and the Enterprise Act 2002.[4]

III. UK enforcement authorities

The enforcement authorities charged with investigating breaches of these laws are:

- **Serious Fraud Office (*SFO*):** The SFO is the lead investigating agency for cases of serious fraud and corruption, and in particular overseas corruption. The SFO is a governmental department and accountable to the Attorney General. The SFO has jurisdiction over England, Wales and Northern Ireland, but not Scotland, the Isle of Man or the Channel Islands.

  The SFO is empowered to investigate any suspected offense which the Director of the Serious Fraud Office considers on reasonable grounds to constitute serious or complex fraud. The SFO's key criterion for whether to accept a case is that the suspected fraud must appear so serious and complex that its investigation should be carried out by those responsible for its prosecution.[5] The SFO has the power to conduct such investigations independently, or in conjunction either with the police or any other person that the Director considers appropriate. The SFO also may require a person to answer questions, provide information or produce documents for the purposes of an investigation.

  In addition to carrying out investigations, the SFO is also empowered to prosecute cases of serious or complex fraud, or to take over the conduct of such proceedings at any stage.[6] The SFO may seek civil and criminal remedies, including Civil Recovery Orders (*CROs*), which can be issued following a determination that property has been obtained as a result of unlawful conduct.[7]

  On September 25, 2009, the SFO announced its first successful prosecution of a company for overseas corruption, when the bridge-building firm Mabey & Johnson was fined £6.6 million after it admitted paying bribes to public officials in Jamaica and Ghana and breaching United Nations sanctions.[8]

- **Financial Services Authority (*FSA*):** The FSA is responsible for enforcing the Financial Services and Markets Act (*FSMA*), together with the FSA's own rules.[9] More generally, however, the FSA is obliged to fulfil its four statutory objectives (set out in FSMA), among which is to reduce

CONTINUED ON PAGE 10

4 Such an investigation was recently launched into alleged fraudulent and anti-competitive conduct on the part of JJB Sports and Sports Direct.

5 The factors to be taking into account in making this determination are: (i) whether the value of the alleged fraud exceeds £1 million; (ii) whether there is a significant international dimension; (iii) whether the case is likely to be of widespread public concern; (iv) whether the case requires highly specialized knowledge (e.g. of financial markets); and (v) whether there is a need to use any of the SFO's special powers.

6 The Crown Prosecution Service would be responsible for investigating and prosecuting more low-level examples of fraud and corruption.

7 In order to obtain a CRO, it is not necessary for the SFO to establish an offence against a particular company or individual. The SFO has had the power to seek such orders since April 2008, and deployed them for the first time in October 2008, when a CRO for £2.25 million was made against construction firm Balfour Beatty in respect of payment irregularities stemming from the dealings of one of its former subsidiaries in Egypt. In this case, Balfour Beatty self-reported the payment irregularities to the SFO, and consented before the court to the imposition of the CRO.

8 See the SFO's press release of September 25, 2009, *available at* http://www.sfo.gov.uk/our-work/latest/mabey--johnson-ltd-sentencing-.aspx.

9 Although the SFO is the primary investigating agency for instances of overseas corruption, the enforcement of the FSA's rules can lead to the FSA taking a role in cases involving overseas corruption, such as the fine that it imposed on Aon Ltd in January 2009 – discussed further below – for breach of the FSA's Principles for Businesses.

IN THE UK Continued from page 9

financial crime. This can lead to the FSA taking a role in cases which involve neither FSMA nor the FSA's rules, such as insider dealing contrary to Part V of the Criminal Justice Act 1993. In carrying out its objectives, the FSA can act both as a regulator (for example, by imposing financial penalties for market abuse, withdrawing a firm's authorization or disciplining authorized firms and authorized persons) and as an investigator and prosecutor. (For example, by applying to the court for injunction and restitution orders, and prosecuting the criminal offenses of insider dealing and market abuse.) It appears that, in appropriate cases, the FSA will work in conjunction with the SFO, although there is no formal memorandum of understanding between the two agencies.[10]

- **Serious Organized Crime Agency (*SOCA*):** SOCA is an executive body sponsored by, but operationally independent from, the Home Office. SOCA has the power to institute criminal proceedings in England, Wales and Northern Ireland, and to act in support of the activities of any police force or law enforcement agency, if so requested.

  SOCA's responsibilities include fighting organized crime and the proceeds of crime, both of which are relevant in the context of investigations. In relation to organized crime, SOCA focuses on fraud and money laundering carried out by organized gangs. As for the proceeds of crime, SOCA's key role is to receive and investigate Suspicious Activity Reports (*SARs*). Such reports form part of the UK's anti-money laundering regime, and can be made as soon as there is a suspicion by a designated reporter that criminal proceeds exist. It is notable that the £5.25 million fine which was imposed on Aon Ltd. by the FSA in January 2009 followed the issuance of an SAR to SOCA.[11]

- **Office of Fair Trading (*OFT*):** The OFT, a non-ministerial government department, is the UK's competition regulator. Like the FSA, the OFT has the power to act as a regulator (for example by imposing heavy fines) and as an investigating authority.

IV. Conducting an internal investigation in the UK

A. Data protection in the UK

The EU Data Protection Directive,[12] which specifies the mandatory protections pertaining to the processing and transfer of personal data, was implemented in the UK through the Data Protection Act 1998 (DPA). Schedule 1 to this Act sets forth eight data protection principles in relation to personal data, of which the most important are the first and eighth principles. The first principle requires that data be processed fairly and lawfully, while the eighth provides that personal data cannot be transferred to a country or territory outside of the European Economic Area unless: (i) the country or territory in question ensures an "adequate level of protection" for personal data, or (ii) one of the exceptions listed in Schedule 4 to the Act applies.[13]

While the UK's implementation of the EU Directive is broadly in line with that in other Member States, it is appropriate to note that the term 'personal data' itself has been interpreted differently in the UK than in other EU States. While other EU States have tended to interpret this term broadly, the Court of Appeal in the *Durant*[14] case rejected a very broad understanding of this term (to mean effectively any data capable of identifying a person) and opted for a more restrictive interpretation to the effect that personal data consisted only of information which affected a person's privacy, whether in his personal or family life, business or professional capacity.[15]

CONTINUED ON PAGE 11

10 Cooperation between the SFO and FSA is discussed in the following article: http://www.compliancereporter.com/Article.aspx?ArticleID=2270085.

11 For details of this, see the FSA's press release on the matter, *available at* http://www.fsa.gov.uk/pages/Library/Communication/PR/2009/004.shtml.

12 Directive 95/46/EC.

13 These exceptions include: (i) the transfer being necessary for the performance of a contract between the data subject and the data controller; (ii) the transfer being necessary for reasons of substantial public interest, and (iii) the transfer being necessary for the purpose of, or in connection with, any legal proceedings.

14 Durant v Financial Services Authority [2003] EWCA Civ 1746.

15 In determining whether or not data affected a person's privacy, the Court of Appeal held that two notions were of assistance: (i) whether the information is biographical in a significance sense, i.e. going beyond the recording of the putative data subject's involvement in a matter which has no personal connotations; and (ii) the focus of the data, i.e. whether or not the data had the putative data subject as its focus.

IN THE UK Continued from page 10

Despite this more restrictive definition, however, data protection considerations will still be highly relevant to conducting an internal investigation in the UK, if this will involve the collection and review of employees' emails and files. In particular, the DPA requirements relating to sensitive personal data[16] and transfer of data to countries outside of the EU will merit careful consideration.

B. Employment law

A related topic to that of data protection law is the effect of UK employment law on internal investigations. An employer owes a duty of confidentiality to its employees, which is quite separate from any duties owed as a result of the DPA. To the extent that an employer discloses confidential information about employees during the course of an investigation – even if it does not fall within the definition of personal data under the DPA – the employer may have breached its duty to its employee.

Employment law could also impact investigations as a result of the mutual duty of trust and confidence implied in every employment relationship. A breach of this duty by an employer may entitle an employee to resign and claim constructive dismissal. It is therefore advisable to seek employment law advice in order not to fall foul of this duty of trust and confidence in conducting an internal investigation in the UK.[17]

C. Attorney-client privilege

The principle of legal professional privilege has to be taken into account in determining the scope of information that can be handed over to an investigating authority during the course of an investigation. There are two parts to the UK principle of legal professional privilege: legal advice privilege and litigation privilege. For present purposes, legal advice privilege is the most relevant.

Legal advice privilege applies to confidential communications between a party and its lawyer for the purpose of giving or receiving legal advice. The privilege is not confined to telling the client the law; it has also been held to include "*advice as to what should prudently and sensibly be done in the relevant legal context.*"[18] This principle would seem to include advice on the presentation of the results of an internal investigation. A lawyer's drafts, working papers and memoranda are also covered by legal advice privilege.[19]

Current case-law gives a narrow definition of 'client' for these purposes: the 'client' has been limited to only those individuals specifically instructed to handle the case or inquiry at issue, rather than the organization as a whole.[20] This point will need to be considered whenever privileged material is distributed by the lawyers conducting the internal investigation.

It is appropriate to note, however, that there are no specific cases applying the principles of privilege in the context of corporate internal investigations. It is, thus, not possible to say with absolute certainty how the rules of legal professional privilege would be applied to internal investigations.

V. Whistleblower protection and leniency for cooperation

A. Protection of whistleblowers vis-à-vis company

UK whistleblowers can be protected from sanctions by their employer if they make certain disclosures which they reasonably believe demonstrate any of a number of situations, including (i) that a criminal offense has been committed; (ii) that malpractice has been committed (or is likely to be committed); or (iii) that a miscarriage of justice has occurred.[21] It is

CONTINUED ON PAGE 12

16 Sensitive personal data is defined in the DPA as personal data consisting of information as to, (i) the racial or ethnic origin of the data subject; (ii) his political opinions; (iii) his religious or other beliefs; (iv) whether or not he is a member of a trade union; (v) his physical or mental health or condition; (vi) his sexual life; (vii) the commission or alleged commission by him of any offence; and (viii) any proceedings for any offence committed or alleged to have been committed by him, the disposal of such proceedings or the sentence of any court in such proceedings.

17 An example of such a breach might be when an employer acts improperly in relation to personal data or confidential information (aside from the obligations under the DPA and the duty of confidentiality which have already been discussed).

18 *Balabel v Air India* [1988] 2 All ER 246, quoted with approval in *Three Rivers District Council and others v Governor and Company of the Bank of England* [2004] UKHL 48 ("*Three Rivers 6*"). *Three Rivers 6* involved advice given by a firm of solicitors to the Bank of England during the course of an inquiry into the Bank of England's supervision of a bank (BCCI) which collapsed as a result of massive fraud. The House of Lords held that legal professional privilege applied not only to advice given as to the state of the law, but also to advice as to how the Bank of England might best present information to the inquiry.

19 *Three Rivers District Council and others v Governor and Company of the Bank of England* [2003] EWCA Civ 474 ("Three Rivers 5").

20 *Three Rivers 5*, *ibid.*

21 Public Interest Disclosure Act 1998, which inserted various provisions into the Employment Rights Act 1996.

IN THE UK Continued from page 11

generally contemplated that the disclosures in question be made to the employer itself, or to a prescribed regulator (such as the Financial Services Authority or Her Majesty's Revenue and Customs). However, broader (public) disclosures are also permitted, although a higher threshold has to be crossed in order for such disclosures to be allowed; specifically, the disclosure must not only be made in good faith, but the person making the disclosure must also believe that the information disclosed, and any allegations in it, are substantially true.[22]

B. Leniency from authorities through cooperation

Historically, plea bargaining has not played a role in the enforcement of criminal laws in the UK. There are signs that this is changing, with the Attorney General having recently issued guidelines on the conduct of plea bargaining in cases involving serious or complex fraud, replacing the informal system of plea discussions which had existed beforehand (and which still exists in all other cases). These guidelines require the prosecutor to act openly, fairly and in the interests of justice, and set out the process by which the plea discussions ought to be initiated and conducted, which includes specifying the various documents which should pass between the prosecutor and the defendant. The guidelines envisage that all matters which are agreed between the prosecutor and the defendant should be reduced to a written plea agreement. Together with supporting information, this agreement is then placed before the judge, who then has absolute discretion as to whether the pleas agreed by the parties ought to be accepted.[23]

The recent shift by the SFO towards a regime in which self-investigating and self-reporting corruption will be viewed as a very major consideration in the decision to prosecute a corporation, as well as discussing pleas with the suspect companies, suggests a growing importance of this issue of plea bargaining.

The SFO issued guidelines in July 2009 on the self-reporting of corruption, which provide that if a company self-reports instances of corruption, the SFO will take this into account and endeavour to settle the case civilly, rather than criminally, if at all possible.[24] By contrast, if the company does not come forward and the SFO discovers the corruption by other means, this will be treated as a significant negative factor, making a criminal prosecution more likely.

The recent successful prosecution of Mabey & Johnson provides further insight into the SFO's approach in this area. In its opening note in this case,[25] the SFO set down a clear marker that it would reward cooperation. More importantly, the SFO also gave some insight into what it considered cooperation to entail, stating that the preferred approach was for a company subject to allegations of corruption to conduct an internal investigation, before disclosing all of the results of that investigation (whether or not privileged) to the SFO. The SFO stated:

> *"Importantly, and in the spirit of exemplary and proper co-operation, the Company provided copies of privileged notes of internal interviews of certain directors and employees, conducted during the internal investigation.* ***As an aside, the SFO regards this approach, namely conducting an internal investigation which is then fully disclosed to the SFO as meriting specific commendation. In cases where this is not the practice of the suspect company, the SFO will not regard the co-operation as a model of corporate transparency*** *(emphasis added)."*[26]

Further, the SFO made the following general statement on its policy of cooperation:

> *"…the policy of the SFO under the present Director…is that boards of companies should be encouraged to approach the SFO and make a full disclosure of fraud or corruption they have discovered together with proposals about the changes and monitoring needed in the future to re-assure the public that the behaviour of those companies meet the highest ethical standards.* ***If companies do this then the SFO is prepared to discuss with them the pleas or other resolution that the SFO considers to be in the public interest****" (emphasis added).*[27]

CONTINUED ON PAGE 13

22 Section 43F Employment Rights Act 1996.

23 Attorney General's Guidelines on plea discussions in cases of serious or complex fraud, *available at* http://www.attorneygeneral.gov.uk/Publications/Pages/AttorneyGeneralsGuidelines.aspx.

24 *Available at*: http://www.sfo.gov.uk/bribery--corruption/self-reporting-corruption.aspx.

25 *Available at* http://www.sfo.gov.uk/media/41953/sfo-annex2-statement-01-250909.pdf.

26 *Ibid*. at paragraph 26.

27 *Ibid*. at paragraph 20.

IN THE UK Continued from page 12

The SFO's intention to try and settle cases civilly wherever possible is vitally important to companies operating in the EU that may otherwise face the risk of a criminal conviction. Under Article 45 of the EU Public Procurement Directive (18/2004/EC),[28] companies found guilty of certain offenses, including corruption and money laundering, are automatically and perpetually barred from participating in public contracts. This bar is imposed regardless of the seriousness of the offense, and despite any mitigating factors. Concern has recently been expressed in the UK (including by the Secretary of State for Justice) that despite the expressed intention to settle self-reported cases civilly, the strictness of the "Article 45" rules may nevertheless be prohibitive in encouraging companies to self-report instances of corruption.
In the field of UK competition law, the OFT may offer lenient treatment to businesses who report the existence of a cartel with which they are involved. Such leniency could lead to the financial penalty to which such a company would otherwise be subject being reduced, or even eliminated altogether.[29]

VI. Recent regulatory developments in the UK

There have been a number of significant developments in the UK, which will impact the legal and enforcement regime in which internal investigations are conducted. These developments include:

- The sweeping changes to UK anti-corruption law that have been proposed. In the Queen's speech in November 2009, the government presented to Parliament a Bribery Bill that would seek to replace the existing statutes with a single statutory regime, based around two general offenses which do not distinguish between public and private bribery: one of paying bribes, and the other of receiving them. The Bill also seeks to create two new offenses: bribery of a foreign public official and a corporate offense of failure to prevent bribery by a "commercial organization."
- Although the UK already sought to give effect to its obligations under the OECD Convention by virtue of the 2001 Act (discussed above), that Act simply gave extraterritorial application to the existing laws. The Bill goes further by providing for a specific new offense of bribery of a foreign public official. It is also appropriate to note that while only UK citizens or corporations are currently subject to the anti-corruption laws, under the new Bill this is extended to individuals ordinarily resident in the UK.
- Two main points need to be made about the new corporate offense of failure to prevent bribery: *First*, the Bill envisages that a company can avail itself of a defense of "adequate procedures" to prevent bribery in certain circumstances. This is expected to raise the stakes considerably in the field of corporate compliance and ethics training programmes.[30] *Second*, the offense applies to "commercial organizations" which is said to include foreign corporations or partnerships carrying on business in the UK. This will make the UK's corporate anti-corruption laws of potentially very wide application and will now affect companies that have hitherto chosen to ignore the UK's anti-corruption regime.
- The SFO's guidelines on self-reporting of corruption and the SFO's new enforcement approach, as evidenced by its first ever corporate bribery prosecution and conviction in the case of Mabey & Johnson (both discussed above).
- Proposals to give the FSA power to grant statutory immunity.[31] At present, the FSA only has power to grant immunity at common law, which is not capable of binding other prosecutors.
- Explicit attempts by Richard Alderman, the Director of the SFO, for the SFO to work more closely with their US counterparts in the Department of Justice.[32]
- Pledges by both the FSA and the SFO that they will become more effective enforcers of the law proceedings. ■

28 As given effect in the UK by Regulation 23 of the Public Contracts Regulations 2006 and Regulation 26 of the Utilities Contracts Regulations 2006.

29 See the OFT guidance on leniency, *available at* http://www.oft.gov.uk/news/press/2008/144-08.

30 It is to be noted that when the draft Bill was first introduced to Parliament it provided for an offense of negligent failure to prevent bribery by a commercial organization. However, following representations which were made to the Joint Parliamentary Committee on the Bribery Bill – see Debevoise client update of 29 September 2009 – this has now been turned into a strict liability offence (subject to the adequate procedures defence).

31 The proposal can be found in section 71 of the Coroners and Justice Bill

32 The recent $579 million settlement of US Foreign Corrupt Practices Act charges by Halliburton and its former subsidiary Kellogg, Brown and Root, which followed an investigation featuring close cooperation between the Department of Justice and the SFO, is an example of such cooperation at work.

IN FRANCE Continued from page 1

As the concepts of plea bargaining and settlement in criminal matters do not exist in the French legal system (with a minor exception for misdemeanors), cooperation or even a purely internal investigation by the company may actually backfire if not handled correctly. An internal investigation may be seen, under certain circumstances, to be intruding on "official" investigations; and an investigating magistrate may even perceive an internal investigation as an attempt to exercise undue influence on a witness and/or to tamper with or to destroy evidence.

As explained below, regulatory and criminal investigations are carried out separately and independently by distinct governmental actors. Due to different prerogatives and means of investigating in administrative and criminal investigations, the information gathered may vary significantly from one investigation to another. Defense strategies, therefore, must be carefully tailored.[1]

II. French laws that could trigger an investigation

Anti-corruption laws. France has ratified a number of international anti-corruption conventions over the past 12 years[2] and has laws prohibiting foreign and domestic, active and passive, bribery:

- In 2001, following the ratification of the European Union and OECD conventions, France incorporated **anti-corruption legislation** into its criminal and criminal procedure codes.[3] Since November 2007, the French criminal code broadly lists foreign officials covered by the anti-corruption laws as "a person holding public office, discharging a mission of public interest or an electoral mandate" in a foreign country or international organization.[4]
- In July 2005, a new chapter was introduced in the French criminal code[5] that targets **private corruption** (i.e., the acceptance and solicitation of a benefit to carry out an act in the scope of a person's "activity or function" or facilitated by such "activity or function" in violation of his/her "legal, contractual or professional obligations").
- **Money laundering** is an *infraction de conséquence* under French law, i.e., an offense that stems from another one. Although there has been no recent change in jurisprudence or legislation on the issue, private and/or public corruption lead to money laundering offenses under French law, which provide separate grounds for sentencing.
- The absence of a historic focus on corruption in France may result from the investigative authorities' attention to other white collar crimes, such as embezzlement, general misuse of corporate assets, insider trading and organized crime.[6]

III. French enforcement authorities

- Under current procedure, the **investigating magistrate** (*juge d'instruction*) is the main actor in a criminal investigation.[7] The Public Prosecutor's office can request the appointment of an investigating magistrate, or a private party's civil complaint can lead to an appointment. The investigating magistrate can be assisted by the police in its fact-finding mission. Once appointed, the investigating magistrate is completely independent and cannot be ordered to extend or narrow the scope of the investigation. The work and documents in the investigating magistrate's criminal file are confidential and can be accessed only by defendants who have been formally charged (*mis en examen*, i.e., targets of the investigation), assisted witnesses (*témoins assistés*, i.e., witnesses who may, in the magistrate's

CONTINUED ON PAGE 15

1 For example, if pattern(s) under investigation by the *Autorité des Marchés Financiers* (*AMF*, the French equivalent to the Securities and Exchange Commission) amount to a criminal offense, the AMF will inform the office of the Prosecutor, who will decide whether or not to appoint a magistrate to investigate the matter. If a criminal investigation is launched, the two investigations will be carried out separately and simultaneously (interviews, document collection, experts, etc.). The work product from the criminal investigation normally will not be available to the AMF or any party that is not a subject or target of the criminal investigation.

2 France ratified the anti-corruption conventions prepared by the European Union (in 1997), the Council of Europe (in 2005), the OECD (in 2000) and the United Nations (in 2005).

3 Law n°2000-595 of June 30, 2000.

4 Law n°2007-1598 of November 13, 2007; see Arts. 435-1 and following of the French criminal code.

5 Art. 445-1 and following of the French criminal code.

6 E.g., Law n°2004-204 of March 9, 2004.

7 There are current discussions in the government which will likely lead to the investigating magistrate being abolished in the near future and the lead over criminal investigations being placed under the authority of the Public Prosecutor's office.

IN FRANCE Continued from page 14

opinion, be charged at some point in the investigation), and parties who have joined the criminal investigation by bringing a civil suit (*parties civiles*). If a company is formally charged, or is considered an assisted witness or a civil party to an investigation, its lawyers will have full access to the file.[8]

- The **financial market regulator** (*AMF*, mentioned in footnote 1) "conducts inspections and investigations" at the instigation of its Secretary General, after observations made in the course of market "surveillance or monitoring," in response to complaints, or "at the request of foreign authorities with equivalent jurisdiction."[9] Based on the report of an investigation, the AMF's board may decide to refer the matter to the Enforcement Committee (*Commission des sanctions*). That committee will impose appropriate sanctions after taking additional investigative steps and holding a hearing.
- In 2001, following the transposition of an anti-money laundering European Directive, the **French Financial Intelligence Unit** (*Tracfin*) was created under the supervision of the Ministry of Finance. New article L. 561-15 of the French Monetary and Financial code created an obligation for a number of professionals (including banks, insurance companies, accountants, auditors and lawyers) to report to *Tracfin* any suspicion of money laundering connected either to offenses punishable by a prison term of one year or more (which includes tax evasion) or to the financing of terrorism.[10] When *Tracfin* determines that a pattern amounts to a criminal offense, it reports the pattern to the Public Prosecutor. *Tracfin* is a member of the Egmont Group and has signed agreements with 31 other FIUs.[11]

IV. Conducting an internal investigation in France

A. Blocking Statute

The French **Blocking Statute** prohibits all persons from requesting, seeking or disclosing any financial, commercial or economic information for the purpose of constituting evidence in view of foreign judicial or administrative proceedings or in the context of such proceedings.[12] Violations of the statute are punishable by a six-month jail term and an €18,000 fine. The objective of the statute was to target the extraterritorial application of foreign laws in connection with overly burdensome litigation (e.g., involving extensive discovery). A recent French Supreme Court decision[13] and a notice issued by a French government agency[14] have increased awareness of the statute, which for many years had been largely unenforced. Another recent Supreme Court decision confirmed that the law applies extraterritorially, although the modalities of its application remain unclear.[15]

The Blocking Statute includes an exception from its coverage when data is sought within the framework of a treaty.[16] Similarly, if it is clear that the collection of data is not for the purpose of constituting evidence "in view of" a foreign proceeding, the Blocking Statute does not apply. Thus, purely internal investigations are permissible if there is no intention to turn the results of that investigation over to a foreign regulatory

CONTINUED ON PAGE 16

8 Importantly, a witness who is not an assisted witness has no right to counsel during the interview by the police, even after an investigation has been opened. This makes preparation all the more important.

9 http://www.amf-france.org/ (the AMF's website has an English version).

10 Art. 2 of Ordonnance n°2009-104 of January 30, 2009 established reporting requirements and sanctions for non-performance, codified at Art. L. 561-1, and following of the Monetary and Financial Code.

11 *http://www.tracfin.minefi.gouv.fr/* (Tracfin's annual reports are available online.)

Tracfin has signed bilateral agreements with FIUs in the United States (FinCEN), the United Kingdom (NCIS), Italy (DIA), Switzerland (MROS) and Russia (FMC). In 2007, *Tracfin* made 882 requests for information from other FIUs and answered 883 requests for information from other FIUs.

12 Law no. 68-678 of July 26, 1968, modified by Law no. 80-538 of July 16, 1980 (JO July 17, 1980).

13 Cass. Crim. Dec. 12, 2007, case 07-83228 (affirming a decision of the Paris Court of Appeal convicting a Franco-American lawyer on charges of violating the Blocking Statute).

14 Notice on the Blocking Statute issued by the French Government (The High Representative in Charge of Economic Intelligence) on September 18, 2007, *available at:* http://www.intelligence-economique.gouv.fr/article.php3?id_article=348&var_recherche=1980.

15 Cass. Crim. Jan. 30, 2008, case 06-84098 (affirming a decision finding no violation of the Blocking Statute but confirming that the law can apply even where no element of the alleged infraction took place on French territory).

16 The Hague Convention of March 17, 1970 on the taking of evidence abroad in civil or commercial matters is the treaty envisioned by the drafters of the Blocking Statute.

IN FRANCE Continued from page 15

authority. If an investigation is conducted with the expectation that the results will be reported to a foreign regulatory authority, however, then the Blocking Statute will apply.

B. Data protection in France

The transfer of any "personal data" (i.e., any data enabling its viewer to identify the author of same) out of the territory of the European Union must be authorized by the **French data protection agency** (*Commission Nationale Informatique et Libertés, or "CNIL"*). Appropriate steps to be taken in this respect include information and consultation of the employee representatives, obtaining the consent of the employees individually, and making a specific notification or asking for a specific authorization from the CNIL. The CNIL has repeatedly expressed concern over transfer of data to the United States in connection with, or in contemplation of, litigation. The CNIL has, however, recently confirmed that single, non-massive transfers out of the EU may be taken without authorization from the CNIL, pursuant to article 69(3) of the French data protection law, which provides an exception for exercising or defending a party's legal rights.[17]

C. Employment law

French labor law imposes the additional requirement that any document collection be "justified" and "proportionate" to the goal pursued.[18]

French **privacy laws** include criminal, civil, employment, and administrative law prohibitions. French law requires that investigations and evidence collections respect correspondence secrecy[19] and the private life[20] of employees. These protections are guaranteed even in the workplace and even when using computers or email addresses belonging to employers. As a result, document collection must strictly be limited to professional documents and must not apply to any documents marked as personal.

D. Attorney-client privilege (or its equivalent)

There is no "attorney-client" privilege per se in France. Rather, professional secrecy and ethical confidentiality rules apply in different situations. Privilege and secrecy protections apply only to outside counsel. Therefore, any communication between in-house counsel (*juristes d'entreprise*) and corporate employees is not protected by privilege. As a result, were a company to carry out an internal investigation itself, the evidence collected would be subject to seizure and use by investigating authorities.

V. Whistleblower protection and leniency for cooperation

A. Protection of whistleblowers vis-à-vis company

The CNIL has provided a set of mandatory rules governing the provisions of a company's whistleblowing system. A company that follows those guidelines strictly can implement a whistleblowing system by following a simplified authorization process. If, however, a whistleblowing system goes beyond the CNIL's mandatory rules, and in particular if it is not limited to matters presenting serious risks to the company in the fields of "accounting, financial audit, the fight against bribery or banking," then the company must undergo a specific review process before an authorization is granted. The CNIL has indicated, however, that it would not likely authorize a whistleblowing system that goes beyond the basic guidelines it has established.[21]

The French Ministry of Labor has confirmed CNIL's position by declaring that whistleblowing systems cannot transfer the employer's responsibility to ensure compliance with the company's internal rules of procedure to employees. As a result, whistleblowing systems cannot impose mandatory disclosure requirements on its employees; in effect, any whistleblowing system thus remains voluntary.

Whistleblowing programs are, at times, accompanied by discretionary amnesty provisions, pursuant to which employers may decide to grant amnesties for acts pertaining to the employment relation. Because only the President of the Republic of France can offer official amnesties, such programs apply only to private employment relationships.

B. Leniency from authorities through cooperation

CONTINUED ON PAGE 17

17 "CNIL Délibération n° 2009-474 portant recommandation en matière de transfert de données à caractère personnel dans le cadre de procédures judiciaires américaines dite de « Discovery »" July 23, 2009, JORF, Aug. 19, 2009.

18 Art. L. 1121-1 of the French labor code.

19 Art. 226-1 of the French criminal code.

20 Art. 6 of the French civil code.

21 CNIL Deliberation n° 2005-305 of December 8, 2005 (JORF n°3 January 4, 2006).

IN FRANCE Continued from page 16

There are no equivalent provisions under French law for the concept of plea bargaining or settlement of criminal charges. Therefore, unlike in several other jurisdictions, most notably the United States, public prosecutors cannot entice companies or individuals subjected to criminal investigations to disclose information with the promise of lighter sentences or lower fines.

VI. Recent regulatory developments in France

The aggregate value of fines handed down by the AMF in 2007 (€19.8 million) was the highest on record since its creation in 2003. Jean-Pierre Jouyet, the new President of the AMF, recently stated that "there can be no trust [in markets] without proper monitoring and no monitoring without effective sentencing. Sentencing achieves its objectives if it can serve as a lesson to others."[22] In a recent interview, Jean-Baptiste Carpentier, Director of *Tracfin*, stated that there were 15,000 declarations of suspicion of money-laundering activities in 2008 (up 17% from 2007).[23] He also stressed that *Tracfin* would increase its ability to tackle tax fraud. An expert report on the reform of white collar criminal law produced in January 2008 suggested that parallel criminal and administrative procedures should be merged into a single, criminal procedure.[24] A report on criminal law and procedure reform, presented on September 1, 2009, proposed dramatic changes to French criminal procedure, including abolishing the investigating magistrate and the principle of secrecy of the investigation.[25] ■

22 February 2009, before the Financial Committee of the French National Assembly.

23 Revue Banque, n°711 March 2009.

24 *La dépénalisation de la vie des affaires*, Jean-Marie Coulon (Jan. 2008).

25 *Rapport du Comité de Réflexion sur la Justice Pénale*, Philippe Léger (Sept. 1, 2009).

IN GERMANY Continued from page 1

Corporate criminal liability generally does not exist in Germany, which means that domestic criminal proceedings triggering an internal investigation will therefore always be initiated against employees or members of company management. However, a fine of up to €1 million may be imposed on the company if its executives breached a duty to the company or enriched the company by committing a criminal act or misdemeanor.[2] Further, a court may also order disgorgement of company profits.[3]

II. German laws that could trigger an investigation

Anticorruption and related laws, found in the German Criminal Code (*Strafgesetzbuch*), have triggered most of the recent internal investigations in Germany. The Code differentiates between **accepting and offering a benefit** (*Vorteilsannahme, Vorteilsgewährung*[4]) and **accepting and offering a bribe** (*Bestechlichkeit, Bestechung*[5]).

An internal corporate investigation might also result from suspicions of taking and offering of **bribes in business transactions** (*Bestechung und Bestechlichkeit im geschäftlichen Verkehr*[6]), **money-laundering** (*Geldwäsche*[7]), **breach of trust** (*Untreue*[8]) (including establishment of company bribery accounts), **fraud** (*Betrug*[9]), **subsidy fraud** (*Subventionsbetrug*[10]), as well as **agreements to restrict competition during a public tender process** (*wettbewerbsbeschränkende Absprachen bei Ausschreibungen*[11]).

III. German enforcement authorities

The authority to enforce the above-mentioned laws in Germany rests solely with the **public prosecutor offices** (*Staatsanwaltschaften*) of the federal states in which the criminal act was committed or in which the criminal offender is domiciled. Some federal states also have **prosecutor offices specialized in combating corruption** (*Schwerpunkt-staatsanwaltschaften*).

IV. Conducting an internal investigation in Germany

A. Data protection in Germany

Unlike other European countries, most notably France, Germany does not have a blocking statute that could prevent internal investigations pursuant to actions taken by foreign regulatory bodies. Nevertheless, internal investigators in Germany need to comply with the strict data protection rules under Directive 95/46/EC of the European Parliament and the European Commission (the "**Directive 95/46/EC**") and the Federal Data Protection Act (*Bundesdatenschutzgesetz*, the **BDSG**) on the collection, processing and transfer of personal data located in Germany or the EU.

According to the directive and the German data protection law, the term "personal data" is to be interpreted broadly and includes all information

CONTINUED ON PAGE 19

Links to related information:

Recent Publication:

- Compliance-Verantwortung in der AG

  This book discusses legal issues in connection with compliance responsibilities at the board level of German corporations and compliance investigations (in German language). (Click here)

1 The most expansive internal investigations of Germany-based companies have been the cases of Daimler AG (where an investigation commenced in 2004 is still ongoing) and Siemens AG (where an internal investigation was carried out between 2006 and 2008).

2 See Sec. 30, 130 of the German Misdemeanor Act (*Gesetz über Ordnungswidrigkeiten*).

3 See Sec. 29a of the German Misdemeanor Act (*Gesetz über Ordnungswidrigkeiten*), Sec. 73 ff of the German Criminal Code (*Strafgesetzbuch*).

4 See Sec. 331, 333 of the German Criminal Code (*Strafgesetzbuch*).

5 See Sec. 332, 334 of the German Criminal Code (*Strafgesetzbuch*).

6 See Sec. 299 of the German Criminal Code (*Strafgesetzbuch*).

7 See Sec. 261 of the German Criminal Code (*Strafgesetzbuch*).

8 See Sec. 266 of the German Criminal Code (*Strafgesetzbuch*).

9 See Sec. 263 of the German Criminal Code (*Strafgesetzbuch*).

10 See Sec. 264 of the German Criminal Code (*Strafgesetzbuch*).

11 See Sec. 298 of the German Criminal Code (*Strafgesetzbuch*).

IN GERMANY Continued from page 18

relating to a particular identified, or identifiable, individual, including, for example, names and postal or email addresses. Pursuant to the applicable data protection rules, in order to safeguard its legitimate interests an employer is entitled to collect and process the personal data of its employees, provided that the legitimate interests of the employer in the personal data outweigh the legitimate interests of an employee in preventing such collection or processing. Balancing the respective interests of employer and employee has resulted in a general recognition that the interest of a company in investigating charges of criminal behavior and in responding to investigations by prosecuting authorities will outweigh any interests of an employee in restricting access to personal data.

The recently enacted Section 32 of the German Federal Data Protection Act, however, provides that in the absence of an employee's consent, an employer may only collect, process and use the employee's personal data if necessary for the conclusion, performance and termination of an employment agreement. The law further provides that personal data may only be collected if clear indications of a criminal act exist, and only if collection appears necessary to detect and determine that a criminal act was, in fact, committed. Also, it is essential under this provision that the nature and scope of the disclosure of an employee's data is proportionate to the criminal act allegedly committed.

The relevant EU data protection laws generally also oblige Member States to prevent the transfer of personal data to countries without adequate data protection. Very few countries outside the EU are deemed to provide the requisite level of data protection. This fact is particularly important when a company faces requests for personal data from US regulators, such as the Department of Justice (DOJ) or the Securities and Exchange Commission (SEC), since the US is considered not to provide adequate personal data protection. However, an exception to the general rule applies when "the transfer is necessary or legally required on important public interest grounds, or for the establishment, exercise or defense of legal claims."[12] For example, if the SEC or DOJ were officially to require the data as part of an investigation into alleged corruption or money laundering, such data transfer may be permissible pursuant to the "public interest" exception.[13]

B. Employment law

Under German law, an employer may instruct employees to provide information within the context of an internal investigation. However, such requirement is limited to information directly related to the employee's work tasks. Moreover, the employee's obligation to provide information within the context of an internal investigation depends on whether the employer can be reasonably expected to obtain the information from a different source. Employees also are not obliged to provide information that might incriminate them, or that otherwise might have a detrimental effect on any potential civil or criminal proceeding against them. If an employee refuses to answer a question he is obliged to answer, the company is entitled to respond by (i) cutting the employee's salary or company pension funds; (ii) warning the employee (*Abmahnung*); or (iii) terminating the employment (although this can only be used as a last resort).[14]

An internal investigation into the conduct of numerous employees without a concrete suspicion against all of the investigated individuals will trigger co-determination rights of the works council. The employer must inform the works council in due course about the investigation so that the works council can fulfill its tasks under the Works Constitution Act (*Betriebsverfassungsgesetz* or *BetrVG*). For instance, the company's works council must consent to measures pertaining to all questions of (collective) employees' surveillance and control by technical means, such as telephone monitoring or data screening using computer programs. Such consent may be granted through a shop agreement (Betriebsvereinbarung) between the company management and the works council.

Investigations of single employees who are the subjects of a concrete suspicion, on the other hand, are considered to be of an individual nature and, therefore, do not require the works council's consent.

The works council also has the general duty to see that effect is given to labor related acts, ordinances, safety

CONTINUED ON PAGE 20

12 Directive 95/46 EC, Art. 26(1)(d). See also German Federal Data Protection Act, Sec. 4c(1)(4).

13 A company which is determined to transfer data is required to obtain written assurances from the SEC or DOJ that: (i) only personal data of specific relevance should be transferred; (ii) the regulator will process and use the data only for the purposes for which it was sought; and (iii) the regulator will not transfer the data, or otherwise make it available, to any third party (even if production of the data in question is required under the US Freedom of Information Act).

14 It should also be noted that an employee remains obligated to provide information to the company even after termination of his/her employment.

IN GERMANY Continued from page 19

regulations, collective agreements and employer/works council agreements for the benefit of the employees,[15] including compliance with employment law and data protection law.

C. Attorney-client privilege (or its equivalent)

The concept of the attorney-client privilege in common law systems does not exist under German law.[16] Instead, German attorneys (*Rechtsanwälte*) have a duty to observe confidentiality regarding all information received from their clients. This duty is mirrored by the attorney's right not to testify or to produce evidence in civil or criminal cases regarding information that the attorney learned in a professional capacity. Such information may also include communications to the attorney from third parties or in the presence of a third party, such as employee interviews during internal investigations.

In criminal proceedings, documents containing attorney-client communications are not subject to seizure by German authorities if in the custody of the attorney. However, documents located at the client's premises that are not related to the client's defense in an *ongoing* investigation (defense correspondence) are not privileged from seizure by the prosecutor. Documents relating to an internal investigation, such as interview memoranda prepared by outside counsel, generally do not qualify as defense correspondence and therefore may be seized by the prosecutor. For this reason, interview memoranda prepared by an attorney should not be shared with the company.[17]

It is important to note that in-house counsel (*Syndikusanwälte*) are entitled to the same legal privilege only if (i) they are admitted to practice as attorneys in Germany; and (ii) they learned the relevant facts in their capacity as lawyers.

V. Whistleblower protection and leniency for cooperation

A. Protection of whistleblowers vis-à-vis company

There is no general protection provided to whistleblowers under German employment law. Despite an initiative to include into the German Civil Code (*Bürgerliches Gesetzbuch, BGB*) provisions on an employee's right to disclose possible violations of the law, no such enactment has taken place. However, the recently amended Civil Servants Act (*Bundesbeamtengesetz*) provides that civil servants may directly notify prosecutors of suspected corruption offenses without breaching their general duty of confidentiality.

Certain specific protections in the whistleblowing context are provided by the EU Data Protection Directive and the BDSG, which relate to the content of whistleblowing reports. These rules require the company to ensure that personal data is kept in a confidential and secure manner, so that the rights of both the data subject and the target remain respected. Companies are also required to discourage anonymous reports, to restrict disclosure of such reports to a limited number of individuals, and to delete (or block access to) personal data after the conclusion of the investigation.

B. Leniency from authorities through cooperation

There have been several recent legislative changes in Germany pertaining to the cooperation of individuals in connection with legal proceedings, which may have a significant effect on internal investigations. Until September 2009, notwithstanding some leeway under German law to honor a criminal offender's cooperation with the authorities, no general explicit provision offered leniency to cooperating criminal offenders. Only with respect to specific offenses, such as violations of the German Narcotics Act (*Betäubungsmittelgesetz*), money laundering (*Geldwäsche*) or establishing a terrorist organization (*Bildung einer terroristischen Vereinigung*), did German law contain explicit provisions enabling courts to mitigate sentences or to grant immunity. On September 1, 2009, Section 46(b) of the German Criminal Code came into force providing for leniency for criminal offenders who voluntarily cooperate with authorities in connection with severe criminal offenses.

Deals between a prosecutor and a defendant have increasingly become common practice in criminal cases in Germany. Until recently German statutory law did not provide for such

CONTINUED ON PAGE 21

15 See Sec. 80 para. 1 no. 1 of the BetrVG.

16 This is, in large measure, due to the fact that German law does not recognize the obligation to disclose documents during litigation in the same way that common law legal systems do.

17 It should also be noted that interview memoranda prepared by an attorney for internal purposes do not need to be provided to the client, unless this has been explicitly contractually agreed. If a memorandum, or part of a memorandum, is included in an employee's personnel file, the employee in question would be able to assert rights under German labor law (such as the right of inspection) with respect to the memorandum.

IN GERMANY Continued from page 20

measures. However, in August 2009, the new § 257(c) of the German Code of Criminal Procedure (*Strafprozessordnung, StPO)* entered into force. This "deal" provision is meant to enable the parties to agree on a sentence, to close proceedings or to refrain from taking further evidence during all stages of the legal proceedings.

Moreover, in the context of employment law, employer-provided amnesties may be useful in encouraging otherwise-reticent employees to come forward. However, there are, at present, no laws which provide that an employee who has been granted amnesty by his employer may also avoid being charged by the investigating prosecutor.[18]

VI. Recent regulatory developments in Germany

Cooperation between German authorities and authorities overseas has been increasing over the past several years. The most evident recent example of such cooperation pertained to the investigation into alleged improper payments by Siemens AG. The Munich Public Prosecutor cooperated with the responsible US authorities to such an extent that their respective cases against Siemens AG were closed on the same day with coordinated sanctions and resolutions. ■

18 However, the employer will typically promise an employee that the investigating prosecutor will be informed of the employee's cooperation in an attempt to ensure that the employee does not suffer any major disadvantages from participating in the amnesty program.