Three to Watch: HR's Growing Compliance Responsibilities for Data Security, Genetic Nondiscrimination, and Anti-Bribery Laws

By W. Scott Blackmer and Richard Santalesa, InfoLawGroup, LLP

Human Resources managers traditionally play an important role in an organization's compliance programs, from recruiting and training to investigations and disciplinary measures.

In three areas, HR is facing new or expanding compliance challenges, which are particularly complex for enterprises that operate across multiple states, provinces and countries:

1. Preventing and responding to HR data leaks, in an environment where databases and applications are often distributed globally and partly entrusted to third-party service providers, yet where the rules vary by jurisdiction;
2. Raising awareness and providing training to avoid liability for genetic discrimination under the Genetic Information Nondiscrimination Act (GINA) regulations that came into effect this year in the United States; and,
3. Revamping policies, training, and investigative techniques to address evolving enforcement priorities under the U.S. Foreign Corrupt Practices Act and the new "tough cop" on the global scene: the UK Bribery Act of 2010.

An overview of recent developments in these three areas highlights the need for global HR management to keep abreast of new compliance requirements, in cooperation with an organization's legal counsel or compliance department. Human Resources management can contribute to an effective compliance approach that avoids costly and embarrassing exposure for a company or nonprofit.

Preventing and Plugging HR Data Leaks

A variety of personal information protection laws and "security breach notification" laws or regulations now affect nearly all enterprises in the United States, Canada, Mexico (beginning in 2012), the European Union (EU) and many non-EU countries in Europe and the Middle East, Japan, Australia and, more recently, an array of other countries in the Asia-Pacific region and in the Americas. Information security obligations are increasingly common, sometimes detailing specific measures that must be taken in the event of a suspected breach of the confidentiality of legally protected data concerning employees or consumers.

The largest, most notorious data breaches in recent history have concerned consumer data – such as the Sony PlayStation and Epsilon hacks, both announced in April 2011, which compromised tens of millions of e-mail addresses that may now be used in spear-phishing scams, and the 2009 attack on Heartland Payment Systems as part of an international cyber fraud scheme, compromising up to 100 million credit and debit cards.

Human resources information systems, fortunately, do not handle such large numbers of records, and HR data leaks typically receive less media attention. But, many databases with information on employees, dependents, independent contractors, and job candidates contain the same kinds of personal information coveted by fraudsters and identity thieves, and in sufficient quantity to attract them:

- Social Security Numbers (SSNs), passport or driver's license numbers, and other forms of official identification;
- Date of birth;
- Bank account numbers (since most employers offer direct deposit of salary and pension payments);
- Payment card details (especially for corporate cards, travel, and T&E management); and
- Health insurance policy numbers (used in medical ID theft, which is a growing problem).

In addition, personal information concerning employees and independent contractors is valuable to those seeking access to the *employer's network* for nefarious

purposes such as theft, commercial espionage, disruption of a competitor's business, access to national security information held by a government contractor, terrorist attacks on critical infrastructure – or simply to embarrass a company (think of "political" hacking by Anonymous and LulzSec). In these cases, the golden ring is the employee's password or other access credentials. These can sometimes be guessed from personal information such as the birth dates of family members (it's amazing how often those are selected as passwords). Or, they can be garnered by phone or e-mail from a helpful IT night staffer with a little clever "social engineering" using credibility-enhancing information culled from the victim's Facebook page or tweets: "I'm in Chicago for the meeting with XYZ tomorrow morning, and I've got to look at a file tonight."

Sobering lists of announced data breaches are published and categorized by DataLossDB (www.datalossdb.org), Privacy Rights Clearinghouse (www.privacyrights.org), and TeamSHATTER (www.teamshatter.com). Unfortunately, those lists have to be updated weekly or biweekly. Many concern data (usually including SSNs) on employees, retirees and job applicants. Some examples are shown in the accompanying Table 1.

Employer	Records	Nature of Breach	Announced
Penn State Altoona	12,000 faculty, staff, and alumni	Virus on computer system	Jun 2011
UMass Memorial Healthcare	13,500 employees	Faulty implementation of HRConnect kiosks	Apr 2011
Schield Family Companies	12,000 employees	Fraud scheme	Apr 2011
St. Louis Univ.	12,800 current and former employees and contractors	Network hack	Mar 2011
U.S. General Services Administration	12,000 employees	Insider	Nov 2010
Houston Indep. School Dist.	30,000 employees	Network hack	Oct 2010
American Airlines (AMR Corp.)	79,000 employees and retirees	Stolen hard drive from headquarters offices	Jul 2010
P.F. Chang's Bistros	8,200 employees	Stolen equipment	Feb 2010
PricewaterhouseCoopers	77,000 current and former employees, retirees	Lost storage media	Jan 2010
National Finance Center	27,000 Commerce Dep't employees	Email with spreadsheet mistakenly sent	Aug 2009
Aetna Insurance	65,000 current and former employees	Website hack	May 2009
Federal Aviation Administration	48,000 employees and retirees	Network hack	Feb 2009
Kaiser Permanente	30,000 employees	Stolen file	Feb 2009
Luxottica Group	59,000 former employees	Hacked mainframe	Nov 2008
Bristol-Myers Squibb	42,000 employees and dependents	Backup tape stolen in transit to storage facility	Jul 2008
AON Consulting	57,000 Verizon job applicants	Stolen laptop	Jun 2008
Pfizer	13,000 employees	Stolen laptop and flash drive	May 2008
Agilent	51,000 current and former employees	Stolen laptop	Mar 2008
The Gap	800,000 job applicants	Laptop stolen from office of Vangent job application management vendor	Sep 2007
Boeing	382,000 employees	Stolen laptop (later recovered)	Dec 2006
Ernst & Young	365,000 employees of clients	3 stolen laptops	Feb – Jun 2006
Boeing	161,000 employees	Stolen laptop	Nov 2005

Table 1. A Sampling of HR Data Breaches.

Some HR data leaks have resulted in a brief flurry of embarrassing media attention, but HR data leaks can have serious consequences for the company even if they do not attract much publicity. Most of these costs are for sending notification letters to affected individuals, operating temporary call centers or Web pages concerning the incident, hiring computer forensics and information security consultants, undertaking remedial IT security measures, getting legal advice, and often paying for safeguards for affected individuals, such as offering credit report monitoring for one to three years or reimbursing individuals for the costs of replacing bank accounts or payment cards.

A data breach involving at least 1,000 records is likely to cost the organization US$214 per record, according to the *2010 Annual Study: U.S. Costs of a Data Breach* produced by Symantec and the Poneman Institute, http://www.symantec.com/content/en/us/about/media/pdfs/symantec_ponemon_data_breach_costs_report.pdf. That study, based on a survey of 51 companies that experienced breaches involving 1,000 to 100,000 records, found that the average cost to the company for a breach incident was US$7.2 million. Companies also report abnormal customer "churn" (and, therefore, lost business and higher expenses to recruit new customers) following the announcement of a major breach.

One problem for companies suffering a data breach is that they must navigate the somewhat different requirements for breach notification in 46 U.S. states and the District of Columbia, as well as quite different requirements (often entailing a consultation with the relevant privacy or data protection commissioner) in some Canadian provinces and in Europe. New data privacy legislation in Mexico must also be added to the mix. In the U.S., three proposed bills for a federal data breach notification law, one endorsed by the White House, were introduced in Congress in May. If adopted, such legislation would establish a more uniform approach in the U.S., but there remains the problem that data leaks sometimes compromise employee and consumer data from abroad as well. For American companies that process personal data in the U.S. from operations in Europe, under the US-EU or US-Switzerland Safe Harbor Privacy Frameworks, there is also the possibility of a Federal Trade Commission (FTC) investigation or enforcement action, in addition to enforcement in Europe. The FTC has launched such investigations for large-scale data breaches involving European employee data.

On top of the costs of notification and remediation, the FTC, which for years focused on consumer data breaches, has been active recently in pursuing companies responsible for large-scale breaches involving employee data. This is done under the FTC's broad authority to enforce against "unfair and deceptive trade practices" in interstate and international commerce. In May, the FTC announced proposed settlements with two HR services vendors, Ceridian and Lookout Services, following data breaches that exposed personal data on 65,000 employees of their clients. Ceridian, according to the FTC, failed to encrypt sensitive data or to take simple precautions against struc-

tured query language (SQL) injection attacks. Lookout Services failed to use strong passwords or an intrusion detection system, or adequately monitor its access logs. The company was also faulted for inadequate training. Under the proposed settlement, both companies would be obliged to implement new security programs and obtain biennial, independent security audits over the next 20 years. The FTC has imposed substantial fines in a number of consumer data breach incidents, and it could do so in an egregious case involving employee data as well.

So far, HR data leaks have not resulted in successful damages claims in civil lawsuits filed by affected individuals. Last year, for example, the federal Ninth Circuit Court of Appeals rejected a complaint brought by one of the estimated 800,000 people whose SSN was compromised when a laptop containing job applications for The Gap was stolen from Vangent, a third-party job application management vendor. The court concluded that there could be no legal claim without proof of actual damages (Ruiz v. Gap, Inc., 9th Circ. May 28, 2010), www.ca9.uscourts.gov/datastore/memoranda/2010/05/28/09-15971.pdf).

Even without mega-dollar negligence lawsuits to contend with, companies suffering a substantial data leak involving employee data can anticipate multimillion-dollar expenses and a temporary disruption of business. Large breaches may also attract the unwelcome attention of the FTC, a state attorney general, or of a foreign privacy commissioner. Finally, companies should not discount the negative impact of a large-scale data breach on the company's reputation, which can affect recruiting and employee morale, as well as brand image.

The unavoidable conclusion is that it matters to get HR information security right, as much as possible, and also to deal promptly and effectively with security breaches.

Genetic Information Nondiscrimination Act (GINA) Rules Take Effect

Managing human resources compliance in the U.S. became a bit more complicated this year when EEOC regulations came into force detailing the implementation of GINA (http//www1.eeoc.gov/laws/statutes/gina.cfm).

Prior to GINA, Executive Order 13145 prohibited federal executive branch agencies from discriminating against applicants and employees on the basis of genetic information and limited access to and use of genetic information by such agencies. With GINA's passage in 2008 and its entry into force on November 21, 2009, these prohibitions were extended to private entities with more than 15 employees.

Many U.S. states already prohibit the use of genetic information in employment contexts, and genetic discrimination claims have been successfully prosecuted against some employers under the Americans with Disabilities Act (ADA), notably Burlington Northern Santa Fe Railway in 2001. Title II of GINA now broadly prohibits discrimination by employers based on a person's "genetic information." The provisions of GINA further dovetail with various portions of the Health Insurance Portability and Accountability Act (HIPAA) and other federal statutes, including incorporating by reference definitions from the Civil Rights Act of 1964. In addition, GINA states that nothing in the statute limits any existing rights or protections provided to individuals under "any other federal or state statute that provides equal or greater protection, including the protections of an individual under the ADA...."

The resulting complex cloverleaf intersection of state law, GINA, and other federal laws, such as HIPAA, ADA, the Employee Retirement Income Security Act of 1974 (ERISA), the Public Health Service Act, the Internal Revenue Code, and the Family and Medical Leave Act (FMLA), create an intricate web for HR to navigate. Further complicating matters is that Congress authorized the Equal Employment Opportunity Commission (EEOC) as the exclusive authority to enforce GINA in employment contexts, and the EEOC's final rules regarding GINA only came into effect as the calendar clicked over on January 1, 2011 (http://edocket.access.gpo.gov/2010/2010-28011.htm).

The EEOC's final rules are a great aid in dispelling much confusion and speculation concerning how the EEOC would interpret and enforce GINA. While lengthy, they are very informative in indicating the EEOC's approach to interpreting and enforcing the law. For example, the EEOC remarks that the final rules "include a definition of 'family medical history' because it is a term used in the statute's discussion of prohibited employment practices, but it is not specifically defined by the statute."

The EEOC rules also highlight the fact that GINA is focused primarily on protecting individuals who may face discrimination in the present because an employer believes they are at increased medical risk of developing a condition in the future. That is, if an individual applicant or employee currently "manifests" a certain disease or condition; they are not protected by GINA, although they may be protected by other state and federal laws, such as the ADA, depending on the specifics.

Even before the EEOC's final rules came into force, nearly 200 genetic-based GINA employment complaints were filed with the EEOC. The first complaint after the final EEOC rules took effect was filed earlier this year by a woman in Fairfield, Connecticut who alleged that she was fired on the basis of disclosed genetic information that she carried a gene linked to breast cancer.

Even before the EEOC's final rules came into force, nearly 200 genetic-based GINA employment complaints were filed with the EEOC.

GINA includes substantial penalties and recourse for noncompliance. The EEOC may impose penalties of up to US$100 per day, with a minimum penalty of US$2,500 for *de minimis* violations and US$15,000 for significant violations. And unlike other EEOC statutes, GINA allows an aggrieved individual to bring a civil action without first exhausting administrative remedies, if the individual can establish that the delay would result in irreparable harm to his health, e.g., in being denied access to employer-provided health benefits.

To avoid compliance issues, HR professionals should be educating management on GINA's requirements and the interaction with other relevant compliance obligations, such as appropriate documentation of sick leave requests. The Genetic Alliance offers extensive free resources on GINA compliance matters at http://www.geneticalliance.org/ginaresource.

In light of this background, what does GINA mean for current HR policies and employment practices?

Any starting point as to what HR departments must do to comply with GINA and the EEOC's final rules requires understanding basic definitions used by GINA, particularly as the EEOC's final rules note that "GINA includes six terms not found in any of the other employment discrimination statutes that the Commission enforces." In response, the EEOC worked closely with the National Human Genome Research Institute in deriving various definitions, or adapting existing definitions for GINA purposes.

Four of the most crucial definitions are those of "genetic information," "genetic services," "family member" and "manifestation." Other notable definitions include those for "employee," "employer," "employment agency," "labor organization," "family medical history" and "genetic monitoring."

Under GINA, "genetic information," according to the EEOC, includes information about:

- An individual's genetic tests and the genetic tests of an individual's family members;
- The manifestation of a disease or disorder in an individual's family members (family medical history);
- An individual's request for, or receipt of, genetic services, or the participation in clinical research that includes genetic services by the individual or a family member of the individual;
- A fetus carried by an individual or by a pregnant woman who is a family member of the individual; or,
- The genetic information of any embryo legally held by the individual or family member using an assisted reproductive technology.

GINA's definition of "genetic information" does not include an individual's sex or age.

GINA's definition of "genetic information" does not include an individual's sex or age.

In turn, the "genetic services" for GINA's purposes include:

- Genetic tests, in particular, "analysis of human DNA, RNA, chromosomes, proteins, or metabolites, that detects genotypes, mutations, or chromosomal changes;"
- Genetic counseling; and,
- Genetic education.

While the definition of genetic services is potentially broad, GINA clarifies that blood tests that do not involve "genotypes or chromosomal changes," but are designed for determining the presence of infectious and communicable diseases, blood counts, cholesterol tests, and liver function tests are not genetic tests for purposes of the GINA.

Another important definition regards who qualifies as a "family member." The explanatory notes in the EEOC's final rules observe that the GINA provides a very broad sweep, to include "any other individual who is a first-degree, second-degree, third-degree or fourth-degree relative." This is a wide net. However, as to who "dependents" of individual are, the EEOC definitively states that they "are limited to persons who are or become related to an individual through marriage, birth, adoption, or placement for adoption."

Lastly, "manifested" and "manifestation" are used 24 times in GINA, with neither defined in the statute. Given the importance of understanding what "manifestation of a disease" is for compliance with GINA, the EEOC provided its own definition in the final rules. The EEOC defines "manifestation" to mean:

"That an individual has been or could reasonably be diagnosed with the disease, disorder, or pathological condition by a health care professional with appropriate training and expertise in the field of medicine involved."

The final rules clarify that a disease is not "manifested" if a diagnosis is based principally on genetic information.

With these several important definitions laid out, what are the most notable potential pitfalls and problems that the GINA can cause in the HR context? And, more importantly, how can HR avoid them?

The practices prohibited by GINA include both discrimination on the basis of genetic information and the acquisition of genetic information, which can be done inadvertently without any intent and yet still run afoul of GINA as interpreted by the EEOC. Employers may never legitimately use genetic information, as defined, for making an employment decision because, as the EEOC states, "genetic information is not relevant to an individual's current ability to work." According to the EEOC, an employment decision includes any aspect of employment, including hiring, firing, pay levels, job assignments,

promotions, layoffs, training, fringe benefits, "or any other term or condition of employment."

Further, GINA prohibits employers from acquiring genetic information, except for six narrow exceptions, which include the functioning of company "wellness" programs, certification of eligibility under the Family and Medical Leave Act (or state and local equivalents), and genetic monitoring programs as required by law or as performed on a voluntary basis in order to measure biological effects of toxic substances that employees may be exposed to in the workplace. Under GINA, the confidentiality of genetic information from applicants and employees must be kept confidential and stored in a separate medical file (which may be the same medical file as one maintained for compliance with the ADA).

GINA also prohibits any retaliation against an applicant or employee for filing a charge of genetic discrimination, participating in a discrimination proceeding or otherwise acting to oppose genetic discrimination. Lastly, GINA makes it illegal for a person to harass another, via offensive or derogatory remarks, because of his or her genetic information or to harass another regarding a relative of an applicant or employee on the basis of genetic information.

Human Resources "Gotchas" and Recommendations

- **EEO Poster** – As a starting point, if you are behind the times and haven't displayed a GINA-compliant EEOC poster, this is an easy first step toward compliance. The EEOC's "EEO is the Law" poster – EEOC-P/E-1 (Revised 11/09) – contains GINA information and is available for free download at http://www1.eeoc.gov/employers/poster.cfm.
- **Pre-employment physicals** – Many employers require pre-employment physicals that are in compliance with the ADA. As a result, it's important that any physicians or other medical personnel retained for such purposes be instructed not to request or record any genetic information or family medical history, and if such information is recorded, steps are immediately taken to purge it from the file maintained by the employer and advise the health care professional to refrain from collecting and recording such information in future evaluations.
- **Small business FAQ** – For small businesses (remember that GINA applies to all employers with more than 15 employees), the EEOC offers simplified FAQ on its final rules, available at http://www.eeoc.gov/laws/regulations/gina_qanda_smallbus.cfm. While designed for small business owners, these FAQs are a good tutorial for instructing managers in larger companies as well.
- **Employee handbooks and employment forms** – Employee handbooks should be reviewed and updated to reflect the prohibitions and definitions that GINA provides regarding use and acquisition of genetic information. Employment forms and applications, likewise, should be reviewed to ensure no family medical history or other genetic information is requested of applicants. Where employers sponsor health plans and are treated as covered entities under HIPAA, employers should review their HIPAA privacy notices and update them if necessary to address the confidentiality of genetic information.
- **Medical information storage and filing** – All genetic information that is obtained under one of the six exceptions to the otherwise broad prohibition on acquisition of genetic information must be stored securely in a separate medical file. Updated training of personnel on this and other aspects of GINA is a crucial component of any compliance effort.
- **Family and Medical Leave Act** – While employees have a right under the FMLA (and applicable state and local equivalents) to request unpaid leave to care for sick or disabled family members, they are required to provide medical information to document the circumstances. Any FMLA forms or documents utilized in such cases should be carefully reviewed and edited to focus only on specific needed information without requesting extraneous or unnecessary genetic information about the family member, where it could reflect a genetic issue for the employee.
- **Be aware of the water cooler problem** – Both Congress and the EEOC, in its final rules, recognize the widespread "water cooler" problem, in which an employer unintentional or innocuously receives otherwise prohibited genetic information in the form of family medical history in casual conversations or by overhearing co-workers' conversations. Congress provided, as one of the six exceptions to the prohibition on acquisition of genetic information, a carve-out covering inadvertent disclosures in casual conversations. However, the range of this exception is not unlimited, and, in all such cases while the acquisition raises no liability, any employment actions taken in response to the information are prohibited. The EEOC final rules contain very detailed discussion and examples on the water cooler problem. These could provide useful "cases" for illustration and discussion purposes in EEO training.
- **Social Media and Social Networking** – Recognizing today's networked social environment, the EEOC final rules include discussion of water cooler and inadvertent acquisition situations that may occur via social networking with other employees, managers and co-workers.

While GINA and the EEOC final rules are complex and require both time to master and a sensitive awareness of how a company utilizes information about employees and job candidates, any well-run HR department should be able to integrate GINA compliance into the already-long list of mandated compliance measures, particularly with respect

to closely related ADA and FMLA compliance mandates. The EEOC's website is a good starting point for any such efforts, and it would be prudent to obtain a legal review of GINA compliance policies and training materials.

The Internationalization of Anti-Bribery Laws

Multinationals are familiar with the U.S. Foreign Corrupt Practices Act (FCPA). It has taken awhile for anti-bribery legislation to truly catch on in other major industrial countries, but now the United Kingdom is contemplating even stricter measures than the venerable FCPA. Meanwhile, the U.S. Department of Justice and the Securities and Exchange Commission have stepped up their enforcement efforts under the FCPA, imposing fines totaling some US$1.5 billion in 2010. As a result, it is a good time for HR managers in multinational companies to check in with legal counsel and update their anti-bribery compliance programs.

The U.S. Foreign Corrupt Practices Act

The FCPA was a pioneering piece of legislation when it was enacted in 1977. Following scandals involving Lockheed, Chiquita Brands, and other major U.S. corporate groups that bribed high-level foreign officials to grant contracts, change laws, or otherwise favor a company's products, the FCPA was intended to restore confidence in the integrity of American business. At the same time, Congress hoped a federal anti-bribery law would give American companies a good excuse to "just say no" to attempted shake-downs by corrupt officials in other countries, or even in the bureaucracies of intergovernmental organizations such as the United Nations.

The FCPA forbids making payments (or providing "anything of value") to foreign government officials in exchange for their help in obtaining or retaining business. The FCPA applies to "U.S. persons" (individuals or companies) and also to foreign persons who engage in an act in the United States in furtherance of such corrupt payments. It also applies to foreign companies with shares listed in the U.S. Publicly traded companies are obliged by FCPA to establish adequate internal accounting controls to detect prohibited payments, which are also not tax-deductible.

Since the 1998 amendments to the FCPA, it is possible for a U.S. company to be liable for conduct by non-U.S. employees or agents that took place entirely overseas, without demonstrating actual knowledge by any U.S. officers or managers. Several recent enforcement actions fit these circumstances. Thus, effective training and supervision is critical, including monitoring or audits of expenditures associated with business development and contract bidding by foreign subsidiaries.

Recent enforcement actions also go beyond payments to officials to obtain government contracts, or contracts with "government instrumentalities" (these are not defined in the statute but may include virtually any state-controlled entities, which are common in China and many other countries). The courts have backed Department of Justice efforts to prosecute companies charged with paying officials in an attempt to obtain lower taxes or customs duties, or to change regulations or regulatory enforcement policies.

The FCPA makes an exception for "facilitation payments" (sometimes called "grease payments") that are meant to expedite the fulfillment of a routine, non-discretionary government responsibility, such as processing paperwork. There are also affirmative defenses for making payments that are lawful under the written laws or regulations of the foreign country, and for reimbursing reasonable expenses in promoting a product or performing a contract. Recent enforcement actions suggest that the Department of Justice is casting a more critical eye on the "facilitation payments" exception in particular.

In 2010, the Dodd-Frank Wall Street Reform and Consumer Protection Act strengthened legal protections for corporate "whistleblowers." Among other things, this means that companies must tread carefully in anti-corruption investigations and ensure that internal allegations of suspected misconduct are neither ignored nor punished.

The Organization for Economic Co-operation and Development

Twenty years after the FCPA was enacted, the Organization for Economic Co-operation and Development (OECD) finally adopted a 1997 *Convention on Combating Bribery of Foreign Public Officials in International Business Transactions*. So far, 38 countries have adopted laws based on the OECD Convention, although typically not in a form as far-reaching as the FCPA. Canada's version, for example, the Corruption of Foreign Public Officials Act (CFPOA), is similar to the FCPA but does not apply unless a significant portion of the prohibited activities take place in Canada.

Those same 38 countries are now in various stages of implementing the OECD's 2009 *Anti-Bribery Recommendation*, which includes "Good Practice Guidance on Internal Controls, Ethics and Compliance (Good Practice Guidance)," available from the OECD at www.oecd.org/dataoecd/5/51/44884389.pdf. The Good Practice Guidance describes how companies can:

- Adopt a clear and visible anti-bribery policy that is strongly supported by senior management;
- Instill a sense of responsibility for compliance with the policy at all levels of the company, as well as independent compliance structures;
- Keep up regular communication and training on foreign bribery for all employees, as well as with business partners; and,
- Encourage observance of anti-bribery compliance measures, and disciplinary procedures to address their violations.

The 2009 OECD Good Practice Guidance should be consulted, and cited, by HR managers charged with

raising the level of awareness and compliance in their organizations.

UK Bribery Act

Though the United Kingdom adopted the Bribery Act in 2010, it only recently published official guidance so that the Act could come into effect in July 2011. The shape of that guidance has been controversial, because the Act itself has a very broad potential scope, outpacing the U.S. FCPA. Penalties under the Act can include unlimited fines, confiscation of property, disqualification of company directors, and imprisonment for up to 10 years.

Under the Bribery Act, bribery offenses are not limited to bribery of public officials. Moreover, the "failure of a commercial organisation to prevent bribery on its behalf" is a separate criminal offense under Section 7 of the Act, which heightens the importance of training and oversight programs. There is no general exception for "facilitation payments," as the FCPA provides.

The statutory language is so broad that it was feared that virtually any company or individual with substantial links to the United Kingdom might be covered by the legislation, which would thus apply to most multinationals. While the courts will ultimately decide when there is a sufficient UK presence to apply the Act, the guidance published by the Ministry of Justice (MOJ) states that prosecutors will take a "common sense" approach toward firms headquartered outside the United Kingdom. Listing a company's stock on a London exchange would not be sufficient alone, according to the Ministry, and even a UK subsidiary might not satisfy the test for jurisdiction over the corporate group, if the subsidiary acted "independently of its parent or other group companies."

The MOJ guidance, which can be found on the MOJ's website at http://www.justice.gov.uk/guidance/docs/bribery-act-2010-guidance.pdf, discusses how companies can benefit from the defense available under the Act if a company has adequate procedures to prevent and detect commercial bribery on its behalf. This will be evaluated according to six principles which, in many respects, echo the OECD anti-bribery recommendation:

- Proportionate procedures (given the risks),
- Top-level commitment within the organization,
- Risk assessment,
- Due diligence,
- Communication, and
- Monitoring and review.

The MOJ guidance also states that "bona fide hospitality and promotional expenditures" are an accepted aspect of doing business, and "it is not the intention of the Act to criminalize such behavior." The guidance does not give examples of hospitality and promotional expenditures that would cross the line into bribery. Presumably, favors that are substantially more costly than a dinner or hosting a hospitality tent at a sporting event could be viewed with suspicion.

Because the Act expands the concept of commercial bribery beyond the involvement of government officials and asserts broad jurisdiction over companies with substantial business in the UK, it is clear that multinationals will have to design (or redesign) their compliance programs to satisfy the requirements of the UK Bribery Act, as well as the FCPA.

Human Resources Impact

The new, and broader, focus on anti-corruption policies for international business transactions has implications for HR management, particularly in these areas:

- Training and awareness programs, as well as ethical compliance "hotlines" and similar reporting mechanisms, must take account of the new UK Bribery Act and current trends in FCPA interpretation and enforcement.
- Human Resources should be involved in reviewing the organization's investigative policies and procedures, balancing anti-bribery compliance obligations with the organization's obligations toward whistleblowers and its commitments to respect employee privacy and fair process.
- Disciplinary measures should be proportional to the employer's exposure to risk, with HR assisting the legal or compliance functions in maintaining consistency in dealing with similar cases of policy violations.
- Employee evaluations and succession planning need to give sufficient weight to an individual's involvement in activities that could result in anti-bribery liability.

About the Authors

W. Scott Blackmer is a founding partner of InfoLawGroup LLP, a California law partnership. His practice emphasizes information privacy and security and the legal issues associated with information technology in global business. Formerly a partner in the Washington, DC and Brussels offices of the international law firm now known as WilmerHale, Blackmer is currently based in Salt Lake City and works on compliance issues and transactions in more than 100 countries. He can be reached at ***sblackmer@infolawgroup.com***

Richard Santalesa is a Senior Counsel at the InfoLawGroup LLP where he focuses on information privacy and security, e-commerce and intellectual property matters. He is currently based in Fairfield, Connecticut and New York City and has a background in IT, computer programming and technology journalism. He can be reached at ***rsantalesa@infolawgroup.com***.