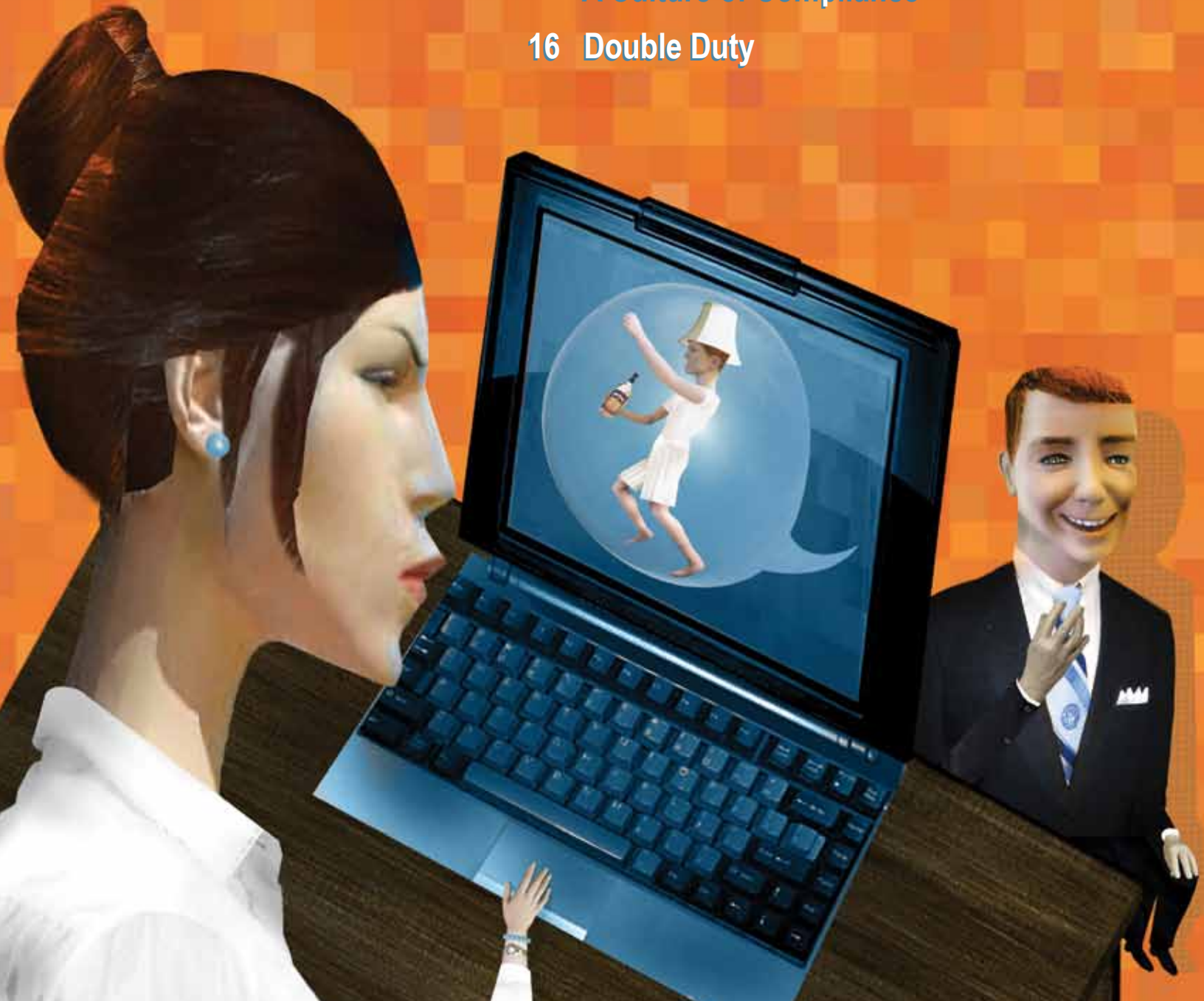




INVESTIGATIONS QUARTERLY

9 The Double-Edged Sword

- 3 Adequate Procedures Guidance
- 7 How Well Do You Know Your ESP
- 13 A New Commitment to
A Culture of Compliance
- 16 Double Duty



Letter from the publishers

Jeff Green, jgreen@navigant.com

Ellen Zimiles, ellen.zimiles@navigant.com

PUBLISHERS

Jeff Green

+1.202.973.2441

jgreen@navigant.com

Ellen Zimiles

+1.212.554.2602

ellen.zimiles@navigant.com

EDITORS

Shannon Prown

Jeffrey Locke

DESIGN

Elliott Robinson

FEEDBACK AND INQUIRIES

Investigations Quarterly welcomes all letters, comments and inquiries to the authors. Please address all correspondence to:

Shannon Prown (U.S.)

+1.215.832.4436

sprown@navigant.com

Suzy Goodwin (U.K.)

+44.207.469.1111

suzy.goodwin@navigant.com

James Gordon (Asia)

+1.852.2233.2520

jegordon@navigant.com

Unsolicited manuscripts on matters dealing with fraud and investigations are welcome and will be considered for publication.

Investigations Quarterly is published by Navigant. Copyright © 2011.

The opinions expressed here in are those of the authors and editors.

Investigations Quarterly (IQ) is not published with the intention of rendering legal, professional or accounting advice or services.

The media are welcome to quote from the contents if properly attributed. Any substantial reproduction of the content of *Investigations Quarterly* requires the permission of the publishers and authors of the articles.

Cover illustration by Josh Leipziger

No bright white line

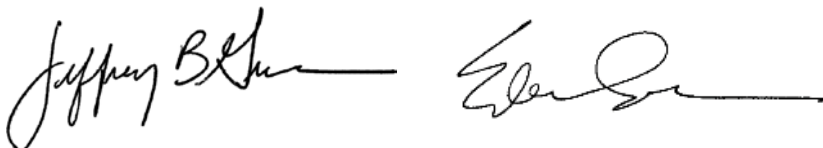
In the context of regulatory compliance, there is an expectation that organizations will establish strong and rigorously maintained compliance systems. Unfortunately, that expectation does not come with a clearly marked roadmap. In fact, there is a significant reliance on individual judgment used to interpret any gray areas, from the Chief Compliance Officer to field personnel. During a forensic investigation or lookback, some of the gray areas look quite clear in retrospect, but that is with lens of independence, free from personal, professional and situational influences.

Over the years, the writers in *IQ* have espoused the benefits of a strong compliance program as the offence that provides the best defense. Even the most sophisticated and comprehensive program, however, is subject to some degree of judgment. The writers' in this issue of *IQ* support the compliance program as the best defense, but offer some themes that may make the difference in those areas that require individual judgment:

- » Tone from the top-ensure that communications from the company's top executives support the culture of compliance and do not convey mixed messages or motivations.
- » Clarity-while some areas of regulation leave room for interpretation, compliance programs should not. If there are such areas, you need to provide access to clear and consistent answers.
- » Transparency-maintaining and sharing, to the extent possible, critical information on business partners and transactions empower individuals to make the appropriate choices on behalf of the company.

The articles in this issue discuss the importance of these three components in a number of contexts. Our article on "Adequate Procedures Guidance" for the UK Bribery Act discusses the expectation that companies will exercise judgment regarding the adequacy of procedures. "How Well Do You Know Your ESP?" discusses the importance of transparency in understanding partners like email service providers. The transparency provided by the internet has to be carefully managed in business inquiries and investigations as noted in "The Double Edged Sword." The excerpt from *Foreign Corrupt Practices Act Compliance Guidebook* illustrates the critical component of tone from the top in Siemens' transformation to a "Culture of Compliance." "Double Duty" authors point out that forensic accountants provide clarity into accounting systems and financial reporting both during an investigation and after in recommending enhancements to internal controls.

We hope you find this issue of *IQ* magazine to be informative and enlightening and welcome your comments and questions.



Adequate Procedures Guidance

The UK Bribery Act

- » The UK Bribery Act of 2010 provides that commercial organisations will be guilty of a criminal offence if a person associated with them bribes another person.
- » The Bribery Act provides commercial organisations with a defence if “adequate procedures” can be proven to be in place during the time of the alleged infraction.
- » The Bribery Act provides that the UK Government should publish Guidance about “Adequate Procedures”.
- » The Guidance was issued in March 2011 containing six principles.
- » Even with this Guidance, the onus is on the organisation to determine the appropriate procedures to prevent bribery within its operations.
- » The best approach to making that determination is to conduct a detailed and comprehensive risk assessment.

The United Kingdom’s Bribery Act of 2010 will come into force on 1 July 2011. The fact that the Act creates a new, strict-liability offence, which will be committed by commercial organisations, including companies, if persons providing services on their behalf pay bribes intending to obtain a business advantage for the organisation, has attracted particular attention and has caused significant concern within the business community. The Act does however contain a defence if the organisation can establish that it had “adequate procedures” designed to prevent the bribery. Inevitably this has generated much speculation about how these procedures need to be structured. The Act obliged the Government to publish Guidance about the procedures.

The Guidance was finally published on 31 March 2011 (“the Guidance”). The Guidance provides clarification regarding the intended scope of the offences provided for in the Act. At the same time, the Director of the Serious Fraud Office and the Director of Public Prosecutions have also

Illustration by Peter Giesbrecht



published guidance on prosecutions under the Act which confirms that Prosecutors must take account of the Guidance when considering the adequacy of organisations’ procedures. In large part the Guidance and the prosecutors’ guidance seek to restore a modicum of calm within the business community that the Government does not intend to apply an unreasonably wide interpretation of the Act’s ostensibly far-reaching provisions.

Nature of the Guidance

The Guidance recommends that an organisation’s anti-corruption procedures should be informed by six principles. The Guidance is at pains to point out that these principles are not intended to be prescriptive, nor are they intended to be exhaustive in their scope. Accordingly, the adequacy of an organisation’s anti-

corruption procedures will depend in the final analysis on the facts of each case. The emphasis therefore remains firmly on the organisation to make its own determination, preferably having regard to the Guidance’s six principles, of what procedures it should put in place.

The Guidance’s six principles are:

1. **Proportionate procedures:** “A commercial organisation’s procedures to prevent bribery by persons associated with it are proportionate to the bribery risks it faces and to the nature, scale and complexity of the commercial organisation’s activities. They are also clear, practical, accessible, effectively implemented and enforced.”

The Guidance highlights the importance of a detailed risk assessment being undertaken in order that appropriate procedures can

be developed which are a practical and realistic means of achieving the anti-corruption objectives. The Guidance provides an indicative but not exhaustive list of areas which such policies may cover. The Guidance recognises that it is difficult for an organisation to apply procedures retrospectively to associated persons, e.g., because there might already be a defined contractual relationship, and suggests that this should be done over time on a risk-based approach.

2. **Top-level commitment:** *“The top level management of a commercial organisation ... are committed to preventing bribery by persons associated with it. They foster a culture within the organisation in which bribery is never acceptable.”*

It is clear that the Government does not consider it acceptable for an organisation to leave anti-corruption matters for junior employees. Top-level commitment will in most cases include senior management involvement not only in the determination of what are appropriate policies for the organisation but also in the communication (both internally and externally) of the organisation’s anti-corruption stance.

3. **Risk assessment:** *“The commercial organisation assesses the nature and extent of its exposure to potential external and internal risks of bribery on its behalf by persons associated with it. The assessment is periodic, informed and documented.”*

The Guidance emphasises that the risk assessment needs to be proportionate to the size and structure of the organisation and the nature, scale and location of its activities. The risk assessment should include both external (e.g., jurisdictional, transaction- and entity-related) and internal (e.g., risks arising from deficiencies in employee training, skills and knowledge or the organisation’s

remuneration policy) risks. The risk assessment is the key determinant of what policies the organisation should have.

4. **Due diligence:** *“The commercial organisation applies due diligence procedures, taking a proportionate and risk based approach, in respect of persons who perform or will perform services for or on behalf of the organisation in order to mitigate identified bribery risks.”*

There is obviously overlap between the requirement to carry out due diligence and the need for a risk assessment referred to in principle 3 above. The Guidance notes that the due diligence procedures should be proportionate to the risks inherent in the particular relationship which the organisation had with the relevant person; e.g., a UK provider of IT services to the organisation is likely to have a very different risk profile than a representative in a country with a poor corruption reputation who seeks to win government work on behalf of the organisation. Due diligence should include not only measures carried out prior to entering into a relationship but should also involve continued monitoring of associated persons.

5. **Communication (including training):** *“The commercial organisation seeks to ensure that its bribery prevention policies and procedures are embedded and understood throughout the organisation through internal and external communication, including training, that is proportionate to the risks it faces.”*

This principle focuses on the need to ensure that policies are properly understood and applied by relevant employees within the organisation through communication and training. The Guidance also notes that communications should include both internal communications and external communications. Companies also need to determine whether specific, tailored training to employees



in particular roles or for persons associated with the organisation is required.

6. **Monitoring and review:** *“The commercial organisation monitors and reviews procedures designed to prevent bribery by persons associated with it and makes improvements where necessary.”*

This principle seeks to highlight the importance of organisations ensuring that their procedures remain relevant to what could be a changing risk profile and also identifies the importance of organisations monitoring their arrangements to ensure that they remain fit for the purpose.

What Therefore Needs to Be Done?

From the perspective of commercial organisations, and at the risk of echoing the

caveats in the Guidance, there is unfortunately no “one size fits all” solution when it comes to determining what are appropriate procedures. What might be appropriate in the case of one company will not necessarily be so in the case of another company. The starting point for commercial organisations in terms of assessing what policies and procedures would be appropriate for them to have is for them to undertake a detailed and comprehensive risk assessment under the direction of senior management and other relevant members of staff.

In the normal course, commercial organisations would seek, as part of the overall risk assessment, to evaluate the nature of the businesses they undertake, the jurisdictions in which business is undertaken and how those businesses are undertaken, e.g., to what extent do individuals and entities perform services for them. In large organisations bespoke questionnaires might be sent to relevant employees to obtain information. Ideally the commercial organisation’s risk assessment should be a stand-alone document which someone unfamiliar with the organisation and business practice can follow and can readily understand why the procedures which have been implemented are



adequate ones having regard to the specific nature of the risks presented by the organisation’s particular business model. The existence of such a document would hopefully assist, in a worst-case scenario, an organisation to explain why its procedures were appropriate.

The risk assessment should include information about the commercial organisation, possibly with a corporate tree attached and a more detailed description of various sorts of business transactions in which it is involved, to include details of how it contracts, whether it ever uses representatives or distributors in any jurisdiction. It might be sensible to list out when a commercial organisation has historically dealt with suppliers, and if different, when it might deal in the next 12 months or so and specify how the organisation deals with such suppliers. The risk assessment should seek to provide information about relevant internal controls and procedures which the organisation has in place and how these are considered to mitigate risk.

The risk assessment should seek to identify those persons who perform services on the organisation’s behalf and then grade them in some way according to risk. Having categorised these risks in this manner, the commercial organisation will then have to decide how to deal with such risks going forward and those which are inherent in any existing relationships. So far as new relationships are concerned this would include undertaking appropriate due diligence on partners and suppliers and the insertion of anti-corruption provisions in contracts.

The risk assessment itself should include some detail around the company personnel who have been involved in undertaking a risk assessment, i.e., levels of seniority and methodology. Consideration should also be given to describing the extent to which conversations have taken place with company employees in order that the risk assessment document demonstrates the importance which the

organisation has attached to undertaking appropriate risk assessment. The company will also need to ensure that it then develops and implements appropriate policies and procedures and ensure that its staff understand the procedures and the reasons for them with appropriate education and monitoring of the procedures being put in place.

With these principles in mind organisations should be reviewing their existing policies to ensure that they are fit for the purpose or, alternatively, ensure that they are putting in place such policies and procedures prior to 1 July 2011.

Other Issues Covered by the Guidance

The Guidance also provides clarification in respect of the nature and scope of the offences provided for in the Act.

Jurisdictional scope – the corporate offence of failing to prevent bribery applies to companies, wherever they might be incorporated, if they conduct part of their business in the UK. Once that is established the Act then applies in relation to the company’s non-UK business. The Guidance clarifies that the mere fact that a company’s shares are traded on the London Stock Exchange should not, of itself, be enough to bring that company within the scope of the Act. Similarly, having a UK subsidiary will not, of itself, mean that the parent company is carrying on business in the UK.

Associated persons – as mentioned above, a commercial organisation commits an offence under the Act if a person associated with it bribes another person intending to obtain or retain business or a business advantage for that organisation. An associated person is defined as someone who provides services for or on behalf of a commercial organisation. In addition to employees, this definition can also encompass agents, subsidiaries, contractors and suppliers where they

can be said to be performing a service rather than simply acting, in the case of a supplier, as the seller of goods. The Guidance recognises the breadth of this provision and notes that, where a supply chain involves several entities or a project involves a contractor and a number of sub-contractors, a commercial organisation is likely only to exercise control over its relationship with its own counterparty. The Guidance therefore suggests that the main way to manage bribery risk in such a situation is by requesting its counterparty to adopt a similar approach with the next party in the chain rather than expecting the commercial organisation, as part of its adequate procedures, to exercise due diligence on all parties in the chain.

Joint ventures and subsidiaries – the Guidance clarifies that simply being a member of a joint venture entity does not create an “association” with other joint venture partners and so a bribe paid on behalf of the joint venture entity by one of its employees will not automatically trigger a liability for the joint venture members simply because they benefit indirectly through their investment in the joint venture. However, a member will incur liability if the joint venture entity is performing services for that member and the bribe was offered or paid with the intention of benefiting the member. The key focus will therefore be on the intention – did the associated person intend to benefit the organisation?

Where a joint venture operates through a contractual arrangement (in contrast to there being a separate legal entity as referred to above), the level of control will be one of the circumstances that will be taken into account in deciding whether a person offering or paying a bribe on a joint venture’s behalf was performing services for that participant. Even in this situation the Guidance makes clear that it is the intention to benefit the organisation that is relevant. A parent entity will not be liable where a subsidiary pays a bribe

simply as a result of receiving dividend income from the subsidiary.

Foreign public officials – the Guidance seeks to clarify that the Act does not seek to prohibit bona fide hospitality and promotional or other business expenditure which seeks to improve the image of a commercial organisation. The offence of bribing a foreign public official (section 6) will be made out only where there is evidence to show a connection between the advantage offered or given and the intention to influence the official and secure a business advantage. The more lavish the hospitality or higher the expenditure, the easier it will be to infer that such an intention existed. The Guidance clarifies that the provision of reasonable travel and accommodation expenses to allow foreign public officials to attend a site visit in the UK should be permissible.

Directors’ Prosecution Guidance

The Director of the Serious Fraud Office and the Director of Public Prosecutions’ Guidance on prosecutions under the Act sets out the various public interest factors for and against a prosecution in respect of each of the offences as well as offering clarification on certain aspects of the Act.

Facilitation Payments

- » The Prosecution Guidance recognises the difficulties which organisations face in some parts of the world and that the eradication of such payments is a long-term objective.
- » Whilst the Prosecution Guidance confirms there is no exemption from the Act in respect of facilitation payments and a prosecution will usually take place unless the prosecutor is sure that the public interest factors tending against prosecution outweigh those tending in favour.

- » The public interest factors against prosecution include circumstances in which there is a single small payment likely only to result in a nominal penalty; the penalty came to light as a result of a proactive approach involving self-reporting and remedial action; the organisation has a clear and appropriate policy setting out procedures which should be followed if facilitation payments are requested and these are correctly followed; or the payer was in a vulnerable position arising from the circumstances in which the payment was demanded.
- » Factors in favour of a prosecution would include circumstances where large or repeated facilitation payments were made, a suggestion of active corruption of the official or payments which are planned for or accepted as part of the cost of conducting business and the failure to follow the organisation’s procedures.

Hospitality and Promotional Expenditure

- » The Prosecution Guidance emphasises that the Act does not seek to penalise legitimate hospitality and promotional expenditure. However, the more lavish the hospitality, the greater the likelihood of an inference being drawn that it was intended to influence, e.g., a foreign public official. This could be the case where the hospitality is not clearly connected with a legitimate business activity or an attempt has been made to conceal the expenditure or activity. ■

Stephen is an Of Counsel in Herbert Smith’s Litigation and Arbitration division. Stephen has extensive experience of advising clients in relation to both domestic and international contentious matters, particularly in relation to banking and financial services. Stephen conducts and manages internal investigations for clients as well as advising clients in relation to investigations by the FSA and SFO. Stephen also advises clients on anti-corruption policies and procedures.

PAUL BOND, pbond@reedsmith.com
 CHRISTOPHER CWALINA, ccwalina@reedsmith.com
 DAN HERBST, dherbst@reedsmith.com

How Well Do You Know Your ESP?

Managing the risks of data security with Email Service Providers

Illustration by Peter Giesbrecht



- » Email Service Providers (ESP) handled confidential data for their clients and for their clients' clients.
- » Data breaches by third-party vendors like ESPs are equally as impactful as data breached within an organization itself.
- » Taking steps to know your ESP and how they protect data is key to limiting reputational and legal risks associated with data breach.

Anxieties were high at hundreds of the world's largest companies when news broke of two recent high-profile data security breaches by email service providers ("ESPs") Epsilon and Silverpop. Compliance officers scrambled to determine what happened, whether data was breached, what data the ESP had, if breach notices were required, and who should receive notice. Called "the Breach of the Century," the press had a field day, with major news

outlets (ABC, WSJ, MSN, CNN) running stories with headlines like "You may not know Epsilon, but they know you." Senators Franken (D-Minn.), Pryor (D-Ark.) and Blumenthal (D-Conn.) all demanded answers and asked for investigations to be conducted by the FTC and DOJ. Where this all shakes out is unknown, but with government inquiries and possible litigation on the horizon, it is certain to be expensive not only for the ESPs, but for

their customers as well. If a lesson is to be learned from these recent events, it is that the company's brand name and bottom line, and not the ESP, are most at risk from data security breaches.


Data security breaches by ESPs pose significant risks to their companies that fail to take appropriate steps to mitigate risk and put in place contingency plans for data breaches. The first thing companies should do now is evaluate their use of ESPs. Do you even know whether you are using outside third parties for email management; and if you are using ESPs, do you need to be using them or is this something you can handle in-house? Once you've done an inventory and know who has your customer data, and you decide to go ahead and use ESPs for email marketing, you should take the appropriate steps to avoid legal and reputational exposure:

- » First and foremost, find the right ESP vendor by performing thorough due diligence into the vendor's capabilities, reputation, and security policies and procedures.
- » Review critical sections of the actual or potential agreements with ESPs: understand rights and demand responsibilities in the event of a breach, including warranties on information security; *force majeure*; indemnification; and duties to cooperate. Ensure adequate representations pertaining to information-security protections.
- » Explore insurance coverage options, including coverage for ESP. This point is often overlooked but can be critical when something bad happens.
- » Disclose what data is collected and how it is used: understand exactly what the data is, and more importantly, exactly the specific data elements that you are providing to

the ESP, and disclose to consumers at point of data collection that a third party may use the data.

- » Use ESPs as ESPs, not as general repositories for all customer information. In other words, only use ESPs for the narrow function of sending email marketing to customers, and limit the amount of customer data provided to the ESP.
- » Establish a proper oversight program for the ESP: conduct periodic oversight or audits to ensure the data is used only for the purposes provided, and that security procedures are maintained.
- » Develop a response plan for a breach.

Although data breaches are certain to occur in the future, taking appropriate steps will help to limit reputational and legal risk associated with data breaches by ESPs. One thing we know for sure, as it seems a new hacking attack is announced daily, the bad guys are out there, looking for data they can make use of, and they are coming after not only the brand name targets, but now they are also coming after the service providers that the brand names use.

Paul Bond is a Partner in the Princeton, NJ office of Reed Smith and a member of the Global Regulatory Enforcement Group, practicing in the areas of data privacy, security, and management. Paul counsels clients on how to meet their obligations under, e.g., the Gramm-Leach-Bliley Act, HIPAA, the Fair Credit Reporting Act and its Identity Theft Red Flags regulations, and the dozens of other federal and state privacy law and regulations. He co-authored the Data Privacy & Security chapter of the Social Media White Paper entitled "A Legal Guide to the Commercial Risks and Rewards of the Social Media Phenomenon." 

Christopher G. Cwalina is Counsel in Reed Smith's Washington D.C office and a member of the Global Regulatory Enforcement (GRE) Group. He has extensive experience in data privacy class action litigation and data privacy compliance. Chris has defended companies in a variety of privacy-related matters including security breach related litigation and flash cookie cases. He has advised corporations on regulatory issues and legislative affairs pertaining to data privacy and information security issues as well as provided counsel on compliance with CPNI rules, GLBA, HIPAA, FCRA, COPPA, FCPA, and international privacy rules including the Data Protection Act.

Daniel Z. Herbst is a senior associate with Reed Smith's Washington Office. He is a member of the firm's Global Regulatory Enforcement Group and has diverse practice which principally involves commercial and administrative litigation and counseling. Dan is a member of the Social and Digital Media Task Force. He co-authored the Government Contracts & Investigations chapter of the Social Media White Paper entitled "A Legal Guide to the Commercial Risks and Rewards of the Social Media Phenomenon."



EDWARD McNICHOLAS, emcnicholas@sidley.com
 SABRINA ROSS, sbross@sidley.com¹

The Double-Edged Sword

Investigations in the age of social media: Practical advice for addressing evolving technologies

Illustration by Josh Leipziger

- » Accessing information available on social media sites can be critical to compliance in employee vetting and litigation strategy.
- » There are significant risks if you run afoul of the legal protections that may be available in certain circumstances.
- » Companies need to balance the pursuit of valuable information with the rapidly evolving law and regulations around data privacy on the web.

Social media sites are rapidly expanding the flow of information about both individuals and corporations. This flood of new information is likewise transforming the tools available to investigators for employee vetting, reputational due diligence, litigation assessments and other investigations. The use of social media, however, can create new risks for investigators and their clients if evolving laws and regulations are not observed. This article provides some practical tips on the appropriate use of social media during investigations.

Employee Vetting

U.S. employment law has long recognized a nearly pervasive ability for employers to monitor their employees at work, and there are many permissible reasons for employers and prospective employers to monitor social networking sites in order to further understand their employees and prospective employees. Social media certainly makes it possible for employers and their investigators to gather additional information on job or acquisition candidates to supplement their application profiles, or corroborate information provided by applicants and/or current employees. Moreover, social networking sites enhance the ability of investigators to investigate employees when there is reason to believe that an employee has engaged in conduct that is detrimental to



the company or the employee's employment relationship with the company.

Indeed, in certain circumstances, the failure to conduct an investigation that includes social media could undercut an employer's defense that it was reasonably diligent in policing workplace harassment and enforcing other norms. Moreover, employees, sometimes unintentionally, can leak very significant information about new products and plans, delays, internal strife, and even the financial viability of their employers on social media. A failure to police the exposure of such trade secrets on the Internet can have significant practical consequences for companies.

Some of the risks of investigating employees are already well known, such as the need to comply with the Fair Credit Reporting Act (and analogous state laws) when obtaining investigative consumer reports from consumer reporting agencies. Investigative use of social media, however, has brought new significance to some existing legal risks, particularly violations of off-duty conduct statutes and violations of non-discrimination laws.

Off-Duty Conduct Statutes. So-called "off-duty conduct statutes" are generally divided into consumption statutes and lifestyle discrimination statutes.

¹ Mr. McNicholas is a partner and Ms. Ross is an associate in the Privacy, Data Security and Information Law Group of the international law firm of Sidley Austin LLP. The views expressed herein are exclusively those of the authors personally and do not necessarily reflect the views of any other entity, client, or association. This article is published for informational and educational purposes only and is not legal advice.

Although many companies add clauses to their social media policies suggesting that outrageous online behavior can have employment consequences, it is important to proceed with care before taking an employment action based on photos of ill-considered weekend activities. Around 30 states have enacted “consumption statutes” protecting employees from adverse employment actions based on their lawful consumption of legal products (such as tobacco or alcohol) while off-duty.² Even where it is legal to discipline employees for their lawful consumption of alcohol and/or tobacco, it is best to proceed carefully when disciplining employees who consume alcohol or tobacco while off-duty, particularly if the company would be unwilling to take such an action against other similarly situated employees in the future (and of course where there are addiction issues that may raise Americans with Disabilities Act concerns).

Far broader and more rare than “consumption” statutes, “lifestyle discrimination” statutes protect employees from discrimination based on a broad range of lawful off-duty conduct, political activities, and/or beliefs. Four states have lifestyle discrimination statutes that restrict the ways employers can discipline and even terminate employees for non-criminal conduct outside the workplace.³ California has what is arguably the broadest example of such a statute. Cal. Lab. Code § 96(k) expressly protects, with limited exceptions, “lawful conduct occurring during nonworking hours away from the employer’s premises.”

Two states, Massachusetts and Connecticut, have weaker laws that afford employees more limited protections. Massachusetts protects employees from unreasonable interference with highly

personal private matters; an exception exists for searches when an employer can articulate legitimate business reasons for seeking the information at issue.⁴ Connecticut prohibits discipline or discharge of employees for the exercise of their First Amendment rights (concerning matters of public concern); an exception exists if activity interferes with an employee’s bona fide job performance or the working relationship between the employee and employer.⁵

All states – except California – recognize a legitimate business need as an exception to the prohibition against adverse employment actions, and courts have generally afforded employers broad discretion to discipline/discharge employees where such off-duty behavior was shown to have damaged a company or its business interests. In other words, if an employee’s off-duty conduct could harm the company, then it can likely discipline or terminate the employee.

Non-Discrimination Laws. Monitoring social media sites also creates risk around non-discrimination laws, which generally require that employers not take any adverse actions against applicants or employees based on knowledge of their race, color, religion, sex, national origin, disability, age, and, in certain jurisdictions, other protected characteristics such as sexual orientation. In addition, an entity may not legally take any adverse actions against an applicant or employee based on knowledge that the employees have engaged in concerted or protected activities, including where employees exercised their Section 7 rights under the National Labor Relations Act (“NLRA”). The NLRA protects employees who engage in concerted activities for their mutual aid and protection, including where they engage

in discussions concerning their wages, benefits, or other terms or conditions of their employment. Individuals may also be protected against retaliation to the extent they are complaining of unlawful harassment or discrimination at work. Although social media postings making false claims about discrimination or unsafe working conditions could certainly provoke employer ire, it is wise to proceed with care in addressing them.

In light of the prohibitions, some companies indeed use outside search firms to conduct the initial scans of information from social media sites with the express, written direction to the search firm that no information about protected activities be contained within the report back to the company. Although it may be tempting for the company attorney or HR personnel to search personally, it is no doubt more prudent if they can shield themselves from knowledge that could be used as the basis for a claim that an action was taken for an impermissible purpose.

Stored Communications Act (“SCA”). Particularly in the context of employer or investigative monitoring of social media sites, it is also important to consider expectations of privacy and the Stored Communications Act, 18 U.S.C. § 2701*et seq.* *Pietrylo v. Hillstone Restaurant Group* makes this point clearly. In that case, an employee created a group on MySpace called “The Spec-Tator,” where employees – by invitation only – could “vent about ... work without any outside eyes spying in on us. This group is entirely private, and can only be joined by invitation.” The site contained ethnic slurs and derogatory comments about guests and managers as well as discussions about drug use and sexual acts. A non-manager employee joined the online group and showed

2. See, e.g., 820 ILCS 55/5 (prohibiting employment action “because the individual uses lawful products off the premises of the employer during nonworking hours.”).

3. See Cal. Lab. Code § 96(k) (protecting, with limited exceptions, “lawful conduct occurring during nonworking hours away from the employer’s premises”); Colo. Rev. Stat. Ann. § 24-34-402.5(1) (protecting, with job and conflicts limits, “any lawful activity off the premises of the employer during nonworking hours”); N.Y. Lab. Law § 201-d(2)(c) (protecting, with a conflicts limit, “legal recreational activities outside work hours, off of the employer’s premises and without use of the employer’s . . . property”); N.D. Cent. Code § 14-02.4-01 (protecting, with a conflicts limit, “lawful activity off the employer’s premises during nonworking hours”).

4. M.G.L. Ch. 214, § 1B; *Bouley v. City of New Bedford*, 2005 US Dist LEXIS 30922 (D. Mass. 2005).

5. Conn. Gen. Stat. § 31-51q.

content to a manager, who then used the non-manager employee's account name and password to access the account and show it to other managers. Two workers were fired; one sued. A jury found that the company's managers had violated the SCA and a state surveillance law by intentionally accessing the MySpace page without authorization.⁶ The jury, however, found in favor of the defendants on the employee's claims for invasion of privacy, finding that the plaintiffs had no reasonable expectation of privacy in the MySpace group.

Social Media in Litigation

As in the employment context, social media is frequently becoming a significant source of information about various participants in investigations and litigation including judges, jurors, attorneys, and witnesses.

Pre-Trial Privacy Expectations and Social Networks

During pre-action and pre-trial investigations, attorneys and investigators can take advantage of social search and monitoring tools to find relevant information and, in some cases, keep up with individuals' activity. The legal contours of privacy expectations, however, are still highly unsettled in social media technologies. For example, privacy policies do not entirely protect social network subscribers from legal processes.⁷ Increasingly, and as has happened with email, social network subscribers' private profile pages are drawn into public processes through subpoena or discovery. Indeed, a growing number of cases involve discovery or related procedural requests by defendants.

On occasion, however, attorneys and consultants have been overly aggressive in collecting semi-public information, and it is certainly clear that attorneys cannot use deception to obtain information from social media or otherwise contact a represented party during the course of litigation. Efforts to hack into social media sites could well violate state computer crime laws as well as the federal Computer Fraud and Abuse Act, 18 U.S.C. § 1030, if computers in interstate commerce are accessed without authorization (or in excess of authorization) and damage results. Moreover, in California, SB 411 – now passed into law – criminalizes “opening an email account or an account or profile on a social networking Internet Web site in another person's name.” Accordingly, it is important to conduct investigations in a prudent manner that respects the legal limitations on technological exploits. In this regard, it is vital for the counsel involved to understand and vet the sources and methods used by investigators in order to avoid the investigation spiraling into collateral litigation.

Most frequently, social media communications are requested by one party to expose alleged duplicity. For example, in *Beye v. Horizon Blue Cross Blue Shield of New Jersey*, a father sued his health insurance company after the insurer refused to pay benefits for the treatment of his child for an eating disorder.⁸ The District Court ordered the plaintiff to produce non-public evidence that was posted on social networking sites, even if it reflected sensitive medical conditions, because of the diminished expectation of privacy due to the posting and sharing of the information.

By contrast, in *Crispin v. Christian Audigier, Inc.*, a California district court recently protected “private content” on social media in a suit for copyright infringement.⁹ Defendant Audigier served subpoenas duces tecum on Facebook, MySpace, and Media Temple (a web hosting service) seeking Crispin's subscriber information, all communications between Crispin and a witness, and all communications that referred to or were related to Audigier or sublicensees of his work. The court held that private messages exchanged on Facebook and MySpace are no different than standard Internet email exchanges.¹⁰ Because the SCA prevents providers of communications services from divulging private communications and has no exceptions for service of civil legal process, the court quashed the subpoenas as they related to private messaging.¹¹ With respect to the Facebook wall postings and MySpace comments, the court remanded the matter to the magistrate judge to determine whether this information was publicly available.¹²

Whether privileges in social media are ultimately respected, it is clear that requests for a “fishing expedition” into social media posts will be met with skepticism. For instance, in *McCann v. Harleysville Ins. Co.*,¹³ a New York state appellate court panel confronted the relevance of social media in a personal injury action. The trial court denied defendant's motion to compel production of photographs from a social media page and full authorization for plaintiff's Facebook account as overly broad, and the appellate court upheld this ruling. The appellate court, however, also ruled that the lower court's granting of a blanket protective order for production

6. 2009 U.S. Dist. LEXIS 88702 (D. N.J. 2009).

7. See, e.g., Facebook's Privacy Policy, <http://www.facebook.com/policy.php> (last visited February 10, 2011) (“We may disclose information pursuant to subpoenas, court orders . . . if we have a good faith belief that the response is required by law.”).

8. *Beye v. Horizon Blue Cross Blue Shield of New Jersey*, No. 06-5337, 2008 WL 3064757 (D.N.J. Jul. 29, 2008).

9. *Crispin v. Christian Audigier, Inc.*, 717 F. Supp. 2d 965 (C.D. Cal. 2010).

10. *Id.* at 979.

11. *Id.* at 991.

12. *Id.*

13. 9 N.Y.S.2d 614 (App. Div. 4th Dept Nov. 12, 2010)

of Facebook account information was an abuse of discretion.

The blurred line between public and private spaces leaves open questions regarding the application of tort law in this area. The common law of privacy consists of a group of limited tort causes of action. Most jurisdictions recognize four causes of action for invasion of privacy: intrusion, public disclosure (or publicity) of private facts, false light, and appropriation of another's name. In the context of an investigation, the intrusion tort is most relevant, and it occurs when there is an unauthorized intrusion or prying into a private matter that is highly offensive or objectionable to a reasonable person and which causes anguish and suffering.¹⁴

As courts' articulation of an actionable intrusion has modernized to keep pace with technology, their approach has become more nuanced, and specific norms will no doubt evolve for social media in the case law. At present, however, investigators should be particularly cognizant of whether the particular social media examined would be considered private by the investigated individual, and whether their search techniques, however clever, could be highly offensive or objectionable to a reasonable person.

Courtroom Social Media

In the courtroom, social media is increasingly used for juror research, evaluating judges, and witness background checks. And lawyers and judges are grappling with these new issues raised by social media technologies.

At present, the rules for jurors remain relatively clear. Jurors who talk about cases on social networking sites, or use the Internet to conduct independent research outside the evidence presented in court,

can cause mistrials, overturn a conviction, or even create liability for themselves.¹⁵ In 2010, the Judicial Conference of the United States released a set of updated juror instructions, advising judges to specifically tell jurors not to talk about a case on social networking sites or do online research. In addition to these explicit instructions, some courts have even issued new restrictions on the use of cell phones, including bans on cell phones in the courthouse or the confiscation of phones from jurors not only because of the annoying rings but also because of the ability to receive news and conduct research on so-called "smart" phones.

States have also considered the "friending" of judges, but approaches have diverged. One Florida ruling did find a violation of judicial ethics based on friending by a judge.¹⁶ In contrast, an Ohio ethics panel was generally comfortable with a judge who is a "friend" on a social media site with a lawyer who appears as counsel before her. Significantly, the decision acknowledges that a friend on sites like Facebook is not the same as a real-world "friend," and it notes that, in certain circumstances, such a relationship could improperly diminish confidence in the fairness of the judicial system or suggest that someone is in a position to influence the jurist in an unfair manner. The panel did not conclude that "friending" between lawyers and judges via this online means is *per se* prohibited by the rules of judicial conduct, but urged caution to avoid those situations where violations could occur. The Kentucky Ethics Committee and other state ethics panels, moreover, have reached similar conclusions.¹⁷

Concluding Thoughts

At present, however, the only certainty is that the norms regarding the use of social

media during investigations are rapidly evolving. Investigators can most thoroughly serve their clients if they develop a comprehensive understanding of the social media tools and industry best practices.

Unless companies make use of investigators who understand the full extent of social media, they can leave valuable information out of their investigations or fail to see the warning signs of leaking trade secrets, harassment and other problems. Companies, however, should exercise restraint in their social media investigations and ensure that their own quest for information does not run afoul of the variety of evolving statutory and common law restrictions at play. ■

Edward R. McNicholas is a partner in the Washington, D.C., office of the international law firm Sidley Austin LLP and a global coordinator of its Privacy, Data Security, and Information Law practice. His practice focuses on clients facing complex information technology, constitutional and privacy issues in civil and white-collar criminal matters. Mr. McNicholas concentrates his practice on trial and appellate representations of technologically-sophisticated clients including telecommunications carriers, electronic service providers, financial services companies, pharmaceutical manufacturers and other companies facing complex personal information issues. He is also an experienced counselor, public policy advocate and internal investigator.

Sabrina B. Ross is an associate in the Washington, D.C., office. Ms. Ross earned her law degree from the Berkeley School of Law at the University of California, where she was a submissions editor of the Berkeley Journal of International Law. She received her undergraduate degree in English, with honors, from Grinnell College. While in law school, Ms. Ross was selected for the Afghanistan Rule of Law Fellowship with the Miller Institute for Global Challenges and the Law and won the Prosser Prize for International Trade.

14. See, e.g., *Lovgren v. Citizens First Nat'l Bank of Princeton*, 534 N.E.2d 987, 989 (Ill. 1989) (recognizing requirement that intrusion must be "highly" offensive); see also Restatement (Second) of Torts § 652B (1966).

15. See, e.g., *State of New Jersey v. Scott*, 2009 N.J. Super. Unpub. LEXIS 1901 (N.J. App. Div. July 20, 2009) certification denied, 2009 N.J. LEXIS 1370 (N.J., Nov. 9, 2009).

16. Florida Sup. Ct., Judicial Ethics Advisory Committee, Op. 2010-06 (2010).

17. Ethics Committee of the Kentucky Judiciary, Formal Judicial Ethics Op. JE-119 (2010).

MARTIN T. BIEGELMAN, martin.biegelman@navigant.com
 DANIEL R. BIEGELMAN, dbiegelman@bakerlaw.com

Siemens

A new commitment to a culture of compliance

For a company with a proud and innovative history dating back to 1847, nothing is more painful and embarrassing than to be connected to the largest bribery investigation and prosecution ever conducted. That was the predicament in which German engineering giant Siemens AG, a member of the Fortune Global 500, found itself. The fact is that for almost two decades, some Siemens employees engaged in a pervasive scheme to bribe foreign government officials on a worldwide basis to obtain and retain business.

Siemens AG is a recognized global leader in electronics and electrical engineering, operating in the energy, and healthcare sectors, with over 430,000 employees in more than 190 countries. After the devastation of World War II, the company began to rebuild with a focus on emerging markets, such as Asia Pacific, the Middle East, Africa, South America, and Central and Eastern Europe.

Corruption and payoffs were entrenched in many of the emerging markets in which Siemens operated. It was not alone as a company in paying bribes in these countries, as it was an accepted and expected practice. Siemens employed a variety of corrupt practices that enabled the collection of corporate funds to be distributed as bribes to foreign government officials and others to win business. Included was the use of off-books accounts to maintain slush funds. Much of the distribution of these bribes was done through third-party business consultants.

Prior to 1999, German companies were able to deduct bribes paid to foreign government officials as a business expense in their tax returns. In practice, this did not always occur, as the deduction required documentation evidencing the fact that the bribe was a necessary part of the business transaction.

When Siemens was first listed on the New York Stock Exchange ("NYSE"), in 2001, it came under the issuer requirements of that stock exchange, including

compliance with securities laws and the Foreign Corrupt Practices Act (FCPA), but the company continued to pay bribes and conceal their existence.

After listing on the NYSE, Siemens' company officials began to address corruption with policies and procedures. Despite these efforts, the company subsequently learned of wrongdoing related to bribery by employees in various countries and failed to adequately investigate the allegations. Its compliance program was the proverbial "paper program," ineffective in stopping corruption.

The worst corruption scandal in Siemens' long history hit the headlines in November 2006, when the Munich Public Prosecutor's Office announced that it had uncovered \$257 million in suspicious transactions after searching the homes and offices of numerous Siemens' employees, including that of the then CEO. Some 36,000 incriminating documents were seized and six suspects were arrested.

One of those arrested, a former sales official, detailed the existence of slush funds, bribes to government officials in Africa, Russia, and the Middle East, and the involvement of senior company officials. Although there were ongoing investigations of Siemens on fraud and corruption allegations in other countries, the German investigation was proving to be the one that threatened to expose a myriad of criminal and civil violations.

Self Discloser and Subsequent Internal Investigation

Siemens realized the need to quickly respond to the growing crisis. On November 29, 2006, its senior executives and representatives of the outside auditor, KPMG, met and pledged to cooperate with the authorities. The company contacted the Department of Justice (DOJ) and the Securities and Exchange Commission to disclose information.

Illustration by Peter Giesbrecht



Siemens also began its own investigation. To ensure the independence of the investigation and to prove to regulators the legitimacy of the results, Siemens partnered with a law firm to conduct an internal investigation and evaluate the existing compliance program.

Siemens wanted the investigation to be comprehensive, to determine how far-reaching and pervasive the corruption was in the various business operations worldwide. The investigation would focus on areas of the business with the highest risk of corruption and the past conduct of senior management and the Audit Committee, as well as their possible knowledge and involvement in bribery.

The investigation "could not identify legitimate business purposes for approximately \$1.4 billion in expenditures and concluded that approximately \$805 million of the \$1.4 billion was intended, in whole or in part, to bribe foreign officials."²

Siemens also established a Project Office Compliance Investigation (POCI) to ensure the success of the investigation in a number of ways. The POCI scheduled interviews, provided technical support for document and data collections, and retained local counsel in countries involved in the investigation.

Siemens made it policy that it would be fully cooperative in all phases of the government investigation. Much of what was disclosed to the government investigators would not have been easily discovered if not for the comprehensive internal investigation, total cooperation and voluntary disclosures.

Compliance Comeback

Siemens began its “compliance comeback” in November 2006 in conjunction with the internal investigation and self-disclosures. The compliance efforts involved a three-phased approach.

First, there was the immediate response with the selection of external experts to conduct an independent investigation, the appointment of an ombudsman, tone at the top town-hall meetings and communications from the CEO and other senior leaders, restrictions on the use of business consultants, and centralized payments and bank accounts.

The second phase involved creating and implementing a comprehensive compliance program called “Prevent–Detect–Respond.” Prevent included new policies and procedures, program communication, creation of a compliance helpdesk, centralization and global expansion of the compliance function, and training. Detect included worldwide compliance investigations to address the many allegations and issues being escalated, compliance reviews, and newly created compliance controls. Respond included disciplinary actions and consequences for misconduct, global case tracking of all issues received and investigated, and monitoring for compliance effectiveness and continuous improvement. Tone at the top and the overall compliance organization resonated across these three elements.

Siemens’ internal investigation took almost two years and included:

- » 1,750 interviews with Siemens employees and other individuals
- » 800 informational briefings with employees to obtain background information
- » 82 million documents electronically searched to identify potentially relevant material
- » 14 million documents reviewed
- » 38 million financial transactions analyzed
- » 10 million bank records reviewed¹
- » 300+ lawyers, forensic accountants, and support staff
- » 1.5 million billable hours of work
- » \$1.4 billion in fees for outside counsel and forensic accountants
- » Investigative work in 34 countries

The third and ongoing phase focuses on becoming a “recognized leader” in corporate compliance. All three phases are intended to build compliance and a “culture of integrity” into the framework of the company.

Criminal Charges, Plea Agreements, and Fines

On December 15, 2008, in a federal courthouse in Washington, DC, Siemens and three of its subsidiaries pleaded guilty to violations of the FCPA.

As detailed in the criminal information charging document filed by the Department of Justice (DOJ), between the mid-1990s and 2007, Siemens used a variety of techniques to falsify its corporate books and records:

- » Using off-books accounts for corrupt payments even after compliance

risks associated with such accounts were raised at the highest levels of management

- » Entering into purported business consulting agreements with no legitimate business purpose, sometimes after Siemens had won the relevant project
- » Engaging former Siemens employees as purported business consultants to act as conduits for corrupt payments to government officials
- » Justifying payments to purported business consultants based on false invoices
- » Mischaracterizing corrupt payments in the corporate books and records as consulting fees and other seemingly legitimate expenses
- » Limiting the quantity and scope of audits of payments to purported business consultants
- » Accumulating profit reserves as liabilities in internal balance-sheet accounts and then using them to make corrupt payments through business consultants as needed
- » Using removable Post-it notes to affix signatures on approval forms authorizing payments to conceal the identity of the signors and obscure the audit trail
- » Allowing third-party payments to be made based on a single signature in contravention of Siemens’ “four eyes principle,” which required authorization of payments by two Siemens managers
- » Drafting and backdating sham business consulting agreements to justify third-party payments
- » Changing the name of purported business consulting agreements to

1. Siemens, “Statement of Siemens Aktiengesellschaft: Investigation and Summary of Findings with respect to the Proceedings in Munich and the US,” press release, December 15, 2008, <http://w1.siemens.com/press/pool/de/events/2008-12-PK/summary-e.pdf>.

2. Marjorie Doyle, “Meet Joel Kirsch, JD, Vice President and Chief Compliance Officer, Siemens AG, U.S. Operations,” *Compliance and Ethics Magazine*, Volume 6, Number 2, April 2009, 16.

“agency agreements” or similar titles to avoid detection³

Siemens pleaded guilty to two criminal counts involving the internal controls and books and records provisions of the FCPA. Subsidiaries in Argentina, Bangladesh and Venezuela each pleaded guilty to one conspiracy count to violate the FCPA.

As detailed in DOJ criminal information, in the period from 2001 to 2007, Siemens made corrupt payments totaling \$1.36 billion.⁴ The DOJ agreed to a plea agreement and penalties that, while strong, could have been far more punitive. Mitigating factors included exceptional cooperation, acceptance of responsibility, and sweeping compliance enhancements.

SIEMENS' COMPLIANCE OBJECTIVES

Create a Culture of Integrity

- » Move toward a value-based culture
- » Act as change agents (“tone from the middle”)
- » Make compliance a competitive advantage

Look Beyond Siemens

- » Benchmark with the best
- » Participate in Collective Action Projects. Show our commitment
- » Support the Compliance Monitor

Become More Efficient

- » Improve and simplify policies and control processes to minimize business disruption while continuing to accomplish compliance objectives

Reprinted with permission from Siemens AG © 2009.

Siemens paid a \$450 million criminal fine, the largest such fine in FCPA enforcement history. As part of its acceptance of responsibility for corporate wrongdoing and subsequent guilty plea, the company agreed to implement a ten-point corporate compliance program and retain an independent compliance monitor for a four-year period.

Siemens' Remedial Efforts

Just as Siemens' cooperation with government authorities was exceptional, its efforts to fix the pervasive corruption were extensive. The company's rebuilding efforts around corporate compliance have been unprecedented. Some of the many compliance program enhancements include:

- » Top management replaced and more than 900 disciplinary actions taken against employees
- » Reorganization of the compliance organization and significant increase in staff, reporting lines, and direction
- » Compliance presentations to top management in over 50 countries
- » 180,000 employees trained in compliance requirements
- » Compliance Helpdesk available 24/7 in more than 100 languages
- » Making compliance a strong component of compensation of senior managers⁵

As a result of this process, Siemens developed a new set of compliance objectives focused on creating a culture of integrity, being recognized as a leader in compliance, and increased efficiencies with respect to policies, controls, and continuous self-examination.

“The reorganization and remediation efforts of Siemens have been extraordinary and have set a high standard for multi-national companies to follow.”⁶

The Road Forward

Siemens corporate leadership has been very public in discussing the compliance failures at the company. While the company had policies and procedures, “the rules were not practiced, the values were not embraced, and leadership failed.”⁷ The company voices the costs of noncompliance in billions of dollars in fines and related costs for external consultants.

Effective compliance is not an option for Siemens. It's a mandate and an absolute requirement. As Joel Kirsch, then Vice President and Chief Compliance Officer, Siemens Corporation, headquarters for U.S. Operations, said, “The fact is, we will not get a second chance and another major compliance failure would likely be disastrous.”⁸

This article is excerpted from *Foreign Corrupt Practices Act Compliance Guidebook: Protecting Your Organization from Bribery and Corruption* by Martin T. Biegelman and Daniel R. Biegelman ©2010, John Wiley & Sons, Inc. Reprinted with Permission.

Daniel R. Biegelman is an Associate at the firm of Baker Hostetler. He works on a variety of litigation, investigatory, customer claims and bankruptcy matters in connection with Baker Hostetler's role as counsel to the court-appointed trustee under SIPA in the liquidation of Bernard L. Madoff Investment Securities LLC. He has worked extensively with claims filed by victims of the Madoff Ponzi scheme.

3. *U.S. v. Siemens Aktiengesellschaft*, Sentencing Memorandum filed December 12, 2008, United States District Court for the District of Columbia, 22–23.

4. *Ibid.*, 24–27.

5. Peter Y. Solmssen, “Fighting Corruption at Siemens” (presentation, University of Passau, Passau, Germany, October 11, 2008 (www.wiwi.uni-passau.de/fileadmin/dokumente/lehrstuehle/lambsdorff/Economics_of_Corruption_2008/Peter_Y_Solmssen.pdf).

6. *U.S. v. Siemens Aktiengesellschaft*, Sentencing Memorandum, 24.

7. Peter Y. Solmssen, “Fighting Corruption at Siemens” (presentation, University of Passau, Passau, Germany, October 11, 2008 (www.wiwi.uni-passau.de/fileadmin/dokumente/lehrstuehle/lambsdorff/Economics_of_Corruption_2008/Peter_Y_Solmssen.pdf).

8. Doyle, “Meet Joel Kirsch.”

Double Duty

The role of a forensic accountant during an internal investigation

Illustration by Nick Craine



receives a credible allegation of financial fraud. An attorney can assess the needs and obligations of the company in this instance, but, depending on the allegation, attorneys alone may not be perfectly suited to investigate the potential fraud. Early on, outside counsel should determine whether it is appropriate to retain a forensic accountant under a Kovel arrangement to assist with an internal investigation. The Kovel arrangement allows the attorney-client privilege to be extended to the work and communications of a forensic accountant working at the direction of counsel in anticipation of or in preparation for litigation.

A forensic accountant can assist counsel in an internal investigation by using investigative skills and an understanding of internal fraud controls and financial records to identify anomalies, irregularities, and evidence of fraud. While assisting with the internal investigation, the financial fraud specialist can provide the company with an assessment of its internal controls germane to the allegation and make recommendations to enhance any relevant control deficiencies.

Is a Forensic Accountant Needed and, If So, Who Should Be Hired?

When a company receives an allegation of financial malfeasance, counsel must consider whether a forensic accountant should be retained as part of the investigative team. Generally, if the alleged fraud is complex, affects a company's accounting and reporting system, or involves circumventing internal controls (if they exist), it is beneficial to the company and counsel to retain a qualified forensic accountant in the early stages of the investigation.

The hiring parties should seek answers to the following questions during interviews of forensic accountants:

- » In selecting a forensic accountant, there are critical questions that need to be asked and answered.
- » As we mark the 50th anniversary of *United States v. Kovel*, we look back at the significant precedent it set in the application of attorney-client privilege.
- » When participating in an internal investigation, forensic accountants should be expected to assess a company's relevant internal controls in addition to providing investigative support.

Between 2002 and 2008, over 1,300 corporate fraud convictions were obtained by the United States Department of Justice.¹ In these cases and others brought by various state law enforcement agencies and regulators, companies may have entered into agreements mandating fines, the disgorgement of ill-gotten gains, and the appointment of a monitor. In addition to financial consequences, companies may suffer irreparable damage to their reputation. Given this enforcement environment, a company is forced to react once it



recognize those privileges that exist at common-law. Second, Congress neither expanded nor restricted the scope of any particular privilege. Third, Congress gave deference to State Law as to determining the scope of the privilege. Therefore, an important factor in establishing privilege may be the law of the State in which the matter is being heard, even if the matter is venued in a Federal Court.

The essential common-law elements of the attorney-client privilege are: where legal advice of any kind is sought from a lawyer acting in that capacity, and the communications between the lawyer and the client are for such legal advice, and such communications are made in confidence, then the communications are protected by the attorney-client privilege.

Under *U.S. v. Kovel*, 296 F.2d 918 (2nd Cir. 1961), what is vital to the privilege is that the communication be made in confidence for the purpose of obtaining legal advice from a lawyer. If the advice that is sought is the advice of an accountant instead of a lawyer, then there is no privilege. This does not mean that the lawyer has to be present at all times when the accountant retained by outside counsel interviews the client, but the interview and work must be done at the request of the lawyer. Further, the advice of the accountant must be necessary, or at least highly useful, for effective consultation between the client and the lawyer.

1. Does the forensic accountant have the necessary investigative and accounting experience?
 2. Will the forensic accountant be able to identify and address weaknesses in internal controls?
 3. Can the forensic accountant conduct or assist with fact-finding interviews of key personnel?
 4. Does the forensic accountant have the experience to translate documented financial evidence and testimony into easily understood written and/or oral reports for the client?
 5. If necessary, will the forensic accountant serve as a credible witness when testifying about his or her findings?²
1. the services to be provided by the forensic accountant;
 2. the services provided are for counsel in connection with its representation of the corporate client;
 3. the work performed by the forensic accountant will be at the direction of counsel; and
 4. the understanding of all parties that all communications, either written or oral, among the forensic accountant, the outside attorney, and the corporate client will be treated as confidential and will be denoted as “privileged and confidential.”

Legal Background

Attorney-Client Privilege

In Federal Court, the attorney client privilege, as well as other privileges, is addressed by Federal Rules of Evidence § 501, which states:

Except as otherwise required by the Constitution of the United States or provided by Act of Congress or in rules prescribed by the Supreme Court pursuant to statutory authority, the privilege of a witness, person, government, State, or political subdivision thereof shall be governed by the principles of the common law as they may be interpreted by the courts of the United States in the light of reason and experience. However, in civil actions and proceedings, with respect to an element of a claim or defense as to which State law supplies the rule of decision, the privilege of a witness, person, government, State, or political subdivision thereof shall be determined in accordance with State law.

This paragraph means three very important things. First, the US Congress did not make a specific set of rules for when, where, and how a privilege such as the attorney-client privilege would apply. Rather, Congress instructs the Courts to

Retaining the Forensic Accountant

United States v. Kovel,³ decided 50 years ago this year, provides much of the framework regarding the extension of the attorney-client privilege to forensic accountants working at the direction of counsel when preparing for or working in anticipation of litigation. In this landmark 1961 opinion, the Second Circuit likened the accountant’s work to that of a translator. Kovel, the accountant, “translated” accounting concepts for counsel that is “...a foreign language to some lawyers in almost all cases, and to almost all lawyers in some cases.”⁴ Thus, Kovel’s work was necessary to allow defense counsel to provide competent legal advice to the client and the attorney-client privilege extended to his communications.

If outside counsel decides to retain a forensic accountant when anticipating or preparing for litigation, an engagement letter should be signed by all parties. The engagement letter should, at a minimum, confirm:

2. Counsel should not expect the forensic accountant to testify as an independent expert witness; however, he or she may serve as a fact witness.

3. 296 F.2d 918 (2d Cir. 1961).

4. *Id.* at 922.

A client may not “buy” a privilege by retaining an attorney to do something that a non-lawyer could do just as well. The client must be seeking legal advice from the lawyer. Courts have found that communications are not privileged when the lawyer is retained to perform tasks that non-lawyers can also do. *See, e.g., In re Feldberg*, 862 F.2d 622, 626 (7th Cir. 1988) (“A business that gets marketing advice from a lawyer does not acquire a privilege in the bargain; so too a business that obtains the services of a records custodian from a member of the bar.”).

Examples of non-privileged situations include:

1. Preparation of tax returns is not legal advice, so communications made in the course of tax return preparation are not generally privileged. *In re Schroeder*, 842 F.2d 1223, 1224 (11th Cir. 1987). The preparation of tax returns does not constitute legal advice within the scope of the privilege.”). However, the situation is different if the lawyer is retained to determine whether a tax position taken by a client could subject the client to legal liability. *United States v. Rockwell Int’l*, 897 F.2d 1255 (3d Cir. 1990).

In a case in which a taxpayer (either a person or corporation) has received a subpoena or summons to testify from the IRS, and the taxpayer seeks to quash the subpoena, the taxpayer has the burden of establishing the attorney-client privilege. But once the privilege is established, the burden

will then shift to the government to establish an exception that defeats the privilege. *Cavallaro v. United States* 284 F.3d 2002 (1st Cir. 2002).

2. The situation in which the privilege is lost most often is when the communication is not in confidence; i.e., when a third party is present. So, while under the Kovel principle, a lawyer may engage an accountant to help the lawyer decipher complex financial transactions and reports, if a third person not engaged by the lawyer is present during any such communication, the privilege, though applicable, will be forfeited.

Attorney Work Product

What is also important is the Work Product Exception to disclosure under the Federal Rules of Civil Procedure. 6(b)(3) (A). This rule states:

Documents and Tangible Things: Ordinarily, a party may not discover documents and tangible things that are prepared in anticipation of litigation or for trial by or for another party or its representative (including the other party’s attorney, consultant, surety, indemnitor, insurer, or agent). But, subject to Rule 26(b)(4), those materials may be discovered if:

1. they are otherwise discoverable under Rule 26(b)(1); and
2. the party shows that it has substantial need for the materials to prepare its case and cannot, without undue hardship, obtain their substantial equivalent by other means.

In the case of *U.S. v. TEXTRON* 553 F.3d 87 (1st Cir. 2009), cert. denied, 130 S.Ct. 3320, the IRS issued a subpoena pursuant to its authority under 26 USCS 7602, seeking tax accrual work papers for a corporation’s return. The corporation showed the papers to an independent auditor. Since these papers were prepared because of the clear risk of litigation, the corporation moved to quash. The Court held that the papers were prepared in anticipation of litigation and as such were not discoverable.

Importantly, unlike the attorney-client privilege, disclosure of the papers to a third party does not destroy the protection. Only disclosure to an adversary does. So showing the papers to an auditor retained for the specific purpose of preparing to defend in litigation did not destroy the “Work Product” protection.

The Internal Investigation Begins

The Work Plan

The forensic accountant should be involved in establishing the scope of work and determining how to most efficiently investigate the allegation of financial wrongdoing. The forensic accountant should be able to identify important financial systems and documents to be examined, as well as employees and third parties that should be interviewed to obtain an understanding of the fraud allegation.

At the earliest stages of the internal investigation, the forensic accountant should also begin thinking about internal controls. The work plan should contain steps to determine:

1. the controls in place to mitigate the risk of the alleged fraud occurring;
2. whether the duties of initiating and approving financial transactions are segregated appropriately; and
3. if the documented controls are being followed.



The Investigation

Whether the financial fraud allegation relates to fictitious sales, corrupt payments to foreign government officials, or any other type of financial fraud scheme, an understanding of the relevant financial records, processes and workflows germane to the fraud allegation, and the company's internal controls are of utmost importance.

Internal controls generally mandate a separate initiator and approver for each financial transaction recorded in the entity's accounting system. In addition to a segregation of duties, there should be adequate supporting documentation and a documented reason for the transaction. Software system controls may also identify who accessed the financial systems at different times and if certain controls were overridden. Each of the above-mentioned items is part of the audit trail. The audit trail should reflect whether company procedures were followed, or if certain controls were circumvented. Forensic accountants follow the audit trail to identify potential culprits and weaknesses in internal controls, which may result in a more cost-effective and efficient investigation.

After analyzing relevant financial records, process flows, and the audit trail, the forensic accountant will identify parties that should be interviewed. In the interview, the forensic accountant should be expected to ask questions relating to financial documents, assist in gathering testimonial evidence regarding the allegation, and address departures from the company's documented practices and procedures.

The Forensic Accountant's Work Product

The forensic accountant's work product can take many different forms including an oral or slideshow presentation, or a detailed written report. If the corporate client is likely to continue operations after the



internal investigation, it is beneficial to ask for work product covering the following:

1. a summary of the investigation and the evidence gathered;
2. control weaknesses identified during the course of the investigation; and
3. recommendations to enhance the control deficiencies.

Implementing recommended enhancements to internal controls could pay dividends immediately. If the internal investigation results in a decision to self-report the alleged fraud to the United States Department of Justice, or if a whistleblower reaches prosecutors first, the company should expect to receive questions regarding its compliance program and internal controls. Title 9, Chapter 9-28.000 *Principles of Federal Prosecution of Business Organizations* is the guideline for prosecutors to use when contemplating charging a corporate entity with a crime.⁵ When making a charging decision, the new guidelines state that prosecutors should evaluate remedial actions to improve programs set up to prevent and detect misconduct "in light of lessons learned."⁶ Furthermore, improvements to internal controls provide evidence that the financial fraud allegation was taken seriously and vigorously investigated by the company, and that the company has taken a proactive approach to combating fraud.

Conclusion

Companies should take advantage of the residual benefits of utilizing a forensic accountant during an internal investigation as a cost-effective opportunity to enhance their internal controls. Although the forensic accountant was retained to assist with the internal investigation, the corporate client is effectively receiving two services: specialized assistance investigating the allegation at issue and a plan to mitigate the risk of fraud occurring in the future. ■

James F. Burke is a Partner in the White Plains office of Wilson Elser Moskowitz Edelman & Dicker LLP. His practice focuses on the areas of general and product liability, pediatric lead poisoning, medical malpractice, and labor law. Previously, Jim had a 20 year career with the New York City Police Department (NYPD) and achieved the rank of Detective Sergeant. He served in the department's investigative branches as an investigator, supervisor and squad commander, specifically in the Narcotics Division, the Detective Bureau, and the Organized Crime Control Bureau.

5. "Principles of Federal Prosecution of Business Organizations," Title 9, Chapters 9-28.000 (available at <http://www.justice.gov/opa/documents/corp-charging-guidelines.pdf>).

6. *Id.* at 15.

They Just Don't Learn

Cases of repeat offenders

Americas

New York – Businessman Liable in \$17M Ponzi Scheme

Would-be real estate impresario Robert Stinson Jr., facing criminal and civil accusations for a \$17m Ponzi scheme, was found liable in the civil matter by a Pennsylvania judge who labeled him a “career fraudster.”

“The record indicates that Stinson is an unrepentant recidivist who continued to maintain the Ponzi scheme even after the SEC filed its complaint,” Judge Schiller wrote. “Indeed, as he earned his livelihood over a number of years perpetrating securities fraud, one may characterize Stinson’s professional occupation as engaging in illegal conduct.”

The SEC claims Stinson solicited investments in his Life’s Good Funds between 2006 and 2010, obtaining more than \$17m from 262 investors, despite the fact neither he or his businesses held any real estate assets.

He was indicted in November 2010 and continued to operate and this resulted in his bail being revoked after prosecutors demonstrated he blatantly flouted the terms of his release.

Stinson faces a maximum of 329 years imprisonment and a \$6.8m fine.

Toronto – Serial Boiler Room Worker Gets Longest Sentence Won by Ontario Securities Commission

In a pair of cases that illustrate the difficulty of shutting down serial “boiler room” crimes, a man the OSC has been pursuing since 2008 has been sentenced to nearly five years in jail.

Abraham Grossman was busy operating a second boiler room while he was in court defending allegations that he had operated the first one.

“One of the things that we have seen is there are certain individuals like...Mr. Grossman who are recidivists,” said Karen Manarin, deputy director of enforcement. “While he was on trial... he was actually perpetrating the fraudulent acts that are captured by the Shallow Oil (second) prosecution.”

Ms. Manarin said the jail term imposed “shows the courts are viewing securities violations that involve boiler rooms as very serious.”

In a related story, the OSC has taken to setting up their own boiler room operation to warn potential victims. As the result of the execution of a search warrant, the OSC uncovered a secret call list with hundreds of names. Signaling a more aggressive approach to combating fraud, the OSC set up a “reverse boiler room” contacting about 380 people over two days as the result of finding their names on the target list.

Asia

Auckland – Repeat Offender Convicted of Widespread GST Fraud

A recidivist fraudster has been jailed for four years for Goods & Services Tax Fraud.

Ian Nigel Clarke was sentenced after being found guilty on 89 charges of fraudulent rebate claims totaling \$302,000.

Clarke’s sentence was appropriate given the deliberate and calculated nature of his offense and his previous history.

Previous to this conviction, Clarke set up two other companies and filed tax refund claims for entities with no taxable activity.

Inland Revenue seized \$228,000 form bank accounts and investments controlled by Clarke.

“Clarke is someone who thinks he is entitled to help himself to money that should go to services like schools and roads, and this sentence shows how seriously the courts view that kind of activity” said Jonathan Matthews of Inland Revenue, Australia.

Europe

London – FSA Fines Repeat Offender 1 Million Pounds

Financial Regulators slapped a 1.09 million pound fine on a repeat offender for a share price scam and secured its first court injunction to prevent him from committing further market abuse.

The Financial Services Authority (FSA) said Samuel Kahn co-ordinated a scheme to deliberately inflate shares of Global Brands Licensing, orchestrating and controlling most of the trades over one month last year.

Kahn was investigated by the FSA and fined in 2007 for his part in overseas boiler room activities and was bankrupted by the regulator in 2008 after admitting liabilities for claims worth up to 3.7 million pounds from 800 investors.