Association of Corporate Counsel

1025 Connecticut Avenue, NW, Suite 200
Washington, DC 20036-5425

Tel 202.293.4103
Fax 202.293.4701

www.ACCA.COM

April 4, 2006

VIA EMAIL AND OVERNIGHT DELIVERY
The Honorable Ethiopis Tafara
Director of International Affairs
Securities and Exchange Commission
100 F Street, NE
Washington, DC 20549

Re: Anonymous Reporting Channels and European Data Protection Requirements

Dear Mr. Tafara:

On behalf of the Association of Corporate Counsel (ACC), thank you for the opportunity to present our perspectives regarding the differences in requirements promulgated by regulatory agencies such as the SEC in the United States and lawmakers in other countries. As you know better than anyone, regulatory agencies have a tremendous impact on the legal compliance initiatives that multinational companies strive to implement to stay in accord with local expectations of corporate responsibility and to establish and maintain internal systems that help protect the integrity of global markets.

ACC is the in-house bar association[SM], serving the professional needs of attorneys who practice in the legal departments of corporations and other private sector organizations worldwide. The association promotes the common interests of its members, contributes to their continuing education, seeks to improve understanding of the role of in-house attorneys and encourages advancements in standards of corporate legal practice. Since its founding in 1982, the association has grown to 18,500 members in more than 55 countries who represent over 8,000 corporations. Its members represent 47 of the Fortune 50 companies and 96 of the Fortune 100 companies. Internationally, its members represent 42 of the Global 50 and 75 of the Global 100 companies. In-house counsel play a critical role in providing leadership and guidance to organizations on compliance and ethics program development and implementation: ACC's members often have primary responsibility for helping their company and board of directors interpret regulatory requirements and support organizational efforts to comply with law and behave in a responsible fashion.

The specific topic we wish to raise involves recent concerns over the differences in provisions requiring anonymous and confidential reporting systems under the Sarbanes-Oxley Act (SOX) and interpretations and guidelines issued by EU data protection authorities. ACC applauds the Commission's openness to input on this important matter and understands you have discussed with in-house counsel, including some ACC leaders, some of the practical considerations global companies face when forced to choose between compliance with one country's regulations over that of another.

But while our comments today arise in the context of this current situation, we respectfully suggest the Commission consider a broader leadership role in the spirit of international comity. Laws affecting the behavior of corporations that operate in global markets need to be principle-based and take into account regional differences in law and policy. Open dialogue among regulators will allow officials to recognize and address cultural differences and local

Association of Corporate Counsel

1025 Connecticut Avenue, NW, Suite 200
Washington, DC 20036-5425

Tel 202.293.4103
Fax 202.293.4701

www.ACCA.COM

needs, such as here, where compliance systems established to comply with SEC rules risk putting companies between a rock and a hard place: either (1) follow U.S. legal requirements and potentially violate EU data protection and privacy rules, or (2) follow EU data protection and privacy rules and potentially violate U.S. legal requirements.

Perspectives on Provisions Presenting Challenges to Companies Needing to Comply with SOX and CNIL guidelines and WP-29 opinion

The perspectives offered herein address challenges relating to program scope and highlight some difficulties in application. We hope these perspectives provide some additional insights on the practical challenges involved in implementing global compliance programs and help illuminate a path by which the SEC and other regulators in other countries might appreciate the extraterritorial implications of certain laws and examine how well-intentioned and reasoned rules can negatively impact an otherwise effective global corporate compliance program. These examples do not represent the entirety of the concerns presented by these collective requirements but instead are provided to illustrate some corporate concerns.

- **Scope of Reporting Programs and Control Mechanisms:** Many companies seek to adopt a single and flexible set of governing principles or company-wide codes of conduct as a means to promote and operate meaningful compliance and ethics programs. When different jurisdictional requirements and restrictions necessitate program segmentation and fragmentation, a company's ability to set and enforce clearly defined standards is frustrated, execution of procedures can be confused and measurement of program effectiveness is significantly impaired. Put most simply, it's hard for a company to send the right message to employees when sending multiple, different messages.

  Sections 301 and 302 of SOX require internal reporting channels for detecting and disclosing financial and accounting irregularities and other types of employee fraud.[1] SOX requires companies to "retain and treat" information on financial and accounting irregularities and to provide confidential, anonymous reporting channels that enable employees to report in good faith any perceived concerns. The provisions of SOX also require information on financial and accounting irregularities and other frauds to be communicated to a corporation's audit committee or other independent committee of the board of directors for oversight and to discharge their duty of care.

  The rules promulgated through SOX 301 allow companies flexibility to implement internal reporting mechanisms through a variety of channels and modeled on any number of corporate best practices, including employee helplines, email drop boxes, web-based submission tools, in-person reporting and a variety of other means. To the extent the laws of other jurisdictions impact these reporting processes, board oversight and overall compliance program effectiveness will be directly affected, including information gathering, retention, escalation and investigation procedures. Having a patchwork of jurisdiction-based reporting processes can invite a myriad of inefficiencies and unwanted results,

[1] Section 301 requires Audit Committees to establish "procedures for the receipt, retention and treatment of complaints received by the issuer regarding accounting, internal accounting controls or auditing matters; and the confidential, anonymous submission by employees of the issuer of concerns regarding questionable accounting or auditing matters." In addition, Section 302 requires Chief Executive Officers and Chief Financial Officers to certify to the Commission in connection with defined financial filings that they have "disclosed to the issuer's auditors and the Audit Committee of the Board of Directors… any fraud, whether or not material, that involves management or other employees who have a significant role in the issuer's internal controls."

Association of Corporate Counsel

1025 Connecticut Avenue, NW, Suite 200
Washington, DC 20036-5425

Tel 202.293.4103
Fax 202.293.4701

www.ACCA.COM

including employee decisions not to report in the first place or failures of corporate management to effectively follow-up on situations that might require immediate attention. We believe that these results are not in the best interests of organizations or regulators (and the public interests they wish to protect).

As noted above, SOX and its progeny require companies to implement and maintain entity level controls that include systems that detect, remediate and disclose financial reporting improprieties and fraud. Many companies use ethics helplines to field calls or reports involving financial matters and do not have separate systems for different types of calls.[2]

Companies that implement single reporting systems do so for a variety of reasons. As a practical matter, the vast majority of reports are not financial related, so having a mechanism for reporting matters only financial in nature may not be practical to implement or an efficient allocation of resources. Moreover, complaints about other workplace issues, such as hostile work environment, might be symptomatic of other business problems where a pattern of behavior can be discerned over time. Most companies periodically inform their audit committees on the aggregate statistical data from these reporting systems as a means to allow proper oversight and review of conduct or operations within an organization that might require closer review.

The November 2005 Guidelines issued by the Le Commission nationale de l'informatique et des libertes (CNIL), and the February 1, 2006 opinion issued by the European Union's Article 29 Working Party (WP-29) appear to carve out for consideration the use of reporting programs to detect financial reporting improprieties and may not address other types of employee frauds and workplace matters. For the reasons indicated above, a fragmented approach for intake and handling reports impairs the ability to detect improprieties early and creates an undue burden on organizations that need reporting systems to handle reports that are not financial in nature on their face.[3]

- **Discouraging Anonymous Complaints:** The CNIL guidelines and WP-29 opinion suggest that a company's reporting program should not encourage anonymous complaints and should not advertise to employees the right to remain anonymous. This is contrary to the SOX requirement that companies establish mechanisms for anonymous complaints to Audit Committees.
- **Deleting Data on Unsubstantiated Complaints:** The WP-29 guidance that data regarding unsubstantiated complaints should be deleted is not consistent with SOX provisions that require companies to implement procedures that detect and prevent fraud. Deleting such data makes it more difficult for companies to investigate and track the disposition of complaints by detecting patterns from data points in the aggregate that may be symptomatic of fraudulent behavior or weaknesses in controls or

[2] See *Everything You Wanted to Know About Helpline Best Practices, Results of 2004 Survey of Ethics Officer Association Sponsoring Partner Members* (Ethical Leadership Group – October 2004).

[3] For companies with operations within the U.S., the U.S. Sentencing Commission's Federal Sentencing Guidelines for Organizations provide really the only 'government definition' of the elements of an effective corporate compliance and ethics program, and include criteria suggesting a need for having and publicizing "a system which may include mechanisms that allow for anonymity or confidentiality where employees and agents may report or seek guidance regarding potential or actual criminal activity without fear of retaliation." With the passage of SOX, corporate compliance and ethics programs are receiving heightened scrutiny. Companies subject to SOX, including Sections 301, 302 and 404, have additional layers of program processes for internal and oversight controls and to support certifications to regulators.

Association of Corporate Counsel

1025 Connecticut Avenue, NW, Suite 200
Washington, DC 20036-5425

Tel 202.293.4103
Fax 202.293.4701

www.ACCA.COM

otherwise would lead to discovery of fraud. Of course, we're not suggesting that data may never be deleted; rather, we're suggesting that a flat requirement to delete unsubstantiated data may not support some corporate efforts to assess larger patterns, weaknesses, and troubling trends.

- **Transfer of Data to Other Countries:** The EU Data Privacy Directive and Member State laws place limits on the ability of companies to transfer personally identifiable information from an EU country to other countries, such as the U.S., which do not have national privacy laws parallel to those in the EU. The CNIL guidelines issued in December 2005 indicate the availability of an expedited single authorization process to facilitate the transfer of personally identifiable information for companies with reporting programs of a certain defined scope. However, this process appears to be available only to the extent that the company's reporting system is narrowly confined to gathering reports of financial reporting, accounting, bribery or banking concerns. For companies with reporting programs that include intake and processing of matters outside such scope (such as companies with programs designed to ensure compliance with legal provisions, company policies, internal professional conduct rules and/or those that include employee fraud or workplace matters), the single authorization approach does not appear to be available and an individual authorization request to CNIL for case-by-case program consideration would appear necessary since such inclusive programs are described as raising a 'difficulty in principle.'[4]

Conclusion

ACC appreciates the opportunity to offer our perspectives on the need for additional clarification of regulatory requirements and guidelines on corporate reporting programs or whistleblower programs. We commend the Commission and the CNIL and WP-29 in taking initiatives to help address differences and hope that with additional dialogue further clarification on the challenges addressed herein may be obtained. We further hope that this issue will offer us all a platform from which we can discuss the larger issues of the preventive need for better coordination between regulators around the world whose work is so integral to the ongoing compliance and governance efforts to multinational organizations.

Please feel free to contact us if you would like more information or if we can be of service.

Respectfully submitted,

Susan Hackett

Susan Hackett
Senior Vice President & General Counsel
Association of Corporate Counsel

[4] Some matters assessed on a case-by-case basis may qualify for processing due to "their particular seriousness." See CNIL's *FAQs on whistleblowing systems* at http://www.cnil.fr/index.php?id=1982.

Association of Corporate Counsel

1025 Connecticut Avenue, NW, Suite 200
Washington, DC 20036-5425

Tel 202.293.4103
Fax 202.293.4701

www.ACCA.COM

cc: Chris Crowder, The Scotts Miracle-Gro Company, ACC European Chapter Liaison
Keith Cheresko, Ford Motor Company
Renee Dankner, Association of Corporate Counsel
Muzette Hill, Ford Motor Credit, ACC Advocacy Committee Chairman
Fred Krebs, Association of Corporate Counsel
Luise Welby, FreddieMac, ACC Corporate & Securities Law Committee
Richard J. Wolf, Cendant Corporation, ACC Greater New York Chapter President