



K&L GATES

GLOBAL BOARDROOM RISK SOLUTIONS

July 2014 Newsletter

CONTENTS

- **Cybersecurity: Five Tips to Consider When Any Public Company Might be the Next Target**
Page 5
- **Financial Services: Regulation in Search of Systemic Risk**
Page 11
- **EU Sanctions: Impacts on Businesses**
Page 15
- **Trends in FCPA Enforcement**
Page 19
- **Changes to the UK Governance Code**
Page 25
- **Legal Professional Privilege in the United Kingdom**
Page 29

The articles above may be accessed by clicking on the title.

KEY CONTACTS

John A. Bicks

New York
+1.212.536.3906
john.bicks@klgates.com

Thomas M. Reiter

Pittsburgh
+1.412.355.8274
thomas.reiter@klgates.com

Tony Griffiths

London
+44.(0)20.7360.8195
tony.griffiths@klgates.com

John W. Mann

Melbourne
+61.3.9205.2011
john.mann@klgates.com



INTRODUCTION

“The first priority of management is ensuring survival of the business.”

Peter F. Drucker, “Managing in Turbulent Times” (1980)

The key point is that this is a “first priority,” and not a subsidiary priority to driving revenue growth, creation of profit, or promoting innovation at all levels of the company. Directors are required to scan the horizon for existential risks to the business and ensure that the business is equipped, ready, and capable of withstanding the shock waves. Over the last 40 years, this idea has become manifest in statutes, regulations, and codes of conduct around the world, and all of these impose upon directors the responsibility to assess risk continually.

In dealing with a significant number of the largest domestic and international internal investigations arising from crises in the last few years, K&L Gates has discerned some trends which won't provide much comfort to directors. First, the days of the one issue, one jurisdiction crisis are gone. An issue can also morph and evolve, either domestically or internationally, to leave the organization having to deal with different regulators and different enforcement agencies on many fronts.


Second, risks bleed into each other and compound. Multiple regulatory and enforcement agencies raising multiple issues in multiple jurisdictions, very often in relation to a single set of facts, are an increasingly common feature of crisis management.

To assist in dealing with these issues, we have developed a multidisciplinary product we call “Global Boardroom Risk Solutions.” It has been designed to provide organizations with synchronized legal advice (in many circumstances bringing with it the protection of legal professional privilege) through every twist and turn of the risk assessment stage and during the interface with regulators and enforcement agencies. This, the first of our Global Boardroom Risk Solutions reports, highlights the critical considerations for the boardroom.



CONTACT

Tony Griffiths
London
tony.griffiths@klgates.com



Proper attention to cybersecurity risk factor disclosures may decrease the likelihood that a company will face securities class action litigation and shareholder derivative litigation in the wake of a cybersecurity incident.

Cybersecurity: Five Tips to Consider When Any Public Company Might be the Next Target


Roberta Anderson

INTRODUCTION

C-suite executives wake to another day, and another data breach. Scarcely a day goes by without the headlines reporting yet another data breach or other serious cybersecurity incident. Cyber incidents are ubiquitous, and no industry or organization, wherever situated, however small or large, is immune. No firewall is unbreachable, no security system impenetrable.

WHO IS AFFECTED?

When they hit, cybersecurity events are expensive. In addition to crisis management expenses, such as forensics, notification, credit monitoring, and public relations, together with lawsuits and regulatory investigations, executives are increasingly facing shareholder litigation. In the wake of its high-profile data breach, for example, Target's directors and officers face shareholder derivative action alleging that "Target ... has suffered considerable damage from [the] breach."²



For a **SINGLE DATA BREACH**, the Ponemon Institute recently reported that the average U.S. organizational cost is more than **\$5.85 MILLION**—with \$509,237 spent on post-breach notification alone.¹

¹ Ponemon Institute, *2014 Cost of Data Breach Study: Global Analysis*, at 6, 15 (May 2014).

² *Collier v. Steinhafel, et al.*, No. 0:14-cv-00266 (D. Minn.) (filed Jan. 29, 2014), at ¶76.

SUMMARY

Proper attention to cybersecurity risk factor disclosures may decrease the likelihood that a company will face securities class action and derivative litigation in the wake of a cybersecurity incident—or at a minimum may mitigate a company’s potential exposure.



SEC Guidance

By way of background, in view of “more frequent and severe cyber incidents,” the U.S. Securities and Exchange Commission (SEC) issued in October 2011 cybersecurity disclosure guidance, which advises companies to “review, on an ongoing basis, the adequacy of their disclosure relating to cybersecurity risks and cyber incidents.”³

Although the guidance does not create new cybersecurity disclosure obligations, failure to make adequate cybersecurity disclosures may subject a company to increased risk of enforcement actions and shareholder suits in the wake of a cybersecurity incident that negatively impacts a company’s stock price.

³ SEC Division of Corporation Finance, Cybersecurity, CF Disclosure Guidance: Topic No. 2 (Oct. 13, 2011). The guidance advises that appropriate disclosures may include the following:

- Discussion of aspects of the registrant’s business or operations that give rise to material cybersecurity risks and the potential costs and consequences;
- To the extent the registrant outsources functions that have material cybersecurity risks, description of those functions and how the registrant addresses those risks;
- Description of cyber incidents experienced by the registrant that are individually, or in the aggregate, material, including a description of the costs and other consequences;
- Risks related to cyber incidents that may remain undetected for an extended period; and
- Description of relevant insurance coverage.

Five Tips to Consider

The following five tips may assist companies in reviewing the adequacy of their existing cybersecurity disclosures based on the SEC's disclosure guidance and comments to data.

1. **Perform a Cybersecurity Risk Assessment.** The SEC staff states in its guidance that it expects companies “to evaluate their cybersecurity risks and take into account all available relevant information, including prior cyber incidents and the severity and frequency of those incidents,” as well as “the adequacy of preventative actions taken to reduce cybersecurity risks in the context of the industry in which they operate and risks to that security, including threatened attacks of which they are aware.” To facilitate adequate disclosures, companies should consider engaging in a thorough assessment concerning their current cybersecurity risk profile and the impact that a cybersecurity breach may have on the company's business.
2. **Consider Known and Potential Breaches.** If a company has suffered a known cybersecurity event, it should anticipate that the SEC will issue a comment letter if the event is not disclosed. Significantly, even where a company states that it has not been the victim of a material cybersecurity event, the SEC nonetheless has requested that the company's risk factor disclosure be expanded to state generally that the company has been the victim of hacking—even if prior events were immaterial. In addition, companies may need to disclose threatened cyber incidents, together with potential costs and other consequences. Companies in targeted industries that are not yet aware of an incident should consider disclosing how the company might be impacted by a cybersecurity incident—even if no specific threat has been made.
3. **Be Specific.** The SEC staff has advised that companies should avoid boilerplate language and vague statements of general applicability. In particular, the guidance states that companies should not present risks that could apply to any issuer or any offering and should avoid generic risk factor disclosure. In addition, the guidance states that companies should provide disclosure tailored to their particular circumstances and avoid generic boilerplate disclosure.

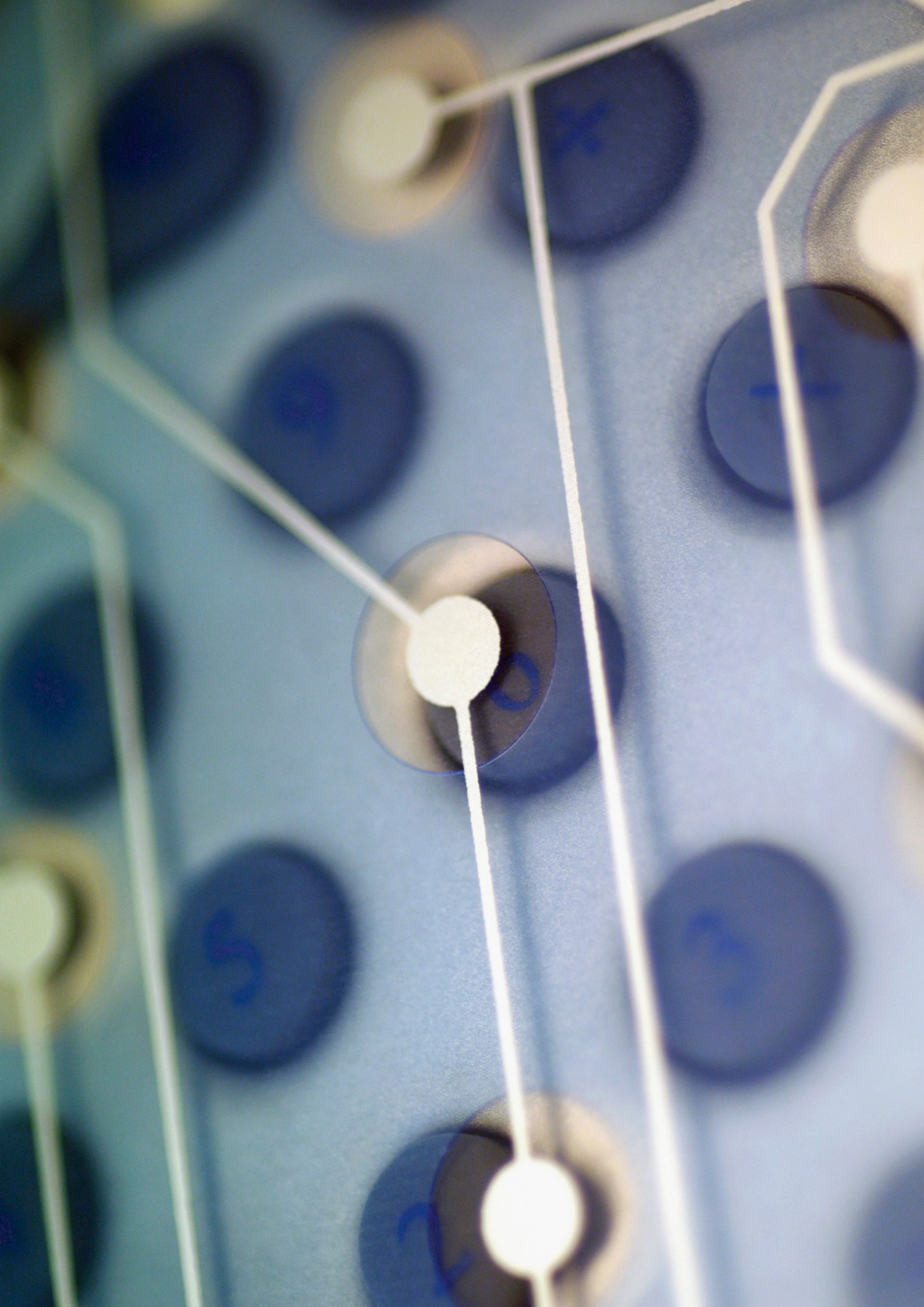
- 4. Remember a “Roadmap” is Not Required.** Although the SEC seeks disclosures that are sufficient to allow investors to appreciate the nature of the risks faced by a company, it has made clear that the SEC does not seek information that would create a road map or otherwise compromise a company’s cybersecurity. At the outset of its guidance, the SEC staff states that it is “mindful of potential concerns that detailed disclosures could compromise cybersecurity efforts—for example, by providing a ‘roadmap’ for those who seek to infiltrate a [company]’s network security—and we emphasize that disclosures of that nature are not required under the federal securities laws.”
- 5. Consider Insurance.** Insurance can play a vital role in a company’s overall strategy to address, mitigate, and maximize protection against cybersecurity risk. Reflecting this reality, the SEC guidance advises that appropriate disclosures may include a description of relevant insurance coverage that a company has in place to cover cybersecurity risks. The SEC’s guidance provides another compelling reason for companies to carefully evaluate their current insurance program and consider purchasing “cyber” and data privacy-related insurance products, which can be extremely valuable.

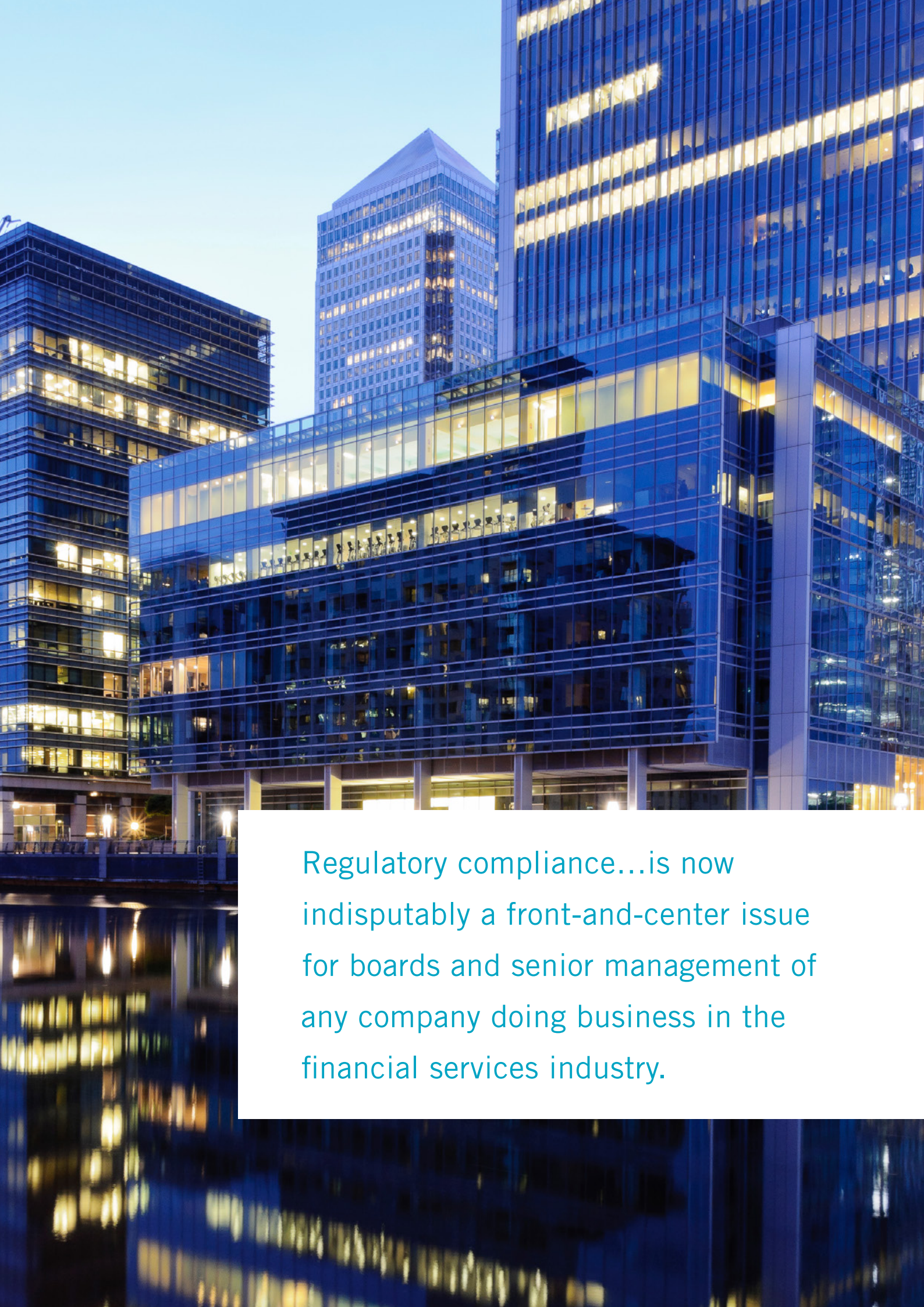
CONCLUSION

Considering these five tips will assist companies in minimalizing their exposure from lawsuits alleging inadequate disclosure in the event of a cybersecurity incident.

CONTACT

Roberta Anderson
Pittsburgh
roberta.anderson@klgates.com





Regulatory compliance...is now indisputably a front-and-center issue for boards and senior management of any company doing business in the financial services industry.

Financial Services: Regulation in Search of Systemic Risk

Diane Ambler

INTRODUCTION

Since the 2008 financial crisis, global regulators have made it a priority to fashion a set of issues presumably contributing to systemic risk that would help identify key players in the financial services industry potentially posing significant risks to the financial system. The foundation of this regulatory model is to designate certain firms as systemically important financial institutions (SIFIs) and to subject them to greater regulatory scrutiny and enhanced regulatory requirements.

WHO IS AFFECTED?

Regulatory compliance—plus the financial and reputational consequences of non-compliance—is now indisputably a front-and-center issue for boards and senior management of any company doing business in the financial services industry. Firms must not only interpret and satisfy the gamut of current regulation, but must also effectively anticipate future compliance demands in a constantly evolving regulatory landscape. Moreover, compliance obligations of various sorts now spill over into virtually every operational area of the typical financial services firm. Against this backdrop, the board and senior management are ultimately responsible for the company's implementation of all appropriate systems required to ensure regulatory compliance, and to drive any cultural change required in the organization to make such compliance meaningful and effective.

SUMMARY

SIFI Designations

In the United States, the Financial Stability Oversight Council (FSOC), and its research arm, the Office of Financial Regulation (OFR), have been assessing various risks and going about the business of identifying SIFIs, which U.S. banking regulators will then oversee and further regulate. Some non-bank financial service institutions that were unregulated before 2008 could receive

a SIFI designation. The SIFI designation could also be applied to institutions already subject to substantial regulation. In either case, it would seem logical that the heavy hand and added costs of substantially increased government involvement should be preceded by a significant justification for additional regulation and a matching of any new regulations to systemic risks not already addressed by existing regulations.

The OFR and FSB/IOSCO Reports

In late 2013 the OFR issued an Asset Manager Report that outlined a series of theoretical risks to investment funds, struggled to identify those risks in a broad range of asset management and investment fund businesses, and characterized these would-be risks as a major threat to financial stability.

The OFR Report, which has been widely discredited for its lack of intellectual rigor, was published a few months in advance of the Assessment Methodologies for Identifying Non-bank Non-insurer Global Systemically Important Financial Institutions (NBNI G-SIFIs) published jointly by the Financial Stability Board (FSB) and the International Organization of Securities Commissions (IOSCO).

Similarly to the OFR Report, the FSB/IOSCO Report finds that systemic risk can be spread through three basic transmission channels: (i) an exposures/counterparty channel; (ii) an asset liquidations/market channel; and (iii) a critical function or service/substitutability channel.

The Problem of Risk Profiles

The FSB/IOSCO initiatives logically categorized NBNI G-SIFIs separately from global systemically important banks and global systemically important insurers. Banks and insurance companies provide investor guarantees and assume all or most of the investment risk of the underlying assets necessary to satisfy those guarantees. By design, banks and insurance companies do not have sufficient underlying assets to pay depositors or contract holders all at once. The U.S. government guarantees U.S. bank deposits up to \$250,000; if the bank is unable to pay depositors, U.S. taxpayers will.

Investment funds, unlike banks and insurance companies, are intended to shift the investment risk from the financial institution to its investors. Investors

own an undivided share of the assets in the fund; they have no interest in the assets of the fund manager. Yet, there are many forms of investment funds, subject to fundamentally different regulatory restrictions currently, that present radically different risk profiles.

Neither the OFR Report nor the more reasoned FSB/IOSCO Report sufficiently distinguishes the risk profiles of different types of investment fund businesses outside of the bank and insurance company context. Both instead defer to a functional analysis of risk through factors such as size, interconnectedness, and substitutability—without considering the operational structure of the business model or the ameliorating impact of current regulation.

CONCLUSION

Developing rational standards of regulation going forward will require a focus on the diversity of risks posed by these different forms of investment funds, and this process would benefit from the input of all players in the financial system. The failure of both the OFR Report and the FSB/IOSCO Report to categorize investment funds according to levels of existing regulation and transparency threatens to severely limit the usefulness of current attempts to assess the risks associated with investment funds, and this threatens to undermine the merit of regulatory decisions, while establishing a misleading international consensus that such funds are systemically risky. Until the SIFI designation construct integrates the important distinctions in risks posed by various different non-bank financial institutions, the next steps—identifying entities for SIFI designation and developing policy measures that would apply to non-bank SIFIs—will be both over- and under-inclusive, and the protections against future dynamics of systemic failure will be flawed.

Industry input during comment processes can provide a broader knowledge base for both standard-setting bodies and regulators to incorporate into the analysis.

CONTACT

Diane Ambler
Washington, D.C.
diane.ambler@kgates.com



Every company should consider whether its business could be affected by EU sanctions.

EU Sanctions: Impacts on Businesses

Vanessa Edwards and Philip Torbøl

INTRODUCTION

The European Union (EU) actively uses restrictive measures, also known as sanctions, to bring about a change in activities or policies such as violations of international law or human rights, or policies that do not respect the rule of law or democratic principles. Sanctions imposed by the EU may target governments of countries or non-state entities and individuals (such as terrorist groups and terrorists). The effects of sanctions can be felt not only by the governments, entities, and individuals targeted by sanctions but also by other unrelated businesses across the globe, including investors, insurers, and importers/exporters.

WHO IS AFFECTED?

Currently, more than 30 countries are subject to EU sanctions, including North Korea, Iran, Syria, Belarus, etc. Most recently the EU adopted restrictive measures in view of the situation in Ukraine which target both Ukrainian and Russian nationals, including companies.



**COUNTRIES
SUBJECT TO
EU SANCTIONS**

SUMMARY

There is a wide range of restrictive measures that the EU can impose to achieve the desired outcome, including:

- financial restrictions (asset freeze, prohibition on financial transactions)
- specific or general trade restrictions (import/export bans)
- restrictions on admission (visa or travel bans)
- various diplomatic restrictions (expulsion of diplomats, suspension of different events or official visits)

The EU most commonly uses economic and financial restrictions, in particular requiring funds and economic resources owned and controlled by designated individuals and entities to be frozen, as well as prohibiting making funds and economic resources available to designated individuals and entities. EU legislation on sanctions is interpreted broadly. This, together with the standard anti-avoidance provision normally included, means that not only the designated individuals and entities, but also parties closely linked to those designated individuals and entities, are caught within the scope of a restrictive measure.

The EU can also impose restrictive measures targeting specific goods or sectors. For example, the EU has prohibited the import into the EU of crude oil and petroleum products from Syria and the export to Syria of key equipment and technology for the oil and gas industry. The ban also includes a prohibition on related technical and financial assistance. Similarly, the EU has prohibited the import into the EU of goods originating from Crimea and Sevastopol to strengthen the EU's non-recognition policy regarding Russia's annexation of those two regions. It is also prohibited to provide financial and insurance services related to the import of such goods.

With regard to sanctions against Russia, the EU has also actively used diplomatic measures. For example, the EU canceled the EU-Russia Summit in June 2014. The EU is currently considering suspending some of the bilateral cooperation programs between the EU and Russia that do not deal exclusively with cross-border cooperation and civil society. The EU is also using its power to influence the European Bank for Reconstruction and Development (Russia is one of the shareholders of the bank) and the European Investment Bank to suspend lending to Russia.

Very often the EU uses a combination of different restrictive measures. The lists of designated individuals and entities are constantly updated, and the EU can introduce additional measures with immediate effect as a given situation evolves. Although it can sometimes be a time-consuming process for EU member states to agree on sanctions, once agreement has been reached the implementation process is very speedy and sanctions can come into force the following day. Therefore businesses should allocate resources to monitor developments in order to minimize their exposure to breaching restrictive measures.

EU sanctions apply to all individuals and entities doing business in the EU, including non-EU nationals, and also to EU nationals and entities incorporated or constituted under the law of any EU member state when doing business outside the EU. The EU member states are responsible for implementing and enforcing sanctions and are required to introduce rules on penalties applicable to the infringement of sanctions which must be effective, proportionate, and dissuasive. In many countries it is a criminal offense to infringe restrictive measures.

The EU usually also includes certain defenses in its sanctions legislation. For example, EU sanctions against Ukrainian and Russian nationals provide an EU-wide defense where the breach was carried out in good faith as long as the individual or entity concerned was not negligent. In addition, no claims (for example, claims for indemnity or compensation) in connection with any contract or transaction, the performance of which has been affected by restrictive measures, can be satisfied if they are made by the designated individuals and entities or parties acting through or on behalf of such individuals and entities.

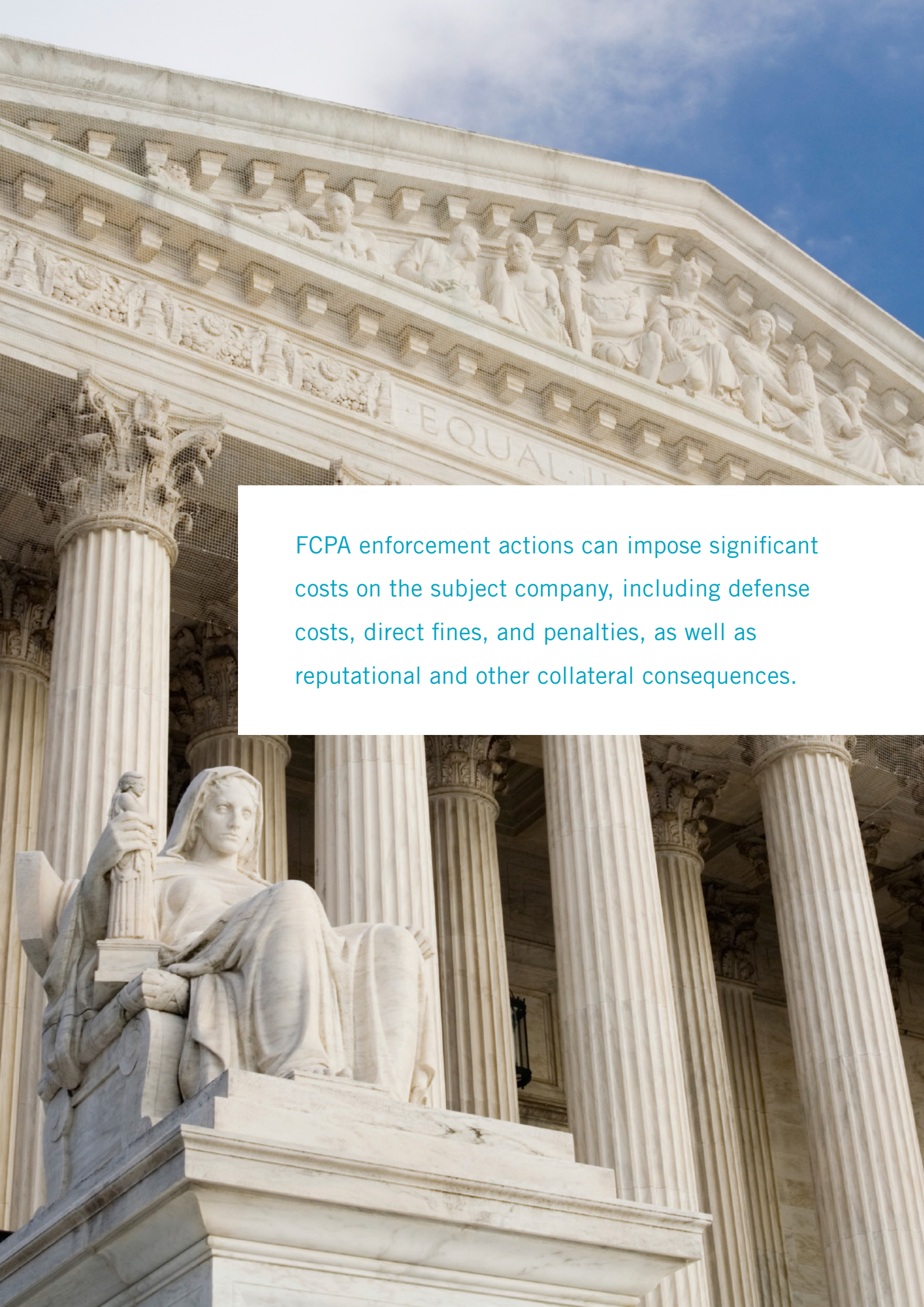
CONCLUSION

Based on the broad application and wide interpretation of EU sanction legislation and the potentially serious penalties for breach, it is in the best interest of companies to implement and carry out precautionary measures to minimize their risk. Every company should consider whether its business could be affected by EU sanctions and whether there are any additional protections available, such as bilateral investment treaties and World Trade Organization (WTO) agreements.

CONTACTS

Vanessa Edwards
London
vanessa.edwards@klgates.com

Philip Torbøl
Brussels
philip.torbol@klgates.com



FCPA enforcement actions can impose significant costs on the subject company, including defense costs, direct fines, and penalties, as well as reputational and other collateral consequences.

Trends in FCPA Enforcement

Matt Morley

INTRODUCTION

This year marks the beginning of the second decade of vigorous enforcement of the U.S. Foreign Corrupt Practices Act (FCPA), which prohibits the bribery of foreign government officials. Prior to 2004, cases under the FCPA were infrequent, but since that time, about a dozen companies per year have been charged with FCPA violations. The fines, penalties, and other amounts paid to the U.S. government to resolve these cases have varied widely, with some as low as \$1 million, and others in the hundreds of millions of dollars, averaging about \$60 million per case. FCPA enforcement has become routine and poses a risk to any company—whether a U.S. company or not—doing international business.

At the same time, the FCPA enforcement environment remains dynamic, and a number of trends will likely continue or accelerate.

WHO IS AFFECTED?

FCPA enforcement actions can impose significant costs on the subject company, including defense costs, direct fines, and penalties, as well as reputational and other collateral consequences. These government actions also may give rise to shareholder derivative suits which often allege that the company's failure to implement appropriate FCPA controls and practices amounts to a breach of fiduciary obligations by the company's directors.

SUMMARY

U.S. federal officials continue to promise that more “big” FCPA cases are on the way, and already in January 2014, one long-pending investigation was concluded with a settlement of \$384 million. Three of the 10 largest FCPA

cases in history, measured by sanctions, have been resolved in the past 18 months. There is no reason to think that the current pace will slow, and other factors suggest that the pace may well increase.

Larger Penalties and More Criminal Actions Against Individuals

Although it can be difficult to discern the significance of differences year to year, most observers agree that the level of fines, penalties, and disgorgement amounts in FCPA cases seems to be increasing steadily. Added to this, as promised by Department of Justice officials for several years, there appears to have been a real focus not only on actions against corporate entities, but on bringing charges, particularly criminal charges, against persons believed to have been responsible for those violations. Many of those convicted have been sentenced to prison terms.



International Cooperation

The United States has always led the way in international anticorruption enforcement, and indeed, the renewed vitality of the FCPA is closely linked with the Organisation for Economic Co-operation and Development's Convention Against Bribery of Foreign Officials in International Business Transactions (the Convention), which came into force in 1999. The Convention obligated signatories to criminalize the bribery of "foreign" government officials, much in the way that every nation already outlaws efforts to corrupt its domestic officials.

Transparency International has identified three other nations—the United Kingdom, Germany, and

Switzerland—that are “actively” enforcing their laws against international corruption. By contrast, efforts by the 34 other nations that have signed the Convention have been lackluster at best. According to Transparency International, there has been “moderate” enforcement by four other signatories (Italy, Australia, Austria, and Finland) and “little or no” enforcement by the remaining 30.



At the same time, there are other, more vibrant forms of international cooperation. For instance, the United States has a variety of agreements with dozens of other nations providing for evidence-gathering and information exchanges between national law enforcement agencies. While these mechanisms can be cumbersome, and cooperation can be very uneven, the clear trend is toward heightened multinational action against corruption.

Whistleblowing

Under the whistleblower provisions of the Dodd-Frank Act of 2010, persons who provide the Securities and Exchange Commission (SEC) with information leading to a successful enforcement action in which more than \$1 million is recovered are entitled to an award of 10 to 30 percent of those amounts. For the average FCPA case, that could mean an award in the range of \$6 million to \$18 million, and in larger cases, considerably more.

The program appears to be working. Since it took effect in August 2011, the SEC has received more than 3,000 tips per year relating to all forms of U.S. securities law violations. Reports come not only from the United States, but also in significant numbers from sources in China, Russia, India, the United Kingdom, and Canada. In 2013, the SEC made its first bounty payments under the program, including one of \$14 million to an unidentified informant.

This case in particular illustrates the potential impact that the whistleblower program may have in streamlining law enforcement efforts; the information provided enabled the SEC to respond exceptionally quickly, completing an enforcement action in less than six months.

This paradigm seems to be spreading: the UK is now exploring ways of further encouraging whistleblowers on a variety of issues, including UK Bribery Act violations.

Anticorruption Enforcement as a Competitive Weapon

UK law enforcement authorities have expressly indicated that they intend to target violations of the UK Bribery Act where an improper payment may have disadvantaged a UK company. While not surprising, the open acknowledgement of this dynamic is unusual. U.S. authorities have repeatedly denied that they single out non-U.S. companies for FCPA enforcement action, but it cannot be overlooked that eight of the 10 largest FCPA enforcement actions of all time have been against non-U.S. companies.

CONCLUSION

Awareness of these trends can help companies in assessing their risks associated with potential anticorruption exposure and in designing and executing anticorruption compliance efforts so as to enable them to reduce the risk of a violation. As always, a company can be best protected by devoting its energies to a compliance program designed to address its specific risks, and by frequently re-evaluating that program in light of changes in its business and in the broader enforcement environment.

CONTACT

Matt Morley
Washington, D.C.
matt.morley@klgates.com





The guidance specifies that risk management should be incorporated within the company's normal management and governance processes and should not be treated as a separate compliance exercise.

Changes to the UK Governance Code

Tony Griffiths

INTRODUCTION

“Risk comes from not knowing what you’re doing.” In their consultation document of April 2014 on Risk Management, Internal Control and the Going Concern Basis of Accounts, the Financial Reporting Council (FRC) in the United Kingdom took the advice of the Sage of Omaha to heart.

WHO IS AFFECTED?

As part of its review of its guidance for directors (Turnbull Guidance) on internal controls for all listed companies, the FRC issued draft guidance, the purpose of which is to “make a clearer link between the assessment of business viability risks and the broader risk assessment that should form part of a company’s normal risk management and reporting processes.” Specifically the guidance requires a link between the going concern certification in accounts and the completion of risk assessment processes.

SUMMARY

The guidance itself states “an understanding of the risks facing the company is essential for the development and delivery of its strategic objectives, its ability to seize the opportunities, and to ensure its longer term survival. It is one of the most important issues with which boards must concern themselves.” As a result, the guidance specifies that risk management should be incorporated within the company’s normal management and governance processes and should not be treated as a separate compliance exercise.

The board is charged with making a “robust” assessment of the principal risks to the company’s business model and ability to deliver its strategy. Both this assessment and the ongoing monitoring and mitigation of risks must be disclosed in the Strategic Report as part of the company’s Annual Report and

linked to relevant disclosures it makes in the financial statement in relation to its going concern status.

“The directive should state whether, taking account of the company’s current position and principal risks, they have a reasonable expectation that the company will be able to continue in operation and meet its liabilities as they fall due, drawing attention to any qualifications or assumptions as necessary.”

CONCLUSION

In practical terms this means that starting in October 2014, in any listed corporate failure or investigation in the United Kingdom by the Serious Fraud Office, the police, the central government, or any other regulator, the authorities or insolvency practitioners, with the benefit of 20/20 hindsight, will carefully examine what steps the board took to comply with FRC requirements. In particular there will be a focus on what the board and individual directors knew or should have known at the point when the relevant risk emerged. The linkage of risk assessment, corporate governance requirements, and going concern certification could lead to wrongful trading-type arguments in the context of overall risk assessment. Under insolvency laws, directors can become personally liable for insolvent company liabilities if they know or should have known that a company was unlikely to avoid insolvency but continue to permit the company to trade. The prospect of similar arguments being used in the context of civil or criminal proceedings relating to risk assessment procedures and what directors did or should have known seems to have become more likely with the new FRC requirements. Importantly, all of this also relates to international companies that are listed in London.

CONTACT

Tony Griffiths

London

tony.griffiths@klgates.com





Privilege within the United Kingdom is a powerful tool. When used properly, it provides the right not to disclose a document or communication to anyone.

Legal Professional Privilege in the United Kingdom

Frank Thompson and Laura Atherton

INTRODUCTION

The term “privileged” is much misunderstood and misused. Privilege within the United Kingdom is a powerful tool. When used properly, it provides the right not to disclose a document or communication to anyone. The privileged status of a document lasts forever and for all purposes unless and until that privilege is consciously waived or inadvertently lost.

WHO IS AFFECTED?

In civil proceedings, the privileged status of documents is most relevant when looking at disclosure when the other side, be it the claimant or the defendant, wants to see the relevant evidence in possession. In criminal and regulatory proceedings, it is most relevant when a regulator or prosecutor is attempting to compel the disclosure of material that may be used against you in proceedings or to further their enquiries.

SUMMARY

Legal advice privilege and litigation privilege are the two distinct types of privilege under English Law. Those wishing to assert either should consider which type they are entitled to claim.

Legal Advice Privilege (LAP)

Definition

LAP applies to communications between a lawyer and their client in relation to a transaction or circumstance in which the lawyer has been instructed to obtain legal advice in “the relevant legal context.”

Important Considerations

- Interacting with a lawyer is not sufficient to establish privilege over related communications and documents. The lawyer must be providing legal as opposed to commercial or other general advice.
- Communication between lawyers and third parties such as accountants and auditors is not applicable.
- It is best practice to identify a small subgroup of individuals who can be considered the client for the purposes of LAP. Create a non-privileged document which contains a non-exhaustive list of the individuals that are defined as the client, leaving room for the possibility of change as matters develop.
- Communications between employees of the company (who are not defined as the client) and the lawyers, for fact finding purposes, can not be classified as privileged.

Litigation Privilege (LP)

Definition

LP applies to communications between a lawyer and a client or client's representative and with any other third party (including experts and witnesses) where those documents and communications are made in connection with and for the primary purpose of existing or contemplated criminal, regulatory, or civil legal proceedings.

Important Considerations

- LP does not make a document which was not privileged when created privileged. Therefore a communication which was subject to LAP will continue to be privileged even though it may later be relevant evidence in

HOW TO MAINTAIN LAP

1 Be explicit and mark it as privileged (may avoid later inadvertent disclosure)

2 Include a purpose in the body of the communication

3 Separate out material that is LAP from material that is not

a litigation or prosecution. However, a communication which is not LP or LAP at the time it was created will not become so at a later date.

- Consider where regulators and prosecutors are likely to seek disclosure of documents and communications created by the company during an internal investigation. One of the most common documents requested are interview notes. A verbatim interview note taken during an internal investigation will not necessarily be subject to privilege and so in order to have the best chance of asserting LP over interview notes, an organization may wish to ensure that:

- the notes are taken by a lawyer
- the notes are not drafted verbatim, but contain also the lawyer's impressions and opinions for the purposes of advising the client
- the notes record the contemplation of proceedings or another basis on which LP is founded and are clearly marked as privileged

Waiver of Privilege

Organizations should maintain privilege unless there is a compelling reason to waive it. Once waived, privilege cannot be reclaimed.

The more widely electronic or hard copies of privileged documents and communications are distributed outside of the organization, the more likely it is that a court will consider that privilege has been waived.



Privileged documents can be disclosed to a third party for a limited purpose while retaining the ability to assert privilege in the future against the same party or the rest of the world. However, this presents risks, both because the organization may misjudge and be deemed to have completely waived privilege, and also because in some jurisdictions, limited waiver is not recognized.

Joint Privilege

Joint privilege arises when a lawyer is jointly retained by more than one client. It has important practical implications—none of those entitled to the privilege can waive the privilege without the other's consent; nor can they assert privilege against the other if a dispute arises in the future.

A recent case has clarified that in asserting joint privilege, one must have been the lawyer's client at the time the advice was received, even if there was no express retainer.

Legal Professional Privilege Across the World

Do not assume that the rules of privilege that apply in the United Kingdom apply elsewhere. A document protected by privilege in the United Kingdom may not be so protected if it travels abroad, electronically or physically.

The privilege which can be asserted in relation to communications between in-house counsel and the company varies throughout Europe. There is no privilege for in-house counsel's documents and communications under the EU Commission in regards to investigations and enforcement actions. Therefore, when considering a possible breach of EU competition law, outside counsel should always be used to investigate and advise.

There is also no privilege in China, although some limited protection is growing in the sphere of criminal defense.

Conversely, U.S. legal privilege exists to protect not only the provision of legal advice but also the provision of information to the lawyer. Employees who give information to the company's lawyer are treated as the client for the

purposes of privilege. Recently, a U.S. court found that documents created in an internal investigation and produced by non-lawyers were privileged as long as one of the significant purposes of the investigation—but not necessarily the only—was to obtain legal advice.

CONCLUSION

In the event of a possible incident or company policy/legal breach, a director, officer, employee, or individual should notify their lawyer immediately, and if at all practical, do so verbally. They may refer to an investigation guide or a crisis management plan, if available, for the practical steps to take.

Notifying lawyers at the earliest opportunity will afford the best possibility that any investigation can be conducted maintaining the maximum potential privilege over communications and documents created.

CONTACTS

Frank Thompson
London
frank.thompson@klgates.com

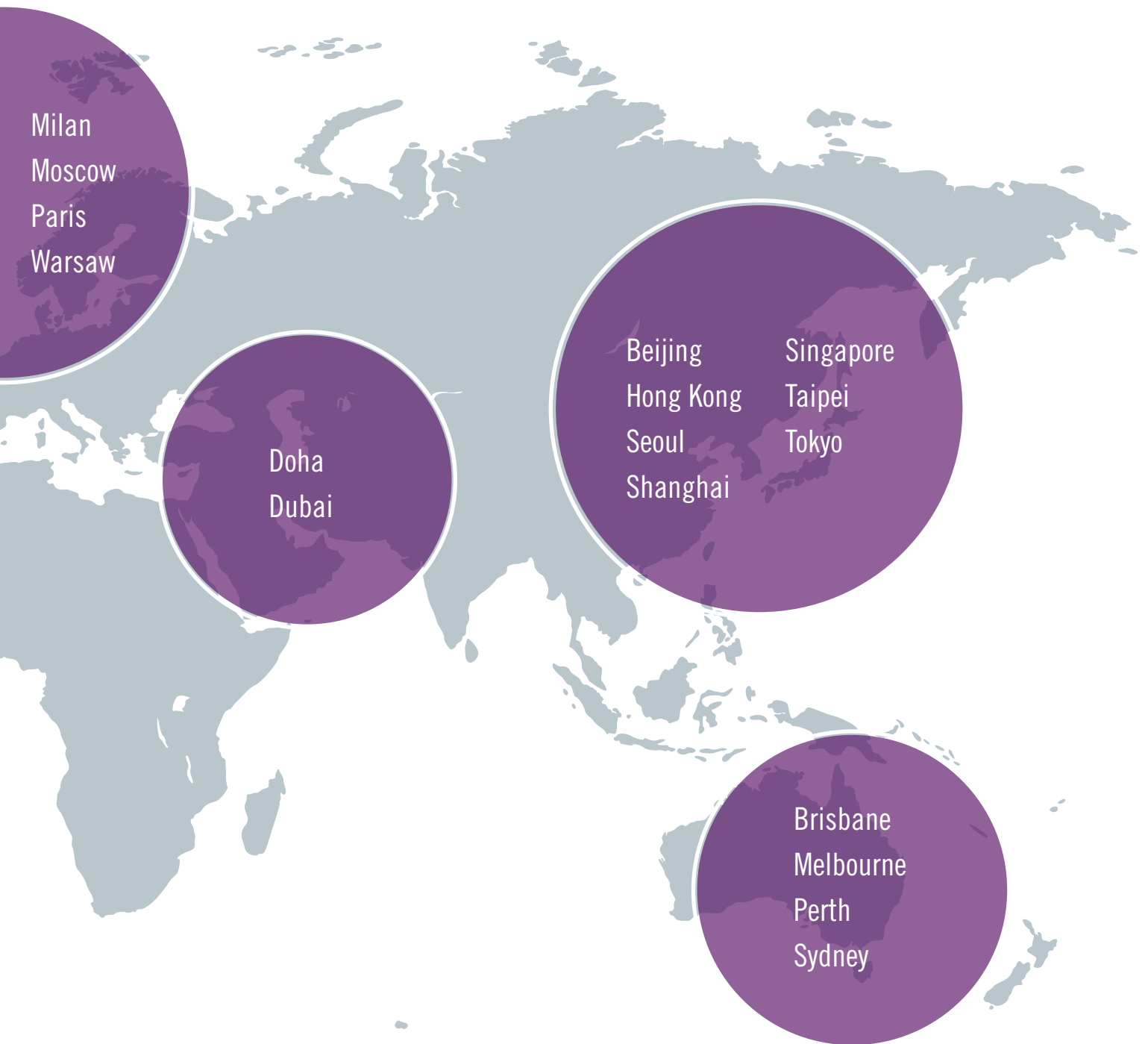
Laura Atherton
London
laura.atherton@klgates.com

Anchorage
Austin
Boston
Charleston
Charlotte
Chicago
Dallas
Fort Worth
Houston
Harrisburg
Los Angeles
Miami
Newark
New York
Orange County
Palo Alto
Pittsburgh
Portland
Raleigh
Research Triangle Park
San Diego
San Francisco
Seattle
Spokane
Washington, D.C.
Wilmington

Berlin
Brussels
Frankfurt
London

São Paulo

CROSS FIVE CONTINENTS



K&L GATES

Anchorage Austin Beijing Berlin Boston Brisbane Brussels Charleston Charlotte Chicago Dallas Doha Dubai Fort Worth Frankfurt Harrisburg Hong Kong Houston London Los Angeles Melbourne Miami Milan Moscow Newark New York Orange County Palo Alto Paris Perth Pittsburgh Portland Raleigh Research Triangle Park San Diego San Francisco São Paulo Seattle Seoul Shanghai Singapore Spokane Sydney Taipei Tokyo Warsaw Washington, D.C. Wilmington

K&L Gates comprises more than 2,000 lawyers globally who practice in fully integrated offices located on five continents. The firm represents leading multinational corporations, growth and middle-market companies, capital markets participants and entrepreneurs in every major industry group as well as public sector entities, educational institutions, philanthropic organizations and individuals. For more information about K&L Gates or its locations, practices and registrations, visit klgates.com.

This publication is for informational purposes and does not contain or convey legal advice. The information herein should not be used or relied upon in regard to any particular facts or circumstances without first consulting a lawyer.

©2014 K&L Gates LLP. All Rights Reserved.