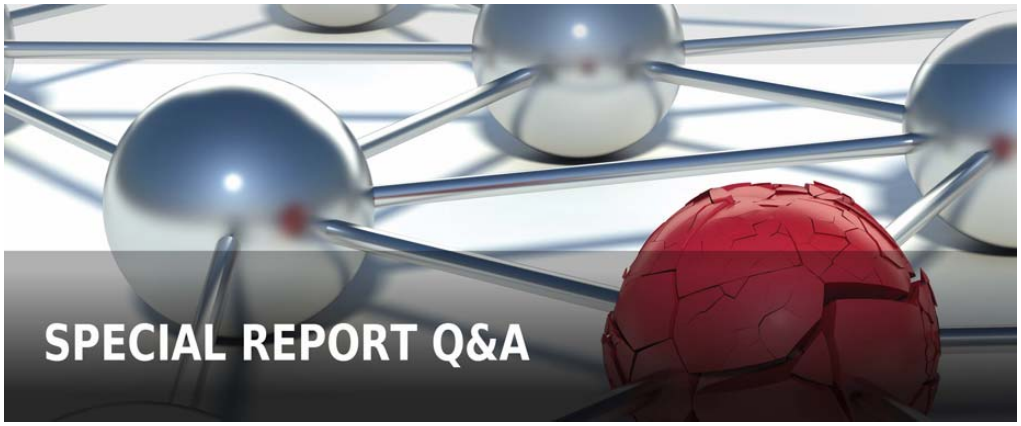


Q&A: Risks arising from agents, intermediaries and other third-parties

July 2014 Issue

July 2014 | SPECIAL REPORT: WHITE-COLLAR CRIME

Financier Worldwide Magazine

3

FW moderates a discussion on risks arising from agents, intermediaries and other third-parties between Anita Esslinger at Bryan Cave, Alexander Stein at Dolus Counter-Fraud Advisors, Walt Manning at InvestigationsMD, and Jonathan D. Schmidt at Ropes & Gray.

THE PANELLISTS

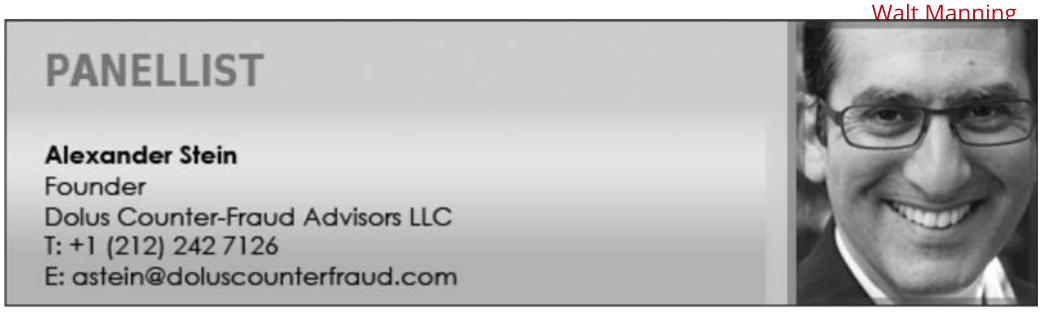
Anita Esslinger

Bryan Cave LLP

Alexander Stein

Dolus Counter-Fraud Advisors LLC

Walt Manning



FW: In your experience, what are the main risks that can emerge from business relationships with agents, intermediaries and other third parties? What types of third parties pose the greatest risks?

Esslinger: It is well known that use of third parties, including agents, sales representatives, consultants, intermediaries and distributors can pose significant risks under anti-corruption laws. A large number of improper offers or payments to or for the benefit of foreign government officials to obtain business or favourable governmental treatment, or to employees of private customers or suppliers to obtain a business advantage, are made by or through third parties. It is for this reason that both the Resource Guide to the US Foreign Corrupt Practices Act published by the US Justice Department and the SEC, as well as guidance published by the UK Ministry of Justice under the UK Bribery Act, focus on the need to do risk-based due diligence when using third-party intermediaries. Large commission payments, sales to governments or in countries or sectors that pose a high risk of corruption – such as those identified on Transparency International's Corruption Perceptions Index – use of intermediaries that have a family or other close relationship with a government official or customer or supplier employee, present particularly high risks. Use of multiple intermediaries in a transaction and use of intermediaries in high value transactions also pose risks.

Stein: Any meaningful conversation or action plan regarding business risk – particularly risks associated with fraud or third-parties – must include deep, sophisticated accounting and understanding of the matrix of human factors involved. Answering "what is risk?" transcends quantifiable differences across industries in definition, classification, measurement, assessment and tolerances. Risk is ever changing in context, and often more perceptual than factual. I frequently find that even in organisations which recognise people's irrationality and self-serving manipulativeness as inescapable realities in its functioning ecosystem, a raft of inscrutable psychodynamic forces are invariably underestimated. Transactions and affiliations involving third-parties or other satellites merely expand an already complicated field of variable unknowns. The establishment of a third-party relationship – which involves trust, confidence, vulnerability and interdependence – creates two separate but interlocking domains of risk – one institutionally external, and the other, internal. At core, the greatest perils are misgauging how these will interact, unintended but preventable executive myopia, and senior team blindspots to deep layer response patterns and decision-making in high-stakes scenarios.

Manning: One of the main risks results from allowing too much access to

White-collar crime

FORUM: Developing a multinational fraud compliance strategy

Navigating the pitfalls of cross-border investigations

FCPA and Esquenazi: if it walks like a duck...

The next step in the United States' campaign against offshore tax evasion

Deferred prosecution agreements, corporate criminal liability in the UK and the position of directors and senior managers

Minimising corruption risks in African investment opportunities

FINANCIER WORLDWIDE corporatefinanceintelligence

Home
Latest Issue
Issue Archive
Annual Reviews
TalkingPoints
10Questions
Advisor Handbooks
ExpertBriefing
FW News

Search Site
About
Contact
Subscribe
Editorial Submissions
Advertising
Terms & Conditions

JOIN MAILING LIST

Corporate Disputes
Risk & Compliance

Follow Us

company data networks. Some companies give outside parties the same access as trusted employees, but without requiring the outside personnel to be subjected to the same hiring scrutiny as their own employees are. Another important factor is to review cultural differences of the companies that could have an impact on security, network access and usage, and fraud prevention. Regardless of the protocols in place, if the operational philosophy and practices are not consistent with the expectations of the contracting organisation, there will be more risk. As organisations increase these external relationships, the perimeter has become harder to define and secure. Consider the affiliates and parties with whom the other company has a relationship. With this ever-expanding network of connections it becomes more likely that programs to mitigate risk can become diluted as they are filtered through the multiple layers of this network.

Schmidt: Anti-corruption enforcement, in the US through the Foreign Corrupt Practices Act (FCPA), in the UK through the Bribery Act, and elsewhere, has often focused on companies' relationships with third parties. EY's 12th Global Fraud Survey found that 90 percent of reported FCPA cases involved allegations about actions taken by third parties. In 2013, the DOJ and the SEC collected over $700m in penalties through FCPA enforcement, with almost every case involving a third party relationship. Third parties that have been the focus of FCPA enforcement include customs brokers, freight forwarders, distributors, sales agents, consultants and joint venture partners.

"Regardless of the protocols in place, if the operational philosophy and practices are not consistent with the expectations of the contracting organisation, there will be more risk."

— Walt Manning

FW: Can you outline any general examples of corporate failure to adequately assess third-party risks – and the consequences of such oversights?

Stein: Every passing news cycle brings some fresh report of fraud or other risk oversight malfunction. Behind the official institutional accounts there is always a shadow narrative. That other tale traces the countless 'small' decisions made, cans kicked, questions unasked and unanswered, incomplete conclusions, misunderstood data, nesting rationalisations, and myriad other 'inconsequential' inflection points setting in motion an unnoticed but inexorably aggregating sequence. Each such scenario unspools in infinitely unique ways. Consider a newly installed CCO. He inherits a cadre of long-established third-party vendor relationships, and soon uncovers his charismatic, well-liked predecessor's low-bar policies and

Analysis of an employee's personal motivations behind fraudulent acts

Q&A: Risks arising from agents, intermediaries and other third-parties

l*aissez-faire* systems. In his first quarter in the seat he must be equal parts sheriff, repairman, flow-master and torch carrier. He's also new to the culture, and wants to succeed long-range. His reports are nose-to-grindstone, his laterals are swamped, and senior team meetings always rushed. Effectively flying solo, a million daily judgment calls: Will this or that be tomorrow's disaster or can it wait? How hard should I push? Who'll listen? Who'll follow-through? Does yesterday matter as much as tomorrow? None of this, like most such 'soft' matters, registers on audit radar. There are no irregularities. Shareholders and regulators are happy. All appears fine. But, actually, it's not; senior management's just decided not to know it yet.

Manning: One of the most recent compelling examples of corporate failure in this area would be the Target data breach. Access to the Target point-of-sale network was through the stolen network credentials of a third-party HVAC provider, who apparently also serviced other retailers. The sad fact of this incident was that Target had monitoring systems in place that had given adequate warning, but nobody read the reports. There are many other examples where companies have outsourced parts of their IT operation, but did not sufficiently address business continuity in their due diligence. When system outages occurred without built-in redundancy, the companies lost significant revenue and productivity. Assumptions that other parties have capabilities and responsibilities that are not contractually addressed can cause needless catastrophic losses.

Schmidt: In 2013, Ralph Lauren Corporation entered non-prosecution agreements with the DOJ and the SEC and paid a fine and disgorgement for actions that occurred at its foreign subsidiary without the parent company's knowledge or involvement. The foreign subsidiary allegedly, over a five-year span, used a customs broker to funnel bribes to government officials in exchange for avoiding inspections and obtaining customs clearance for its imports. During the time in which the bribes allegedly occurred, the parent company did not have an anti-corruption program in place and did not provide anti-corruption training or oversight to its foreign subsidiary.

Esslinger: The lack of internal controls and allocation of adequate resources sufficient to determine whether arrangements with third parties are legitimate and comply with applicable law, as well as the failure to provide appropriate training and incentives for compliance with anti-corruption and ethics programs, are examples of corporate failures reflecting inadequate failure to assess third-party risks. There is also a tendency in many companies to rely on urgings to engage third parties by marketing personnel anxious to make sales above all. Several companies have paid a heavy price in terms of costs of responding to enforcement investigations, fines and reputational damage. In 2013, eight of nine FCPA corporate enforcement actions involved misconduct by or through third parties and resulted in heavy penalties.

FW: Do you believe companies pay sufficient attention to due diligence when forging a new business relationship? What basics should third-party due diligence cover?

Manning: The initial focus of due diligence is usually a high-level analysis of the mutual benefits to each party. Many times it is this portion of the

process that receives the most attention. Management is frequently more open to facts that favour the new relationship. Employees directly involved with the due diligence process may be reluctant to ask questions related to risk assessment where the results might be negative. The first step in the due diligence process should examine whether the new relationship is consistent with the strategy and goals of the company. Due diligence should include at minimum a thorough review of the other party's financial viability, management and firm history, and the existing controls and risk management protocols already in place. Clear definitions of roles and responsibilities must be included in related contracts, along with continual monitoring to ensure that the third party continues to have financial and operational ability to fulfil its obligations.

Schmidt: An effective third party due diligence process in the anti-corruption context should be designed to identify any red flags. Some examples of red flags are requests for cash payments, relationships with government officials, hesitancy to identify owners, or having little experience in the industry but claiming to 'know the right people'. To uncover these red flags, a due diligence process might include having the prospective third party complete a questionnaire identifying its corporate structure, its ownership interests, its key management personnel, any prior anti-corruption violations, and the company's current compliance policies. A company might also supplement and verify these responses by conducting media searches, or perhaps engaging an investigator if appropriate. It is important to remember that companies should use a risk-based approach to anti-corruption diligence. For example, third parties that interact with government entities merit a higher level of scrutiny than third parties that will not.

Esslinger: Many companies do not pay sufficient attention to due diligence when forging new business relationship with intermediaries, sometimes looking only to credit checks or anecdotal information that supports the desire to make sales. While there is no 'one size fits all' when it comes to determining how much due diligence is enough, at a minimum companies should understand the qualifications and ownership structure of third-party intermediaries, their relationships with government officials, employees of customers and suppliers, and their business reputations. In addition, companies should examine the rationale for using third-party intermediaries and understand the nature of the services to be provided, the compensation to be paid and the method of paying such compensation. References should be checked and information received from the third party should be verified or confirmed through independent evidence. Red flags suggesting potential issues should be resolved and may require more in depth due diligence.

Stein: A common refrain, especially though not exclusively in instances of fraud, is any variation on "we should've caught or known that, but didn't". Why is hindsight 20/20? Because now you know something you did not before. But that itself begs yet another important question: *why* didn't you? Certainly, many forms of malfeasance and breaches of trust are stealthy by design and can be difficult to discern beforehand. But often these incidents are rakes in short-cropped grass which could surely have been seen before being stepped on. How? Psychologically savvy appraisals of key

stakeholders and contexts, not merely hard data-driven assessments of conventional risk factors. I advise using due diligence as both an agnostic intelligence-gathering expedition and a diagnostic tool. It's not witch-hunting, fail-testing, or stink-sniffing. The benchmark for green light should never just be *not* finding corpses or negative strikes. Due diligence is an opportunity to learn. The critical factor is the substance and quality of attention. Sufficiency is a relative metric.

"In 2013, eight of nine FCPA corporate enforcement actions involved misconduct by or through third parties and resulted in heavy penalties."

— Anita Esslinger

FW: Organisations continue to migrate their IT services to the cloud and also allow a growing number of devices access to their networks. Could you outline the implications of third-party risks via technology?

Esslinger: Use of cloud technology to store and process data can have implications under export control and data protection regulations. Transfers of export-controlled software, technology and personal data to, and unauthorised access to such information by, third parties may take place in violation of applicable rules, potentially of multiple jurisdictions. Concerns with respect to adequate security to prevent unauthorised access or transfer need to be addressed.

Stein: Technological advances create new opportunities, advantages and risks of all stripes. Popular buzzwords like 'agile' and 'nimble' notwithstanding, real adaptation to new environments is incremental. Recent large-scale data breaches such as at Target, eBay and the Heartbleed flaw, underscore the imperatives for more sophisticated cyber-security mechanisms, but also stand as cautionary reminders of both the constant susceptibility of technologies to innovative exploitation and, more significantly, the exponentially ballooning domino effect of relatively minor but critically unnoticed oversights. The problem of the fortification principle in cyber-security – the far greater challenge and expense of trying to defend against every conceivable weakness compared to what's needed for attackers to find just one way in – is no less applicable to non-tech-related scenarios.

Manning: In many cases cloud providers do not have the risk management needs of the client as their first priority. I frequently see organisations migrating to the public cloud environment without adequately addressing litigation response and investigations issues and including the necessary language in the Service Level Agreement. Who possesses the encryption keys and whether data could be subpoenaed directly from the cloud provider are issues that are frequently overlooked. Determining the format of the data stored by the cloud provider, and whether that format would

facilitate data portability should the company later decide to change providers, are other topics to consider. Data backup strategies, how backup data is stored, and on what media are also important questions for a cloud provider. Organisations may want to consider maintaining a local independent backup or having an additional backup stored with a redundant escrow provider.

FW: What advice can you offer to companies on implementing and maintaining robust systems to monitor third-party risk?

Schmidt: To defend everywhere is to defend nowhere. Risk assessment is crucial and companies should prioritise monitoring based on the geographies in which a company operates, the scope of the business in each geography, and the types of activities and relationships in which the company engages. There are five steps to implement and maintain an anti-corruption compliance program: risk assessment; a written anti-corruption compliance policy, including a 'tone at the top' memo; training that is tailored to the country and the employee's role in the company; guidelines for third party due diligence, which should include sample questionnaires and representations and warranties for third party agreements; and ongoing oversight.

Esslinger: It is not enough simply to do due diligence on third parties and ensure that appropriate contractual arrangements are entered into up front. Ongoing monitoring needs to take place, including when payments are made. Monitoring of payments should be done with a view to ensuring that such payments and the method of payment are consistent with contract requirements, that they relate to well-defined and identifiable services that have actually been performed, that expense reimbursements are reasonable and properly documented and that there are no red flags raising questions about the appropriateness of such payments. Contractual arrangements should not be 'evergreen' or automatically renewable. They should have fixed terms that require periodic review and due diligence. In addition, periodic audits of arrangements with third parties should be undertaken, at least by internal auditors who are trained to look at matters from the point of view of compliance with anti-corruption policies and procedures and not just from the point of view of a financial audit.

Stein: Conventional fraud risk prevention and management programs canvas for deviations at pre-set margins. A form of static sonar, such monitoring scans for knowable anomalies. But what protocols are in place to notice, interpret and respond to variances outside established spectra? Even in respect of risk categories which hold within tight expectation values, there's always a near infinite array of potential human factor variables – from the vampiric rogue actor to a quiet unravelling of modest but meaningful ligatures within the corporate ecosystem. Additive to hard data-centric methodologies, I advise soft structure audits: sophisticated human factor and organisational analyses. These are designed like an institutional fMRI to render detailed composite images – 3-D profiles – of the interconnecting matrix of key people and relationships, to assess potential vulnerabilities, diagnose predicating contextual elements giving rise to problems, and implement viable strategies for micro and macro corrections in personnel, corporate policy or governance, and board and senior

leadership oversight and decision-making.

Manning: The first key is developing a rules-based due diligence strategy and identifying the appropriate risk levels associated with pending new business relationships. It is all too easy to implement a generic due diligence process that may not provide a sufficiently deep review for the levels of risk involved. Organisations should assess new relationships based on the inherent risks, and ensure that their due diligence process is detailed enough to address them. If monitoring systems are in place, their output must be continually reviewed and any anomalies immediately investigated. This has historically been a weakness in many risk management operations. It is human nature to pay less attention to systems that never indicate a problem. These systems are then checked less frequently, and other activities tend to push the monitoring down the list of immediate priorities.

"Emerging markets present serious opportunities for business growth, but depending upon the locale, can also present anti-corruption challenges. Companies operating in emerging markets are often dependent on third parties."

— Jonathan D. Schmidt

FW: How can companies reduce potentially damaging exposure to third parties in high-risk regions, such as emerging markets?

Stein: This calls to my mind a former client who had established ties in an Eastern Bloc region. An entrepreneur with a strong track-record prospecting for gap-leaping expansion, he saw exciting opportunity and potential economic upside for his business in this emerging market despite its reputation as rife with political corruption, unsavoury practices and a kangaroo judiciary. Entering into a known high-risk scenario requires preparatory reconciliation with, rather than attempted avoidance of, the inevitable. Embed thoughtful and agile damage control and resiliency plans. Consider the model analogues of aeronautics and surgery. These endeavours require extensive planning, preparation, study, R&D, practice, testing, sophisticated team-based diagnostic and problem-solving capacities, and multi-faceted knowledge-competency compounds. Redundancies and recourse options are baked-in to design and execution in realistic anticipation of expected error or failure. False confidence and bias confirmation are minimised or quarantined.

Manning: Companies must understand the realities of differences in business culture, history and customs – particularly in emerging markets. Security practices that are accepted or mandatory to management in one country may not be viewed from the same perspective in other countries. Governance and compliance may be difficult – if not impossible – to attain

when business cultures collide. Management must be in agreement and consistent on critical risk issues on a global scale. Companies should carefully examine jurisdictional legal questions related to choice-of-law covenants, and their enforceability. Templated contract language may not be sufficient across all international borders.

Schmidt: Emerging markets present serious opportunities for business growth, but depending upon the locale, can also present anti-corruption challenges. Companies operating in emerging markets are often dependent on third parties. Companies should first ensure that their employees understand the companies' legal risks and are trained on corporate policies. Before entering into a relationship with a third party – diligence, diligence, diligence. Then, if the company is prepared to enter into a business relationship with a third party, be sure to include contractual protections in the form of warranties, representations, certifications, and, if appropriate, audit rights.

Esslinger: With respect to due diligence in high-risk regions, such as emerging markets, where information is not readily available or transparent, a higher level of due diligence will often be necessary, including possibly engaging reputable investigation firms with expertise on the ground. It is also important for non-marketing compliance personnel to meet with potential intermediaries, and to understand why such intermediaries are being considered. In addition, training of intermediaries with respect to the need for and compliance with the company's ethics program and applicable law is desirable.

FW: Have any regulatory or legislative changes affected third-party risk in recent months? To what extent are government authorities focusing more of their enforcement activities on this issue?

Manning: Technology and globalisation have caused disruptions to the historic regulatory framework. The volume of regulations and frequently vague bureaucratic interpretation of new rules have made it almost impossible for companies to be in compliance. In recent years, US government agencies such as the SEC, the IRS and the DOJ and been much more active in targeting foreign financial institutions and companies to insist on the enforcement of US laws. I think we are beginning to see resistance on the part of some countries that perceive threats to their sovereignty. Admittedly, this is a hard line to draw, but when investigation and enforcement activity becomes a one-way street dictated rather than negotiated by one country, the overall effectiveness of compliance may actually be reduced.

Schmidt: While it does not directly impact third-party risk, the Court of Appeals for the 11th Circuit, in *United States v. Esquenazi*, recently found that state-owned companies can be an 'instrumentality' of a foreign government sufficient to be a basis for FCPA liability. This decision endorses the government's expansive view of the FCPA and I anticipate we will continue to see robust anti-corruption enforcement with a continued emphasis on third parties.

Esslinger: Much enforcement in several jurisdictions has been focused on bribery by or through third party intermediaries. In 2013, eight of nine FCPA

corporate enforcement actions involved misconduct by or through third parties and resulted in heavy penalties. The UK Bribery Act provides for a strict liability offence for companies that fail to prevent bribery by associated persons, including third party intermediaries, unless companies have adequate procedures in place aimed at preventing bribery by associated persons. As enforcement of the Act gains traction, this section promises to provide a powerful basis for enforcement with respect to any companies – not just UK companies – doing business in the UK with respect to bribery that takes place anywhere in the world. Already, one sees companies requiring their service providers to warrant contractually that they also have in place adequate procedures to prevent such bribery.

Stein: By the time most major pieces of regulation or legislation – SOX, AML, Dodd-Frank, Volker – are finally brought online, they've been pushed, pulled, twice-baked, refried and recast by so many competing constituencies that original blueprints for circles might ultimately be rendered as trapezoids. There are, unsurprisingly, significant divergences among precipitating needs, first-draft intentions, and the eventual on-the-ground consequences. Most important is any organisation's ability to usefully integrate positive precepts and isolate deficiencies for proposed revision or excision. I would offer this analogy with traffic safety approaches in urban planning. Most American policies rely on education and enforcement to reduce pedestrian and vehicle fatalities. By contrast, the Swedish Transport Administration's guiding credo is "design around the human as we are". Critical is how the scope and contours of issues are first defined – innovative solutions frequently derive from reconsidering what the problem actually is – and then designing and deploying responses that realistically account for how people think and act.

"Risk programs must be customised to context, moment and purpose before; during; or after. They should be holistic not balkanised, and must account for the unavoidable friction between ideal standards and actual human tendencies."

— Alexander Stein

FW: What final guidance can you offer to companies on effectively managing and monitoring ongoing relationships with third parties?

Esslinger: Effective managing and monitoring of relationships with third parties requires first and foremost tone from the top – not just words, but buy-in from and participation of senior management in the compliance function, including allocation of adequate resources to that function. Frequent communication throughout the organisation and training, including targeted training for employees in positions that pose a higher risk, with a view to embedding a culture of compliance throughout the

organisation are all important elements. It is also important that the internal audit function be able – and be trained – to test the adequacy of any compliance program, and not just material financial issues.

Stein: Risk isn't unitary or static, it's dynamic and fluid. Uncertainty, risk's fundamental, is defined, measured, perceived and experienced differently in different situations. Risk programs must be customised to context, moment and purpose before; during; or after. They should be holistic not balkanised, and must account for the unavoidable friction between ideal standards and actual human tendencies. Reject pseudo-explanations: 'because' is rarely an answer; 'for whatever reason' always means there's another reason; 'risk averse' and 'adrenaline junkie' sound meaningful but merely proclaim a superficial behavioural propensity. They're ultimately devoid of utility in substantively clarifying or addressing underlying drivers in decision-making. No mechanisms for monitoring or managing risk can be fully effective without first deeply surveying and understanding the many connected and disparate institutional elements, no matter how ostensibly inconsequential, which could be a possible fail point.

Manning: In any relationship, things change over time. Once the initial due diligence has been completed, too many organisations fail to conduct periodic reviews of their relationships to determine whether any changes have occurred that fundamentally change the nature of the agreement. Continual monitoring and compliance reviews related to existing relationships are necessary to ensure that no gaps have been created in the risk management infrastructure. Risk management and security are usually viewed as cost centres rather than revenue centres, and historically this has made these areas easy targets for budget and staff reductions. The current business environment has created organisational structures that are more fragmented globally. Managing the inventory of multi-tiered third-party relationships is infinitely more challenging, and companies should think carefully about cuts that diminish their capability. Advances to technology and the evolving global business environment will only increase risk. Companies must have the personnel and systems in place to proactively evaluate and manage these risks.

Schmidt: As enforcement authorities take expansive views of the reach of anti-corruption laws, companies need to maintain a culture of compliance and communicate that culture to their employees and third party partners abroad. A proactive approach to third party anti-corruption issues will serve a company well if it is later under investigation, as the DOJ and SEC have made clear in their FCPA guidance that meaningful credit will be given to companies that have implemented a good faith, risk-based compliance program, even if it fails to prevent the alleged infraction being investigated.

Anita Esslinger *is dual-qualified as an English solicitor and an American lawyer and is a partner in the London and Washington DC offices of Bryan Cave. Her practice is focused on US, UK and EU export controls and economic sanctions, the UK Bribery Act 2010, the US Foreign Corrupt Practices Act, the OECD Bribery Convention and other corruption initiatives. Ms Esslinger is a co-leader of the firm's Global Anti-Corruption Team.*

FINANCIER WORLDWIDE corporatefinanceintelligence

Home
Latest Issue
Issue Archive
Annual Reviews
TalkingPoints
10Questions
Advisor Handbooks
ExpertBriefing
FW News

Search Site
About
Contact
Subscribe
Editorial Submissions
Advertising
Terms & Conditions

JOIN MAILING LIST

Corporate Disputes
Risk & Compliance

Follow Us

Dr Alexander Stein *is founder of Dolus Counter-Fraud Advisors, a psychodynamic intelligence analysis and fraud risk consultancy. Dr Stein is widely regarded as a leading authority in the psychology of fraud, and a groundbreaking specialist in both institutional fraud risk management and complex multinational fraud investigation and asset recovery matters. He is a former monthly FORTUNE columnist, and frequent speaker, panellist and writer.*

Walt Manning *is recognised as an investigations futurist, and is also known as 'The Investigator's Coach'. Mr Manning has 35 years of international experience in the fields of criminal justice, investigations, fraud prevention, security, digital forensics and e-discovery.*

Jonathan Schmidt *is a San Francisco-based member of Ropes & Gray's government enforcement practice group. Mr Schmidt focuses on white-collar criminal matters, internal corporate investigations, and complex civil litigation. Prior to joining the firm, Mr Schmidt worked as an Assistant US Attorney for the Northern District of California, where he tried dozens of white-collar and violent crime cases and argued multiple appeals.*