REPRINT

MANAGING THIRD-PARTY RISK: DUE DILIGENCE AND EVALUATION

REPRINTED FROM:
RISK & COMPLIANCE MAGAZINE
JAN-MAR 2021 ISSUE

www.riskandcompliancemagazine.com

Visit the website to request
a free copy of the full e-magazine

Published by Financier Worldwide Ltd
riskandcompliance@financierworldwide.com

EXPERT FORUM

MANAGING THIRD-PARTY RISK: DUE DILIGENCE AND EVALUATION

MODERATOR

Bryant Aaron
Vice President & Chief Compliance Officer
Novartis Pharmaceuticals Corporation
T: +1 (862) 778 3949
E: bryant.aaron@novartis.com

Bryant Aaron is vice president and chief compliance officer at Novartis Pharmaceuticals Corporation and US country head of ethics, risk & compliance. Mr Aaron is responsible for all compliance matters in the US pharmaceuticals business, and he has US country level responsibility for the compliance function across all Novartis US divisions. He is a member of the US pharmaceuticals executive committee, the compliance committee and the country leadership team for Novartis Corporation.

PANEL EXPERTS

Wayne Anthony
Managing Director, Forensic & Litigation Consulting
FTI Consulting
T: +44 (0)20 3727 1613
E: wayne.anthony@fticonsulting.com

Wayne Anthony is a managing director in the forensic and litigation consulting segment at FTI Consulting and is based in London. He has more than 18 years of experience working in the forensic accounting field undertaking fraud investigations, financial crime investigations, asset-tracing projects, litigation and dispute advisory work.

Shahin Shamsabadi
Managing Director, Forensic & Litigation Consulting
FTI Consulting
T: +97 1 502 371 771
E: shahin.shamsabadi@fticonsulting.com

Shahin Shamsabadi has extensive experience conducting compliance and dispute-related investigations in the MENA region and has led several hundred investigations for local, regional and multinational clients in a wide array of industries and markets. For more than 12 years, Mr Shamsabadi has managed teams handling large-scale fraud, asset tracing and parallel imports investigations across the Middle East, Asia and Europe on behalf of legal counsels, monitors and supervisory authorities.

Andrew Durant
Senior Managing Director, Forensic & Litigation Consulting
FTI Consulting
T: +44 (0)20 3727 1144
E: andrew.durant@fticonsulting.com

Andrew Durant is a senior managing director in the forensic and litigation consulting segment at FTI Consulting and is based in London. He has worked in the forensic accounting sector for over 20 years and he has gained experience investigating a range of issues including financial statement fraud, stock and other asset losses, theft of confidential data, procurement and sales fraud, corruption and bribery, and investment fraud. He also has extensive experience in carrying out due diligence and asset tracing assignments.

Jamal Saleh
Senior Associate
Withers
T: +44 (0)20 7597 6167
E: jamal.saleh@withersworldwide.com

Jamal Saleh is a senior associate in Withers' corporate team. He is part of a team of trusted advisers to a number of high-net-worth individuals and private capital investors, with a particular focus on investments into the sports, hotels and hospitality, and technology sectors.

Aaron: What steps should a company take if there is any refusal or hesitancy by a third party to disclose its owners, partners or principals?

Shamsabadi: A third party's refusal or hesitancy to disclose ownership is typically the exception and not the rule. Put simply, such a refusal should be treated as a red flag and be investigated further. The compliance team should escalate the matter and the relevant team would make a decision on the next steps, such as seeking to identify the ownership independently or potentially engaging a service provider to conduct a due diligence investigation. There could be several reasons why a third party is hesitant to disclose this information. A common situation, for example, is that the point of contact is not comfortable requesting the information internally or is unwilling to provide the corporate details due to cultural sensitivities. Even so, the third party should be made aware that the requested information is mandatory for onboarding and approvals, so as to encourage them to be forthcoming and explain their position. Ultimately, the onus is on the third party being considered to supply the requisite documentation and information for onboarding and review. Their cooperation to do so should be viewed as a willingness to abide by their partner's standards and legal obligations. If, ultimately, they decline to provide the requested information, they should not be onboarded.

Saleh: Typically, as a first step in corporate and commercial due diligence, one may make a reasonable enquiry to the directors or company secretary of the relevant company to understand the ownership of the company. However, failing reasonable cooperation, any person may make an application under section 116 of the Companies Act 2006 to see the register of members of the relevant company and, provided that the applicant has a 'proper purpose' for applying, access should be granted. While 'proper purpose' has not been defined within the statute, there are high-level guidelines from the Institute of Chartered Secretaries and Administrators, in addition to case law on its interpretation. A proper purpose may include shareholders wanting to reach out to fellow shareholders about matters pertaining to the company, their shareholding or the exercise of their rights. Meanwhile, an improper purpose may include a communication to shareholders that the company considers would threaten, harass or intimidate members or would otherwise constitute an unwarranted misuse of the member's personal information.

Anthony: The globalisation of trade and communications has increased the need to contract with a range of third parties across multiple jurisdictions, creating a borderless commercial environment. It is therefore critical for organisations to manage their third-party risk in order to manage their overall business risk. In recent years, there have been numerous high-profile cases of organisations caught up in major bribery and corruption scandals resulting from actions, sometimes knowingly, of their third-party suppliers. A third-party's refusal to disclose its beneficial owners, partners or principals could be a deliberate attempt to obscure its true owners. In this case, the organisation should, in the first instance, understand why the third party is refusing to provide the information. Following this, it should conduct its own enhanced due diligence. This includes detailed research into the organisation using reputable databases, local and international media research to see if there is any adverse publicity, detailed research into the senior management to see if there are connections to politically exposed persons (PEPs) or similar, and asking to speak to the third party's bank or other customers. Ultimately, if an organisation has concerns and cannot gain comfort over who it is potentially working with, it should not enter a relationship with the third party.

Aaron: When soliciting third-party due diligence assessments in jurisdictions with strict data privacy laws, what alternatives are customary and required for a proper politically exposed persons (PEP) review of owners, partners or principals?

Shamsabadi: Privacy laws can considerably impact the effectiveness of due diligence assessments, particularly if they are solely focused

> **"A third party's refusal or hesitancy to disclose ownership is typically the exception and not the rule. Put simply, such a refusal should be treated as a red flag and be investigated further."**
>
> *Shahin Shamsabadi, FTI Consulting*

on publicly accessible sources of information. The alternatives that would be available in such cases vary depending on the jurisdiction. No matter what the case, a business should make sure that the service provider gives a full assessment on what can and cannot be done. The service provider should also be in a position to assure that no local laws would be violated and that all the information that is gathered is legally obtained. With regard to investigations conducted in a data-poor jurisdiction, the best approach would be to commission an assignment that will supplement the gaps in publicly accessible information with human intelligence. Again, any third-party due diligence investigations service provider should be in a position at the outset to provide a clear and comprehensive list of the steps they will take and the types of sources that they will contact as part of a project. This is of vital importance since it demonstrates that the service provider can collect the relevant information as well as ensuring that the commissioner can immediately step in if they feel any potential issues might arise from the line of enquiry.

Aaron: What should companies consider when a third party declines an agreement that requires mandatory and periodic 'monitoring and auditing' of their systems, transactions and operations?

Saleh: First, the company should consider the commercial aspects. Is the third party already subject to similar monitoring and auditing requirements on a frequent basis already? In particular, if the third party is a company listed on a stock exchange like the London Stock Exchange Main Market with a "premium" listing, it is likely to be subject to rigorous scrutiny already, such that additional requirements may be unduly burdensome. Conversely, is the third party sufficiently small in business size that such monitoring and auditing requirements would be overly burdensome for the everyday running of that business? If so, one may need to consider tempering the requirements imposed. In the absence of the above, the third party may need to provide business-specific reasons as to why such a request

"A 'right to audit' clause has become standard in many commercial contracts with third-party suppliers and is an important tool as part of an organisation's risk management."

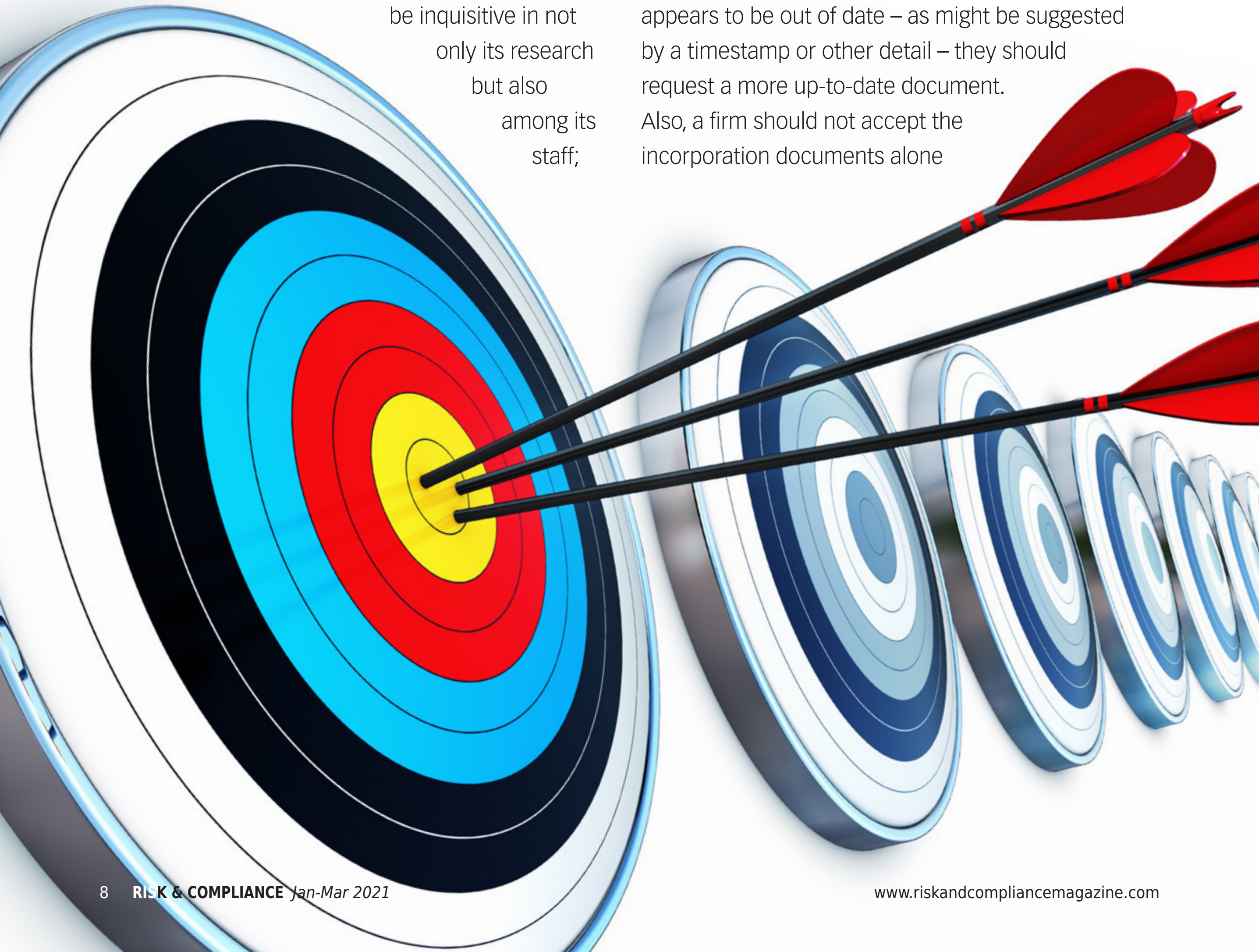
Andrew Durant, FTI Consulting

should be refused, such as having to employ specific people, or recalibrate the job specifications of existing employees, so as to comply with such obligations. However, notwithstanding the above, if the agreement merely reflects an obligation which is already imposed by law or regulation, this should raise concern and the company should consider what actions to take so as to best protect itself in respect of the third party.

Durant: A 'right to audit' clause has become standard in many commercial contracts with third-party suppliers and is an important tool as part of an organisation's risk management. When a supplier refuses to sign up to these contractual terms, the first thing to consider is why the supplier is declining the agreement. For example, are there data privacy rules or other regulations in the supplier's jurisdiction that make 'right to audit' difficult? Are the terms considered too onerous for the type of goods or services? Is it a one-off transaction? How critical is this supplier to your ongoing business operations? What are the current risks of engaging with this third party? An organisation will need to consider what actions it can take to satisfy itself that it can proceed with engaging with the third party. This might include identifying alternatives that can be put in place, such as requiring the third party to submit monthly financial information along with a signed attestation to its compliance with the organisation's code of conduct, policies and procedures, provide copies of its signed audited financial statements, or undertake regular independent desktop research into the third party to identify any adverse publicity. Ultimately, if a third party refuses to agree to these terms, you will have to decide, based on a risk assessment, whether you should continue to engage with them. As always, you should fully document all the discussions and steps taken in the decision process, and you should obtain senior management approval and sign off.

Aaron: What methods might a third party use to obscure its ownership without adequate business justifications? What can be done to manage this scenario if the third party conceals this information during a due diligence process?

Shamsabadi: The most common forms of obfuscating beneficial ownership are through the use of offshore investment vehicles and the use of proxies. The latter has alarmingly increased as offshore jurisdictions have been the subject of major leaks of corporate information. In practice, identifying the ownership structure of a business can be the easiest part of a due diligence investigation in jurisdictions where corporate information is readily accessible. Unfortunately, several jurisdictions do not have robust disclosure requirements and therefore a great deal of effort can be spent trying to identify shareholding details through the manual retrieval of records, commissioning of third-party due diligence providers and review of alternative sources of corporate information. Further complicating such an exercise is the potential that the ownership traces to a jurisdiction where it is difficult to 'pierce the veil'. With regard to the use of proxies, a shareholding structure for a business in these circumstances is purposely made to appear innocuous. For this reason, it is imperative that whoever is reviewing the records keeps in mind the nature of the partnership, as well as digging deeper into understanding whether the owners and principals on the other side have the requisite skills and experience to be engaged. The most obvious use of proxies is when a government official is indirectly a stakeholder or beneficial owner. These officials will frequently take painstaking steps to obscure their involvement. In order to avoid finding yourself caught out in such a situation, a business should be inquisitive in not only its research but also among its staff; asking the right questions about a market or country might shed light on a potential red flag. If the relevant team still has concerns regarding the counterparty, they can consider engaging an investigations firm to dig deeper into the matter. Any business should put a specific emphasis on checking the veracity of records that are provided by a third party. If a record appears to be out of date – as might be suggested by a timestamp or other detail – they should request a more up-to-date document. Also, a firm should not accept the incorporation documents alone



as part of the due diligence process, specifically if the company has been active for a substantive amount of time. It should also be encouraged to independently verify all corporate records provided by a third party. Lastly, it would be prudent that any future or scheduled review of a business partner require them to submit an up-to-date copy of their commercial registration, trade licence and shareholding details.

Anthony: A third party can obscure its ownership in several ways. The common ones are the use of the following. Shell companies with no independent operations, significant assets, ongoing business activities or employees. Complex group structures with numerous layers, often involving shell companies in offshore jurisdictions. Nominee shareholders and directors, such as spouses, children, extended family and other personal or business associates used to conceal the real owner. Professional intermediaries, such as trust and company service providers, used in the establishment of legal persons, legal arrangements and bank accounts. If you discover these types of structures or arrangements during your due diligence process, you need to raise this with the third party to obtain an explanation to justify the arrangements. In addition, you need to undertake a detailed review of the parties involved in the structure to identify any issues such as connections to PEPs, adverse media publicity, or appearance on sanctions lists or international watch lists. A lack of justifiable legitimate business purpose for such an arrangement is a clear red flag that the third party is attempting to obscure the true beneficial owner of the organisation.

Saleh: Under English law, the legal owner – person A – and the beneficial owner – person B – of shares in a company can be two separate persons. For example, this may be pursuant to trust or nominee arrangements – person A acts as trustee or nominee of person B. In such a scenario, only the legal owner would be recorded as the shareholder, with a minor reference on the statutory registers – and the corresponding share certificates – to the beneficial shareholder. This minor reference can be as simple as a combination of numbers, letters or symbols and it may be the case that a small number of people will know the identity of person B. In the absence of knowing who the beneficial owner of shares may be, a potential purchaser may need to find a different approach through due diligence to get suitable comfort about the identity of the shareholder. This may be a bit like playing a game of 'Guess Who?'. Are any of the shareholders subject to any international sanctions? Have any of the shareholders incurred any criminal liability or any contractual or civil liability above a certain threshold? Do any of the shareholders have any principal business interests in sectors which compete with the principal business interests of the purchaser?

Aaron: When dealing with a single source vendor of goods or services that declines to submit to a due diligence process, what options or controls can companies put in place to mitigate unforeseen risks to the organisation?

Durant: If your single source supplier declines to cooperate in your organisation's due diligence process, this would be a major red flag. If the supplier is a critical supplier you may, in the short term, have little choice but to carry on engaging with the supplier. In these circumstances it is important that the organisation undertakes procedures to mitigate this risk. It is crucial to fully document the steps taken, and to get senior management's approval and sign off. Doing nothing is not an option. An organisation should consider the following. First, seek alternative support information. For example, if the supplier will not release financial information, see what can be obtained from public records, reputable credit agencies or request a statement from its auditors as to its financial standing. Second, at the pre-contract stage, include a contractual clause that the information will be provided after signing the contract. Third, if post-contract, make a call, keeping detailed notes, to see what information the supplier can offer as an alternative and to understand what the issues and concerns are in providing the information. Fourth, visit the third-party supplier to inspect the required documents without taking copies, making sure to document the visit. Finally, request senior management to approve an exception waiver, fully documenting the issues and the criticality of the supplier. In the medium to long term, it will be important for the organisation to identify an alternative supplier willing to cooperate in the due diligence process and agree to abide by your organisation's policies and procedures.

Saleh: English law is based on the premise of 'buyer beware' and so the burden ultimately falls on the purchaser to take whatever measures are available to mitigate unforeseen risks. As the counterparty, you may wish to try and understand why the vendor has declined and to understand if that decision has been made reasonably. It is prudent to try and ask the vendor why it has declined to submit to due diligence, as the reasons for doing so may be well-founded or otherwise commercially acceptable. A fundamental step for the company would be to examine all publicly available information to determine whether the company needs to take any immediate or more obvious steps. For example, is the vendor subject to any insolvency proceedings? Have the company's prior actions been noteworthy in the media? Beyond this, the company may wish to renegotiate the purchase price or revert the burden of the lack of knowledge back onto the vendor in another way: the company can seek a widely cast indemnity from the vendor which pays out upon some or perhaps even any breaches of the agreement. This indemnity may be complemented by a guarantee from the vendor's shareholder or a fellow group company. However, an indemnity and guarantee will only be as good as the financial wherewithal of the person providing it, so a company will need to conduct sufficient due diligence on them. A more drastic scenario may see either money being put in escrow by one or both parties, to pay for any breaches of the relevant agreement, or perhaps even to secure certain assets of the vendor, which may be enforced upon a breach. Ultimately, much will turn on the respective commercial bargaining positions of the purchaser and the vendor. The purchaser may be put in a position to either accept a deal with little to no due diligence or simply walk away from the deal.

Aaron: If a third party relies on sub-vendors for the primary goods or services provided to the organisation, and has disclosed that it does not conduct a reciprocal due diligence process on its own vendors, how should the organisation respond?

Shamsabadi: Apart from ignoring what could be a major liability to a business, there are measures that can be taken to avoid potential risk exposure from such a situation. One option would be to emphatically stress and encourage that a stringent compliance system be integrated into the third party's business model. Indeed, there are international companies that explicitly require that a partner or vendor have compliance and corporate governance measures in place as a prerequisite of any arrangement.

> **"English law is based on the premise of 'buyer beware' and so the burden ultimately falls on the purchaser to take whatever measures are available to mitigate unforeseen risks."**
>
> *Jamal Saleh, Withers*

Anthony: It is an organisation's responsibility to ensure that its whole supply chain is compliant with its codes of conduct, policies and procedures, as well as regulations in its home territory and the territories in which its suppliers, including sub-vendors, operate. As the supply chain extends, it can be increasingly difficult for an organisation to have oversight and control of its suppliers. An organisation must therefore rely, to some extent, on the supplier to ensure its suppliers, such as sub-vendors, are compliant. In the first instance, you need to explain to your supplier the importance and, in some instances, the legal requirement, that such an arrangement is in place. You should explain that if arrangements are not in place, there may be an impact on your ability to continue engaging with the supplier. In addition, you should obtain the details of sub-vendors and undertake your own due diligence as a matter of priority. If red flags are identified, undertake the appropriate steps to mitigate risks, which may include requesting that your supplier seek an alternative sub-vendor.

Aaron: In the event that third-party due diligence raises red flags, could you provide examples of permissible flags and what steps may be reasonable and customary to safely address them and proceed with the third-party engagement?

Durant: It is important to recognise that a red flag during the due diligence process does not prove the existence of nefarious or improper activity. I would not say there is such a thing as a 'permissible red flag', but there are some typical red flags that might be seen as concealment of inappropriate arrangements but are, in fact, normal for that third party or the jurisdictions they operate in. This includes instances such as where the third party resides outside the country from which the services are being provided, payments to the third party being made to a country with a track record of money laundering, or a request from the third party that payments be made to a country outside of where the services are being provided. What is important is that you apply a suitable level of professional scepticism, evaluate the information you have and take appropriate steps to mitigate the risk to your organisation including, where appropriate, a detailed investigation. This should be clearly documented and recorded, with consultation at each step, and with

> **"Having a defined procedure for how you will carry out a post incident remediation review will help reduce the disruption to your organisation's supply chain."**
>
> *Wayne Anthony, FTI Consulting*

the appropriate senior management approval and sign off.

Aaron: Following third-party engagement, what steps should companies take to manage potential cases of a third party failing to comply with contractual codes, policies and procedures? How can it do so while preventing business continuity risks to the organisation?

Anthony: If you become aware that a third party has potentially breached your contractual arrangements or violated your organisation's code of conduct, you will need to ensure your organisation has clearly defined procedures in place to investigate the incident as quickly and thoroughly as possible. Having defined procedures in place for such breaches reduces the risk of the incident escalating while you work out what to do and, where appropriate, you can quickly remediate the issue, minimising the disruption to the supply chain. It is crucial that your code of conduct, agreed with the third party, includes provisions requiring the third party to fully cooperate and support an investigation of the incident to determine the nature and severity of the breach. Following your investigation, you may require the third party to undertake remediation action, which you will need to satisfy yourself resolves the incident. Again, having a defined procedure for how you will carry out a post incident remediation review will help reduce the disruption to your organisation's supply chain.

Aaron: What kinds of ongoing notifications – such as the emergence of legal action, an investigation or a change in due diligence representations – should third parties typically be required to provide throughout the relationship? What actions are customary when this information is identified by the organisation, rather than directly from the third party?

Saleh: For a corporate acquisition agreement, where there is a delay between execution of the acquisition agreement and the transfer of the relevant shares or assets, the third party may be asked to agree to a 'conduct of business' obligation. This obligation ensures that the third party does not conduct its business in a way that is out of kilter with its ordinary course of business before entering into the acquisition agreement. This in turn provides greater certainty as to the value of the shares or assets being acquired. In a similar vein, the third party will need to notify the company if it is subject to any event which is not in accordance with the conduct of business obligation. For a commercial agreement, it may be usual for a third party to notify the counterparty if it encounters any material adverse change which affects its ability to perform its obligations under the agreement. This may include a material change to its financial position and prospects, becoming subject to legal proceedings, entering into a contract with onerous terms or becoming subject to specific third-party rights or security. An additional example of ongoing notifications is where the third party is subject to a change of ownership or control of the third party. This may sometimes give rise to a termination right. However, such a provision may also be qualified: a change of control may not give rise to a termination right if, say, it does not bring the counterparty into disrepute or if the new controlling shareholder or person otherwise in control is not a competitor of the counterparty. Typically, where a company finds out that its counterparty is in breach of a matter covered by its agreement or of an ongoing obligation, a commercially sensible approach may be to approach the counterparty informally and instigate a commercially reasonable solution for both parties – which is then reflected in a legal document to ensure that both parties benefit from the amended arrangements. In the absence of a commercially reasonable approach, more formal communication or action may be required, such as sending a formal reminder of the company's rights or even exercising contractual rights of an indemnity, enforcement or termination. When doing so, such communication should be conducted in accordance with the notice provisions of the relevant agreement. Failure to do so can result, and has resulted, in serious contractual consequences, such as the invalidity of a claim under the agreement. One major caveat to the above is a circumstance where it becomes clear to a company that the counterparty is conducting its obligations or business generally in breach of any money laundering obligations or any other financial crime. In such a circumstance, the company should avoid contacting the relevant counterparty – so as to avoid falling foul of the 'tipping off' offences under financial services legislation, which incurs criminal liability – but should instead approach the company's anti-money laundering officer, who will then take the necessary steps under the Proceeds of Crime Act 2002.

Durant: During an organisation's dealings with a third party, one would expect both a periodic flow of information, such as completion of regular declarations of compliance or provision of financial information, and notification of significant one-off events, insofar as they relate to the contract or change the third party's ownership, as and when they happen. It is not uncommon for an organisation to include provisions in its supplier codes of conduct requiring its third-party suppliers to immediately notify it of any investigation or legal action insofar as they relate to its contracts. If you become aware of a significant event from another source, such as a whistleblower or media alert, then you have to question the strength and openness of the relationship and ask yourself why the third-party supplier did not notify you immediately. Irrespective of the source of the incident, you will want to undertake an investigation to assess the risk and impact on your organisation. However, non-notification from the third party creates a lack of trust, and you will naturally have a heightened sense of suspicion going forward. Typically, you would identify as much information in the public domain as possible, through your own desktop research, to attempt to determine the veracity of the allegations and the impact on your organisation. Once you have this information, and provided you have the necessary provisions in your supplier codes of conduct or contractual arrangements, you should notify the third-party supplier that you will initiate an investigation and they will be required to cooperate. R&C

The views expressed in this article are those of the author(s) and not necessarily the views of FTI Consulting, its management, its subsidiaries, its affiliates, or its other professionals.

FTI Consulting is an independent global business advisory firm dedicated to helping organisations manage change, mitigate risk and resolve disputes: financial, legal, operational, political & regulatory, reputational and transactional. FTI Consulting professionals, located in all major business centres throughout the world, work closely with clients to anticipate, illuminate and overcome complex business challenges and opportunities. For more information, visit www.fticonsulting.com and connect with us on Twitter (@FTIConsulting), Facebook and LinkedIn. www.fticonsulting.com.