NORDIC NEWSLETTER

TOPICS COVERED

Welcome to Jenner & Block's Nordic Newsletter

Dear friends and colleagues,

We are delighted to share with you the fifth edition of the **Jenner & Block Nordic Newsletter**. As you may have noticed, the political arena in the United States has been quite active recently and that activity definitely spills over to our professional lives. A few weeks ago, I participated in the IBA European M&A conference in Paris and met with many of Europe's leading M&A lawyers. Although the conference itself was a great success and I had the chance to catch up with many good friends and colleagues, I failed on one of my main goals for the conference. Before my arrival, I challenged myself to have at least one meeting in which US politics was not discussed. Needless to say, despite my (best/reasonable/commercially best/commercially reasonable best) efforts, I failed. Everybody I spoke with wanted to discuss US politics and their global impact. And when we were done with the United States, conversation turned to Brexit.

Why am I telling you all this? The answer is simple - with any new administration comes regulatory uncertainty. And with the new administration in the United States and Brexit looming in the United Kingdom, the uncertainty is even greater. It is because of this environment that this newsletter has an increased focus on certain regulatory and compliance issues that may be impacted by the current and future political climates in the United States and the United Kingdom that are relevant to Nordic companies doing business there. In this issue, we have included:

- Our periodic "Transactional Practice Tip," which discusses US government national security review of transactions involving foreign buyers of US businesses and how to manage the risks associated with CFIUS review;
- A link to our most recent "Business Guide to Anti-Corruption Laws," which includes updates and analyses regarding significant FCPA and anticorruption developments that will shape enforcement and compliance efforts in 2017;
- A discussion of continuing corruption enforcement risks for Nordic-based companies, even though there is a perception of "cleanliness" throughout the region;
- An article addressing the lessons learned from Rolls-Royce's recent settlement and deferred prosecution agreement with the UK Serious Fraud Office;

- An overview of the US Department of Justice's recently released "Evaluation of Corporate Compliance Programs," which sheds light on how the DOJ's new compliance expert will differentiate between effective compliance programs and those that are superficially pretty; and

- A link to Jenner & Block's inaugural "Trade Secret Update," which focuses on recent court decisions that have been shaping trade secret law in the United States.

We hope you find the newsletter informative. We welcome any comments you may have and are open to suggestions regarding future content that is of interest to you. And if you no longer wish to receive this newsletter, feel free to unsubscribe.

Sincerely,
Uri Doron

Head of the Nordic Practice, Jenner & Block LLP
udoron@jenner.com +1(212) 891-1677 Download V-Card

BACK TO TOP

Transactional Practice Tip

Managing CFIUS Risks and Other Strategic Considerations in Certain Transactions Involving US Businesses

The Committee on Foreign Investment in the United States (CFIUS) is an inter-agency committee that conducts national security reviews of foreign investments in the United States. CFIUS, chaired by the US Department of the Treasury, has the authority to impose conditions on a deal and, in extreme cases, effectively block a deal before closing or unwind a deal after closing, all in the name of protecting US national security.

Although CFIUS's authority and general processes are set forth in statutes and regulations, they can be challenging to decipher and the statutes and regulations offer little in the way of direct guidance to dealmakers. As a result, it can be difficult to know how to conduct a comprehensive risk assessment and how to assess whether and when parties should approach CFIUS. If parties to a transaction do not approach CFIUS, because they determine that a notice was not necessary, they are willing to live with the risks of not filing or for some other reason, CFIUS may choose to approach the parties, which could lead to increased scrutiny in the review process. This practice tip is intended to convey some lessons learned from past deals and provide guidance on handling (or not handling) the CFIUS process in a transaction.

Risk Assessment — Which Transactions Are Subject to CFIUS Review?

Will the Foreign Investor (or Buyer in an Acquisition) Obtain Control or Influence?

CFIUS does not review all foreign investments in the United States. Rather, CFIUS only reviews "covered transactions." A covered transaction is one that might result in foreign "control" over a US business involved in national security. There are detailed regulations on what constitutes "control," but generally, the test is functional and extremely broad (i.e., could the foreign investor cause the US business to take action or prevent it from taking action?). This power can be direct or indirect, and is relevant to CFIUS regardless of whether or not the investor exercises such power. The only explicit exception to CFIUS coverage is where a foreign entity owns 10 percent or less of the voting interest in the US business and holds it "solely for the purpose of *passive* investment." Note that, no matter how small the equity percentage, the ability to hold or appoint a seat on the board, for example, means that the foreign ownership is not solely for the purpose of passive investment.

What Industry and Business Functions Are Involved?

Even if a deal is a "covered transaction," CFIUS is interested only in investments related to "national security." As with "control," the concept of "national security" is wide-ranging and can be difficult to define. In addition to traditional defense and government contractor businesses, CFIUS has construed information and communications technology, transportation, energy, chemical production, and biotechnology and the life sciences, among other areas, as relevant to national security. As a general rule of thumb, deals involving businesses that do any classified work with the US government should anticipate a CFIUS review.

From What Country is the Foreign Investor?

CFIUS's mission is to manage risks to US national security, so it is unsurprising that CFIUS takes into account relations with foreign sovereigns and the jurisdiction of the investor and its ultimate beneficial owner (and the non-US intermediate subsidiaries in between and other affiliates). Companies from Russia and China, for example, have historically received greater CFIUS scrutiny than others. This does not mean, however, that if an investor is from a traditional US ally, that it will not receive similar attention. The level of CFIUS scrutiny also depends on the relationship of the investor to a government or governmental organization. When the investor is a private company rather than state-owned or controlled, CFIUS will likely have fewer concerns. By contrast, if an investor has direct or indirect ties to a foreign country's government or national security apparatus, there is likely to be a higher risk of CFIUS intervention, including potential mitigation measures.

Strategic Considerations

When Should CFIUS be Notified?

If a transaction is "covered," then CFIUS generally expects to receive a joint notice submitted voluntarily by the parties after the deal has been signed but prior to closing. However, parties have given notice to CFIUS using letters of intent or other agreements (so long as they are specific and the deals fairly certain). Less commonly, parties may decide to file with CFIUS pre-closing but intend to close prior to CFIUS clearance. The timing of the notice has potential advantages and disadvantages, depending on the individual transaction. In addition, there are potential consequences if the parties decide that a joint notice is not necessary, and if CFIUS later learns of the transaction and invokes its authority to approach the parties about the transaction. In such situation, it can often be the case that CFIUS imposes greater scrutiny of a transaction and there may be increased risk of interference.

What Are Some Potential Costs of the CFIUS Process?

When evaluating CFIUS risks, parties to a deal should consider the following potential costs:

- The *transaction costs* of due diligence, the determination of whether a CFIUS filing is required, and negotiation of the CFIUS-related deal terms;
- The *process costs* of informing CFIUS and responding to any informational inquiries;
- The *time costs* of any potential delay to deal closing (possibly, three months or more once CFIUS accepts a notice);
- The *mitigation costs* of any measures required by CFIUS as conditions to closing; and
- The *prohibition costs* of any impediment to closing imposed by CFIUS or unwinding of a closed transaction.

These costs are not exhaustive, but rather demonstrate the kinds of issues that parties should consider when evaluating whether and when to file a voluntary notice with CFIUS.

With respect to the time costs, if the parties decide to submit a joint notice to CFIUS, obtaining clearance is often an agreed-upon condition to close. The process of preparing and submitting the notice will depend on the nature of the transaction, but is typically a collaborative process that can take several weeks (or more) even in relatively straightforward transactions.

Once CFIUS "accepts" the submission (rather than the date the parties actually file with CFIUS), CFIUS typically has 30 days to "review" the transaction, after which it will either clear the transaction or initiate an investigation. A CFIUS investigation can extend the review by another 45 days, at which time CFIUS must clear the transaction, require a mitigation agreement or recommend that the transaction be blocked or unwound.

The ultimate decision to block or unwind a transaction is left to the President of the United States, who has 15 days after the conclusion of CFIUS's investigation to do so.

How Do You Allocate CFIUS Risk with Deal Terms?

Parties entering into a transaction that may implicate CFIUS review should consider the following:

- Whether and how to include CFIUS approval in a regulatory best efforts clause—particularly in light of a investor's tolerance for potential mitigation demands and agreed upon efforts in the antitrust (or other regulatory) approval context (e.g., "hell or high water");
- Whether to include CFIUS rejection or unacceptable mitigation demands as a trigger for the imposition of a breakup or reverse breakup fee (and whether the fee should be spread over time to account for the time costs of any CFIUS delay); and
- Whether and how to treat CFIUS review in the definition of "Material Adverse Event"—particularly whether to (i) limit the target's risk related to inaccurate representations and warranties, or (ii) limit the foreign investor's risk related to a duty to close with onerous mitigation measures or excessive CFIUS delay.

Strategic Considerations for Managing CFIUS Risk

1. **As always, plan ahead and start early**. The CFIUS process is time consuming, both throughout the notice preparation phase and the committee approval phase. Parties to a transaction should take CFIUS into account early and plan strategically to account for its potential risks and costs. To avoid any preparation and filing delays, parties should plan ahead and begin collecting the relevant information needed for the joint notice as early as possible. While the investor may have a greater interest in getting through the CFIUS process unscathed, the interests of both parties to a deal are aligned before CFIUS and parties should cooperate with each other to collect the relevant information and prepare the notice. After all, it is a joint notice.

2. **Be aware of latent risks**. Parties should be aware that latent CFIUS risks may lurk in many transactions, even when a target business does not appear, on its face, to involve national security. For example, a company whose primary activities do not involve national security may have a minor business line or limited number of products or services that implicate national security. Relevant information may be revealed throughout the due diligence process and recognizing from the outset that there may be "more than meets the eye" in many transactions will allow investors to appropriately incorporate CFIUS considerations into their deal planning.

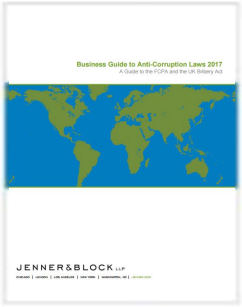
3. **Address CFIUS risks head on**. Parties are free to negotiate provisions into their deal documents that allow flexibility (or do the opposite) to close the deal in the face of a negative reaction from CFIUS. Often times these provisions mirror those addressing antitrust approvals; however, investors should focus on what consequences they are willing to accept. For example, an investor should ask itself if it would be willing to do the deal if the US business was not included. If so, maybe it could agree to a "hell or high water provision," which is a requirement that it take any and all actions necessary to obtain CFIUS approval (even divesting the US business or engaging in endless litigation).

4. **Consider other potential regulatory regimes**. In addition to CFIUS, foreign investors into the United States must also consider whether or not they are subject to other regulatory regimes, including antitrust review, foreign ownership, control or influence (FOCI) review by the Defense Security Service (DSS) (e.g., if the target business holds a facility security clearance to possess or access classified information) or a 60-day notice requirement to the Directorate of Defense Trade Controls (DDTC), which administers and enforces the International Traffic in Arms Regulations (ITAR) (e.g., if the US business exports or manufactures defense articles and is registered with DDTC). These regulatory regimes have their own unique requirements and sometimes onerous processes that should be assessed before entering into a transaction. Indeed, for companies that perform classified work, the parallel DSS process – which will typically require separate, Department of Defense-mandated mitigation measures – can be a particularly complicated and time-consuming process which if mismanaged could place the target's facility clearance in jeopardy.

Jessica R. Hertz, Partner • jhertz@jenner.com
Andrew D. Irwin, Partner • airwin@jenner.com
Jared S. Manes, Partner • jmanes@jenner.com
David A. Wishnick, Associate • dwishnick@jenner.com

BACK TO TOP

Jenner & Block Publishes 2017 Business Guide to Anti-Corruption



This year's edition of Jenner & Block's *Business Guide to Anti-Corruption Laws* provides updates and analysis regarding significant FCPA and anticorruption developments that will shape anticorruption enforcement and compliance efforts in 2017. Please click on the icon at right to read the full *Guide*.

Topics covered in the latest edition include:

- **Increased US Department of Justice (DOJ) and Securities and Exchange Commission (SEC) FCPA Enforcement and Major Monetary Penalties**: 2016 brought a significant increase in the number of cases resolved by the DOJ and SEC, nearly doubling 2015's total. Five cases included monetary components topping $100 million. In particular, two major global settlements with US and other international authorities reached new heights: Odebrecht agreed to a global resolution of approximately $2.6 billion, and VimpleCom agreed to monetary payments totaling $795 million.

- **DOJ Pilot Program and Declinations of Prosecution Reflect Carrot and Stick FCPA Enforcement Strategy**: In April 2016, the DOJ announced a one year pilot program describing the DOJ's expectations for self-disclosure, cooperation, and remediation from corporations facing an FCPA investigation and how those expectations will guide its assessment of an appropriate resolution of the matter. Pursuant to the Pilot Program, in resolving enforcement actions, the DOJ has expressly described how those factors drove the resolution, including five cases where, in light of a company's disclosure of an FCPA violation and cooperation with the DOJ's investigation, the DOJ declined to bring charges despite a finding of wrongdoing.

- **UK Anti-Corruption Enforcement Ramps Up**: In the United Kingdom, the Serious Fraud Office pursued corporate violations of the UK Bribery Act (UKBA), seeking to impose stiff penalties and stressing that companies with a potential UKBA issue must disclose and cooperate with the authorities to have a chance of avoiding criminal charges.

- **ISO Anti-Corruption Compliance Standard**: The international standard setting organization, ISO, announced a new standard for anti-bribery compliance programs, which is intended to become a universally applicable baseline for an adequate anti-bribery compliance regime. The standard, if it becomes widely adopted, could be a significant development in streamlining compliance related obligations and due diligence.

As with past versions, the Guide also provides an overview of the FCPA and the UKBA and discusses common questions and practical guidance about how these laws apply in the international market place.

BACK TO TOP

Even Clean Nordics Have Continuing Enforcement Risk

In the 2016 Transparency International Corruption Perceptions Index released in late January, Nordic countries again received the most favorable rankings. Yet, for the second year in a row, Transparency International's website draws a negative example from the Nordics, citing a scandal involving members of the Danish parliament to illustrate corruption in European countries.

Last year, Transparency International used a Swedish bribery investigation to show that countries with reputations for domestic compliance may have "dodgy records overseas." The organization noted that "just because a country has a clean public sector at home, [that] doesn't mean it isn't linked to corruption elsewhere."

As signatories to the OECD, the Nordic countries have been subject to a series of reports and recommendations, all of which called on authorities to step up the investigation and prosecution of bribery abroad. Follow-up reports praised the increased resources and expertise devoted to foreign bribery across the region. However, the reports also identified continuing weaknesses and the need for more progress, especially in Denmark and Finland.

At the same time, the US Department of Justice (DOJ) has expanded its tactics to investigate foreign bribery and increased its coordination with law enforcement agencies abroad. For Nordic companies subject to the jurisdiction of the US Foreign Corrupt Practices Act, this greatly increases the ways in which a corruption issue elsewhere in the world could come to the attention of authorities in the United States or their home country.

A 2014 speech by Marshall Miller, then a high-ranking official in DOJ's Criminal Division, described the use of "proactive investigative tools" and tactics previously used in organized crime and drug cases tactics such as "wiretaps, body wires, physical surveillance, and border searches." This strategy has become a staple of US white collar investigations and the aggressive use of those techniques is illustrated by the prosecution of PetroTiger's former CEO, whose conversations were secretly recorded by the company's general counsel, who wore a wire for the FBI.

International cooperation has continued to expand since Miller's 2014 speech, in US Securities and Exchange Commission (SEC) as well as DOJ investigations. A recent speech by Andrew Ceresney, then Director of SEC Enforcement, discussed the critical role of international collaboration in SEC FCPA investigations, and pointed to the growing trend of global settlements with payments divided among authorities in the United States and elsewhere.

DOJ's Pilot Program stresses that leads, documents, and witnesses are increasingly shared across international borders. The OECD Working Group on Bribery, which includes all five Nordic countries, has also held quarterly meetings where US authorities were invited to share information with other anti-bribery prosecutors.

In sum, Nordic companies can expect to see more aggressive enforcement of their own foreign bribery laws – and more cooperation with US authorities (which could also lead to more Nordic companies being pursued for violations of the FCPA) and increased use of investigative techniques previously reserved mostly for drug and organized crime cases.

This article was originally published on The FCPA Blog.

Nancy C. Jacobson, Partner • njacobson@jenner.com

BACK TO TOP

Rolls-Royce - Finally Some Bragging Rights for UK's Serious Fraud Office?

Rolls-Royce plc, the British engineering giant, announced on January 16, 2017 that it had agreed to pay a total of approximately £671 million by way of settlement with the UK Serious Fraud Office (SFO), US Department of Justice (DOJ) and the Brazilian Ministry Público Federal (MPF), after years of investigations into allegations of bribery and corruption by several of the company's subsidiaries. The Rolls-Royce agreement is the third approved deferred prosecution agreement (DPA) for the UK prosecutor since DPAs were introduced in the United Kingdom in 2014. It is also by far the highest penalty imposed under a DPA, and for once, the penalty imposed in the United Kingdom was significantly higher than that imposed by the DOJ.

The Facts

The SFO began its criminal investigation of Rolls-Royce's subsidiaries, Rolls-Royce plc and Rolls-Royce Energy Systems Inc., in December 2013, and it became the largest investigation the SFO has conducted. The conduct investigated was alleged bribery and corruption offences committed by intermediaries used by Rolls-Royce's conduct in Nigeria, Indonesia, Russia, Thailand, India, China and Malaysia, over a period of 24 years and in

relation to its defense, energy and civil engineering businesses. The misconduct includes: agreements to make corrupt payments; concealment or obfuscation of the use of intermediaries; failure to prevent bribery by employees or intermediaries; and failure to prevent the provision by its employees of inducements which constituted bribery.

Rolls-Royce's conduct first came to light in 2012, after the SFO became aware of internet posts that raised concerns over Rolls-Royce's civil engineering business in China and Indonesia. The SFO requested information from the company, which immediately launched an internal investigation. In 2013, the company voluntarily provided the SFO with reports from its internal investigations, which included further indications of corrupt conduct previously unknown to the SFO.

Under the DPA, Rolls-Royce agreed to disgorge profits and pay a fine totaling approximately £497 million (plus interest) over five years, as well as pay £13 million to cover the SFO's costs. The £497 million payment comprises disgorgement of approximately £258 million of profits and a penalty of roughly £239 million. Upon entry into the DPA, the SFO's indictment, which alleges six offenses of conspiracy to corrupt, five offenses of failure of a commercial organization to prevent bribery and one offense of false accounting, was immediately suspended.

The DPA lasts for five years (or four if the SFO confirms that all payments and obligations have been satisfied), during which Rolls-Royce is required to comply with a series of conditions relating to its continued cooperation with the SFO, as well as its adherence to a compliance program. That a DPA was available to Rolls-Royce at all, given the extremely serious nature of the allegations and the fact that it did not self-report the conduct to the SFO, is testament to the breadth and depth of the company's cooperation throughout the SFO's four-year investigation. Should the company breach any of the terms of the DPA, the SFO may make an application to the Court for termination of the DPA and if that application is successful, criminal proceedings may be reinstituted.

The company has also agreed to pay the DOJ and MPF approximately $170 million and $25.5 million, respectively, in relation to similar conduct by a subsidiary involved in its energy business. It is notable that this is the first instance in which a payment to the SFO is greater than the DOJ (albeit that the two settlements do not relate to exactly the same conduct).

Commentary on Judgment

In approving the DPA, Lord Justice Leveson concluded (as he is required to do) that the DPA was in the interests of justice and that its terms were fair, reasonable and proportionate. Given the limited number of DPAs that have been entered into by the SFO, the judgment provides useful guidance and insight for other companies that may wish to enter into discussions with the SFO about concluding such an agreement.

Cooperation

In his judgment, Leveson LJ noted that the investigation was, "*in a very large part conducted and voluntarily revealed to the SFO by Rolls-Royce itself*." He frequently emphasized the very high level of cooperation demonstrated by the company - described by the SFO as "*extraordinary.*" The company conducted 229 internal interviews and reviewed more than 250 of its relationships during the course of the investigation. Leveson LJ went as far as to say, "*that Rolls-Royce could not have done more to address the issues that have now been exposed.*" It is clear that this level of cooperation, maintained over many years and at a high price to the company (estimated around £123 million), was crucial in persuading the Judge that this DPA should be approved. The SFO persuaded the Judge that the DPA was in the interests of justice, despite the usual position being that a DPA is unavailable to companies that have not self-reported the criminal conduct.

Improvements and changes

The company appointed a 'quasi-monitor' of its compliance program in 2013. The court noted that Rolls-Royce made significant efforts to improve its compliance procedures, in particular by addressing the possible risks associated with its use of intermediaries. Noting that no current member of the Board was involved in any of the wrongdoing, the judge stated that the decision to approve the DPA could have been different had any current senior management been implicated in the criminal conduct, or been in a position where they should have been aware of the culture and practices at Rolls-Royce, which were described as "clearly endemic."

Never too big to be punished

Leveson LJ noted that Rolls-Royce is a very large company, the success of which is important to the British national interest. He acknowledged that a criminal conviction against Rolls-Royce would be highly detrimental to the company, which would in turn impact the UK defense industry and innocent persons who did not commit any misconduct. While this was a factor in whether the DPA was in the interests of justice, it could not be determinative in a case of such grave conduct as this. However, the Judge found that the company was a changed organization, which will still have to suffer the impact of negative publicity regarding the DPA, and that the financial penalty imposed was commensurate with that of a guilty plea (as required by law), thus, he considered that it was in the interests of justice to approve the DPA.

Size of fine

Leveson LJ has stated that the size of a fine under a DPA should be sufficient to punish wrongdoing and deter others from engaging in similar conduct, while being sufficiently small so as to encourage companies to self-report and to confront misconduct. Under the DPA, Rolls-Royce received a 50% percent reduction in the penalty (not disgorgement of profits) that would have been imposed had it been convicted. This reduction was clearly linked to Rolls-Royce's high level of cooperation with the SFO.

Conclusion

This DPA signals a serious step up for the SFO, marking a successful end to its largest investigation to date. The prosecutor (and it seems, the Judge) will no doubt be hoping that the level of penalty will deter companies from engaging in misconduct, motivate them to ensure their compliance procedures are up to scratch and that companies will be incentivized to confront serious issues of bribery and corruption head-on.

The (still rather small) body of UK case law in this area now seems clear – self-reporting and committed, long-term cooperation with the SFO should enable organizations to use DPAs and avoid the potentially disastrous consequences resulting from a criminal conviction, even if that conduct is very serious and long-running. While the level of financial penalty imposed on Rolls-Royce is high, it would have been much higher but for the DPA, and this case should serve as an example to companies of how damage can be limited in even the most difficult circumstances.

A version of this article was also published in *Fraud Watch*.

Kelly Hagedorn, Partner • khagedorn@jenner.com
Jessica G. Veitch, Associate • jveitch@jenner.com

BACK TO TOP

DOJ Releases Under-the-Radar Paper on "Evaluation of Corporate Compliance Programs"

In early February, the US Department of Justice (DOJ) Fraud Section quietly released a short paper entitled "Evaluation of Corporate Compliance Programs," which sheds more light on how the DOJ's new compliance expert will differentiate effective compliance programs from those that are superficially pretty. In the paper, the Fraud Section reiterates that the factors it considers in deciding whether to investigate, charge or negotiate with a corporation (called the "Filip Factors") necessarily require a fact-specific assessment. The topics the Fraud Section considers in conducting its assessment – like tone at the top, third party risk assessments and compliance resources – are not new. Yet, the paper provides an important glimpse into "common questions that we may ask" in evaluating how an individual organization passes muster under the Filip Factors. Many of the "sample questions" highlight where the Fraud Section will press to ferret out those corporations that have simply adopted a check-the-box compliance program, versus those that have embraced compliance as a cultural imperative.

Sample Topics

The paper enumerates 11 sample topics that the Fraud Section "has frequently found relevant in evaluating a corporate compliance program." Many of these topics appear in other compliance resources, but their presence here shows their durability as measures by which corporations will be judged. The topics include:

- Analysis and remediation of underlying misconduct, including root cause analysis of compliance failures and whether similar incidents occurred in the past;
- Senior and middle management words and deeds to convey and model proper behavior;
- Autonomy and resources of the compliance function including stature, qualifications and funding;
- Operational integration of compliance policies and procedures into a control framework;
- Risk assessment process and the role of metrics;
- Incentives and disciplinary measures and whether they are effective, consistent, and fairly meted out; and
- Continuous improvement, periodic testing, and review.

Thematically, the topics convey that a successful compliance program responds and reacts to each compliance failure. Compliance needs to bear the visible support of top – and middle – management and run under the leadership of well-resourced compliance professionals. Compliance does not exist isolated from a company's day-to-day operations and strategic decision-making, but is integrated throughout both.

"Common Questions" to Probe a Company's Compliance Program

The Fraud Section is careful to note that it "does not use any rigid formula to assess the effectiveness of corporate compliance programs" and that each company's "risk profile and solutions to reduce its risks warrant particularized evaluation." Yet, the paper sets forth "common questions" that the Fraud Section may ask in making that individualized determination.

Many of the questions coalesce around three critical avenues to explore whether a company has embedded compliance into its culture: (1) the company's processes for lessons learned, (2) the effectiveness of its gatekeepers and (3) the integration of compliance into the business.

Processes for lessons learned

These questions probe whether the company is learning from prior compliance mistakes or simply punishing the wrongdoer without seeking and correcting systemic failures. For example:

- "Were there prior opportunities to detect the misconduct in question, such as audit reports identifying relevant control failures . . . ? What is the company's analysis of why such opportunities were missed?"
- "What controls failed or were absent that would have detected or prevented the misconduct? Are they there now?"
- "Has the company's investigation been used to identify root causes, system vulnerabilities, and accountability lapses, including among supervisory manager and senior executives?"
- "What information or metrics has the company collected and used to help detect the type of misconduct in question? How has the information or metrics informed the company's compliance program?"

Effectiveness of gatekeepers

These questions explore not only stature and skill of compliance personnel and personnel in other control functions in the organization, but also whether reports of misconduct get to the right responders. For example:

- "What has been the turnover rate for compliance and relevant control function personnel?"
- "Who reviewed the performance of the compliance function and what was the review process?"
- "Has the company outsourced all or parts of its compliance functions to an external firm or consultant? . . . How has the effectiveness of the outsourced process been assessed?"
- "Has there been clear guidance and/or training for the key gatekeepers . . . in the control processes relevant to the misconduct?"
- "Has the compliance function had full access to reporting and investigative information?"

Integration of compliance into the business

Many of the Fraud Section's questions attempt to shine light on whether a company has woven compliance into its day-to-day business, from board room to the factory floor. Questions include:

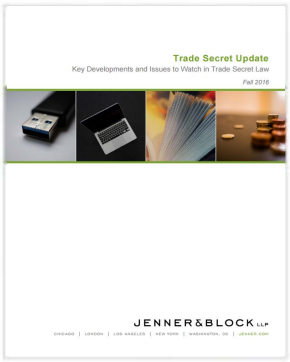
- "What specific actions have senior leaders and other stakeholders (e.g., business and operational managers, Finance, Procurement, Legal, Human Resources) taken to demonstrate their commitment to compliance . . . ?"
- "What compliance expertise has been available on the board of directors?"
- "What role has compliance played in the company's strategic and operational decisions?"
- "Have business units/divisions been consulted prior to rolling [new policies and procedures] out?"

These questions suggest that the Fraud Section will continue to press on a key vulnerability that plagues the compliance efforts of many organizations – how to translate a well-designed compliance program into the cultural fabric of the company. And prosecutors will not likely be impressed without demonstrable proof of action at all levels of the organization and across all aspects of its business.

Erin R. Schrantz, Partner • eschrantz@jenner.com
Nathaniel K.S. Wackman, Associate • nwackman@jenner.com

BACK TO TOP

Trade Secret Update: Key Developments and Issues to Watch in Trade Secret Law



Not long ago, few American companies had reason to be concerned that their intellectual property would be taken by vendors and replicated overseas. It is now fairly common. Similarly, going to work for a direct competitor was once considered taboo. Now, it's simply called a "lateral move" – executives, engineers and researchers rarely spend their entire careers with one company. These changes in the business world and corporate mobility, coupled with new technology that makes it easier than ever to transfer proprietary business information from one computer to the next, have set the stage for a continued increase in trade secret litigation.

Jenner & Block's Inaugural "Trade Secret Update"

Last year was a significant year for trade secret law, with several notable verdicts and settlements in the United States, key developments in state law, and the implementation of a new federal statute, the Defend Trade Secrets Act, which for the first time authorizes federal civil claims for trade secret misappropriation. To inform our clients and friends on these important trends, Jenner & Block recently published its inaugural "Trade Secret Update," which focuses on reported decisions applying and changing trade secret law. Important aspects of trade secret law continue to be shaped across jurisdictions, including the propriety of various damages theories, trade secret specifications and the preemptive effect of the US Uniform Trade Secrets Act. The publication also addresses recent cases involving criminal aspects of trade secret misappropriation and the US Computer Fraud and Abuse Act, which continues to play a role in many trade secret cases, and the split between the courts that continues to plague that statute.

Click the icon above to download a PDF of the full update.

BACK TO TOP