JUSTICE NEWS

Assistant Attorney General Leslie R. Caldwell Delivers Remarks at the Compliance Week Conference

Washington, DC, United States ~ Tuesday, May 19, 2015

Thank you, Matt [Kelly]. It is a pleasure to be here to kick off day two of Compliance Week's 10th annual conference. This conference represents a great opportunity for corporate executives, compliance officers, auditors and in-house and outside counsel to share information about effective compliance policies and practices.

This morning, I want to discuss corporate accountability. How corporations should be holding themselves accountable by designing compliance programs that don't just look good on paper but actually work. Compliance programs that are designed to protect the company's reputation, customers, counterparties and the public, as well as ensuring compliance with the law.

I also will take a few moments to tell you about how we in the Criminal Division are trying to hold ourselves accountable and provide increased transparency by explaining our decision making when we can and setting forth our expectations with respect to corporate cooperation in our investigations.

For the past year, it has been my privilege to lead the Criminal Division of the U.S. Department of Justice and the nearly 1,000 dedicated prosecutors and support staff who work every day to investigate and prosecute federal criminal cases, to develop criminal law and sentencing policies and to promote the rule of law around the world.

While the U.S. Attorneys' offices generally focus on investigating and prosecuting crime in their respective districts, the Criminal Division – often in partnership with U.S. Attorneys' offices – generally handles large matters with national or international significance.

Because of the global nature of our cases, the Criminal Division has personnel in more than 45 countries around the world who, among other responsibilities and in conjunction with the Criminal Division's Office of International Affairs, help facilitate the collection of evidence from abroad through collaboration and cooperation with our international law enforcement partners.

Among the 17 sections and offices that make up the Criminal Division, the Fraud and Asset Forfeiture and Money Laundering Sections are most involved in the investigation and prosecution of corporate crime. Both sections play critical roles in the department's efforts to combat sophisticated economic crime. It is the work of these sections that is most relevant to our discussion today.

A corporation's internal compliance policies and practices, and its compliance professionals, are the first lines of defense against fraud, abuse and corruption.

As all of you know, there is no “one size fits all” compliance program. Rather, effective compliance programs are those that are tailored to the unique needs, risks and structure of each business or industry.

While a corporate compliance program must, by definition, address regulatory risk and the risk of potential violations of law, a strong compliance program will not stop there.

A strong program also will aim to deter employee misconduct, whether or not that misconduct poses obvious regulatory risk.

While companies have for years appropriately adopted a “risk-based” approach to compliance, we have seen that corporations all too often misdirect their focus to the wrong type of risk. We have repeatedly seen corporations target the risk of regulatory or law enforcement exposure of institutional and employee misconduct, rather than the risk of the misconduct itself.

The result: compliance programs are too often behind the curve, effectively guarding against yesterday’s corporate problem but failing to identify and prevent tomorrow’s scandals.

In designing compliance programs, companies would be wise to examine all of their lines of business – including those not subject to regulation – and determine where specific risks are and how best to control or mitigate them.

It is also critical that compliance programs take into account the operational realities and risks attendant to the particular company’s business, and are designed to prevent and detect particular types of misconduct likely to occur in a particular line of business.

For example, to comply with the Foreign Corrupt Practices Act (FCPA), businesses that tend to be exposed to corruption must employ different internal controls than businesses that have less exposure to corruption.

Similarly, in the anti-money laundering context, a financial institution must ensure that its compliance policies and practices are tailored to identify and mitigate the risks posed by its specific portfolio of customers, and that those customers are providing complete and accurate information.

Too often we have heard companies say that a particular course of criminal conduct took them by surprise, when a hard look at the business practices would have identified the risk. And, far too often, we have heard companies exclaim in defense that everyone else is doing it – that others in the industry are engaged in the same misconduct. But as you all know, an industry-wide compliance failure is not a defense to knowing and willful criminal activity.

With this principle that compliance programs should be proactive, and not merely reactive in mind, there are some general hallmarks of effective compliance programs that I’d like to share with you today.

- A company must ensure that its senior leaders provide strong, explicit and visible support for its corporate compliance policies.Corporate management must enforce compliance policies, not tacitly encourage or pressure employees to engage in misconduct to achieve business objectives.
- We look not just at the written policies, but to other messages otherwise conveyed to employees, including through in-person meetings, emails, telephone calls, incentives/bonuses, etc.; and will make a determination regarding whether the company meaningfully stressed

compliance or, when faced with a conflict between compliance and profits, encouraged employees to choose profits.

- Senior executives should be responsible for the implementation and oversight of compliance.Those executives should have authority to report directly to independent monitoring bodies – for example, internal auditors or the board of directors.
- A company's policies should be clear and in writing and should easily be understood by employees.But having written policies – even those that appear specific and comprehensive "on paper" – is not enough.
- Compliance teams need adequate funding and access to necessary resources.And they must have an appropriate stature within the company.
- A company should have an effective process – with sufficient resources – for investigating and documenting allegations of violations.
- A company periodically should review its compliance policies and practices to keep it up to date with evolving risks and circumstances, including when the company merges with or acquires another company.In particular, if a U.S.-based entity merges with, acquires or is acquired by a foreign entity, all compliance policies should be reviewed and revised accordingly.
- A company should have an effective system for confidential, internal reporting of compliance violations.
- A company should implement mechanisms designed to enforce its policies, including incentivizing compliance and disciplining violations.
- A company should sensitize third parties with which it interacts (for example, vendors, agents or consultants) to the company's expectation that its partners are compliant.This means more than including boilerplate language in a contract.It means taking action – including termination of a business relationship – if a partner demonstrates a lack of respect for laws and policies.

Corporations also must ensure compliance with the laws of all the countries in which they operate. We appreciate that this may present a major compliance challenge, as international corporations often must bridge cultural, as well as geographic, divides. But such challenges do not justify non-compliance.

Likewise, if a foreign-based corporation or institution operates in the United States or transacts business in the United States, it must ensure compliance with U.S. laws.

For example, if a foreign bank that operates in the United States identifies suspicious activity related to a foreign account held by a customer that also maintains an account in the United States, compliance personnel in the United States should be alerted to the suspicious activity.

Overall, our message is simple: we expect corporate entities to take compliance risk as seriously as they take other business-related risks.

As all of you know, the adequacy of a compliance program is a factor when we decide how and whether to prosecute a company. The lack or insufficiency of a compliance program can have real consequences for a company when a violation of law is discovered.

For example, this past December, Alstom S.A., the French power company, pleaded guilty to violating the FCPA by falsifying its books and records and failing to implement adequate internal controls. Alstom admitted to its criminal conduct and agreed to pay a penalty of over $772 million.

The scheme involved the payment of bribes to various government officials and the falsification of books and records in connection with power, grid and transportation projects for state-owned entities around the world, including Indonesia, Egypt, Saudi Arabia, the Bahamas and Taiwan. Alstom attempted to conceal that it was the source of the corrupt payments to government officials by funneling the bribes through third-party consultants.

In reaching the global resolution, the department considered many factors, including the company's failure to voluntarily disclose the misconduct; its refusal to cooperate with the government's investigation for several years (i.e., until the government charged several company executives); the breadth of the misconduct – which spanned many years, occurred in several countries and crossed business lines; and the company's criminal history.

And we considered the company's lack of an effective compliance program at the time of the misconduct. As a result of all of these factors, Alstom pleaded guilty and paid a significant criminal penalty.

When a compliance program works and a company suspects or discovers potential criminal wrongdoing, a company would be wise to conduct a thorough internal investigation.

While we in the Criminal Division will not tell a company how it should conduct an investigation, we evaluate the quality of a company's internal investigation, both through our own investigation and in considering what if any charges to bring against a company. In that regard, we have seen some "best practices" with regard to internal investigations.

Good internal investigations uncover the facts. They don't promote corporate talking points or whitewash the truth. The investigation should be focused on rooting out the relevant facts, identifying and interviewing the knowledgeable actors and capturing and preserving relevant documents and other evidence. The investigation should seek to identify responsible individuals, even if those individuals hold senior positions at the company.

It is reasonable to take resources – time and money – into account. If an internal investigation unearths criminal conduct, the inquiry should be thorough enough to identify the relevant facts, players, documents and other evidence, and to get a sense of the pervasiveness of the misconduct.

But, we do not believe that it is necessary or productive for a company to employ its internal investigators to look under every rock and pebble – particularly when a company has offices or personnel around the globe that do not appear to be involved in the misconduct at issue.

In fact, doing so will cost companies much more in the end, both in fees but also because it ultimately will delay our investigation and delay resolution and closure for the company.

For example, if a multi-national corporation discovers an FCPA violation in one country, and has no basis to suspect that the misconduct is occurring elsewhere, the Criminal Division would not expect that the internal investigation would extend beyond the country in which the violation was discovered. By contrast, if the known offenders operated in multiple countries, we would expect that the internal investigation would extend into those locations as well.

Once your company learns of potential criminal conduct and confirms it through a reasonable internal investigation, the company then must choose whether to disclose the conduct to the government, and whether to cooperate in the government's investigation.

These are the company's choices, and very few companies have a legal obligation to disclose criminal misconduct to the department. Likewise,

there is no obligation to cooperate beyond compliance with lawful process.

But if a company chooses to cooperate with the government in its investigation – particularly at an early stage – the company likely will receive significant credit for such efforts when the government is contemplating what prosecutorial action to take.

In conducting an investigation, determining whether to bring charges and negotiating plea or other agreements, federal prosecutors take into account, among other factors, the corporation's timely and voluntary disclosure of wrongdoing and its willingness to cooperate in the investigation of its agents. Prosecutors also consider the availability of alternative or supplemental remedies such as civil or regulatory enforcement action.

To receive cooperation credit, a company must do more than comply with subpoenas or other compulsory process. Companies must provide a full accounting of the known facts about the conduct or events under review, and affirmatively must identify responsible individuals (and provide evidence supporting their culpability), including corporate executives and officers – and they must do so in a timely way.

A company's cooperation may be particularly helpful where the criminal conduct continued over an extended period of time, and the knowledgeable or culpable individuals and/or the relevant documents are dispersed or located abroad.

Under these circumstances, cooperation includes helping to circumvent barriers to the investigation by making knowledgeable personnel available for interviews or testimony, and by producing documents and other evidence that otherwise may not be readily accessible to the government.

We recognize that some foreign data privacy laws may limit or prohibit the disclosure of certain types of data or information. Over the years, the Criminal Division has developed an understanding of certain oft-cited data privacy laws, and we will challenge what we perceive to be unfounded reliance on these laws to justify withholding requested information. Companies should avoid this by giving careful consideration to the government's requests for information, refraining from making broad "knee jerk" claims that large categories of information are protected from disclosure and producing what can be disclosed.

The consequences of refusing to cooperate in an ongoing investigation are evident in department's recent, landmark criminal resolution with BNP Paribas (BNPP) – the fourth largest bank in the world.

Between 2004 and 2012, BNPP knowingly violated the IEEPA and the Trading with the Enemy Act (TWEA) by moving more than $8.8 billion through the U.S. financial system on behalf of Sudanese, Iranian and Cuban entities subject to U.S. economic sanctions. The majority of the transactions facilitated by BNPP were on behalf of entities in Sudan, which is subject to a U.S. embargo due to the Sudanese government's role in facilitating terrorism and committing human rights abuses.

BNPP's criminal conduct took place despite repeated warnings expressed by the bank's own compliance officers and its outside counsel. In response to the concerns identified by compliance personnel, high-ranking BNPP officials explained that the questioned transactions had the "full support" of BNPP management in Paris. In short, BNPP expressly elected to favor profits over compliance.

BNPP refused to cooperate with our investigation. In fact, the bank hindered the investigation by dragging its feet and making exaggerated assertions that certain information was precluded from disclosure by foreign data privacy laws. BNPP's intransigence thwarted the government's ability to prosecute responsible individuals or satellite banks.

Ultimately, BNPP pleaded guilty to conspiracy to violate the IEEPA and the TWEA, and agreed to pay record-setting penalties of over $8.9 billion. And the company admitted its misconduct – including its disregard of compliance advice – in a detailed statement of facts that was made public. BNPP's refusal to cooperate was a key factor in the department's decision to seek a parent-level guilty plea.

Corporate accountability through a strong, tailored compliance program and thorough internal investigations should be the standard for your companies.

I'd like to speak briefly about another significant risk these days that can bring law enforcement to your door: data breaches.

In recent years, there has been a proliferation of significant data breaches – exposing millions of innocent consumers to violations of privacy, identity theft and other harms resulting in hundreds of millions of dollars in losses – both to individuals and to corporate entities. The breaches have been carried out by lone hackers and – increasingly – by transnational organized criminals.

Given the financial, reputational, privacy-related and other harms that a data breach may cause, it is essential that corporations establish and maintain policies and practices designed to prevent and detect data breaches, and to mitigate the attendant damage.

The Criminal Division is not looking to investigate or prosecute victim companies. Rather, we are seeking to partner with the private sector to prevent the breaches in the first place. To make this partnership as effective as possible, we encourage companies to report actual or suspected breaches to law enforcement authorities – even if the intrusion may have been caused by inadequate safeguards – and cooperate in both the investigation and in what we hope will be the eventual prosecution of the hackers and thieves.

To consolidate and focus our expertise and resources, during this past year, the Criminal Division created a Cybersecurity Unit within the Computer Crime and Intellectual Property Section (CCIPS). While the unit in particular and CCIPS as a whole are committed to identifying and prosecuting the hackers that commit the breaches, the unit also is dedicated to partnering with both the private sector and the public to combat cybercrime.

To that end, we have engaged in targeted cybersecurity consultations with members of the private bar, computer security specialists, industry groups and trade associations, financial institutions and others.

And, earlier this month, based on input from both law enforcement authorities with experience investigating and prosecuting cybercrime and from victims, we released guidance reflecting "best practices" for preventing, detecting and responding to data breaches. This guidance, which is available on the Criminal Division's website, is a living document, and we will revise it as necessary to reflect up-to-date vulnerabilities and recommended solutions.

Corporate accountability through compliance, investigations and protections against breaches is a good practice for all of your companies. And in the Criminal Division, I am emphasizing accountability on our side as well, particularly through our work with regulators and other law enforcement agencies, and through increased transparency about our decision-making where possible.

Many of the cases handled by the Criminal Division also involve parallel investigations or civil or enforcement actions by civil or regulatory authorities. Even if certain misconduct could be pursued civilly or through regulatory action, criminal investigation and prosecution often is appropriate.

It is department policy that criminal prosecutors and civil attorneys coordinate with one another and with agency attorneys, to the extent permissible, to protect and advance the government's overall interests. Early and effective coordination is critical to ensuring the efficient use of resources and the best ultimate outcome.

We have heard concerns expressed about regulatory "piling on." We agree that there is the potential for unfairness when a company is asked to pay penalties and fines to different regulators and enforcement authorities based on the same set of facts.

Different law enforcement authorities have distinct and important functions. Companies know who their regulators are, and they know that they are subjecting themselves to those regulatory schemes and the laws of the countries in which they operate. But we are trying to address this concern and are mindful of making sure that companies are not punished unfairly.

Since becoming Assistant Attorney General, one of my priorities has been to ensure that the Criminal Division is as transparent as possible about its decision making. While we are limited in the information we can disclose to the public about matters in which we decline to prosecute, when we file charges, secure a guilty plea or enter into a deferred prosecution or non-prosecution agreement, the Criminal Division will place in the public record detailed information explaining the rationale for the particular resolution whenever possible.

Whether we secure a guilty plea or enter into an NPA or DPA, these resolutions generally have the same key components: admissions, a detailed statement of facts, remediation and/or enhanced compliance requirements and penalties. Depending on the facts and circumstances of a particular case, the Criminal Division also may require the imposition of a compliance monitor.

Companies would be wise to study these publicly-available documents to measure their compliance or to assess their exposure.

In our view, increased transparency benefits everyone. From the Criminal Division's perspective, if companies know the benefits that likely will flow from self-reporting or cooperating with the government's investigation, we are confident that more companies will be willing to voluntarily disclose identified misconduct and cooperate, including against culpable individuals.

In addition, transparency takes a significant amount of the guess work out of assessing the likely benefits of cooperation, as well as the costs of refusing to cooperate or offering limited or partial assistance.

Regardless of the form of resolution, the Criminal Division is committed to enforcing compliance with its terms. In particular, when a company that is subject to the terms of an NPA or a DPA violates the terms of the agreement, if proportional to the breach, the Criminal Division will not hesitate to tear up the agreement and prosecute the offending entity based on the admitted statement of facts.

If we do so, as with the other resolutions, the Criminal Division will be transparent and include its rationale in publicly-filed documents.

In addition to statements contained in public filings in cases investigated or prosecuted by the Criminal Division, our commitment to transparency also is effectuated by the participation of Criminal Division personnel in conferences such as this one.

We are grateful for the opportunity to use this public forum to communicate our priorities and expectations to corporations.

Thank you.

Component:
Criminal Division

Updated May 19, 2015