# Health Care Compliance Communiqué



# FCPA Lessons from 2015

The Foreign Corrupt Practices Act (FCPA) may remain the same year after year but its enforcement shifts over time. Staying abreast with the current winds of change can help companies optimize oversight and upgrades to their anti-corruption compliance programs.

## Two key takeaways from 2015:

- The SEC's role in FCPA enforcement
- Individual accountability

## The SEC Focus on Companies

The Securities and Exchange Commission (SEC) has emerged as the US government's most active enforcement agency in FCPA cases. In his keynote address at the ACI's 32nd FCPA Conference, Andrew Ceresney (SEC Director, Division of Enforcement) highlighted some of the Commission's recent actions. In FY 2015, the SEC filed 14 actions against individuals and organizations for FCPA violations, racking up more than $215 million in financial remedies. It's worth noting the different types of violations that produced those returns. In one finalized case, a global company failed to put controls in place to detect and prevent its subsidiary from making improper payments and gifts to Chinese government officials. In another action, a company sponsored the attendance of foreign government officials at a major sporting event. A third case cited by Ceresney involved a company that made improper payments to a company serving as a front to a foreign ruling political party in order to secure lucrative contracts. Finally, a fourth case centered on improper cash payments and other benefits provided by a company's overseas joint venture partner.

Ceresney expects 2016 to be equally or even more active for SEC's FCPA cases. Unlike the trend of the US Department of Justice's growing interest in prosecuting individuals for FCPA violations, the SEC has focused heavily on corporate enforcement. It would be a mistake to assume that either agency has exclusive interest in one type of enforcement action vs. the other, but the SEC has become an anti-corruption enforcement agency with both clout and determination.

A significant aspect of SEC's enforcement strategy has been its emphasis on corporate self-reporting and cooperation. Ceresney noted, "Companies should understand that the benefits of cooperating with the SEC are significant and tangible." Self-reporting is a notable element in receiving those benefits. "Benefits range from reduced charges and penalties to deferred prosecution or non-prosecution agreements ... in instances of outstanding cooperation, or in certain instances when the violations are minimal, no charges."

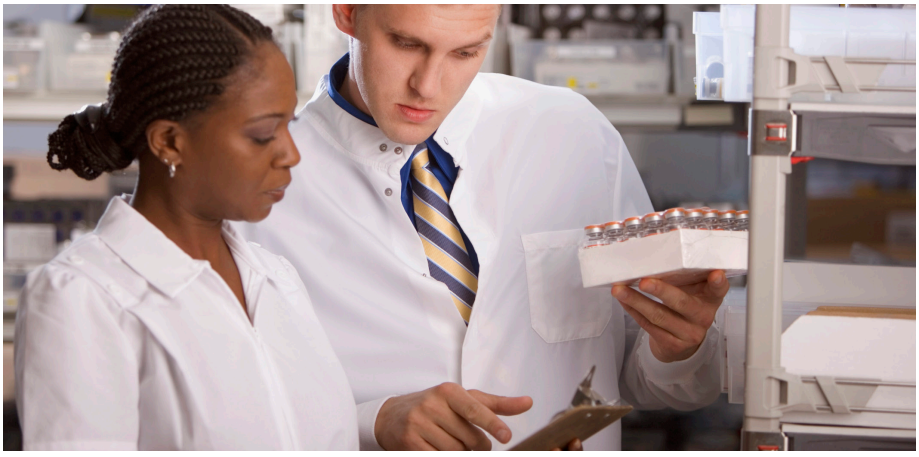
Ceresney dubbed those benefits "the carrot" before moving on to "the stick." "Companies that make a decision not to self-report misconduct take the chance that the Enforcement Division will learn of this misconduct through other means. The SEC's whistleblower program has created real incentives for people to report wrongdoing to us," he said.

Whistleblowers are an essential source of information in the investigation of FCPA and other anti-corruption violations. In our experience, companies that treat whistleblowers as a danger rather than a source of knowledge are missing important opportunities to resolve potential issues before they become ongoing patterns of misconduct, violations and legal liability. As enforcement agencies including the SEC ramp up their incentives for whistleblowers to report actual or suspected misconduct, companies should be equally attentive to upgrading and reinforcing their own training and communication programs to employees and third parties. Instruction should focus not only on "what not to do" but on the responsibility of each individual to report potential problems – and the commitment of the company to follow up on those reports quickly and thoroughly.

## Individual Accountability

The now-familiar "Yates memo" issued by US Deputy Attorney General Sally Yates in 2015 established a policy for DOJ of holding individual corporate officers accountable for corporate misconduct. The risk, however, is not only for the individual. According to its 2015 Year-End FCPA Update, law firm Gibson Dunn reports that "... individuals make up 80% of DOJ's FCPA enforcement docket in 2015, but in no case this year did DOJ bring an enforcement action against a corporation without also prosecuting officers associated with that corporation."


Individuals make up 80% of DOJ's FCPA enforcement docket in 2015



While much attention has been paid to the memo's direction to focus on individual accountability, it is important to recognize the way in which it also emphasized the interrelationship between corporate and individual enforcement actions. Criminal and civil DOJ investigators are directed to focus on individuals from the very beginning of their investigations and to be in regular contact with one another. The DOJ policy also emphasized that corporate settlements cannot release individuals from civil or criminal liability.

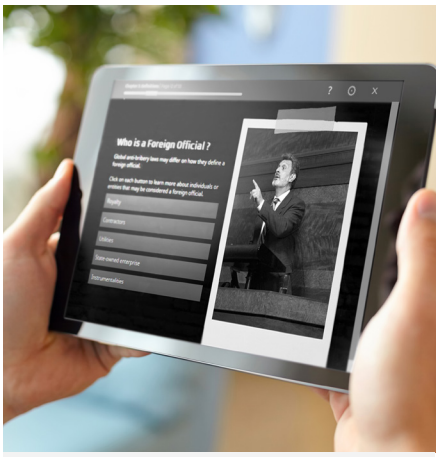
## Moving Forward

Beyond the clarified enforcement strategies of US federal agencies, state anti-corruption units and international enforcement agencies are actively enforcing a new generation of anti-corruption and anti-bribery regulations and laws.

Global companies and their executives are increasingly vulnerable, not only because of multiple overlapping laws and increased enforcement but also because of the risks posed by their third party partners and organizational siblings. Especially notable is the growing risk to companies from the escalating practice of outsourcing business functions including routine data processing and payroll management. Our experience with companies successful in navigating this potential minefield of risks illustrates specific characteristics:

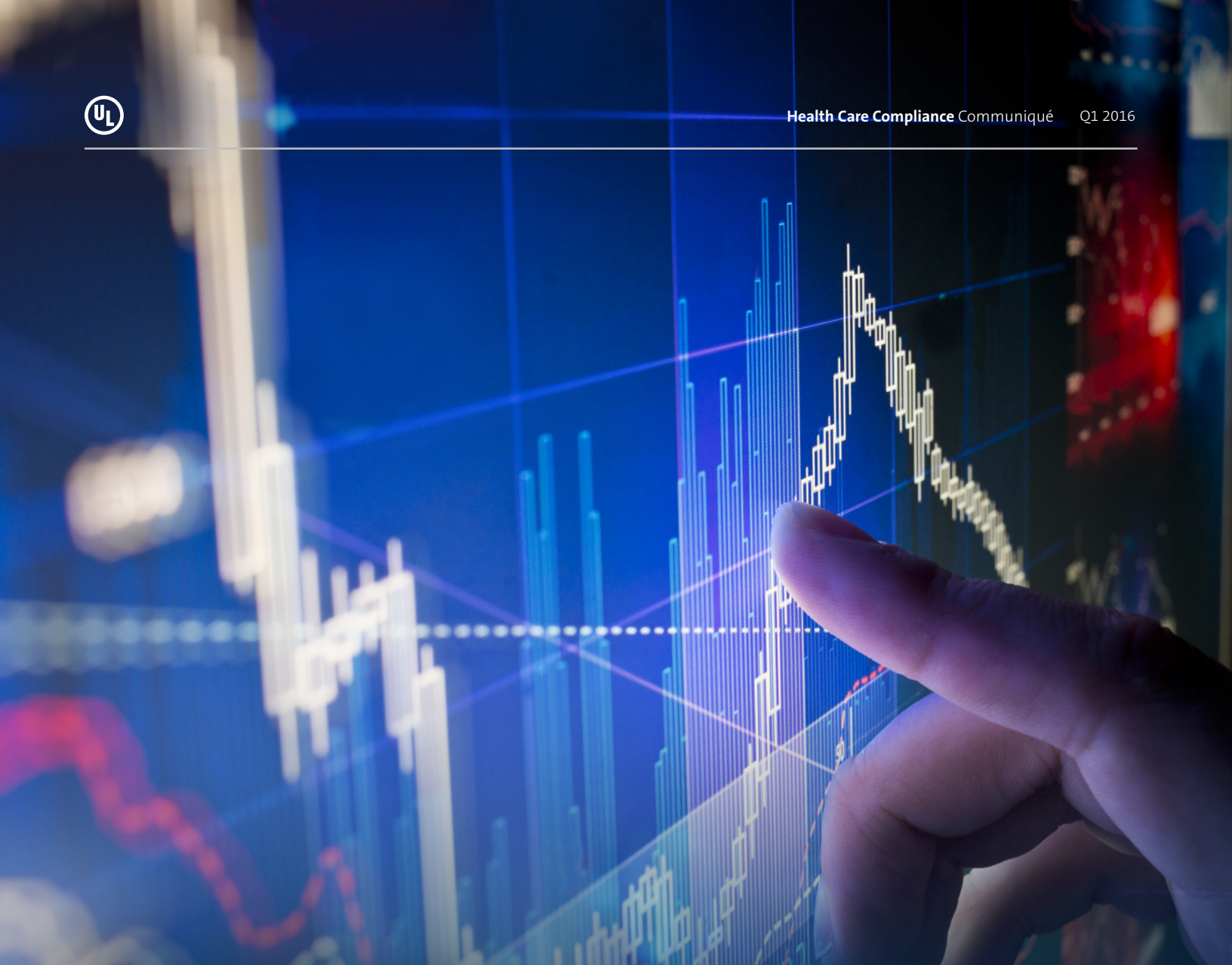
- Consistent, thorough oversight of third parties to include regular audits;
- Integration of corporate business functions and managers in the "compliance" function of the company;
- Empowerment of employees to report suspected misconduct before it becomes a long-term, entrenched problem of corruption;
- Regular assessments of risk areas to reflect potential vulnerabilities stemming from new corporate structures, mergers and acquisitions, emerging international law and adjusted policy perspectives of enforcement agencies;
- Continually updated training that addresses the learning needs of new hires, established employees, outsourced partner organizations and fluctuating workforces. As new generations of employees enter the workforce, learning and communication must be adapted to engage and educate them.

Regulatory compliance has never been more complex or important, both from a legal and financial perspective. While few companies have the luxury or need to scrap existing compliance programs, virtually all companies can benefit from regular reviews and adjustments of their compliance resources, their policies and their procedures.




## UL's Global Anti-Bribery Course Now Mobile – Ready

UL's Global Anti-Bribery course was upgraded to our mobile-friendly EduFlex format in 2015. This course is available in 11 languages, so that global compliance teams can ensure a consistent training program that spans multiple regions. To review the course for 30 days, contact Pat Thunell at pat.thunell@ul.com.



# Life Sciences, Data Theft and HIPAA

Massive data breaches occur all too frequently and are likely to become an even more familiar headline in the news. Data breaches are not some distant threat for consumers, millions of whom have been warned that their private information has been exposed. Nor are they minor threats to companies hit by regulatory violations, civil litigation and loss of consumer confidence.

Until recently, the retail and health insurance industries received the lion's share of attention for data breaches that affected millions of personal records including individuals' names, birthdates, Social Security numbers and other personal information. For healthcare companies, the risk of lost or stolen data was particularly worrisome; not only did it threaten the company's reputation and consumer trust but also violated HIPAA protections of personal health information (PHI). Now, there is growing evidence that pharmaceutical and medical device companies have become targets for data loss and theft. The risks to these life science companies goes beyond HIPAA violations and reputational damage. It also carries the risk of losing intellectual property and trade secrets, compromising clinical trial data and slowing the process of drug development and approval.

In 2015, cybersecurity companies and even representatives of government agencies including the US Department of Homeland Security warned life science companies about growing threats of cyber attacks on their organizations and their third-party partners, putting them at heightened risk of data breaches. In late 2015, the Office of Inspector General issued its 2016 Work Plan which called for increased scrutiny of "networked medical devices" and HIPAA compliance.

Both pharmaceutical and medical device companies are equally vulnerable through their escalating reliance on outsourcing business functions, with the corresponding transfer of protected or sensitive data across organizations. While life science companies share the risks of data loss with other industries, the treasure trove of proprietary intellectual property and PHIs makes them especially tasty targets for data thieves. Of particular concern is the potential for loss or compromise of data relating to clinical trials and drug approvals.

The cybersecurity risk requires technology capable of providing a deep and real-time look into networked activities as well as the human resources to identify, resolve and report risks and breaches. Life science companies have lagged behind organizations in other industries in implementing comprehensive cybersecurity risk management programs. As they adjust to the growing risks aimed at their industry, there may be a temptation to overlook the most common risk of data loss: individuals inside the company or one of its third parties.

Surveys continue to show the growth in risk to pharmaceutical and medical device companies from both external and internal sources. The Cisco 2015 Annual Security Report reported that the pharmaceutical and chemical industries were at high risk from non-targeted attacks such as adware and scams, often stemming from employee online activities. In too many cases, these risks are the cause of employees' internet use. In mid-2015, a small pharmaceutical industry sent required notification of a data breach resulting from four company e-mail accounts uncovered when some employees had trouble accessing their company email accounts. The company's investigation acknowledged the possibility of a potential breach that exposed information from emails or attachments including names and Social Security numbers of individuals associated with the email accounts as well as other personal information in the company's human resources or payroll-related records.

In light of the growing risk, life science companies should reassess their cybersecurity systems and, if necessary, increase their monitoring of third parties for security and compliance, and intensify their employee training on protection of corporate resources and online communications. The risk is real, and growing. Thorough, properly resourced attention is required by any life science company seeking to avoid headlines as the "next Target" breach.


UL provides a targeted eLearning course focused on HIPAA and Privacy Guidelines training for sales professionals. This 40-minute course explains the basic provisions of the HIPAA Privacy Rule, and helps sales professionals understand how HIPAA affects detailing and customer support activities.

The course also explains HIPAA issues around products using real-world scenarios. For example, some physician's offices, clinics, and hospitals may have policies that restrict access to sample rooms and other areas. The healthcare provider may be concerned that a salesperson can overhear discussions about patients or see a patient's medical record if the salesperson is allowed into these storage areas. The salesperson should explain to the customer that the company shares their privacy concerns. However, the course also notes that the HIPAA Privacy Rule itself does not prohibit a salesperson from directly accessing sample storage areas.

To view the HIPAA Privacy course for 30 days, contact Pat Thunell at pat.thunell@ul.com.

# DOJ Expands FCPA Resources

In two separate but related moves, the US Department of Justice has expanded its resources devoted to enforcement of the FCPA – and, in the process, put to rest many of its critics' comments that the Department was backing away from FCPA.

In November, Hui Chen joined the Department's Fraud Section as a full-time compliance expert. Chen will provide guidance concerning issues including the existence and effectiveness of the compliance program a company had in place and whether any meaningful remedial action had been taken toward conduct that triggered potential criminal charges.

Shortly after announcing Chen's appointment, Assistant Attorney General Leslie R. Caldwell highlighted additional resources for the Department. In remarks at the ACI's International Conference on the FCPA, AG Caldwell noted the addition of three new fully operational squads to the FBI's International Corruption Unit that focuses on FCPA and kleptocracy matters. In addition, he announced plans to add 10 new prosecutors to the Fraud Section's FCPA Unit, saying "These new squads and prosecutors will make a substantial difference to our ability to bring high-impact cases and greatly enhance the department's ability to root out significant economic corruption."

The expansion of FCPA resources at the Department signals a renewed vigor for DOJ's anti-corruption activities, specifically its enforcement of the FCPA. That vigor joins the SEC's robust commitment to FCPA enforcement and the emergence of multiple international anti-corruption laws to signal an increasingly robust move forward for anti-corruption and anti-bribery enforcement.

## About UL EduNeering

UL EduNeering is a division within the UL Ventures business unit. UL is a premier global independent safety science company that has championed progress for 120 years. Its more than 10,000 professionals are guided by the UL mission to promote safe working and living environments for all people.

UL EduNeering develops technology-driven solutions to help organizations mitigate risks, improve business performance and establish qualification and training programs through a proprietary, cloud-based platform, ComplianceWire®. In addition, UL offers a talent management suite that provides companies the ability to improve workforce skills & competencies within established role-based talent training programs to drive business performance.

For more than 30 years, UL has served corporate and government customers in the Life Science, Health Care, Energy and Industrial sectors. Our global quality and compliance management approach integrates ComplianceWire, training content and advisory services, enabling clients to align learning strategies with their quality and compliance objectives.

Since 1999, under a unique partnership with the FDA's Office of Regulatory Affairs (ORA), UL has provided the online training, documentation tracking and 21 CFR Part 11-validated platform for ORA-U, the FDA's virtual university. Additionally, maintains exclusive partnerships with leading regulatory and industry trade organizations, including AdvaMed and the Duke Clinical Research Institute.

NLTR/15/120815/HC