

Inside

A publication of the Corporate Counsel Section
of the New York State Bar Association

Message from the Chair

Thank you for reading this Fall edition of the Corporate Counsel Section's newsletter, *Inside*. I hope you enjoyed the summer! The Corporate Counsel Section has certainly been busy. Thanks to the wonderful work of our editors, Jessica Thaler and Elizabeth Shampnoi, you are about to embark into an issue of *Inside* all about compliance as it pertains to corporate counsel.

We met many wonderful people at the Member Appreciation Event on the rooftop of the Kimberly Hotel this past June 16th. This yearly reception serves as a "thank you" for members of our Section. This year we also invited all those who contribute to the Section in meaningful ways, including speakers for CLEs, event sponsors and authors of articles for issues of *Inside*. This event is always a wonderful way to network in a relaxed and beautiful setting. We encourage all to attend next year.

In August, the Section hosted a reception in honor of the alumni of the Kenneth G. Standard Diversity Internship Program at Pryor Cashman LLP. Since 2006, there have been 54 interns in the program and with each year that number and the internship program continues to grow. This year we honored nine interns and their host companies, including Pitney Bowes, Pepsi Co., Salesforce, Ace Group, NYSTEC, AllianceBernstein and the Visiting Nurse Service of New York, to name a few. With over 80 people in attendance, including current, past and future leaders of the New York State Bar Association, this event serves to demonstrate the importance



Inside

Inside <i>Inside</i>	3
(Jessica Thaler and Elizabeth Shampnoi)	
5 Ways to Improve Regulatory Compliance at Universities	4
(Dennis M. Cariello)	
The Three "Ds" of a Top-Marks Antitrust Compliance Program: Design, Deter, Detect	6
(Stacey Anne Mahoney)	
Inside Interview: Jana Springer Behe, Esq.	9
(Amir Alimehri)	
Is Your Data Your Greatest Liability or Asset?	10
(Christopher O'Brien)	
Meeting Your Cybersecurity Obligations	12
(Steve Rubin and A. Jonathan Trafimow)	
E-Contracting: What Corporate Counsel Need to Know	15
(Matthew D. Sobolewski and Chester R. Ostrowski)	
Compliance With EU Data Protection Regulation	17
(Laura Liguori and Federica De Santis)	
Parallel Lives: How Brazil and the United States Consider Leniency Agreements and Compliance Programs	20
(Adria Perez)	

Beyond Compliance: Inside Counsel Should Drive Sustainable Business	24
(John Wood)	
Getting Issuers to Market: An Update	26
(Carol Spawn Desmond)	
Paradigm Shift? The SEC Intensifies Its Focus on Prevention of Retaliation Against Whistleblowers	28
(Gail Gottehrer)	
ERISA: An Overview	30
(Lilah Loughran)	
Changing Rules: The National Labor Relations Board Speaks	33
(Nancy B. Schess and Jesse Grasty)	
Inside Books: <i>Finding Bliss</i>	37
(Reviewed by Janice Handler)	
Structuring for Success: Effective Compliance and Ethics Program Organization	39
(Rebecca Walker and Jeffrey M. Kaplan)	

of diversity and the future of our young lawyers to this Section as well as to NYSBA.

Since the publication of our Spring newsletter, the Corporate Counsel Section was busy organizing the 2015 Corporate Counsel Institute. The Corporate Counsel Institute is a two-day CLE event organized every odd year and a great way to obtain updates regarding current legal trends, to network with your peers and to fulfill your CLE requirements. The topics for this year's Institute included employment law, arbitration, human trafficking, privacy and cyber-security, not-for-profit law, intellectual property valuation and ethics with a keynote address from Benjamin Lawsky, New York State's first Superintendent of Financial Services.

We encourage you to continue to look out for Corporate Counsel Section events. We are working on events including a collaboration with the Young Lawyers Section

where we will explore the many stories of in-house counsel and their individual paths to their current positions. We anticipate that, through events like these, young lawyers can obtain tips and "inside" information on how they can steer their career to find the position they are looking for as in-house counsel.

We are always looking for new initiatives and ideas that you, the member, will benefit from. Please do not hesitate to contact me about any ideas you may have for the Section. Lastly, if you want to contribute to *Inside* with an article or book review, contact the editors. We are always looking for content.

Until then, we hope you enjoy reading this edition of *Inside* as much as we have enjoyed preparing it.

Natalie Sulimani

NEW YORK STATE BAR ASSOCIATION



January 25th–30th, 2016
New York Hilton Midtown, NYC

ANNUAL MEETING 2016

**CORPORATE COUNSEL SECTION/BUSINESS LAW SECTION
JOINT PROGRAM**

Wednesday, January 27, 2016



Inside Inside

With an ever-changing regulatory environment and more and more laws being created to protect the public, the consumer and the marketplace, the field of compliance has grown and now touches on many different aspects of business. Most of us think of the financial industry when we think “compliance” and, although that industry is compliance-heavy, regulation and law requires companies to monitor their compliance in other areas too—education, employment, data protection and otherwise. We have worked to find a group of practitioners who, through their articles in this issue of *Inside*, speak to an array of compliance matters in connection with requirements under ERISA, the securities laws, NLRB policies, cross-border issues, antitrust, cybersecurity and technology.

We have also included a book review of *Finding Bliss*, a book on lawyers finding happiness in their careers, and an interview with Jana Springer Behe, Director of Contracts and General Counsel of the New York State Technology Enterprise Corp., of one of our fellow Executive Committee members and her career path.

In addition to our authors, we wanted to especially thank Jaclyn Schess, a undergraduate student entering her second year at Yale, who interned with the Dispute Advisory & Forensic Services Division within Stout Risius Ross, Inc. this past summer and helped to coordinate with our contributors, as well as Upnit Bhatti, who graduated from Syracuse Law School May 2015 and joined the Syracuse office of Bond, Schoeneck and King in September 2015, who assisted in the editing process.

We hope that you will find value in this issue of *Inside* as it relates to your regulatory compliance framework. As always, we are looking for authors and articles for topics of interest to in-house practitioners. If you or your colleagues are willing to write, please contact us and we can talk through the topic ideas and process. We look forward to hearing from you!

Jessica Thaler and Elizabeth Shampnoi

Jessica Thaler is an attorney with Bliss Lawyers, currently working on secumdent for Credit Suisse. Prior to engaging with Bliss, she spent a year acting as the Chief Legal Officer of My Sisters’ Place, a not-for-profit organization working for the benefit of domestic violence and human trafficking victims throughout Westchester County. Jessica has a rich experience as a corporate-transactional generalist, gained through her work at NYC law firms and her solo practice. She is an active member of NYSBA, acting as immediate past chair of the Committee on Lawyers in Transition, on the executive committees for the EASL and Corporate Counsel Sections, as a long-standing member of the Membership Committee and the Committee on Law Practice Management and, now, as a co-editor of *Inside*. Jessica is also a House of Delegates representative for the Westchester County Bar Association.

Elizabeth J. Shampnoi is an Attorney and Director in the Dispute Advisory & Forensic Services Group of Stout Risius Ross, Inc. (“SRR”). She regularly provides litigators, in-house counsel and senior executives with a broad range of business and legal advice concerning cost-effective and timely alternative dispute resolution. Many times this involves identifying which cases are appropriate for mediation or arbitration, proper forum selection, drafting clauses pre-dispute and post-dispute, selecting the arbitrator or mediator, rule interpretation/enforcement and best practices in advocacy. Additionally, Ms. Shampnoi advises counsel in the selection of experts and consultants for a variety of matters, including, but not limited to, commercial disputes, investigations and valuation. Prior to joining SRR, Ms. Shampnoi was a Litigation Associate at the law firm of Storch, Amini & Munves, PC and District Vice President of the American Arbitration Association. Ms. Shampnoi is an active member of NYSBA and serves on the executive committees for the Dispute Resolution and Corporate Counsel Sections.

5 Ways to Improve Regulatory Compliance at Universities

By Dennis M. Cariello

With thousands of new rules published since 2009, maintaining regulatory compliance has become one of the most difficult jobs for in-house counsel. While this is an issue that cuts across every industry, higher education has been uniquely hit with new regulatory requirements in the past six years. The impact of these regulations is staggering—the Senate Committee on Health Education Labor and Pensions Task Force on Federal Regulation of Higher Education (the “Task Force”) found that Vanderbilt University spent \$150 million—or roughly 11% of the school’s 2013 expenditures—on compliance with federal regulations.¹ The Task Force report also noted that the American Action Forum (the “Forum”) found that “the number of individuals in higher education with the title of ‘compliance officer’ has grown by 33 percent in the past decade.”² Further, “using publicly available data, the Forum also determined that institutions spend 26.1 million hours annually completing [U.S.] Department of Education-mandated forms.”³

Of course, the consequences of noncompliance are becoming equally staggering. For example, on August 3, 2015, Wheeling Jesuit University agreed to pay \$2,300,000 to settle claims that it misused grant funding awarded by the National Aeronautics and Space Administration, the United States Department of Labor, and the National Science Foundation.⁴ The U.S. Department of Education (“Department”) imposed two severe penalties on Corinthian Colleges, Inc. (“Corinthian”), a publicly traded chain of career schools in the last year. In June 2014, in response to Corinthian’s perceived failure to provide information responsive to two document requests, the Department imposed a 21-day delay on the receipt of Title IV funding (federally issued loans and grants provided to pay the tuition of students). This dramatic penalty caused the closure and forced sale of the school. Then, in April 2015, after the sale of Everest Colleges, the principal school system run by Corinthian, the Department imposed a nearly \$30 million fine over alleged misrepresentations regarding the job placement rates of Heald College, another institution run by Corinthian. On a less dramatic scale—but equally concerning—is the Department’s trend in fining colleges for failing to capture every crime required to be included in the Annual Campus Security Report, mandated by the Jeanne Clery Disclosure of Campus Security Policy and Campus Crime Statistics Act (20 U.S.C. §§ 1092(f), *et seq.*). A number of nonprofit institutions face paying a fine of \$35,000 per crime that was not reported.

Given the consequences for violating regulatory standards governing higher education, it is no surprise that universities have been focusing even greater amounts of time and effort on compliance. There are, however, five things a university (or any enterprise) can do to better ensure a compliant operation.

Know the Requirements and Key Dates

As surprising as it seems, knowing the regulatory requirements can be quite a challenge. With so many regulations and regulators overseeing higher education, universities are forced to keep track of regulatory requirements related to core business issues like education and accreditation requirements, to grants management, immigration, employment, data privacy, marketing, real estate, finance and import export—just to name a few. Moreover, many regulatory agencies, like the U.S. Department of Education, post guidance documents on a daily basis. While this guidance is helpful, a university general counsel or compliance office can easily get overwhelmed by the magnitude of it all.

It is critical that counsel get a handle on the laws and regulations that govern the university’s activities. Having a checklist of relevant standards and requirements imposed on the university will be a great tool. In addition, a calendar with dates for required submissions is a must. There are just too many things to keep track of and failure to comply can easily lead to fines and other significant actions taken by regulators.

Put Someone in Charge of Compliance

Once you have a handle on what is required, universities will quickly see the value in having someone in charge of overseeing compliance. Of course, while a compliance officer is preferred, having someone responsible for compliance does not require hiring new full time employees. However, it does require assigning responsible parties for each of the compliance items on the list counsel created and then assigning a party to confirm that compliance has been achieved.

Communicate

Most compliance failures result from poor implementation rather than poor policies. As a result, communication is key to compliance success. There are three key forms of communication that are critical to meeting regulatory demands: training, operational communication and communication throughout the university.

The need for effective training seems obvious. Administration and staff need to know what is required of them and what to watch out for as compliance issues. Given how accepted the need for training is, it is still surprising that lack of training is often the root cause of compliance failures. Sometimes this is the result of ineffective training—how many times have we all clicked through some computer-based training on this or that topic only to fumble our way to a perfect score and a certificate of completion? Good training must have the necessary information but must also engage. Training people in a live format and in multiple sessions—whether done by the university or at a conference—is likely to yield the best results. While such training

methods use more resources than other training methods, the savings that results for a compliant operation are likely to offset the cost.

Once trained, the university should establish the proper communication system so everyone obtains the information required to do his or her compliance job. This often entails communication across the various offices in a university. The academic department needs to talk with the financial aid department and the financial aid department needs to talk with the bursar. There are many examples where a communication breakdown between the academic or registrar functions, which would keep track of whether a student withdraws from college; the financial aid office, which calculates whether any unused aid funds needs to be returned to the U. S. Department of Education, and the bursar's office, which cuts the check to the Department of Education, have led to multi-million dollar liabilities for failing to return money to the federal government. Moreover, the failure of "campus security authorities" (a defined term that includes campus police and other individuals with responsibilities for students and student activities) to tell the campus security office—which typically keeps track of all crimes on campus—about a reportable crime will result in a annual security report that misses information and is noncompliant.

Lastly, all those with compliance responsibilities should meet periodically to ensure everyone has a handle on his or her obligation. A mandatory monthly or quarterly compliance meeting will provide a forum to identify and respond to compliance issues. Further, the institution will be better able to deploy resources to fix a problem. If an institution has cohort default rate above 20%, it makes sense to watch that metric carefully—considering continued eligibility for federal loans and grants is conditioned on having a cohort default rate below 30%—and deploy resources to ensure students are not defaulting on their loans. In addition, various campus stakeholders should also attend to increase sensitivity to compliance matters, and for compliance personnel to hear what is going on throughout the campus. For example, when a university is taking on programs at a new degree level, there are a host of regulatory notifications and approvals required. Failure to get those approvals will turn an exciting—and permissible—institutional choice into a compliance headache.

Install Redundant Systems

Another problem that impedes even a well-trained organization is that we are all human. Whether it is a case of people just making honest mistakes or letting things slip due to understaffing (by design or due to absences), human error contributes greatly to compliance failures. As a result, creating redundancies in your processes can help reduce such problems. Something as simple as an email alert to various relevant stakeholders (inside and outside the relevant office) reminding all concerned that an action is pending or required can do wonders to reduce such failures.

Have Relationships With Your Regulators

Lastly, you need to have a relationship with your regulators. Most organizations—and universities are no exception—are content to remain hidden from their regulators unless they have to engage. "Out-of-sight, out-of-mind," however, is not a smart compliance strategy. For one thing, regulators always catch up with you; the Department of Education, for example, has random program reviews of every university. While it may take a while to get to you, the regulator will come to visit. Worse, for all the time you have spent hiding, you have missed the opportunity to create a positive impression with the regulator and to gain the benefits that come from such a relationship. These benefits can take the form of additional guidance to taking a role in creating new policy. As one government lawyer told me, "I've known these guys for a long time. I really don't like them, but I've never known them to lie to me." That type of benefit of the doubt only comes with a track record formed by interaction over time.

Conclusion

Having compliant policies is a great start, but it is simply not enough to ensure regulatory compliance. Knowing and calendaring your regulatory requirements and putting someone in charge of meeting the requirements is a great start. But you need to communicate throughout your organization about the requirements—including with your regulators—if you want to stay out of regulatory trouble consistently. Lastly, by installing redundant policies and procedures, you can take care of the errors that come with absent employees or mistakes. Compliance personnel are still just people—but by following these tips, your university is sure to help them excel.

Endnotes

1. See Task Force on Federal Regulation of Higher Education, *Recalibrating Regulation of Colleges and Universities*, at 11 (Feb. 12, 2015), located at http://www.help.senate.gov/imo/media/Regulations_Task_Force_Report_2015_FINAL.pdf (last visited on August 3, 2015).
2. *Id.*
3. *Id.*
4. See Department of Justice Press Release, "Federal grant fraud claims settled with Wheeling Jesuit University," located at <http://www.justice.gov/usao-ndwv/pr/federal-grant-fraud-claims-settled-wheeling-jesuit-university> (last visited Aug. 4, 2015).

Dennis Cariello is a Shareholder at Hogan Marren Babbo & Rose, Ltd. and the co-chairman of the firm's education practice. With more than 15 years of experience, and having served at the U. S. Department of Education as Deputy General Counsel for Postsecondary Education and Regulatory Services and Deputy Assistant Secretary for Enforcement in the Office for Civil Rights, Mr. Cariello has a diverse national law practice that allows him to provide a wide range of services on Education Law and Policy, Corporate Transactions, Government & Regulatory Affairs, Title IX & Civil Rights, Privacy Law and Litigation.

The Three “Ds” of a Top-Marks Antitrust Compliance Program: Design, Deter, Detect

By Stacey Anne Mahoney

Introduction

After decades of disregarding antitrust compliance programs, the United States Department of Justice (“DOJ”) has finally come around to providing some degree of credit to a target of a DOJ investigation for having an antitrust compliance program. This long-awaited recognition gives companies an additional tool in their toolbox to mitigate the exposure resulting from a finding of an antitrust violation as such a finding is expensive in numerous different ways, including (1) the costs involved in responding to and defending against the investigation and potential governmental and civil follow-on damages litigation, (2) the payment of any fines, restitution or damages resulting from the violation, (3) the negative reputational impact to the company that finds itself publicly branded as an antitrust violator, and (4) the loss of senior executives to jail time or through requirements that the company cease professional relations with all individuals who participated in the challenged conduct. Given these significant expenses, and the comparatively small expense of implementing a credible and effective antitrust compliance program, simple math will suggest that an antitrust compliance program is a worthwhile investment.

Antitrust Compliance Programs Were Previously Deemed Worthless

Historically, the Antitrust Division of the DOJ was one of, if not the only, DOJ Division to disregard the value of an existing corporate compliance program in the event that a company was found guilty of violating the antitrust laws.¹ The rationale could be summed up as follows: If the company committed an antitrust violation, any pre-existing antitrust compliance policy was not worth the paper it was printed on since it did not work (the Division’s sentiment, not mine). The Antitrust Division believed that the compliance policy was its own reward; if it worked optimally, it prevented antitrust violations from occurring in the first place, and if the policy was less than optimally functional, but still worked somewhat, it would enable a company to detect an antitrust violation and self-report that violation to the government. Certain representatives of the corporate compliance community argued in response that the Antitrust Division’s position discouraged companies from investing in meaningful and effective antitrust compliance efforts because, regardless of how well designed and implemented a compliance policy was, it could not prevent furtive and violative behavior by a rogue employee who was determined to engage in criminal conduct.

After years of disregarding these counter-arguments, the Antitrust Division recently seems to have conceded the soundness of their logic

What Changed?

In 2013, William J. Baer, an appointee of President Barack Obama, was sworn in as the Assistant Attorney General in charge of the Antitrust Division. Baer is a seasoned antitrust practitioner who, having spent much of his career in private practice, brought to his post a well-informed pragmatism about productive and unproductive enforcement efforts. He also brought to the Antitrust Division Brent Snyder, who became the Deputy Assistant Attorney General in late 2013. Antitrust Division policy regarding compliance programs historically was communicated to the bar through carefully crafted speeches made by senior Division personnel. This trend continued when, in 2014, Snyder addressed the International Chamber of Commerce (“ICC”) in a speech entitled “Compliance Is a Culture, Not Just a Policy.” That speech conveyed a tempered, but notable, trend-reversal regarding the Antitrust Division’s treatment of corporate compliance programs: “[W]e are actively considering ways in which we can credit companies that proactively adopt or strengthen compliance programs after coming under investigation.”² This new position brought the Antitrust Division into line with the United States Sentencing Guidelines, which provide that a Court can reduce the fine imposed on a company if that company had an effective compliance program in place when the offending conduct occurred.³ This shift in Antitrust Division policy underscores the value for corporate America of prophylactic antitrust compliance programs.

What Should a Compliance Program Look Like?

Although the Antitrust Division takes the position that there is no “one size fits all” antitrust compliance program, there are certain things that should be included in all of them: (1) regular training,⁴ (2) on-going compliance monitoring by someone whose job description (and her evaluation) makes her responsible for that monitoring, and (3) a defined reporting mechanism through which issues and concerns can be raised by employees.

Best practices in the creation (or modification) and implementation of an antitrust compliance program can be driven by the three “Ds” that inspired the title of this article—Design, Deter, and Detect. If you keep these highly interrelated principles top-of-mind when considering your company’s program, you will be maximizing

the likelihood that your program will be efficient and effective.

Design

Your company's antitrust compliance program should be designed with the company, the industry and the specific applicable risk factors in mind; a generic out-of-the-box compliance program is not likely to be effective. You will want to conduct a realistic assessment of the particular risk areas for your company. That may be done by product, by job description, by geographic area, or with other characteristics in mind. In particular, you will want to assess who within the company has the greatest regular access to communications directly with competitors; these communications can occur, for example, at trade association meetings or even while passing competitors in the lobby of customers the companies regularly compete for. Frequently, companies are primarily (and properly) concerned with members of their sales forces, who have access to pricing and cost data, as well as future-looking business plans, and may be most likely to cross paths with their counterparts from competitors. Companies should also carefully consider the roles that their marketing and finance personnel play in creating external communications, i.e., shareholder conference calls in which statements can be made that could be perceived to be illegally signaling competing firms.

Crucially, effective compliance programs will also consider the impact of internal policies on personnel. For example, if sales targets substantially exceed reasonable expectations, it can be anticipated that personnel tasked to reach legally unobtainable goals might push the envelope in an effort to keep their jobs. Accordingly, compliance programs must be developed with the entire company in mind, as well as its specific constituents, in order to manage the particular risks attendant to that entity and its industry.⁵

The design of your compliance program must facilitate its universal and vigorous enforcement. Anything less will be a waste of time, effort and energy; not only will it not work to deter or detect any violations, but if a violation is uncovered, the Antitrust Division may infer an attitude of corporate non-compliance that could place the company in an even worse position than if it had had no compliance program at all. Participation and enforcement must be company-wide; senior executives must be required to attend the training, and optimally, will be voluble in their endorsement of the policy, including the training.⁶ In order to enable enforcement, the reporting structure of the compliance executive should be designed so that he or she has direct, unencumbered access to the Board of Directors (the "Board"), or if there is no Board, to the highest levels of company management.

Deter

Of course, one of the primary goals of an effective antitrust compliance program is to deter company personnel from engaging in conduct that violates the antitrust laws.⁷ That is easy to say, but can be harder to execute as a practical matter. For a business person, obtaining greater market penetration and/or increasing his or her company's profitability are laudable goals, and can be ones on which performance is evaluated and remuneration is based. And although business people can be clearly instructed not to talk about prices or allocate customers with competitors, a truly useful training module will provide them with hypothetical situations catered to the most likely types of potentially problematic situations they will find themselves in, and give them general and specific advice regarding how to respond appropriately. For example, if a competitor during a trade association meeting suggests that the attendees should boycott a customer that is driving a particularly hard bargain, the training could provide alternative responses to a suggestion made (1) one-on-one (a clear verbal rejection of the proposal by the recipient), or (2) on the floor of an association meeting (walking out of the room). Providing this type of concrete guidance will enable company personnel to react quickly, without having to conduct a possibly time-consuming weighing of the pros and cons of various responses and missing an opportunity to respond appropriately.

In addition, a program provides an effective deterrent when enforcement action is undertaken publicly within the company (names may or may not be omitted but the violative conduct should be explained) so that it puts other people on notice that the company takes its compliance obligations seriously. Since the DOJ will be publicizing information about the violation, a company would be wise to avail itself of such a teaching moment; minimizing the event will only create the impression among the other employees that this kind of conduct will be swept under the corporate rug. It is worth emphasizing that, in order for a policy to provide meaningful deterrence, it has to be applied evenly by the company across-the-board; neither the senior-most nor the junior-most people should be treated differently from one another. Engaging in disparate treatment of employees will not deter problematic conduct, and will likely invite the special ire of the DOJ.

Detect

It is important to have an action plan in place *before* a violation is detected. In the United States, a company may be able to obtain immunity from criminal prosecution of an antitrust violation, as well as contain civil damages, if it is the first to alert the Department of Justice of the illegal conduct. Accordingly, time is of the essence when a company believes it may have detected a violation.

The plan should clearly identify the various stakeholders within the company who must be consulted

immediately in order to make the initial determination regarding whether to alert antitrust authorities. In developing this list, companies should keep in mind that problematic conduct can have an international impact, so highly inter-related decisions may need to be made in very short time frames regarding possible notifications to numerous antitrust regulators around the world. In addition, while it is often the case that the front-line sales people are the primary personnel engaged in the conspiratorial communications, it is also often the case that the communications were made at the direction of, or with the knowledge of, very senior executives within an organization. Thus, care must be taken when developing the action plan that there are appropriate checks and balances in place to ensure that the plan will be executed, regardless of who within the company might be implicated by the resulting antitrust investigation.

Conclusion

It is no longer a reasonable conclusion for companies in America to decide to roll the dice on whether an antitrust compliance program is a worthwhile investment. With credit now being given by the DOJ for the existence of these programs, even when there has been a violation of the antitrust laws, it behooves all companies to engage in this self-help before disaster strikes. The savvy compliance executive will be able to use this shift at the Antitrust Division to justify to higher-ups that such a program will be worth the investment.

Endnotes

1. Compare U.S. Dep't of Justice, United States Attorneys' Manual, 9-28.300 (2008) (recognizing pre-existing compliance programs as a mitigating factor in charging generally) *with* U.S. Dep't of Justice, United States Attorneys' Manual 9-28.400(B) and 9-28.800(A)-(B) (carving out antitrust from that general rule) (U.S. Dep't of Justice 2008).
2. U.S. DEP'T OF JUSTICE, COMPLIANCE IS A CULTURE, NOT JUST A POLICY 9 (2014), <http://www.justice.gov/atr/file/517796/download> at 9.
3. U.S. Sentencing Guidelines Manual § 8C2.5(f)(1) (U.S. Sentencing Comm'n 2014).
4. Training should be engaging and memorable for at least two reasons: (1) you want employees to absorb the training so that even if they do not remember the particulars, they know when and how to elevate an issue, and (2) Antitrust Division lawyers will always ask employees if they were trained and what they remember from the training.
5. In addition to designing a compliance program that satisfies the mitigation requirements set forth in the United States Sentencing Guidelines, counsel can consult the ICC Antitrust Compliance Toolkit, available at <http://www.iccwbo.org/Advocacy-Codes-and-Rules/Document-centre/2013/ICC-Antitrust-Compliance-Toolkit/>, for further guidance.
6. Training is specifically called out here because companies can be inclined to excuse their senior executives from participation because they are too busy; this inclination should be resisted.
7. That this goal is critical has recently been reinforced by the September 9, 2015 Individual Accountability for Corporate Wrongdoing memorandum issued by DOJ Deputy Attorney General Sally Quillian Yates, available at <http://www.justice.gov/dag/file/769036/download>, which highlights the importance, from an enforcement perspective, of holding individual wrongdoers accountable.

Stacey Anne Mahoney focuses her practice on antitrust litigation, including representing clients as plaintiffs and defendants in federal and state courts throughout the U.S., in cases involving restraints of trade, monopolization, tying, exclusive dealing, price discrimination, false advertising, unfair competition, and related business torts; merger advocacy, including trial as needed, in the United States and abroad; and counseling, including advising on distribution and pricing issues, as well as joint ventures and other competitor collaborations. Stacey develops and updates antitrust compliance programs and materials, frequently conducts on-site training for clients, and has conducted clients' internal investigations. She regularly represents clients before the DOJ, FTC and state attorneys general in various matters, including regarding antitrust, consumer protection and privacy issues. Stacey is the Chair of the Antitrust and Trade Regulation Committee for the New York City Bar Association and is a former Chair of the Antitrust Law Section of the New York State Bar Association.

**NYSBA
WEBCAST**

View archived Webcasts at
**[www.nysba.org/
webcastarchive](http://www.nysba.org/webcastarchive)**

Inside Interview

Jana Springer Behe, Esq.

Director of Contracts and General Counsel
New York State Technology Enterprise Corporation
Conducted by Amir Alimehri

Jana received her Bachelor of Arts from the University of Rochester, with honors, and her Juris Doctor from the University of Pittsburgh School of Law. She is admitted to practice law in New York and Pennsylvania.

As Director of Contracts and General Counsel of New York State Technology Enterprise Corporation ("NYSTEC"), Jana is primarily focused on risk management, compliance, and governance for NYSTEC. Jana has vast experience with contractual and procurement development and compliance. She has assisted numerous agencies with procurement advice and functions as internal quality review on a variety of NYSTEC engagements. She is also a member of the NYSTEC Leadership Team and provides direct support to the CEO and the NYSTEC Board of Directors.

Jana is a co-chair of the New York State Forum IT ("NYS IT") Procurement Work Group which reviews suggested enhancements to the NYS IT procurement process. She is also an Executive Committee member of the Corporate Counsel Section of the New York State Bar Association, Corporate Counsel Section Delegate to the NYSBA House of Delegates, Kenneth G. Standard Diversity Internship program committee member and sponsor mentor, Chair of the Albany YMCA, and a member of the Executive Women's Golf Association Albany/Capital Region.

Jana was kind enough to provide insight about her journey as a lawyer and her experience as an in-house lawyer.

Discuss your career path prior to NYSTEC?

Jana spoke about a career in contract administration prior to law school working at Ogden Entertainment. She was responsible for contracting with vendors and concessions for Woodstock 99. She then obtained internships at ALCOA and Highmark Blue Cross Blue Shield, while attending law school.

Upon graduating from law school, Jana sought a non-traditional legal job as a Senior Contract Administrator at NYSTEC. She explained that once NYSTEC split from its parent company in 2005 and became wholly independent, her roles and responsibilities expanded. Jana was promoted to Director of Contracts and in 2008, General Counsel was added to her title.

Does NYSTEC hire, and how do you choose, outside counsel?

"On occasion, yes. For very specialized matters." Jana said that she looks for somebody who "understands the goals of the organization" and somebody "who has

subject-matter expertise." Jana noted that every organization has a different philosophy. She further explained that "outside counsel should not just give advice but should also take into account the effect the advice has on the organization and its employees." And, when asked what her biggest pet peeve was when it comes to outside counsel, she said "not taking the time to understand our business or our business needs and high rates."

How much do you like to manage outside counsel as opposed to deferring to them on everything they handle?

Jana likes to be involved in discussions with outside counsel to make sure the organization's goals are understood and are taken into consideration. Besides that, Jana typically steps back and defers to outside counsel.

How is the work-life balance as an in-house lawyer?

Jana personally likes it but indicated that "there are some extremely long hours sometimes," adding that "work-life balance at NYSTEC means feeling valued as an employee and having opportunities for growth."

What would you suggest to a student or attorney who is interested in working as an in-house lawyer eventually?

She recommended that people create a strong network by making real connections with people that they meet along their career path and staying in touch with them.

What is something you enjoy as in-house counsel?

Jana explained that being in-house provides an opportunity to partake in making important business decisions in addition to practicing law. She also noted that the most rewarding thing for her is that she gets "a chance to interact with smart people outside of the legal profession" and she gets to "work directly with the Leadership Team to get things done." Jana added that working in-house requires a lawyer to "understand risks, present options for consideration, and make the best informed business decision; this may mean assuming some degree of risk." She also cautioned against being "too risk-adverse" in the in-house setting.

This interview was conducted by Amir Alimehri, a rising 2nd year law student at Rutgers Law School. He wrapped up his first summer legal experience as a legal intern at AstraZeneca. Amir started the school year as a judicial intern for the Honorable Mark A. Kearney of the Eastern District of Pennsylvania. He is also a member of the Rutgers Business Law Review and various other student organizations. Amir enjoys playing soccer, basketball, and tennis, as well as skiing in the winter. Amir is a native New Yorker and is very involved with the NYSBA.

Is Your Data Your Greatest Liability or Asset?

By Christopher O'Brien

Information: it is the lifeblood of your organization. But while it can be a valuable source of business intelligence, it can also become your worst enemy if not properly controlled. For example, data at one of the world's largest tire companies recently revealed \$3.2 million in bribes that violated the Foreign Corrupt Practices Act ("FCPA").¹

Earlier this year, the U.S. Securities and Exchange Commission ("SEC") entered a cease-and-desist order in an administrative proceeding against the Goodyear Tire & Rubber Co ("Goodyear").² The case alleged violations of the FCPA's books, records, and internal control provisions, which require organizations to record accurate transactions and maintain a system of internal accounting controls.

For four years, from 2007 to 2011, two of Goodyear's African subsidiaries bribed local authorities and employees of government-owned entities and private companies to facilitate tire sales. The subsidiaries recorded these payments as legitimate business expenses. One paid bribes by writing checks to cash, recording them in the books as expenses for phony promotional products, and cashing the checks to make improper payments to employees of government-owned and private-sector companies. The other marked up the cost of its tires with trumped-up fees for freight and customs clearing costs that were recorded as payments to vendors but were later reclassified to a balance sheet account and paid to employees of customers. The cease-and-desist order asserted that Goodyear failed to detect or prevent these payments because it did not conduct adequate due diligence when it acquired the subsidiaries and thereafter failed to "implement adequate FCPA compliance training and controls."³

The good news for Goodyear is that its internal reporting mechanism eventually worked: employees alerted the corporate office of the violations, so the company could halt the improper payments and report them to the SEC. Thanks to Goodyear's cooperation during the SEC investigation, its divestiture of the subsidiaries, its discipline of employees who failed to properly oversee the subsidiaries, and its ongoing efforts to enhance its compliance program, the company avoided criminal liability and civil penalties beyond a disgorgement and interest payment of slightly more than \$16 million.

But if Goodyear had a more robust, data-driven compliance program in place, it could have spotted these transgressions before buying the subsidiaries or soon after their acquisition. Corporate counsel should take this lesson to heart and step up to ensure that their organizations anticipate the fallout from emerging risks.

They must ensure their organizations have an immersive culture of forward-looking, data-driven enterprise risk identification.

A Transformation in the Risk Landscape

Over the last decade, the risk landscape has evolved significantly. As new forms of technology, communication channels, and data have arisen, the speed of business has accelerated. Add the trends of increased globalization and a regulatory complexity, and organizations can no longer afford to ignore the potential impact of even seemingly minor risks.

More data mobility, both through smart devices and the cloud, means organizations wield less control over their data than ever. The simple transfer of data from one location to another, or between the organization and a vendor, can run afoul of a host of regulations, including data privacy laws. If that data is lost, it can have serious implications for data preservation. Using e-mail and social media, employees can unwittingly (or maliciously) broadcast a company's confidential information, such as trade secrets, or malign their colleagues or the competition.

Furthermore, a global, cross-border approach to business raises the specter of unprecedented risk. Businesses that operate in multiple countries must understand how the laws of those nations intersect and conflict and find ways to ensure their operations remain compliant. This is particularly true when organizations outsource work to third parties located abroad; organizations must undertake thorough due diligence of all business arrangements.

Finally, increased activity on the regulatory front—federal, state, and local—also poses greater challenges. Regulators are focused more than ever on finding weaknesses in the flow of information to and from organizations. The bar has been raised for compliance, and the expert guidance of the legal team is necessary to prioritize the areas of greatest risk and design compliance strategies.

Traditional Risk Detection Is Not Enough

Traditionally, organizations have viewed risk according to the silo where it originated. For instance, finance might monitor risk associated with credit, information technology may focus on risks associated with cybersecurity, while the benefits team may consider potential violations of the Health Insurance Portability and Accountability Act. But a more holistic view that crosses departmental boundaries, subject matters, and geographies is necessary, as risks rarely remain confined to one area. Given the speed of information, risks often cross-pollinate between departments: a cyberbreach could leak protected

health information and thereby turn into a PR, legal, and financial nightmare.

Policies and procedures are essential methods for compliance with these risks, but relying on people to implement them can only take organizations so far. Risk detection is also required, but internal audits are not fool-proof: studies have revealed that audits may only detect 14 percent of corporate fraud.⁴ Internal audit software can often parse structured data for patterns in transactions, but, problematically, it cannot sort through unstructured data, such as e-mail and instant messaging, where the indicia of deeper problems often lurk.

No matter how thoroughly in-house counsel are involved, the traditional, backward-looking approach to Enterprise Risk Management (“ERM”) is not enough. Tried-and-true tools such as policies, procedures, and audits can help prevent risks from becoming crises, but they are often deployed after the fact and are not comprehensive. More forward-looking measures are necessary to convince regulatory agencies that organizations take their duty of compliance seriously. Indeed, the U.S. Department of Justice (“DOJ”) and the SEC “will give meaningful credit to thoughtful efforts to create a sustainable compliance program if a problem is later discovered. Similarly, undertaking proactive evaluations before a problem strikes can lower the applicable penalty range under the U.S. Sentencing Guidelines.”⁵ Therefore, a company must design its compliance program carefully to achieve three goals: to prevent, detect, and remediate violations promptly and thoroughly. This requires the use of “Big Data.”

A Forward-Looking Approach to Enterprise Risk Management Is Essential

As risks continue to multiply, organizations must develop innovative ERM strategies that focus on long-term results, not short-term compliance. Organizations that continue to take a backward-looking approach—or worse, no approach at all—to their data are begging for costly internal investigations and regulatory penalties.

One simple way that organizations can mine their teeming stores of unstructured data for red flags is keyword searches. The legal team should work with subject-matter experts and linguists to determine the appropriate keywords. But standing alone, keywords can lead to inaccurate conclusions. Over-inclusive keywords can overwhelm reviewers with irrelevant information that masks true risk; under-inclusive keywords can lead reviewers to overlook key information. Moreover, many employees opt to obscure their bad behavior in code words that cannot be picked up with a standard keyword search.

More forward-looking data analytics tools exist that can go beyond the surface, search for hidden risks, and transform seemingly unrelated data into meaningful pat-

terns. For example, technology-assisted review (“TAR”) can help organizations facing a morass of data prioritize documents based on the likelihood that they contain responsive material. Using TAR, experienced lawyers code a seed set of documents for responsiveness to potential compliance issues. A computer algorithm interprets the lawyers’ logical reasoning and applies it across an entire document population. Lawyers then refine the computer’s logic until its coding closely resembles the human decisions.

In addition, other advanced tools are at the legal department’s disposal for detecting patterns in data. For instance, anomaly detection tools can scan records for irregular payments. Data visualization tools allow organizations to analyze relationships between employees, vendors, and foreign officials at a high level. Linguistic analysis techniques can identify instances where people subtly discuss suspicious activity using seemingly innocuous words and phrases. Concept clustering can identify hidden patterns within documents that appear to have no relationship on their surface.

As businesses continue to expand globally, regulatory complexity increases, and data velocity and variety multiply, the need to take a holistic, future-oriented view of compliance risks has never been greater. Instead of waiting for an issue to erupt and then examining data, organizations must ensure their legal teams are working in tandem with risk and compliance professionals to explore their data before issues surface. That way, they can identify the full spectrum of risks, assess their potential to cause damage, and allocate their resources properly.

Endnotes

1. 15 U.S.C. § 78dd-1 (20xx).
2. Goodyear Tire & Rubber Co., Exchange Act Release No. 74356, 2015 SEC LEXIS 672 (Feb. 24, 2015) (Order Instituting Cease-and-Desist Proceedings, Pursuant to Section 21C of the Securities Exchange Act of 1934, Making Findings, and Imposing a Cease-and-Desist Order, File No. 3-16400), available at <http://www.sec.gov/litigation/admin/2015/34-74356.pdf>.
3. *Id.*
4. ASS’N OF CERTIFIED FRAUD EXAM’RS, REPORT TO THE NATIONS ON OCCUPATIONAL FRAUD AND ABUSE: 2014 GLOBAL FRAUD STUDY (2014), <http://www.acfe.com/rtnn/docs/2014-report-to-nations.pdf>.
5. U.S. DEP’T OF JUSTICE & U.S. SEC. & EXCH. COMM’N, A RESOURCE GUIDE TO THE U.S. FOREIGN CORRUPT PRACTICES ACT (2012), <http://www.sec.gov/spotlight/fcpa/fcpa-resource-guide.pdf>.

Christopher O’Brien, Esq. is Senior Vice President, Corporate Development and Business Operations, with Xerox Litigation Services, the e-discovery division of Xerox Corp. He was previously a litigator and also served as Senior Counsel to New York State Governor George E. Pataki and Deputy Commissioner and General Counsel of the New York State Department of Taxation and Finance.

Meeting Your Cybersecurity Obligations

By Steve Rubin and A. Jonathan Trafimow

The Federal Trade Commission (“FTC”), currently the predominate enforcer of cybersecurity regulations, has commented that “security is an ongoing process of using reasonable and appropriate measures in light of the circumstances”¹ which is not covered by any checklist.² Failure to take appropriate steps to adequately come into compliance subjects a business to possible enforcement actions by agencies, lawsuits from affected consumers and fines from various state regulations. Compliance with the number and complexity of federal and state cybersecurity laws and regulations is no simple task. In this evolving legal environment, a Written Information Security Plan (“WISP”) provides the necessary structure companies need to identify and implement conforming practices. A WISP not only allows a company to adapt to industry and regulatory changes, but also incorporates legal principles to mitigate damages in the event of an incident.

Cybersecurity Regulations—Specific and General

Nearly every business is subject to some form of cyber security regulation. The U.S. Securities and Exchange Commission (the “SEC”), Office of the Comptroller of the Currency (the “OCC”), and Centers for Medicare & Medicaid Services (the “CMS”), along with several other state and federal agencies, have all begun to incorporate cybersecurity principles into their regulations. This has led to a myriad of rules, each having its own jurisdictional scope and requirements. These rules generally require a number of technical safeguards, such as the implementation of firewalls, anti-virus software, system audits and that the company’s security standards be documented. But, depending on the type of information a business collects, agencies may also impose additional constraints. Where information has traditionally been highly regulated, agencies have begun to require specific safeguards. The Health Insurance Portability and Accountability Act of 1996 (“HIPAA”) requires that covered entities restrict and document access to protected health information;³ determine which applications are important to patient care;⁴ and record the movement of hardware and electronic media.⁵ For registered investment companies and advisors, the SEC has provided that failure to prepare for a cyber incident could result in a breach of their fiduciary obligations,⁶ and make the company liable for fraudulent activity.⁷ The SEC has also suggested that a covered entity’s cybersecurity obligations may extend to commercial or market-sensitive information.⁸ Finally, the Sarbanes-Oxley Act of 2002 (“SOX”) imposes severe penalties on corporate officials who fail to implement internal controls, including technical safeguards,⁹ to ensure the truth and accuracy of each annual or quarterly report.¹⁰

Even when a company’s practices are not regulated by the above agencies, they may still be subject to the regulations of the FTC. Under section 5(a) of the Federal Trade Commission Act (“FTCA”), the FTC may sue any business subject to its jurisdiction for engaging in “acts or practices in or affecting commerce” that are “unfair” or “deceptive.”¹¹ The FTC has brought several actions against defendants where those defendants claimed to have reasonable security, but failed to implement sufficient measures to prevent, detect, and respond to unauthorized access to their computer networks.¹² As a result, companies have been subjected to fines, required to implement a comprehensive information security plan and obligated to obtain audits by independent third party security professionals for 20 years.

A company’s compliance obligations do not stop with its internal practices, but also extend to their relations with company affiliates. In *GMR Transcription Services, Inc.*, the FTC found that the defendant failed to implement reasonable and appropriate security by not contractually requiring appropriate safeguards and not monitoring its vendor to ensure its compliance.¹³ While a company may not be able to directly control its affiliates’ practices, a business can nonetheless take precautions to show that it assessed its affiliates’ cybersecurity and required them to implement appropriate safeguards.

As a part of any information security program, counsel should review any vendor agreements along with its vendor’s WISPs and security audits. Attorneys should make sure that these agreements include, among other things, a provision mandating notification if the vendor updates its security practices or significantly changes its operating procedures. While it is unclear what constitutes appropriate monitoring, counsel should review its vendors’ WISPs to assess their cybersecurity practices. Depending on the nature of the information being shared, it may be necessary to require the vendor to undergo a security audit immediately or at random intervals throughout the business relationship.

A company’s cybersecurity practices need not be perfect. Where a company has taken every reasonable precaution, the FTC has provided that a breach “will not violate the laws that [it] enforces.”¹⁴ Companies seeking to implement appropriate cybersecurity safeguards should ensure their WISP is in compliance with the National Institute of Standards and Technology’s Cybersecurity Framework (“NIST Framework”). In response to growing cybersecurity concerns, President Obama signed Executive Order 13636 which directed the National Institute of Standards and Technology to develop a Cybersecurity Framework. Following the release of the draft standards, on February 12, 2014, the final NIST Framework took effect. The FTC

has already stated that the NIST Framework “is fully consistent with the FTC’s enforcement framework”¹⁵ as to matters of risk assessment and mitigation.

WISP Comes to the Rescue

As an essential part of a cybersecurity program and before a potential breach occurs, companies need to develop a WISP, an internal company document that enumerates a company’s regulatory requirements, risks and responses to determine its conformity. A WISP identifies and ranks the critical components of a business according to its business objectives and legal obligations. The company can then concentrate its available resources in areas requiring heightened security and eliminate those where such protection is not incumbent. As a company’s obligations fluctuate, a WISP offers an effective means of continuing to provide appropriate safeguards.

As a result of technological developments and changes in business practices, companies must continuously adapt their security structure to meet the demands of new regulations and industry best practices. Events such as acquiring business from other countries, outsourcing company functions and utilizing new software can all have profound effects on a business’s compliance needs. A WISP pinpoints how data traverses a company’s network and helps identify gaps in its security practices. A company can then assess potential risks and implement reasonable cost-effective responses to meet its regulatory requirements.

While the law continues to struggle to keep up with technology, old regulations may be interpreted broadly in an attempt to address the technologically changing landscape. A WISP structures a company’s review and organization of its cybersecurity infrastructure and facilitates improvements. For example, a WISP can develop a record of how a company: identifies sensitive information, addresses threats, manages risk and continuously improves its security infrastructure by learning from previous incidents. Without such a structure, a business may fail to recognize a critical component of its cybersecurity framework and will be less prepared to adapt to the evolving law.

A WISP Can Limit Customer Actions

The benefits of a WISP are not limited to proving a company’s regulatory compliance; it also has the potential to limit customer lawsuits by showing a company took reasonable steps to protect its data. As discussed below, companies that can demonstrate that their stolen data was effectively protected or that they employed reasonable practices but could not prevent an incident (both of which are required in a WISP), may persuade a court to dismiss an action. In one case, several tapes containing protected information, including medical records and social security numbers, were stolen.¹⁶ Yet, the court

determined that the plaintiffs had not suffered an injury-in-fact because defendant’s practice of storing encrypted data on tapes made it unlikely the attacker would be able to “open and decipher” the stolen information.¹⁷ In another case, the court found that even though unencrypted customer data was stolen, the company had not violated its duty of reasonable care.¹⁸ The court reasoned the event was unforeseeable, and that defendant acted reasonably by “transmitt[ing] and us[ing] data in accordance” with its WISP.¹⁹

Lawyers Provide Even More Protection by Protecting Your WISP

Legal counsel is an integral part of the WISP creation process because the utilization of legal advice in connection with the WISP creates an argument that at least some aspects of the process are shielded from disclosure in litigation because of the attorney-client privilege or attorney work product doctrine. Where a lawyer needs outside help to provide effective consultation to the lawyer’s client, the attorney-client privilege may attach.²⁰ To be covered by the doctrine, a document must have “been prepared in anticipation of litigation by or for a party, or by the party’s representative.”²¹ The doctrine protects an attorney’s mental impressions, which receive virtually unlimited protection, and work product.²² Both the attorney-client privilege and attorney work product can be waived.²³ As constructing a WISP requires a thorough review of a company’s procedures and technical practices, counsel should take every precaution to preserve a company’s potential claims of privilege and work product.

Conclusion

While technology continues to evolve, so will the complexities of a company’s cybersecurity obligations. It will not be long before all companies are subjected to at least some form of cybersecurity compliance. Having a properly drafted WISP can help your business comply with this ever-changing legal environment.

Endnotes

1. Orson Swindle, *Prepared Statement of the Federal Trade Commission On Protecting Our Nation’s Cyberspace*, FED. TRADE COMM’N (Apr. 21, 2004) (statement of Orson Swindle, Former Commissioner, FTC), <https://www.ftc.gov/public-statements/2004/04/prepared-statement-federal-trade-commission-protecting-our-nations>.
2. Joseph J. Lazzarotti, *Checklists Not Enough When Developing a WISP*, FTC Director Comments at IAPP Global Privacy Summit, NAT’L L. REV. (Mar. 9, 2015), <http://www.natlawreview.com/article/checklists-not-enough-when-developing-wisp-ftc-director-comments-iapp-global-privacy>.
3. 45 C.F.R. § 164.308(a)(4)(ii)(A) (2013); 45 C.F.R. § 164.308(a)(4)(ii)(C).
4. *Id.* § 164.308(a)(7)(ii)(E).
5. *Id.* § 164.310(d)(2)(iii).

6. See, e.g., 17 C.F.R. § 270.17j-1 (2012); 17 C.F.R. § 275.204A-1.
7. See, e.g., 17 C.F.R. § 270.17j-1 (2012); 17 C.F.R. § 275.204A-1.
8. SEC, IM GUIDANCE UPDATE No. 2015-02 2 (2015), <http://www.sec.gov/investment/im-guidance-2015-02.pdf>.
9. Auditing Standard No. 5, PUB. CO. ACCOUNTING OVERSIGHT BD. (2007), http://pcaobus.org/Standards/Auditing/Pages/Auditing_Standard_5.aspx (Under section 36 audits include a review of the “effect of information technology on internal controls over financial reporting.”).
10. 15 U.S.C. § 7241 (2002).
11. *Id.* § 45(a)(1).
12. *Cord Blood Bank Settles FTC Charges That It Failed to Protect Consumers Sensitive Personal Information*, FED. TRADE COMM’N (Jan. 28, 2013), <http://www.ftc.gov/news-events/press-releases/2013/01/cord-blood-bank-settles-ftc-charges-it-failed-protect-consumers>; *BJ’s Wholesale Club Settles FTC Charges*, FED. TRADE COMM’N (June 16, 2005), <http://www.ftc.gov/news-events/press-releases/2005/06/bjs-wholesale-club-settles-ftc-charges>.
13. *Provider of Medical Transcript Services Settles FTC Charges That It Failed to Adequately Protect Consumers’ Personal Information*, FED. TRADE COMM’N (Jan. 31, 2014), <https://www.ftc.gov/news-events/press-releases/2014/01/provider-medical-transcript-services-settles-ftc-charges-it>.
14. Orson Swindle, *Prepared Statement of the Federal Trade Commission On Protecting Our Nation’s Cyberspace*, FED. TRADE COMM’N (Apr. 21, 2004), <https://www.ftc.gov/public-statements/2004/04/prepared-statement-federal-trade-commission-protecting-our-nations> (“Although a breach may indicate a problem with a company’s security, breaches can happen...even when a company has taken every reasonable precaution. In such instances, the breach will not violate the laws that the FTC enforces.”).
15. FED. TRADE COMM’N, ON THE FRONT LINES: THE FTC’S ROLE IN DATA SECURITY (2004), http://www.ftc.gov/system/files/documents/public_statements/582841/140917csisspeech.pdf.
16. *In re Sci. Applications Int’l Corp. (SAIC) Backup Tape Data Theft Litig.*, 45 F. Supp. 3d 14 (D.D.C. 2014).
17. *Id.* at 29.
18. *Guin v. Brazos Higher Educ. Serv. Corp.*, No. Civ. 05-668 RHK/JSM, 2006 WL 288483, (D. Minn. Feb. 7, 2006).
19. *Id.*
20. *United States v. Kovel*, 296 F.2d 918, 922 (2d Cir. 1961) (“What is vital to the privilege is that the communication be made in confidence for the purpose of obtaining legal advice from the lawyer.”).
21. *United States v. Ghavami*, 882 F. Supp. 2d 532, 539 (S.D.N.Y. 2012) (internal citations omitted) (The work product doctrine, partially codified by Rule 26(b)(3) of the Federal Rules of Civil Procedure, is designed to allow “a lawyer [to privately] prepare and develop legal theories and strategy ‘with an eye toward litigation.’”); see also *Doe v. Poe*, 244 A.D.2d 450, 451-52 (N.Y. App. Div. 1997), *aff’d*, 92 N.Y.2d 864 (N.Y. App. Div. 1998); *Bras v. Atlas Constr. Corp.*, 153 A.D.2d 914, 915-16 (N.Y. App. Div. 1989).
22. *Ghavami*, 882 F. Supp. 2d at 540.
23. *Id.* (internal citations omitted).

Steven S. Rubin is a partner at Moritt Hock & Hamroff LLP where he chairs the firm’s patent practice and co-chairs the firm’s cybersecurity practice. With an electrical engineering background, Mr. Rubin concentrates his practice on all phases of patent-related matters, both domestically and internationally.

A. Jonathan Trafimow is a partner at Moritt Hock & Hamroff LLP where he chairs the firm’s employment practice and co-chairs the firm’s cybersecurity practice. Mr. Trafimow represents employers in all areas of workplace discrimination, retaliation, harassment and civil rights claims, and class actions. He also routinely advises employers on compliance with local and federal employment laws and regulations.

The authors thank Stephen E. Breidenbach, student of the Maurice A. Deane School of Law at Hofstra University, for his assistance in the research and drafting of this article.

Request for Articles



If you have written an article and would like to have it considered for publication in *Inside*, please send it to either of its editors:

Jessica D. Thaler
410 Benedict Ave.
Tarrytown, NY 10591
jthaleresq@gmail.com

Elizabeth J. Champnoi
Stout Risius Ross, Inc. (SRR)
120 West 45th Street, Su. 2800
New York, NY 10036
eshampnoi@srr.com

Articles should be submitted in electronic document format (pdfs are NOT acceptable), and include biographical information.

www.nysba.org/Inside

E-Contracting: What Corporate Counsel Need to Know

By Matthew D. Sobolewski and Chester R. Ostrowski

Introduction

With the rapid increase in the use of computers, tablets, mobile phones, wearable devices, and other electronics in general, it is likely that your company—or corporate clients—are already considering ways to take advantage of new technologies. One of the many ways in which companies, both large and small, can do exactly that is through electronic contracting (“e-contracting”)—i.e., the creation and execution of valid and enforceable agreements in electronic, rather than traditional paper, format.

Indeed, the potential benefits of e-contracting are vast. Some of these benefits are obvious, including the ability of parties to bind themselves to the terms of an agreement from anywhere in the world without the extra time and effort required to print, sign, mail, fax, scan, and/or e-mail the “original” documents. Some of the other benefits may be less obvious, including the cost savings associated with eliminating the need for physical storage and retrieval of traditional paper documents. Of course, all of these things will ultimately affect the company’s bottom line.

To take full advantage of e-contracting opportunities, however, companies need guidance from in-house and corporate counsel to ensure that the contracts they enter into are legally binding and enforceable. The laws and requirements governing e-contracts may vary from state to state and understanding them, in advance of execution, may be crucial to protecting the underlying transactions from legal challenges.

This article aims to provide in-house and corporate counsel with an overview of the current state of the law on e-contracting in New York, New Jersey, and Connecticut and some tips for helping develop sound e-contracting policies, practices, and procedures.

The Law on E-Contracting

In 2000, Congress enacted the federal Electronic Signatures in Global and National Commerce Act (the “ESIGN Act”). The ESIGN Act provides that “a signature, contract, or other record relating to [any transaction in or affecting interstate commerce] may not be denied legal effect, validity, or enforceability solely because it is in electronic form.”¹ With respect to e-contracts, in particular, the ESIGN Act provides that “a contract relating to [any transaction in or affecting interstate commerce] may not be denied legal effect, validity, or enforceability solely because an electronic signature [(“e-signature”)] or electronic record was used in its formation.”²

To date, 47 states and the District of Columbia have also enacted some version of the Uniform Electronic Transactions Act (the “UETA”). Both New Jersey and Connecticut are among those states that have adopted a version of the UETA.³ New York, on the other hand, is not. Instead,

New York has enacted its own law—i.e., the Electronic Signatures and Records Act (the “ESRA”).⁴

Generally speaking, the New Jersey UETA, the Connecticut UETA, and the New York ESRA are all designed to give legal effect to both e-contracts and e-signatures.⁵ Like the ESIGN Act, each of these state laws broadly defines “electronic signature” to include not only electronic forms of a handwritten signature (e.g., a scanned copy) or the typewritten name of the signatory, but also any “electronic sound, symbol or process, attached to or logically associated with an electronic record and executed or adopted by a person with the intent to sign the record.”⁶ Given this broad definition, there are countless ways in which a potential signatory can provide an electronic indication of assent to be bound by an e-contract, including checking a box or clicking an “I Agree” button on an Internet site, entering a unique personal identifier, or typing his or her name at the bottom of an e-mail responding to an offer.⁷

Regardless of the method of assent, however, an e-signature is generally not attributable to a particular individual—and, therefore, not legally binding—unless it can be shown that the e-signature was the act of that same individual through the use of an adequate “security procedure.”⁸ Under both the New Jersey and Connecticut versions of the UETA, “security procedure” is defined as a procedure used “for the purpose of verifying that an electronic signature, record or performance is that of a specific person or for detecting changes or errors in the information in an electronic record,” including procedures that require “the use of algorithms or other codes, identifying words or numbers, encryption, callback, or other acknowledged procedures.”⁹

As a result of these laws, e-signature software—such as Adobe, DocuSign, and RightSignature—typically includes one or more standard security measures designed to authenticate the identity of the purported signatory and to verify that a document has not been changed since it was signed. Audit trails, for example, are used to demonstrate when and by whom a document was sent, viewed, and signed.¹⁰

Despite these security measures, however, e-contracts and e-signatures are still subject to legal challenges on the same grounds as paper contracts and “wet ink” signatures. These grounds include forgery, mistake, and duress. In addition, although the federal and state laws discussed above allow for e-contracting and the use of e-signatures in most commercial contexts, there are still some circumstances in which an e-signature will not suffice, including in the execution of a will, trust, or power of attorney.¹¹ In some states, certain real estate transactions also cannot be consummated by electronic means, although, in September 2012, New York’s ESRA was amended to allow for the use

of e-signatures on conveyances and other instruments recordable under Article 9 of New York State Real Property Law and to allow state, county, and municipal officials to accept real property instruments, such as deeds and mortgages, in electronic format.¹²

Notably, companies are not *required* to use e-contracts or to accept e-signatures.¹³ Nor can a consumer be required to contract electronically without consent.¹⁴ Accordingly, potential signatories should generally be given the opportunity to opt-out and elect to use traditional paper versions of the contract documents.

Developing Sound Policies, Practices, and Procedures for E-Contracting

By following these tips, in-house and corporate counsel can help the companies they work for develop sound policies, practices, and procedures for e-contracting:

- **Know the Law.** As noted above, even states that have adopted the UETA may have made significant changes to the original “model” language. Courts in various jurisdictions may also be inclined to interpret the statutes differently based on applicable precedent or public policy. In-house and corporate counsel should make sure they know the laws that apply to their companies and clients and how courts in the relevant jurisdictions are currently dealing with e-contracting in litigation.
- **Be Cautious.** In helping develop a method for e-contracting within a particular company, make sure to include one or more ways to authenticate signatories, identify alterations of the underlying e-contract documents, and address claims that such documents were signed or transmitted by mistake. The method used should be specifically tailored to the company’s business needs, such that the resulting e-contracts will be legally valid and admissible in court without the process being so cumbersome as to dissuade usage.
- **Get Non-Legal Experts Involved.** When implementing e-contracting policies, practices, and procedures, be sure to enlist assistance from business and marketing professionals, as well as technical experts. In addition to the bottom line, security, software, and programming issues are of the utmost importance.

Endnotes

1. 15 U.S.C. § 7001(a)(1) (2015).
2. *Id.* § 7001(a)(2).
3. See N.J. STAT. ANN. §§ 12A:12-1 to -26 (2015); CONN. GEN. STAT. §§ 1-266 to -286 (2015).
4. See N.Y. TECH. LAW §§ 301-309 (McKinney 2004). The only other states which have not adopted a version of the UETA are Washington and Illinois. Both states, however, have similar state laws giving legal effect to e-contracts and e-signatures.
5. N.Y. TECH. LAW § 304(2) (stating that, “unless specifically provided otherwise by law, an [e-signature] may be used by a person in lieu of a signature affixed by hand,” and the use of such e-signature “shall have the same validity and effect as the use of a signature

fixed by hand.”); N.J. STAT. ANN. §§ 12A:12-7(a)-(d) (“A record or signature may not be denied legal effect or enforceability solely because it is in electronic form.... A contract may not be denied legal effect or enforceability solely because an electronic record was used in its formation.... If a law requires a signature, an electronic signature satisfies the law.”); CONN. GEN. STAT. § 1-272(a)-(d) (“A record or signature may not be denied legal effect or enforceability solely because the record or signature is in electronic form.... A contract may not be denied legal effect or enforceability solely because an electronic record was used in the formation of the contract.... If a law requires a signature, an electronic signature satisfies the law.”). Each of the state laws also provides for admission into evidence of e-signatures in legal proceedings. See N.Y. TECH. LAW § 306 (“In any legal proceeding where the provisions of the [CPLR] are applicable, an electronic record or electronic signature may be admitted into evidence pursuant to the provisions of [CPLR Article 45].”); N.J. STAT. ANN. § 12A:12-13 (“In a proceeding, evidence of a record or signature may not be excluded solely because it is in electronic form.”); CONN. GEN. STAT. § 1-278 (“In a proceeding, evidence of a record or signature may not be excluded solely because such record or signature is in electronic form.”).

6. N.Y. TECH. LAW § 302(2); see also N.J. STAT. ANN. § 12A:12-2; CONN. GEN. STAT. § 1-267(8).
7. See, e.g., *Berkson v. Gogo LLC*, No. 14-cv-1199, 2015 WL 1600755, at *26-33 (E.D.N.Y. Apr. 9, 2015) (discussing validity and enforceability of various types of “internet agreements”); *Stevens v. Publicis, S.A.*, 50 A.D.3d 253, 254-55, 854 N.Y.S.2d 690, 692 (1st Dep’t 2008) (citations omitted) (“The e-mails from plaintiff constitute ‘signed writings’ within the meaning of the statute of frauds, since plaintiff’s name at the end of his e-mail signified his intent to authenticate the contents.”).
8. See N.J. STAT. ANN. § 12A:12-9 (“An electronic record or electronic signature is attributable to a person if it was the act of the person. The act of the person may be shown in any manner, including a showing of the efficacy of any security procedure applied to determine the person to which the electronic record or electronic signature was attributable.”); Conn. Gen. Stat. § 1-274 (same).
9. N.J. STAT. ANN. § 12A:12-2; Conn. Gen. Stat. § 1-267(14) (same).
10. Depending on the needs of your company or client, even greater security—in terms of authenticating signatures and preserving the integrity of contract documents—may be provided through the use of digital signatures. Note, however, that administration of digital signatures will come with a corresponding increase in time and cost.
11. See N.Y. Tech. Law § 307; N.J. STAT. ANN. § 12A:12-3 (excluding, *inter alia*, transactions governed by “the law governing the creation and execution of wills, codicils, or testamentary trusts”); Conn. Gen. Stat. § 1-268 (excluding, *inter alia*, “execution of wills, codicils or testamentary trusts”).
12. See N.Y. Tech. Law § 307.
13. N.J. STAT. ANN. § 12A:12-5a. to 5b. (providing that New Jersey UETA does “not require a record or signature to be created, generated, sent, communicated, received, stored or otherwise processed or used by electronic means or in electronic form” and applies “only to transactions between parties each of which has agreed to conduct transactions by electronic means”); Conn. Gen. Stat. § 1-270(a)-(b) (same with respect to Connecticut UETA); N.Y. Tech. Law § 309 (“Nothing in this article shall require any entity or person to use an electronic record or an electronic signature unless otherwise provided by law.”).
14. See *id.*

Matt Sobolewski is Partner at McLaughlin & Stern, LLP in New York City. He practices primarily in the areas of complex commercial, bankruptcy, and consumer finance litigation.

Chet Ostrowski is a Senior Associate in the firm’s Litigation and Bankruptcy, Reorganization and Restructuring Departments.

Compliance With EU Data Protection Regulation

By Laura Liguori and Federica De Santis

Introduction

By means of an innovative and modern directive (Directive 95/46/EC—the “Data Protection Directive”¹), in 1995, the European Community adopted its first data protection legislation aimed at providing common legal principles (to be implemented by European Union (“EU”) Member States by means of national legislation) to protect personal data and to align the bases of Member States’ provisions in respect to privacy and data protection.

However, the Data Protection Directive was adopted when the Internet was not widely used. The Internet technology has advanced in recent years and has posed new challenges to the protection of individuals’ data. The accelerating take-up of social networking, user-generated content platforms, mobile apps, cloud computing, location-based services, the “Internet of Things” (i.e., the ability of everyday objects to connect to the Internet and to send and receive data, e.g., wearables devices, home automation, etc.) and the growing globalization of data flows have significantly increased the risk for individuals to lose control of their own personal data.

Further, one of the main recurrent complaints about the Data Protection Directive is the lack of actual harmonization, which led to a certain fragmentation in the way personal data protection has been implemented across EU Member States. This resulted in additional costs and administrative burdens for operators as well as widespread uncertainty. This is particularly true for data controllers established in several Member States, who should comply with the requirements and practices in each of the countries where they are established. Guidance provided by the Article 29 Data Protection Working Party, an independent advisory body to the EU Commission set up under Article 29 of the Data Protection Directive (the “Working Party 29”), on several data protection issues certainly contributed to harmonization of data protection principles at the EU level, although the Article 29 Data Protection Working Party’s opinions are not binding.

A uniform and coherent application of the data protection rules among the European countries is fundamental, in light of the proposed creation of the Digital Single Market.²

Seventeen years after, on January 25, 2012, the EU Commission proposed new uniform legislation on privacy and data protection in Europe, by means of a General Data Protection Regulation (the “Regulation”) which, once adopted, would be directly applicable in all Member States without the need for national legislation. The Regulation comes together with a proposed direc-

tive 5833/12 on the processing of personal data with the purpose to prevent, investigate or prosecute crimes, or to adopt criminal sanctions, intended to replace the 2008 Data Protection Framework Decision.³

Henceforth, the European legislators have been discussing the new proposals and on March 12, 2014 the European Parliament (the “Parliament”) adopted its position on the Regulation, proposing amendments aimed at enhancing the guarantees of data protection, in respect to the text approved by the EU Commission.⁴

On June 11, 2015, the EU Council (the “Council”) approved its General Approach⁵ and the discussion among the three organisms (the so-called “trilogue”) has officially started,⁶ with the purpose to reach an agreement and to finalize the approval of the Regulation and the attached directive before the end of 2015.

This article focuses on some of the most groundbreaking provisions of the proposed Regulation which are expected to be a major concern for in-house counsel, in particular those advising businesses with multi-jurisdictional operations. The Regulation also introduces new provisions that, amongst others, would: (1) make international data transfers easier; (2) decrease the requirements and the costs of dealing with more than one Privacy Authority with differing rules (so-called “one-stop shop”); (3) implement specific provisions on the so-called “right to be forgotten,” as interpreted by the European Court of Justice in the *Google Spain* case;⁷ and (4) provide for more effective sanctions and penalties for data controllers and data processors.

Territorial Scope of the Regulation

One of the major changes to be brought by the Regulation concerns the territorial scope of the EU data protection laws.

Today, Article 4 of the Data Protection Directive contains the rules governing its territorial scope and jurisdictional reach. According to this provision, the EU rules apply to personal data processing:

- where the processing is carried out in the context of the activities of an “establishment” of the data controller in the territory of the Member State. If the same controller is established in more than one Member State (e.g., by means of subsidiaries), the controller must take the necessary steps to ensure that each of these establishments complies with the obligations laid out by the applicable national law. Security measures depend on the location of a

possible processor, as provided in Article 17, paragraph 3 of the Directive; and

- where a controller not established in the EU, for purposes of processing personal data, makes use of “equipment,” automated or otherwise, located on the territory of that Member State, unless such equipment is used only for purposes of transit through the territory of the EU.

Article 3, paragraph 1, of the Regulation, as recently amended by the Council based on the Parliament’s position, would still keep the “establishment criterion” mentioned above for the applicability of its provisions to controllers or processors established in the EU. In addition to that, the Regulation would expand the “use of equipment” criterion currently provided by the European data protection law by making data controllers established outside the EU, but “targeting” EU residents, subject to EU data protection obligations.

Indeed, the Regulation would be applicable whether the processing of personal data concerns:

- (1) the offer of goods or the provision of services to residents in the EU, even where no payment is required (e.g., “free” services, where individuals in fact pay for the service by providing their personal data); and
- (2) the monitoring of data subjects’ behavior within the EU. In order to determine whether a processing activity can be considered to ‘monitor the behavior’ of data subjects, it should be ascertained whether individuals are tracked on the Internet with data processing techniques which consist of profiling an individual, particularly in order to make decisions concerning her or him for analyzing or predicting her or his personal preferences, behaviors and attitudes.⁸

Because of its potential broad reach, the new criterion poses challenges for businesses directing their activity to the EU and also gives rise to questions on how the Regulation’s requirements can be readily enforced outside the EU.

It is worth mentioning that the Council uses different wording from the position adopted by the Parliament: in fact, the latter proposed that controllers, and even processors not residing in the EU, would be subject to the provisions of the Regulation. In its opinion regarding the proposed regulation, the Working Party 29 stressed the fact that the Regulation should also cover non-EU processors, in order to provide legal liability for these subjects.⁹

Automated Data Processing and Profiling

Generally speaking, “profiling” enables an individual personality or aspects of his or her personality—especially behavior, interests and habits—to be determined,

analyzed and predicted. “Profiling” of individuals is increasingly used by companies to offer personalized and targeted services (e.g., discounts, special offers and targeted advertisements based on the customer’s profile).

The Data Protection Directive does not contain any specific provision on “profiling,” but it includes a general provision concerning “automated individual decisions” in Article 15, which grants data subjects the right not to be subject to a decision which “produces legal effects” concerning him or “significantly affects” him and which is based solely on automated processing of data intended to evaluate certain personal aspects relating to him, such as his performance at work, creditworthiness, reliability, conduct, etc. An automated decision by a bank not to grant credit may fall within the aforementioned provision.

Automated decisions can, however, be made in certain cases, notably in the course of entering into or performance of a contract, provided that the data subject’s legitimate interests are protected, e.g. by making arrangements allowing him to express his point of view, or as otherwise provided by the law.

This provision has sometimes been implemented across EU Member States in different ways. It is worth mentioning Italy, where the prohibition to make decisions involving the assessment of a person’s conduct based solely on the automated processing of personal data aimed at defining the data subject’s profile or personality is limited to measures or acts taken by judicial or administrative authorities.¹⁰

The Regulation builds on Article 15 of the Data Protection Directive and on the Council of Europe’s Recommendation on profiling¹¹ and it specifically addresses “profiling” of data subjects.

Article 4 of the Regulation defines “profiling” as *“any form of automated processing of personal data evaluating personal aspects relating to a natural person, in particular to analyze or predict aspects concerning performance at work, economic situation, health, personal preferences, or interests, reliability or behavior, location or movements.”*

The main provision on profiling is Article 20 of the Regulation (“Automated individual decision making”), which, similar to the Data Protection Directive, grants to the data subject the right not to be subject to a decision based solely on automated processing (like automatic refusal of an online credit application or e-recruiting practices without any human intervention¹²), including profiling, which produces legal effects concerning him or her or significantly affects him or her. The Regulation expands the cases in which decision-making based on such processing, including profiling, is allowed, introducing the possibility to carry it out with the data subject’s explicit consent.

Different from the various national provisions adopted in each Member State, profiling would be treated by the new EU rules as processing alone and, as a consequence, it would require, amongst others, that controllers:

- inform data subjects about the existence of profiling, and the consequences of such profiling; and
- obtain a specific and explicit consent for it (unless one of the exceptions provided by the Regulation applies).

This course of action would not be a new one for Italy, where, for example, profiling is traditionally considered an autonomous processing, which requires a specific consent, separate from the consent for other purposes (such as, marketing purposes). In other European countries, profiling is usually treated as a modality of processing personal data and not as an autonomous processing, therefore it is generally deemed that no specific consent is required for profiling once the controller has obtained consent for marketing purposes.

Conclusion

In conclusion to this brief overview of the most groundbreaking provisions of the proposed Regulation, it is worth reminding that the latter is currently subject to discussions between the Parliament and the Council. Even though it is likely that the proposal will be amended before enactment, the general structure would probably remain the same, especially in the parts described above, which represent momentous innovations and will surely ensure effectiveness and confidence in the processing of people's personal data.

Endnotes

1. Directive 95/46 of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data [1995] OJ L281/31.
2. http://ec.europa.eu/priorities/digital-single-market/index_en.htm.
3. See Article 29 Data Protection Working Party's Opinion no. 1/2013, of February 26, 2013, providing further input into the discussions on the draft Police and Criminal Justice Data Protection Directive, available at the following link: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp201_en.pdf.
4. <http://www.europarl.europa.eu/news/en/news-room/content/20140307IPR38204/html/MEPs-tighten-up-rules-to-protect-personal-data-in-the-digital-era>.

5. <http://data.consilium.europa.eu/doc/document/ST-9565-2015-INIT/en/pdf>.
6. http://europa.eu/rapid/press-release_STATEMENT-15-5257_en.htm.
7. European Court of Justice, decision of May 13, 2014, case C-131/12 (*Google Spain*).
8. See Recital 21 of the Regulation, in the text approved by the Council on June 11, 2015.
9. http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2015/20150617_appendix_core_issues_plenary.pdf.
10. See article 14 of Legislative Decree of June 30, 2003, no. 196 (the Italian Data Protection Code).
11. Council of Europe, Recommendation CM/Rec(2010)13 of the Committee of Ministers to member states on the protection of individuals with regard to automatic processing of personal data in the context of profiling, November 23, 2010. See also the Article 29 Data Protection Working Party's "Advice Paper" on essential elements of a definition and a provision on profiling within the EU General Data Protection Regulation, adopted on May 13, 2013.
12. See Recital 58 of the Regulation.

Laura Liguori is among only five "most highly regarded individuals" in Information Technology in Europe by Who's Who Legal TMT 2015; during the past 20 years Laura has been focusing on all legal issues relating internet and e-commerce, data protection, consumer protection, advertising, IT and new technologies and digital media. In the field of data protection she works on profiling, use of cookies, big data, employee monitoring, whistleblowing hotlines, location-based services, cross border transfers of data, etc. Laura is a partner with Portolano Cavallo Studio Legale and a member of the Rome Bar Association (A-27003).

Federica DeSantis' practice focuses on intellectual property, consumer law, data protection, advertising, antitrust, e-commerce for a broad range of industries (fashion/luxury, etc.), new technologies and digital media. With particular respect to data protection, she advises clients on all aspects of European and Italian data protection law, including cross-border data transfers, location-based services, use of cookies, big data, profiling, employee monitoring, etc. In 2015 she obtained a PhD in Intellectual Property law from the University of Milan defending a dissertation on "Copyright and Appropriation Art." She is a research fellow at the Intellectual Property, Competition and Communications Institute of the LUISS Guido Carli in Rome. Federica joined the firm in 2010 after graduating cum laude from the school of law of LUISS Guido Carli in Rome and is a member of the Rome Bar Association (A-44230).

Parallel Lives: How Brazil and the United States Consider Leniency Agreements and Compliance Programs

By Adria Perez

In today's global environment, conduct in one country can potentially violate anti-corruption laws of more than one country. When faced with this possibly debilitating scenario, companies need to understand both the commonalities and differences between the anti-corruption laws and their implementation to avoid further increasing their exposure.

Recent international news has focused on the Brazilian government's corruption enforcement. Under the Brazilian civil law system, generally companies cannot be convicted of crimes. Almost two years ago, the Brazilian government promulgated the Brazilian Clean Company Act (the "Act"). The Act imposes civil or administrative liability on "legal persons," including companies, for conduct against the Brazilian or foreign governments, which includes promising, offering or giving, directly or indirectly, any "improper advantage" to a public official or a related third person.¹ Other articles have discussed the elements and penalties in Brazilian and U. S. anti-corruption laws, but little attention has been given to comparing how the two governments consider leniency agreements and corporate compliance or integrity programs. This article fills that gap.

Many similarities exist between the two countries with regard to leniency agreements and corporate compliance programs. The most overt difference is likely based on the differences between the common law and civil law legal systems. The Brazilian decrees and regulations outline the procedures and factors for entering into leniency agreements and the government's review of corporate compliance programs. The decrees and regulations appear definite and structured. What may be less clear is how the Brazilian government will follow them. On the other hand, the United States government has published principles and guidelines that appear less structured or definite. Again, how the government authority or court follows the principles and guidelines is key. When faced with a parallel investigation in both countries, the Brazilian regulations appear to provide more predictability or a "road map" to follow when a company is determining how to react to possible misconduct.

I. Leniency Agreements

Whether characterized as a "leniency agreement" as in Brazil or a deferred prosecution or non-prosecution agreement as in the United States, both governments consider self-reporting to be a necessary prerequisite for an agreement. The decision whether to disclose voluntarily a potential violation to a government authority is

difficult. One of my clients recently described voluntary disclosure as "calling an air strike" on oneself. Although self-reporting can be risky, there may be potential gain or at least an avenue to mitigate the exposure. In both countries, in order to enter into a leniency agreement (using the Brazilian term), the governments require a commitment from the company to cooperate and provide information about the misconduct.

The Brazilian regulations dedicate an entire chapter to leniency agreements. To obtain a leniency agreement, the company must:

1. "[B]e the first to state their interest in cooperating with the investigation of the specific injurious act;"²
2. Identify all other persons involved in the infringing conduct;³
3. Collect and provide information and documents concerning the conduct;⁴
4. Stop its involvement in the conduct on the day it proposes entering into a leniency agreement;⁵
5. Admit its participation in the conduct;⁶
6. "Fully and permanently" cooperate in the investigation and proceedings;⁷ and
7. Implement or enhance its compliance program.⁸

For companies, the first factor appears the most difficult. As previously mentioned, determining whether to disclose in order to seek leniency can be a challenging question even though the Brazilian Act does not require specific intent (it is strict liability) and prohibits facilitation or grease payments.⁹ Even more challenging is weighing *when* to disclose because there may be a competitor, employee or third party intermediary also seeking to benefit from self-reporting and the government may already know about the company's misconduct.

The benefit for a company disclosing in Brazil is that a leniency agreement can include a fine that is less than the regulated minimum value under the Act.¹⁰ Additionally, entering into a leniency agreement could prevent the:

1. Publication of the Brazilian authorities' decision to sanction the company;
2. Prohibition on receiving government funding, loans, donations, subsidies or incentives in the future; or

3. Imposition of civil sanctions delineated in other Brazilian statutes concerning government tenders and contracts.¹¹

The United States government does not provide a list of requirements for entering into an agreement when seeking leniency for a corruption offense. However, the Brazilian list above could persuade the United States government to enter into an agreement. When determining how to resolve a matter, such as whether to enter into an agreement, the United States Department of Justice (“DOJ”) and Securities and Exchange Commission (“SEC”) consider voluntary disclosure. With the disclosure, the United States government expects the company to cooperate by providing information and evidence as well as identifying the involved actors.¹²

In the United States, self-reporting and accepting responsibility may lead to a fine reduction under the Sentencing Guidelines.¹³ There is no requirement to be the first actor to disclose the misconduct. However, if a company becomes aware of the misconduct through its compliance program and “unreasonably” delays its disclosure to government authorities, the sentencing court may not allow the company to benefit from a reduction of its culpability score due to the ineffectiveness of the compliance program.¹⁴ Unlike in Brazil, a company cannot rely on government regulations to show why the United States government should consider a leniency agreement if the company satisfied the above Brazilian requirements list.

II. Compliance or “Integrity” Programs

Under the Brazilian regulations, the largest potential reduction of a fine under the Act occurs when the company maintains an integrity program with the certain characteristics that are outlined below. The use of a compliance program can reduce a fine between one and four percent.¹⁵ An effective compliance program could yield double in terms of a fine reduction than even voluntary disclosure, which has up to a two percent reduction.¹⁶ The potential reduction percentages show how the Brazilian government seeks to incentivize companies to implement effective compliance programs. In the United States, the Sentencing Guidelines that govern the sentencing of corporations consider the effectiveness of a company’s compliance program, which could potentially lead to a reduction in a monetary penalty.¹⁷

The Brazilian regulations describe an integrity program as a “set of mechanisms and internal procedures on integrity, auditability, and incentivized reporting of irregularities, as well as the effective application of codes of ethics and conduct, policies, and directives aimed at detecting and correcting deviations, fraudulent acts, irregularities, and illicit acts performed against the [Brazilian] government or a foreign government.”¹⁸ The regulations emphasize that the company must “constantly improve[] and adapt[]” the compliance program.¹⁹ The

United States government agrees that effective compliance programs are “dynamic and evol[ving].”²⁰ The Sentencing Guidelines further note that an effective compliance program responds to conduct by modifying the program to prevent future similar violations.²¹

The Brazilian regulations delineate the characteristics the Brazilian government will look for when considering the effectiveness of a compliance program, including:

1. “Tone at the top” commitment, such as the company’s senior management;
2. Code of conduct or ethics for company personnel and third parties, such as intermediaries and suppliers;
3. Training on the compliance program;
4. Risk analysis to determine how to modify and improve the compliance program;
5. Accurate books and records;
6. Specific policies or procedures to prevent fraud or illegal acts when the company engages with the public or government sector directly or indirectly through intermediaries;
7. Independent corporate body with authority that will review and enforce the compliance program;
8. Mechanism for employees and third parties to report issues as well as protection for whistleblowers;
9. Disciplinary action for violating the compliance program; and
10. Due diligence procedures for hiring third parties and before any mergers and acquisitions.²²

The Brazilian regulations provide that the Brazilian authorities, when evaluating the compliance program, will consider the company’s:

1. Size;
2. Corporate structure;
3. Use of third-party intermediaries;
4. Market sector;
5. Geography and operational footprint; and
6. Work with the public or government sector.²³

Additionally, the Brazilian authorities will review “the importance of government authorizations, licenses, and permits for [the company’s] operations.”²⁴ These factors are included in the “Profile Report” and “Program Conformity Report” forms that an April 2015 Brazilian regulation requires the Brazilian government to review when evaluating a company’s compliance program.²⁵ For both reports, the company must provide documentation

concerning the compliance program, which could include Board of Directors minutes, training presentations and participation statistics, documents concerning the use of any hotlines or reporting mechanisms and accounting records.

In the United States, a court may subtract up to three points from the company's culpability score if the offense occurred while a company maintained an effective compliance program that identifies and prevents misconduct and promotes an ethical and legally compliant corporate culture.²⁶ Cooperation in the investigation and acceptance of responsibility can lead to a two point reduction.²⁷ A reduction in the company's culpability score may reduce the company's fine.

Although the United States government does not provide requirements for corporate compliance programs or ask companies to complete reports, the DOJ and SEC's "Resource Guide to the U. S. Foreign Corrupt Practices Act" provides the "Hallmarks of Effective Compliance Programs." The hallmarks comprise the same characteristics that the Brazilian government lists in its regulations and reports, including:

1. Commitment from senior management and a clearly articulated policy against corruption;
2. Code of conduct and compliance policies and procedures;
3. Risk assessments;
4. Training and continuing advice;
5. Third-party due diligence;
6. Continuous improvement, such as periodic testing and review; and
7. Due diligence for mergers and acquisitions.²⁸

The Resource Guide further emphasizes the importance of providing:

1. Resources to the independent compliance department that oversees the program;
2. Incentives for those who report any issues; and
3. Resources toward any integration after a merger or acquisition.²⁹

There are similarities between what the two governments expect from an effective compliance program. Additionally, both governments provide incentives for maintaining an effective compliance program, including the potential reduction in fines if an offense occurs. The difference between the two governments lies in the more highly-structured Brazilian process as compared with the more subjective United States process. In Brazil, companies seeking the compliance program fine reduction are required to complete forms and submit evidence support-

ing the information about the programs. The submission of supporting information further stresses the importance of documenting a compliance program's features, effectiveness and improvement over time.

III. Conclusion

A company that is part of a parallel investigation in both Brazil and the United States has the option to seek a leniency agreement and persuade both governments to reduce the company's exposure due to the company's compliance program. Although Brazil appears to have implemented a more structured approach, few concrete differences appear when seeking leniency agreements and maintaining an effective compliance program.

The key is that a company operating or doing business in both countries needs a strong compliance program to detect and prevent misconduct. If the program detects wrongdoing, the company should consider disclosing the misconduct to both governments. This is especially so in Brazil because the Brazilian authorities provide a leniency agreement when the company is the first to convey its interest in cooperating with the investigation. If the company voluntarily discloses to the Brazilian government in order to obtain a leniency agreement, it may also need to disclose to the United States authorities.

Depending on the strength of the compliance program, the company may be able to obtain up to a four percent fine reduction under the Brazilian regulations. An effective compliance program could also result in a better resolution for the company with the United States government, especially if the company discloses the misconduct, which could lead to a deferred prosecution or non-prosecution agreement and possibly a fine reduction.

The above Brazilian requirements and United States recommended characteristics can help companies implement effective compliance programs that can prevent possible offenses and detect misconduct in time for the company to determine how best to mitigate the exposure in both countries.

Endnotes

1. Lei No. 12.846 [Clean Company Act], de 1 de Agosto de 2013, DIÁRIO OFICIAL DA UNIÃO [D.O.U.], capítulo II, art. 5(I) de 2.8.2013 (Braz.) [hereinafter Clean Company Act], available at https://www.cov.com/files/upload/E-Alert_Attachment_Brazilian_Clean_Companies_Act_Original.pdf.
2. Decreto No. 8.420, de 18 de Março de 2015, DIÁRIO OFICIAL DA UNIÃO [D.O.U.], capítulo III, art. 30 de 19.3.2015 (Braz.) (translated courtesy of Merrill Brink International at merrillbrink.com/fcpa-and-bribery-act-translation.html) [hereinafter Decreto No. 8.420].
3. *Id.* at capítulo III, art. 28(I).
4. *Id.* at capítulo III, art. 28(II) & 30(V).
5. *Id.* at capítulo III, art. 30(II).
6. *Id.* at capítulo III, art. 30(III).
7. *Id.* at capítulo III, art. 30(IV).

8. *Id.* at capítulo III, art. 37(IV).
9. Clean Company Act, *supra* note 1.
10. *Id.* at capítulo II, seção II, art. 20(II)(b).
11. Decreto No. 8.420, *supra* note 2, at capítulo III, art. 40(I-II) & (IV).
12. U.S. DEP'T OF JUSTICE & U.S. SEC. & EXCH. COMM'N, *A RESOURCE GUIDE TO THE U.S. FOREIGN CORRUPT PRACTICES ACT* 54-55 (2012), <http://www.justice.gov/sites/default/files/criminal-fraud/legacy/2015/01/16/guide.pdf>.
13. *Id.*
14. U.S. SENTENCING GUIDELINES MANUAL § 8C2.5(f)(2) (U.S. SENTENCING COMM'N 2014).
15. Decreto No. 8.420, *supra* note 2, at capítulo II, seção II, art. 18(V).
16. *Id.* at capítulo II, seção II, art. 18(IV) & (V).
17. U.S. SENTENCING GUIDELINES MANUAL, *supra* note 14, at § 8C 2.5(f)(1).
18. Decreto No. 8.420, *supra* note 2, at capítulo IV, art. 41.
19. *Id.*
20. U.S. DEP'T OF JUSTICE & U.S. SEC. & EXCH. COMM'N, *A RESOURCE GUIDE TO THE U.S. FOREIGN CORRUPT PRACTICES ACT*, *supra* note 12, at 56.
21. *Id.* at 54.
22. Decreto No. 8.420, *supra* note 2, at capítulo IV, art. 42 (I)-(XVI).
23. *Id.* at capítulo IV, art. 42 (XVI), para. 1, at VI.
24. *Id.*
25. Portaria No. 909, de 7 de Abril de 2015, DIÁRIO OFICIAL DA UNIÃO [D.O.U.] de 8.4.2015 (Braz.).
26. U.S. SENTENCING GUIDELINES MANUAL, *supra* note 14, at § 8C 2.5(f)(1).
27. *Id.* at § 8C 2.5(g)(2).
28. U.S. DEP'T OF JUSTICE & U.S. SEC. & EXCH. COMM'N, *A RESOURCE GUIDE TO THE U.S. FOREIGN CORRUPT PRACTICES ACT*, *supra* note 12, at 57-63.
29. *Id.*

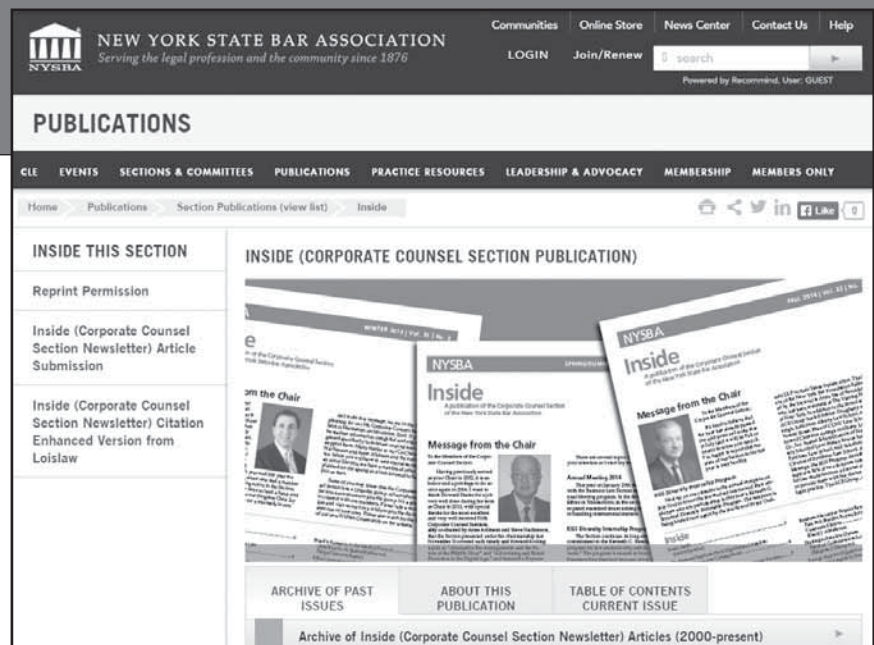
Adria Perez is a partner in Kilpatrick Townsend & Stockton LLP's Government Enforcement & Investigations team. She focuses her practice on representing both corporations and individuals in white collar criminal defense matters, government enforcement issues, as well as internal, criminal and SEC investigations. Her experience includes handling matters relating to the Foreign Corrupt Practices Act, False Claims Act (including government contracting, health care and tax matters), Civil Investigative Demands and export enforcement.

Inside (the Corporate Counsel Section Publication) is also available online

Including access to:

- Past Issues of *Inside* (2000-present)*
- *Inside* (2000-present) Searchable Index
- Searchable articles from *Inside* (2000-present) that include links to cites and statutes. This service is provided by Loislaw and is an exclusive Section member benefit*

*You must be a Corporate Counsel Section member and logged in to access. Need password assistance? Visit our Web site at www.nysba.org/pwhelp. For questions or log-in help, call (518) 463-3200.



Go to www.nysba.org/Inside


NEW YORK
STATE BAR
ASSOCIATION

Beyond Compliance: Inside Counsel Should Drive Sustainable Business

By John Wood

Introduction

This article takes as a starting point the Effective Compliance and Ethics Program (the “Compliance Program”) provisions of Chapter 8 of the 2011 Federal Sentencing Guidelines Manual.¹ Chapter 8 instructs courts how to punish organizations for wrongdoing, laying out factors that increase or decrease the punishment level when sentencing organizations for felony and Class A misdemeanors.² The Compliance Program may be the single most influential section of federal regulation for corporations in the modern era, to the extent that it provides the template for internal risk management protocols for organizations. However, it creates suboptimal incentives for a modern corporate ethics program in that it does not incentivize sustainable business practices. Inside counsel should strive to take corporate clients beyond mere compliance.

The Program

The Compliance Program was a response to the Sarbanes-Oxley Act of 2002, which directed the Sentencing Commission to establish guidelines “sufficient to deter and punish organizational criminal conduct.”³ The Compliance Program was “intended to achieve reasonable prevention and detection of criminal conduct for which the organization would be vicariously liable.”⁴ Chapter 8 enumerates the minimum required elements of an effective compliance program, which are mainly procedural and will not be recounted here.

Under the Compliance Program, the court reviewing corporate conduct should try to “order the organization to remedy any harm caused by the offense.”⁵ Notably, “the resources expended to remedy the harm should not be viewed as punishment, but rather as a means of making victims whole for the harm caused.”⁶ This indemnification provision is not meant to be the source of deterrence under the law. Victims of corporate misconduct deserve to be made whole.

Beyond compensation for harms, the court proceeds to determine the fine for deterrence purposes, based on the culpability of the organization and the seriousness of the offense. One of the mitigating factors used to determine the ultimate punishment of an organization in the event criminal conduct is discovered is the existence of an effective compliance and ethics program.⁷

The *Federal Sentencing Guidelines Manual* provides that companies promoting the adoption and implementation of corporate-wide effective compliance and ethics

program can enjoy reduced fines in the event they are levied for exposed wrongdoing. By laying out the ways fines are increased and decreased, the guidelines aim to create incentives for corporations to “self-police its own conduct through an effective compliance and ethics program.”⁸ According to the Director of the Office of Compliance Inspections and Examinations of Security Exchange Commission (the “SEC”), “a corporate culture that reinforces ethical behavior is a key component of effectively managing risk across the enterprise.”⁹

The Problem

There are three problems with the incentives created by the Compliance Program. First, it is an uninspired approach to corporate ethics. Second, the relationship between compliance and ethics is complicated and the two are not equal. What is legal is not always what is ethical. Third, it is not clear that inside counsel are prepared to lead ethical culture changes within organizations, as this is not the typical job description of inside counsel.

A problem with the Compliance Program’s ‘deter and punish’ approach to shoring up corporate compliance is that, “shooting for mere compliance is the equivalent of shooting for a C-.”¹⁰ At the end of the day, we are left with corporations adopting compliance and ethics programs aimed at avoiding punishment. The desire to avoid punishment is perhaps the least respectable reason for being virtuous.

Avoiding punishment in the form of a corporate fine is also not a very compelling incentive for *individuals* to behave ethically when acting as an agent of a corporation, because the individual is not liable for the damages. Recall, the Compliance Program applies to situations where the corporation is vicariously liable. As a result, the Compliance Program is not likely to create a culture of ethics within an organization, much less a company that could be described as socially or environmentally sustainable. Rather, the Compliance Program fosters a compliance culture meant primarily to “C.Y.A.”¹¹

Secondly, the Compliance Program’s attempt to inspire a culture of ethics that is not simply coterminous with legal compliance appears at odds with the traditional view of corporate responsibility espoused in Milton Friedman’s influential essay, “The Social Responsibility of Business Is to Increase Its Profits.” The Friedman view, perhaps shared by many corporate executives, is that the moral and social responsibility of a corporation ends with legal compliance. However, it is pretty clear to most

people that what is lawful is not always the same as what would fairly be characterized as ethical behavior.

“Legal” and “ethical” are not synonyms in popular usage, nor in the philosophical literature on law and ethics. Legal compliance “is not so much a recipe for success as it is a means of avoiding failure.”¹² The Compliance Program is oriented toward noncompliant firms and preventing bad conduct, not rewarding good conduct per se.

Lastly, it is not clear that inside counsel is expected, or blessed, to lead ethical cultural campaigns within organizations. The traditional law school curricula does not cover how to lead organizational change; it does not even cover applied business ethics. Most corporate counsel I have spoken to see themselves more as servants to executives than leaders or ethicists within an organization.

If fostering an effective culture of ethics is part of a legal compliance officer’s job description, inside counsel must take on a more active role in addressing normative issues within the realm of business strategy.

Going Beyond Mere Compliance

A sustainable business not only avoids risks to the enterprise, it also takes responsibility for, and eliminates, the risks created by the enterprise, which would otherwise be externalized onto the broader environment and stakeholder community. *Sustainable legal compliance* means “avoiding social and environmental harms that the law would otherwise permit by going beyond mere compliance.”¹³

It takes more than just the threat of punishment to make a thoroughgoing business case for corporate social responsibility and environmental stewardship. A sustainable enterprise does more than avoid punishment. The literature on sustainable business strategy is burgeoning and inside counsel should be familiar with this new paradigm for the role of corporations in modern life.

In-house counsel should strive to take their client “beyond mere compliance” with applicable laws because striving for mere compliance subjects a firm to risk. Going beyond mere compliance involves a different way of thinking about the role of in-house counsel.

Inside counsel must be comfortable expressing moral judgments beyond what promotes the most profit for a firm, or what promotes short-term tactical advantages for the firm. The chief legal officer should be the conscience of the corporate board, not just the advocate for the or-

ganization. Inside counsel should be leading discussions with corporate clients about going beyond mere compliance. Behaviorally, there is a big difference between striving for virtue and seeking to avoid punishment.

Conclusion

Inside counsel should learn how to help their organizations “get paid to do the right thing,” not just minimize punishment. Such a development would help transition compliance-related work from an ethically bankrupt “C.Y.A.” exercise into a value-adding strategic and long-term approach to achieving sustainable business performance with respect to social, economic, and environmental stakeholders. We as inside counsel should advise our corporate clients to aim higher than mere compliance.

Endnotes

1. United States Sentencing Commission, Guidelines Manual, §8B2.1 (Nov. 2014).
2. United States Sentencing Commission, Guidelines Manual, §8A1.1 (Nov. 2014).
3. Sarbanes-Oxley Act, § 805(a)(2)(5) (2002).
4. USSG §8B2.1, comment. (backg’d.).
5. USSG Ch.8, intro. comment.
6. *Id.*
7. *Id.*
8. *Id.*
9. Di Floria, C.V., *Speech by SEC Staff: The Role of Compliance and Ethics in Risk Management*, Office of Compliance Inspections and Examinations, NSCP National Meeting: U.S. Securities and Exchange Commission (October 17, 2011).
10. Fagan, B., *Regulatory Compliance Is Bad for the Environment, and It Could Also Be Bad for Business*, SW Studio, stormwatertools.com (2013) last accessed January 22, 2014.
11. This acronym means what you think it means.
12. John D. Wood, *THE ROLE OF LEGAL COMPLIANCE IN SUSTAINABLE SUPPLY CHAINS, OPERATIONS, AND MARKETING*, 14 (Business Expert Press, 2014).
13. John D. Wood, *THE ROLE OF LEGAL COMPLIANCE IN SUSTAINABLE SUPPLY CHAINS, OPERATIONS, AND MARKETING*, 4 (Business Expert Press, 2014).

John D. Wood, JD (NYU School of Law, ’11) is an attorney, author, scholar, and keynote speaker. He is the Founder/President of Econautics Sustainability Institute, a 501(c)(3) providing research, education, and advising on sustainable business strategy, including going beyond compliance. His corporate clients are in health care, manufacturing, nonprofit, and P&C insurance recovery.

Getting Issuers to Market: An Update

By Carol Spawn Desmond

Many practitioners who never knew they were securities lawyers (a group that not surprisingly includes in-house counsel) find themselves having to give advice in this field, often because of belated information from their client. Frequently, this results from the client's pressure to raise capital.

For many issuers, the JOBS Act¹ raised expectations of easing access to capital markets. Clients that want to raise capital in a private placement have found some promises of the JOBS Act remain unfulfilled. The uncertain status of these different avenues for unregistered offerings is matched by doubts about the ability to use unregistered finders or solicitors. This article briefly updates and explores these two market-access issues.

Background

The JOBS Act proposed expanding securities laws to provide new options for unregistered offerings. For many issuers, current private placement rules were insufficient, access to capital markets was constricted. As well, time and costs required to mount a public offering through registration was prohibitive for most small businesses.²

Testimony during the JOBS Act hearings referenced RocketHub and Kickstarter as models for market access.³ Among the hopes for the JOBS Act was to provide similar means for issuers to access a wider pool of investors and decrease costs to raise capital. Title II and Title III of the Jobs Act made this possible through general solicitation using Rule 506 private offerings and crowdfunding, respectively.⁴ Importantly, both titles offered the ability to raise capital through using the Internet, avoiding costs of using registered broker-dealers.⁵

Title II allowed general solicitation within a private placement framework. The restriction would occur only at time of sale: all purchasers must be accredited investors or qualified institutional buyers.⁶ Further to support general solicitation, the statute authorized "a platform or mechanism...online...or through any other means" ("506 platforms"), which issuers could use for "general solicitations, general advertisements, or similar or related activities."⁷ Because of the exemption from broker-dealer registration available to 506 platforms, issuers would presumably be able to widely broadcast information about these types of general solicitations, without incurring registered broker-dealer fees.⁸

Title III allowed for "crowdfunding" and the buzz of a pool of Internet-based offerees to help promote offerings, thereby lowering barriers to capital markets. Unlike 506 platforms under Title II, which issuers could use as another means to distribute offering materials, Title III

authorized crowdfunding "intermediaries" to manage issuers' pools of offerees. The intermediaries would be either registered brokers or "funding portals" (which would be exempt from broker-dealer registration).⁹

Titles II and III Today

General solicitation under Rule 506(c) became effective in July 2013,¹⁰ but remains under the consideration of the U.S. Securities and Exchange Commission (the "SEC"). The day it adopted Rule 506(c), the SEC proposed regulations to change that Rule. The proposals would require advance and more detailed filings, including written solicitation materials. To date, these have not been finalized.¹¹

In frequently asked questions ("FAQ"), the SEC took the position that Title II's prohibition on a 506 platform's "compensation in connection with the purchase or sale of such security" extends beyond transaction-based compensation. Instead, merely offering the services of operating a 506 platform (presumably even with other services) and receiving any pay violates the prohibition. The sole exclusion recognized is a 506 platform provider acting as a co-investor in the securities being offered—a role more appropriately played by venture capital funds.¹² That is unlikely company for many issuers who had hoped to use Rule 506(c), but who had counted on access to 506 platforms that were conduits open to the Internet and priced differently from registered broker-dealers.¹³

Crowdfunding under Title III is not yet possible. The SEC proposed regulations in late 2013, but they are not final.¹⁴

Revisiting Finders and Unregistered Broker-Dealers

Means of accessing capital might be less easy than hoped because of constraints on Titles II and inaction on Title III. Adding to that, the SEC has recently signaled an increased focus on the use of finders and solicitors that are not registered broker-dealers.¹⁵ The result could be further cost barriers to small issuers hoping to access the market.

For decades, issuers have relied on an analysis supporting use of unregistered "finders," and avoided transaction-based compensation except when the "finder's" involvement with an offeree is remote. Where there was more close engagement with offerees (personal communications, arranging meetings, etc.), issuers relying on that analysis should avoid payments tied to success.¹⁶ Current SEC actions have apparently eroded the ability to rely on this analysis, particularly for any transaction-based compensation.¹⁷ In 2013, a senior SEC official cautioned that

broker-dealer assessment was fact-based on activities, not simply how compensation was paid.¹⁸ These developments, together with the Title II FAQ mentioned above, suggest that issuers should review their “finder” arrangements. The potential costs of being wrong in relying on an unregistered broker-dealer can be high: costs of an enforcement action and possible rescission of the securities sale.¹⁹

Conclusion

Unfortunately, issuers face significant barriers to the market of potential investors, even using private placements. Costs to use current options, including general solicitation, might remain beyond a client’s reach. The vision of crowdfunding for securities sales has not—and possibly will never—meet desired expectations raised by the JOBS Act. At the least, however, making clients aware of potential issues and problems provides the information needed to better manage expectations.

Endnotes

1. The Jumpstart Our Business Startups Act, Pub. L. 112-106, 126 Stat. 306 [hereinafter the “JOBS Act”].
2. See, e.g., Doug Rand, *American Business Leaders Speak Out About the Jumpstart Our Business Startups (JOBS) Act*, WHITE HOUSE (Apr. 20, 2012, 3:35 PM), <https://www.whitehouse.gov/blog/2012/04/20/american-business-leaders-speak-out-about-jumpstart-our-business-startups-jobs-act>. In addition, to rely on some private placement rules to reach would-be investors, issuers must show pre-existing relationships. See *Use of Electronic Media*, Exchange Act Release No. 33-7856 (Apr. 28, 2000) (“pre-existing relationship” is one means to show proper reliance on Regulation D safe harbor).
3. See, e.g., The RocketHub Team, *RocketHub Testifies in Congress – JOBS Act & Crowdfunding*, ROCKETHUB (June 27, 2012), <http://blog.rockethub.com/post/46875577822/rockethub-testifies-in-congress-jobs-act-crow>.
4. See generally JOBS Act §§ 201, 301-305. The focus of this article is the Jobs Act proposals that embraced Internet access for issuers and offerings not requiring Securities and Exchange Commission (the “SEC”) filing and review processes. The information to be filed for Title III is not as detailed or comprehensive as in Titles I and IV. See *id.* § 302(b); see also JOBS Act §§ 101-108, 401-402.
5. See JOBS Act §§ 201(c), 304(b).
6. *Id.* § 201(a)(1), (2).
7. *Id.* § 201(c) (exempting platform providers from broker-dealer registration).
8. *Id.* 506 platform providers could not receive “compensation in connection with the purchase or sale of such security.”
9. *Id.* §§ 302(b), 304(a) (funding portal registration would be limited).
10. Eliminating the Prohibition Against General Solicitation and General Advertising in Rule 506 and Rule 144A Offerings, Exchange Act Release No. 33-9415 (July 10, 2013) (Rule 506(c) is codified at 17 CFR section 230.506(c). A parallel amendment was made to Rule 144A, permitting offers to persons other than qualified institutional buyers, so long as those others are not buyers.
11. Re-opening of Comment Period for Amendments to Regulation D, Form D and Rule 156, Exchange Act Release No. 33-9458 (Sept. 27, 2013).
12. See Jumpstart Our Business Startups Act Frequently Asked Questions About the Exemption from Broker-Dealer Registration in Title II of the JOBS Act, February 5, 2013, <http://www.sec.gov/divisions/marketreg/exemption-broker-dealer-registration-jobs-act-faq.htm>. Even paying employees’ salaries would violate this.
13. As recently as July 15, 2015, the SEC acknowledged small businesses are not able to use registered broker-dealers, given lower capital-raise yields. See *Advisory Committee on Small and Emerging Companies*, SEC (last modified July 16, 2015), <http://www.sec.gov/news/otherwebcasts/2015/advisory-committee-small-emerging-companies-071515.shtml>. While Rule 506(c) expands in use, the 506 platforms posting reports are registered broker-dealers. Without the SEC’s restrictions on those platforms, Rule 506(c) numbers might be higher.
14. Crowdfunding, Exchange Act Release No. 33-9470 (Oct. 23, 2013).
15. See 15 U.S.C. § 78o(a), (b) (unless otherwise exempt, persons acting as broker or dealer must register). There is no bright-line rule as to the actual activities entailed in being a broker or a dealer.
16. Compare Paul Anka, SEC No-Action Letter (available July 24, 1991) (permitted transaction-based pay for contacts list), with Brumberg, Mackey & Wall, PLC, SEC No-Action Letter (available May 17, 2010) (simple introduction to possibly interested people gave law firm “salesman’s stake,” coupled with transaction-based pay, made it broker-dealer).
17. Ranieri Partners LLC and Donald W. Phillips, Exchange Act Release No. 69091 (Mar. 8, 2013) (Order Instituting Administrative and Cease-and-Desist Proceedings) (communications with offerees beyond simple mailings, with transaction-based pay, indicated broker-dealer status); see also Brumberg, Mackey & Wall, PLC, SEC No-Action Letter (available May 17, 2010) (introduction limited to interested people gave law firm “salesman’s stake”).
18. See David W. Blass, Chief Counsel, Division of Trading & Markets, SEC, *A Few Observations in the Private Fund Space* (April 5, 2013), available at <http://www.sec.gov/news/speech/2013/spch040513dwg.htm> (the “Blass Speech”). The Blass speech also confirmed the FAQ position that even regular employees can be deemed unregistered broker-dealers.
19. *Id.* While beyond the scope of this article, it is important to note that each state has its own broker dealer rules requiring registration, which could have additional repercussions (in the event state law applied to the situation). For New York, however, as the New York State Bar Association has noted, Article 23-A of the General Business Law does not require registration of broker dealers, among others, in private offerings (if not intrastate). See The Committee on Securities Regulation of the New York State Bar Association, *Position Paper on Private Offering Exemptions & Exclusions*, N.Y.S.B. Ass’n, http://www.nysba.org/Sections/Business/Committees/Securities_Regulation_Committee/Position_Paper_on_Private_Offering_Exemptions_and_Exclusions.html.

Carol Spawn Desmond is a securities and finance attorney, practicing in capital markets and regulatory compliance here and abroad. Her clients include domestic and foreign advisers, investment companies, and technology companies. She is a member of the Securities Regulation Committee and Private Funds Subcommittee of NYSBA, and is a regular presenter for them and other groups on adviser and funds issues, and cybersecurity and technology topics.

Paradigm Shift? The SEC Intensifies Its Focus on Prevention of Retaliation Against Whistleblowers

By Gail Gottehrer

Introduction

While the monetary award that the U.S. Securities and Exchange Commission (the “Commission”) gave to the whistleblower in the case of *Paradigm Capital Management, Inc.*¹ was smaller than the monetary awards the Commission has given to whistleblowers in other cases, the significance of the case should not be underestimated. *Paradigm* is the first enforcement action brought by the Commission based, in part, on alleged retaliation against a whistleblower. The whistleblower, a Paradigm employee who informed the Commission about potential securities law violations by Paradigm and who, the Commission found, was subjected to retaliation by his employer after it learned of that report, received the maximum possible whistleblower award. Discussing the award, Commission Chair Mary Jo White explained that the Commission sees itself as the “whistleblower’s advocate” and will continue to make bringing retaliation cases a high priority for the Commission because “[s]trong enforcement of the anti-retaliation protections is critical to the success of the SEC’s whistleblower program.”²

The award in *Paradigm*, combined with recent statements by Chair White and others at the Commission, make clear that the Commission is focused on protecting whistleblowers from retaliation and that *Paradigm* is the first, and certainly not the last, case in which the Commission will aggressively enforce the anti-retaliation provisions of the Securities Exchange Act of 1934 (the “Exchange Act”). The award underscores the need for companies regulated by the Commission to ensure that their anti-retaliation policies and procedures are compliant and effective.

Commission Brings and Settles First Whistleblower Anti-Retaliation Action

On June 16, 2014, the Commission announced that it had accepted an offer of settlement from Paradigm, a hedge fund advisory firm registered with the Commission, and its owner, Candace King Weir, to resolve an anticipated action against them for alleged prohibited trading activity and retaliation against the employee who reported the misconduct to the Commission.³ The Commission concluded that Paradigm’s conduct towards the whistleblower constituted retaliation, in violation of Section 21F(h) of the Exchange Act, which prohibits an employer from taking an adverse employment action against a whistleblower—which includes discharging, demoting, suspending, threatening, harassing, or discriminating against that employee—because the whistleblower engaged in lawful conduct, such as reporting alleged securities law violations to the Commission.⁴

Paradigm Takes Adverse Employment Actions Against the Whistleblower

The whistleblower in *Paradigm* was the firm’s head trader during the time the alleged unlawful trades were made and at the time he provided information to the Commission. Approximately four months after he provided information about Paradigm to the Commission, the whistleblower informed Weir and others that he had made a whistleblower submission to the Commission and described the conduct he had reported. The whistleblower was permitted to return to his job at the trading desk and continued trading for the rest of the day. The following day, however, Paradigm removed him from the trading desk, relieved him of his supervisory responsibilities, moved him to a different office building and instructed him to prepare a report detailing the facts that supported the alleged violations he had reported to the Commission. Paradigm’s explanation for the change in the whistleblower’s job duties was that it had to investigate the whistleblower’s actions since he had executed some of the trades that he had reported to the Commission.⁵

Paradigm granted the whistleblower’s request to work from home while preparing the report. It denied him access, however, to trading and account systems to which he had previously had access and to his company email account. After the whistleblower completed the report and expressed his intention to report to work as head trader, Paradigm told him he could not do so because it was still evaluating the situation. A few days later, Paradigm told the whistleblower’s attorney that the whistleblower’s employment relationship with the company was “irreparably damaged.”⁶ The company and the whistleblower attempted, unsuccessfully, to reach a severance agreement that would include the whistleblower’s resignation or termination of employment, after which the whistleblower notified Paradigm that he was prepared to return to work as the head trader at the firm. Paradigm told him he could return to work, but that he could not work as the head trader until the firm had completed its investigation. Until that time, the whistleblower was told, his duties would be “meaningful and, to some extent, parallel or overlap those of head trader” and that Paradigm “need not explain further.”⁷

The whistleblower returned to work under the conditions set by Paradigm. Rather than sitting at the trading desk, the whistleblower was placed in an office on another floor. He was told that his “top priority” was to review more than 1,900 pages of hard-copy trading data, sorted by security, to identify any potential wrongdoing by Paradigm so it could investigate his claims. The whistleblower told Paradigm that generating electronic reports would be more

effective than reviewing paper documents and asked for access to the trading system to generate the necessary reports. Paradigm refused. The whistleblower then suggested that another Paradigm employee could generate the reports and was told by Paradigm that it could not identify the reports based on the description he had provided. The whistleblower subsequently reported to Paradigm that its trading-related compliance policies were deficient. Paradigm then instructed him to consolidate trading procedure manuals into a single document and suggest revisions to it.⁸

In addition, even though Paradigm had agreed to let the whistleblower use his personal email address while he was working from home and for future communications with Paradigm, after receiving a confidential report from the whistleblower's personal email address, the company took the position that the whistleblower had previously removed confidential business records from Paradigm using his personal email address. Paradigm reprimanded the whistleblower, accused him of violating company policies and the terms of his employment, and accused him of violating a confidentiality agreement he had signed when he began working at the company. A little more than a month after he informed Weir that he had provided information to the Commission, the whistleblower resigned from Paradigm.⁹

Commission Finds Paradigm's Actions Constitute Retaliation

Based on these findings, the Commission determined that Paradigm had taken adverse employment actions against the whistleblower—including demoting him from his job as head trader, assigning him to prepare a report about the conduct he had reported to the Commission, changing his job from head trader to a “full-time compliance assistant,” eliminating his supervisory responsibilities and “otherwise marginalizing him”—without a legitimate reason. Important to the Commission's analysis was the fact that Paradigm took these adverse actions immediately after it learned that the whistleblower had reported possible securities violations to the Commission.¹⁰ As part of the settlement, Paradigm and Weir were required to pay in excess of \$2.1 million in disgorgement, prejudgment interest and civil penalties; to retain an independent compliance consultant to review the company's policies and procedures; and to adopt all recommendations made by the consultant for changes to Paradigm's policies and procedures.¹¹

On April 28, 2015, the Commission granted the whistleblower the maximum whistleblower award payment—30% of the amounts collected in connection with the action. The whistleblower, who the Commission noted had “suffered unique hardships, including retaliation, as a result of reporting to the Commission,” received over \$600,000.¹² Acknowledging the “sacrifice” made by the whistleblower, Andrew Ceresney, Director of the Commission's Division of Enforcement, stated that “[t]he Enforce-

ment Division is committed to taking action when appropriate against companies and individuals that retaliate against whistleblowers.”¹³ Describing retaliation against whistleblowers as “entirely unacceptable,” Sean McKessy, Chief of the Commission's Office of the Whistleblower, expressed his hope that the Commission's “demonstrated commitment” to protect whistleblowers from retaliation and to make “significant financial awards” to whistleblowers who are victims of retaliation encourages potential whistleblowers to come forward.¹⁴

Takeaways

The *Paradigm* case reminds companies of the importance of assessing and refining their compliance policies and practices on an ongoing basis. Companies are well served by having clear policies that encourage employees to report potential violations of the securities laws (and other laws) internally and procedures that give employees confidence that if they make such reports, the information they provide will be promptly investigated by an objective party, and the company will protect them from retaliation and any other negative consequences. Equally important is for companies to impress upon their employees—through policies, procedures and training—what whistleblowing is and that it is protected by law, as well as what retaliation against whistleblowers is and that it will not be tolerated.

Endnotes

1. Paradigm Capital Mgmt., Inc. and Candace King Weir, Exchange Act Release No. 72393, 2014 WL 2704311 (June 16, 2014).
2. Mary Jo White, Chair, SEC, Ray Garrett, Jr., The SEC as the Whistleblower's Advocate (Apr. 30, 2015), available at <http://www.sec.gov/news/speech/chair-white-remarks-at-garrett-institute.html>.
3. Press Release, SEC, No. 2014-118, SEC Charges Hedge Fund Adviser with Conducting Conflicted Transactions and Retaliating Against Whistleblower (June 16, 2014), available at <http://www.sec.gov/News/PressRelease/Detail/PressRelease/1370542096307>.
4. Paradigm Capital Mgmt., Inc. and Candace King Weir, Exchange Act Release No. 72393, 2014 WL 2704311, ¶ 42 (June 16, 2014).
5. *Id.* ¶¶ 23-27.
6. *Id.* ¶¶ 28-31.
7. *Id.* ¶¶ 32-34.
8. *Id.* ¶¶ 35-37.
9. *Id.* ¶¶ 38, 39, 41.
10. *Id.* ¶¶ 40.
11. *Id.* ¶¶ 45, 51-55, pt. IV.C.
12. Press Release SEC No. 2015-75, SEC Announces Award to Whistleblower in the First Retaliation Case (Apr. 28, 2015), available at <http://www.sec.gov/news/pressrelease/2015-75.html>.
13. *Id.*
14. *Id.*

Gail Gottehrer's practice focuses on class action defense, management-side labor and employment litigation, and other complex commercial matters, including privacy and technology litigation, digital workplace-related actions and cybersecurity. She is one of the few defense lawyers to have been involved in the successful trial of a class action to verdict before a jury.

ERISA: An Overview

By Lilah Loughran

The Employee Retirement Income Security Act of 1974 (“ERISA”)¹ is a federal law that sets standards for private retirement, health and other welfare benefit plans. The U.S. Department of Labor (“DOL”) is responsible for the interpretation and enforcement of ERISA. Among other things, ERISA provides that those individuals who manage plans (and other fiduciaries) must meet certain standards of conduct. The law also contains detailed provisions for reporting to the government and disclosure to participants. There also are provisions aimed at assuring that plan funds are protected and that participants who qualify receive their benefits.

The two most common ERISA-covered retirement plans are: (1) defined contribution (e.g., 401(k), 403(b), profit sharing, etc.) and (2) defined benefit or “pension” plans. However, Individual Retirement Accounts (“IRAs”) are governed by the Internal Revenue Code of 1986, as amended (the “IRC”). IRAs are retail brokerage accounts that allow individuals to save for retirement with tax-free growth or on a tax-deferred basis. IRAs are governed by the IRC, which has many analogous provisions to ERISA, including the definition of fiduciary and the prohibited transaction rules.

Being a Fiduciary

ERISA does not require any employer to establish a plan. It only requires that those who establish plans must meet certain minimum standards, such as acting in a fiduciary capacity. A person is considered a fiduciary regarding a plan if he/she is exercising any discretionary authority or discretionary control with respect to the management of such plan or exercises any authority or control with respect to the management or disposition of its assets. Additionally, if a person is rendering investment advice for a fee or other compensation, direct or indirect, with respect to any moneys or other property of such plan, then such person is also a fiduciary.

There is a difference between offering investment advice and investment education. A person is considered a fiduciary by providing investment advice but is not considered a fiduciary by providing investment education. Both terms are defined by the DOL. Investment advice is defined as a recommendation that relates to the value of securities or other property or the advisability of investing in securities or other property, is rendered on a regular basis, pursuant to a mutual understanding that it will serve as a primary basis for investment decisions and is individualized based on the needs of the plan and/or participant. By contrast, investment education includes plan information, general financial and invest-

ment information, asset allocation models and interactive investment materials.

Fiduciary “Duties”

ERISA requires a fiduciary to act under several “duties”:

- **Duty of Care**—Fiduciaries must act with the care, skill, prudence and diligence under the circumstances that a prudent person, acting in a similar capacity and familiar with such matters, would use. The analysis focuses on the procedures used in making an investment decision (not the result). There is a flexible standard that corresponds to the complexity of the investment decisions involved and fiduciaries must give “appropriate consideration” to relevant facts. This includes risk of loss and opportunities for gain and the diversification of the ERISA plan’s assets, suitability of the investment in light of the ERISA plan’s size, anticipated liabilities, cash flow needs and investment objectives.
- **Duty of Loyalty**—A fiduciary must discharge its duties on behalf of a plan solely in the interests of plan participants and beneficiaries, and for the exclusive purpose of providing benefits and defraying reasonable expenses of administering the plan. A fiduciary is generally prohibited from causing a plan to engage in a transaction with a party in interest, and may not take any action, when its judgment may give rise to a conflict of interest.
- **Diversification**—A fiduciary must diversify plan investments so as to minimize the risk of large losses unless, under the circumstances, it is clearly prudent not to do so. Evaluations of diversification generally take into account the underlying investments held by a pooled investment vehicle in which a plan invests. To the extent a fiduciary manages a fund or account subject to ERISA (rather than the assets of an entire plan), the requirement to diversify investments extends only to the fund or account that the fiduciary manages, and not to the assets of the entire plan.
- **Compliance With Plan Documents**—A fiduciary must act in accordance with the documents governing the Plan to the extent that the documents are consistent with ERISA. If a fiduciary believes the documents governing the Plan are not consistent with ERISA, the fiduciary should undertake to amend the documents as necessary.

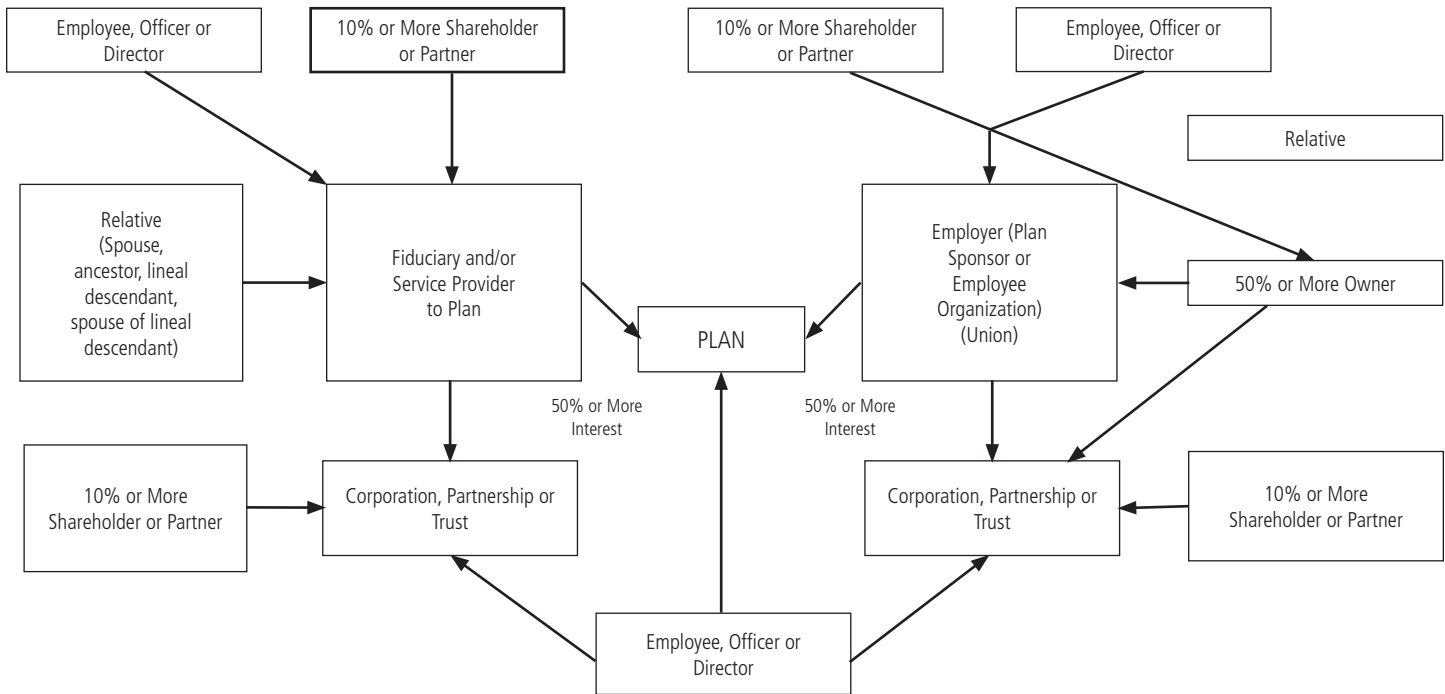
Prohibited Transactions

ERISA prohibits most transactions between an ERISA plan and a “party in interest” unless an exemption applies. Without an exemption, virtually every financial transaction and service, including direct and indirect sales or exchanges, loans or extensions of credit, transfers of plan property and the provision of investment management, custodial and brokerage services, is prohibited under ERISA. The ERISA rules generally do not determine whether any particular transaction is appropriate for an ERISA plan. This will be governed by the investment guidelines for the applicable mandate. The definition of “party in interest” is very broad:

- An exemption under Section 408(b)(17) of ERISA, which is more commonly known as the “Service Provider Exemption”;
- PTE 91-38, which is more commonly known as the “Bank Collective Trust Exemption,” or
- An exemption under Section 408(b)(2) of ERISA, which is more commonly known as the “Necessary Services Exemption.”

Proposed DOL Fiduciary Rule

In 2010, the DOL proposed a change to the definition of “investment advice” that would have expanded the



ERISA’s self-dealing prohibited transaction rules generally prohibit a fiduciary from dealing with the assets of a plan for the fiduciary’s own benefit, representing a party whose interests are adverse to a plan in a transaction and receiving consideration for the fiduciary’s own account in connection with a transaction involving a plan. The DOL interprets these prohibitions broadly and these rules often prevent certain transactions that might otherwise be beneficial for an asset manager’s clients.

ERISA exemptions

As noted above, ERISA generally prohibits a plan from entering into direct or indirect transactions with a party in interest to the plan absent an exemption. There are certain exemptions that are most commonly used in order to participate in these types of transactions, such as:

- Prohibited Transaction Class Exemption (“PTE”) 84-14, which is more commonly known as the “QPAM Exemption”;

scope of those who become fiduciaries to 401(k) plans and IRA providers. After significant objections were raised by numerous groups, including Members of Congress from both parties, the DOL withdrew its initial proposal and stated it would conduct further economic analysis. In February 2015, President Obama announced that the DOL should move forward with its proposed rulemaking. On April 14, 2015, the DOL announced a re-proposal of the rule. In May 2015, the DOL granted a 15-day extension to the original 75-day comment period, resulting in a total of 90 days for public comment, which ended July 21, 2015.

Under the DOL’s New Proposal on ERISA Fiduciary Status for Investment Advisers, a person will be providing “investment advice” if that person provides (i) an investment recommendation, investment manager recommendation, an appraisal of investments or a recommendation of persons to provide investment advice and (ii) renders such advice pursuant to a written or verbal agreement, arrangement, or understanding that the ad-

vice is individualized, or that such advice is specifically directed to the advice recipient for consideration in making investment or management decisions with respect to securities or other property of the plan or IRA. A recommendation is defined broadly to include any communication that would be reasonably viewed as a suggestion to engage in or refrain from taking a particular course of action. Notably, the “mutual agreement,” “primary basis,” and “regular basis” prongs of the current investment advice definition have been removed. The impact of this re-proposal would transform many current non-fiduciary discussions in the brokerage industry into “investment advice,” thereby causing the fees and compensation resulting from any transactions in connection with those discussions to be prohibited.

Accordingly, the DOL also proposed a new exemption called the best interest contract exemption (“BICE”), which would provide relief to the prohibited transaction rules for the receipt of compensation by investment advice fiduciaries and their affiliated financial institutions for services provided in connection with the purchase, sale, or holding of certain investments by participants and beneficiaries, IRAs, and certain plans with fewer than 100 participants (retirement investors).

BICE is designed to address the issue that the receipt by a fiduciary adviser (or financial institution) of certain types of compensation from a plan (such as a commission) or from third parties (such as 12b-1 fees, revenue sharing, sales loads, etc.) would typically violate the ERISA prohibited transaction restrictions against self-dealing because the amount or when such compensation is received by the fiduciary adviser would be affected by the advice the fiduciary adviser provides. In order to rely on the BICE, there is a best interest standard of care that must be provided to IRAs and small plans as well as contractual, disclosure and operational requirements, a permitted asset list, and specific rules on compensation.

The financial services industry is challenging the DOL’s proposal and asserting that such drastic reform would not be in the best interest of retirement investors. Self-regulatory agencies, such as Financial Industry Regulatory Authority, Inc. (“FINRA”) and the SEC, have vocalized their view that the proposed rule dismisses suitability as a proper standard of care for broker dealers. The proposal does

not contemplate potential SEC rules and the FINRA arbitration system for regulating broker dealers and investment advisors. In order to work together with the DOL and the SEC on an implementable standard, the DOL should have included in its proposal some type of substituted compliance mechanism, in which compliance with an SEC fiduciary standard would satisfy the DOL rules. However, the proposal’s current view will deny investors a choice in products, services, and financial professionals.

Endnote

1. 29 USC 1001, *et seq.*

Lilah Loughran is a Vice President, Private Banking Compliance Officer with Credit Suisse. She has been in compliance within the financial industry for 15 years. Lilah started her tenure with Prudential Securities for three years followed by five years with Lehman Brothers. She moved to the banking side with Sumitomo Mitsui Banking Corporation and then returned to broker-dealer services at Macquarie Capital for three years. Lilah has been with Credit Suisse since 2013 as a Compliance Coverage Officer and ERISA contact for the Private Banking Branches, as well as maintaining related Policies and Training.

Follow NYSBA on Twitter

visit www.twitter.com/nysba
and click the link to follow us and
stay up-to-date on the latest news
from the Association

NYSBA

Changing Rules: The National Labor Relations Board Speaks

By Nancy B. Schess and Jesse Grasty

You run a small company. One day, your Human Resources manager notices two unhappy employees deep in conversation around the coffee machine. That night, her Facebook feed lights up with posts between those same employees about how much they dislike their jobs and their difficult manager. Firm in your convictions that such behavior cannot be tolerated, you call both employees into your office the next day and terminate their employment. Unfortunately, your next meeting with these employees may be in connection with the charge they file at the National Labor Relations Board (“NLRB” or the “Board”).

The National Labor Relations Act (“NLRA” or the “Act”) prohibits employers from having a policy or practice that prohibits, or which an employee may *reasonably construe* as prohibiting, concerted activity protected under Section 7 of the Act.¹ Concerted activity occurs when two employees act together, one employee solicits the other, or one employee takes action on a matter of common concern, regarding a protected subject matter (*i.e.*, wages, hours, working conditions or other terms and conditions of employment).

Interpreting the scope of Section 7, over the past several years a particularly active NLRB has drawn into question previously ordinary employer policies making for a complex compliance scenario. In an effort to clarify and consolidate the Board’s evolving positions, on March 18, 2015, the General Counsel of the NLRB issued a detailed memorandum summarizing types of employer rules that would be considered unlawful because employees could reasonably believe those rules would chill their Section 7 rights: Memorandum GC 15-04 from Richard F. Griffin, Jr., General Counsel, to All Regional Directors, Officers-in-Charge, and Resident Officers on Report of the General Counsel Regarding Concerning Employer Rules, (March 18, 2015) (the “GC Memo”). The report’s conclusions may be surprising—and particularly since these rules apply whether the workplace is unionized or not.²

Consider some of the types of previously standard clauses that are under scrutiny.

Confidentiality

Employers commonly seek to restrict the disclosure and use of confidential information both in handbooks and employment agreements. Under current Board precedent, the issue is whether the restriction is too broad. Any iteration that may reasonably be read as prohibiting employees from discussing information connected to

their wages, hours, benefits, or working conditions will be found to be in violation of the Act.

Broad provisions prohibiting employees from discussing “work matters” or defining confidential information to include “all information...” are problematic.³ Lawful provisions are carefully tailored so that the description of protected information is really the essence of the business, such as trade secrets and customer/client information, and ideally, provide sufficient examples of information covered by the prohibition to make it clear that protected communications are not covered.⁴

Employee Conduct Toward the Employer and Non-Disparagement Rules

A policy that imposes discipline when an employee is rude and disrespectful towards management is no longer safe. According to the GC Memo, for example, a rule that requires that employees “[B]e respectful to the company, other employees, customers, partners and competitors” is problematic because it could reasonably be interpreted to prohibit criticism of the company and management.⁵

Non-disparagement provisions that prohibit public criticism of employers violate the Act. Consequently, employer policies or agreements prohibiting communications that negatively reflect on the employer could be unlawful.⁶

Even a policy that prohibits “false and defamatory statements” can be problematic since false and defamatory speech is still protected.⁷ Maliciously false statements, however, are not protected and consequently a policy that prohibits this type of speech will not be considered to be overbroad.⁸

Restrictions on Leaving Work

Employers frequently have policies restricting when an employee can leave work. Section 7, however, protects the employees’ right to strike. Consequently, policies that could reasonably be construed to prohibit an employee from walking off the job will be considered overbroad and violative of the NLRA.⁹ Employers must be careful about using any language about “work stoppage” or “walking off the job” in an employee handbook. These are triggers for NLRB consideration.

Social Media Policies

The NLRB has been very vocal about employer policies that could reasonably be construed as prohibiting em-

employees from discussing the terms and conditions of their employment on social media. The crux of these decisions is that if conduct would be protected in the physical world, then it is also protected in the virtual world.

For example, in two cases decided within days of each other, broad social media policies restricting employees from posting comments about their employer were found to violate the Act.¹⁰ In particular, the Board was concerned that the policies in question had failed to: (a) identify the specific types of information employees could not post; (b) distinguish between what employees could not post and protected speech; and (c) provide examples.¹¹

In *Hoot Winc, LLC* (“*Hooters*”),¹² the company fired an employee for “posting disparaging comments about co-workers and managers on social media,” in violation of the company’s rule against “insubordination to a manager or lack of respect and cooperation with fellow employees or guest.” Following the rationale described above with respect to non-disparagement, the ALJ found that this rule with respect to conduct on social media could be construed as limiting employees’ right to engage in concerted activity because it did not adequately define “insubordination,” “lack of respect” or “cooperation.” The ALJ was also concerned that the rule lacked limiting language, such as describing what would constitute “uncooperative conduct.”

In *Hooters* and then in *Laurus Technical Institute*,¹³ the Board held that policies broadly restricting employees from using social media in ways that damage the company’s goodwill or may create problems within the company violate the Act. However, in *Landry’s Inc.*,¹⁴ the ALJ upheld the company’s policy, which “urge[d] all employees not to post information regarding the Company, their jobs, or other employees which could lead to morale issues in the workplace or detrimentally affect the Company’s business” and went on provide examples of how to meet this goal.¹⁵

Personal Email Usage

In late 2014, the NLRB issued a landmark opinion. In *Purple Commc’ns, Inc.*,¹⁶ the Board held that “employee use of email for statutorily protected communications on nonworking time must presumptively be permitted by employers who have chosen to give employees access to their email systems.” Thus, employers are no longer permitted to have broad prohibitions of personal use of their email systems.

Purple Commc’ns represents a reversal of the Board’s 2007 decision in *Register Guard*.¹⁷ *Guard Publishing Co. v. NLRB*, 571 F.3d 53 (D.C. Cir. 2009), which held that employees do *not* have a right to use their employers’ email systems for Section 7 purposes. In overturning *Register Guard*, the Board explained that “[i]n many workplaces, email has effectively become a ‘natural gathering place,’

pervasively used for employee-to-employee conversations.”¹⁸ The Board further explained that “email’s effectiveness as a mechanism for quickly sharing information and views *increases* its importance to employee communication.”¹⁹

Employers may still restrict or prohibit the use of email if they can establish “special circumstances,” such as system overload, the nature of the business and excessive cost, where such a restriction is necessary to “maintain production and discipline.” However, the Board explained that “it will be the rare case where special circumstances justify a total ban on nonwork email use by employees,” and an employer seeking to meet its burden “must demonstrate the connection between the interests it asserts and the restriction.”²⁰

The Board did, however, uphold employers’ right to monitor employees’ email communications “so long as the employer does nothing out of the ordinary, such as increasing its monitoring during an organizational campaign or focusing its monitoring efforts on protected conduct or union activists.”²¹

Conclusion and Recommendations

What is clear at this juncture is that the NLRB continues to look critically at once routine employer policies and consequently, the compliance landscape is rapidly changing. The boundaries of lawful and unlawful rules move with regularity.

In light of the GC Memo and evolving Board decisions, employers would be wise to study their employee handbooks and employment agreements to ensure that they are crafted to conform to NLRB interpretations. Some narrowing of provisions and clarifying their intent will likely be required.

In addition, employers should consider adding specific disclaimers wherever appropriate, stating that policies are not intended to interfere with employees’ Section 7 rights. While these “safe harbor” disclaimers do not guarantee that the NLRB will find the underlying provisions to be compliant, it will be helpful to argue that employees could not reasonably believe that their rights to engage in Section 7, protected activity were restricted. Last, employers should actively train their supervisors with respect to employees’ Section 7 rights and the appropriate enforcement of employer policies.

While the landscape continues to evolve, so much has already changed that failing to adapt now could be a dangerous choice.

Endnotes

1. “Employees shall have the right to self-organization, to form, join or assist labor organizations, to bargain collectively through representatives of their own choosing, and to engage in *other concerted activities* for the purpose of collective bargaining or *other*

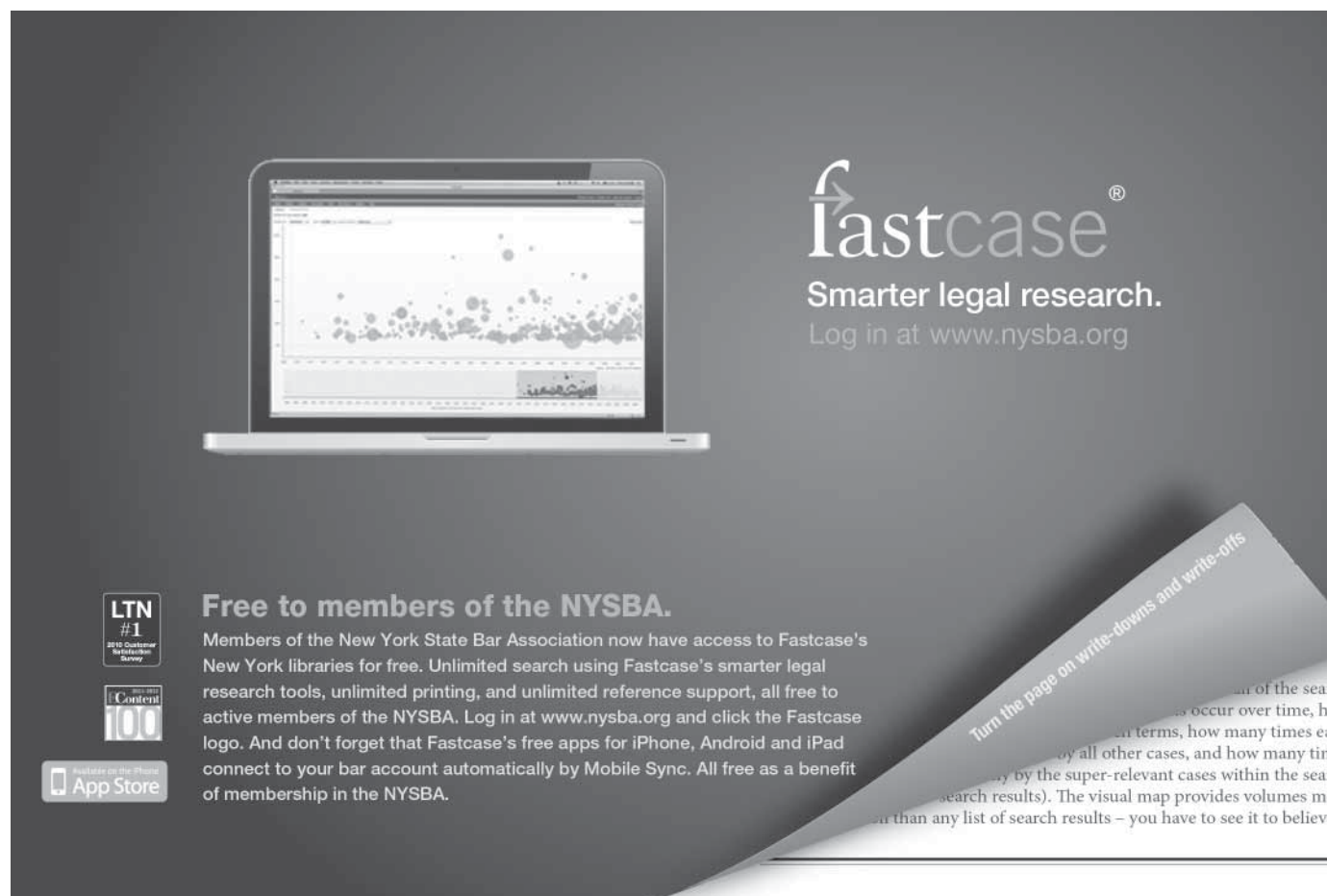
mutual aid or protection...." 29 U.S.C. §157 (2006) (emphasis added). Section 8(a)(1) states that it is an unfair labor practice "for an employer to interfere with, restrain, or coerce employees in the exercise of the rights guaranteed in section 157 of this title." 29 U.S.C. §158(a)(1)(2006).

2. Supervisors are excluded from the definition of "employee" under the NLRA and, therefore, these rules do not apply to supervisors meeting the definition under the Act. 29 U.S.C. §152(3) (1935).
3. GC Memo, pp. 4-5.
4. GC Memo, p. 6.
5. GC Memo, p. 7; see *Casino San Pablo*, 361 N.L.R.B. No. 148, 3 (December 16, 2014).
6. GC Memo, pp. 7-8 (citing *Quicken Loans, Inc. & Lydia E. Garza*, 361 NLRB No. 94 (Nov. 3, 2014)).
7. *Id.*
8. GC Memo, p. 7 (citing *Casino San Pablo*, 361 N.L.R.B., at 4).
9. See GC Memo, p.17 (citing *Purple Commc'ns, Inc.*, 361 N.L.R.B. No. 43, 2 (Sept. 24, 2014)).
10. *Durham School Servs. L.P.*, 360 N.L.R.B. No. 85 (Apr. 25, 2014); *Lily Transp. Corp. & Robert Suchar*, 01-CA-108618 (2014), 2014 WL 1620731.
11. In *Lily*, the ALJ also determined that a social media policy that contains an overly broad summary of a confidentiality policy,

without a specific reference to the full confidentiality policy, violates the Act, even if the full confidentiality policy is compliant.

12. 199 L.R.R.M. (BNA) 1567 (N.L.R.B. May 19, 2014).
13. 360 N.L.R.B. No. 133 (June 13, 2014).
14. 199 L.R.R.M. (BNA) 2103 (N.L.R.B. June 26, 2014).
15. *Id.* at 5.
16. 361 N.L.R.B. No. 126 (Dec. 11, 2014).
17. 351 N.L.R.B. 1110 (2007), *enforced in relevant part and remanded sub nom. Guard Publ'g Co. v. NLRB*, 571 F.3d 53 (D.C. Cir. 2009).
18. *Guard Publishing v. NLRB*, 571 F.3d 53 (D.C. Cir. 2009).
19. *Id.* at 33-34 (emphasis in original).
20. *Id.* at 62, 63.
21. *Id.* at 68.

Nancy B. Schess, Esq. is a partner, and Jesse Grasty, Esq. is an associate, in the firm of Klein Zelman Rothermel Jacobs & Schess LLP. Klein Zelman is a boutique firm representing employers in labor and employment law.



fastcase®
Smarter legal research.
Log in at www.nysba.org

Free to members of the NYSBA.
Members of the New York State Bar Association now have access to Fastcase's New York libraries for free. Unlimited search using Fastcase's smarter legal research tools, unlimited printing, and unlimited reference support, all free to active members of the NYSBA. Log in at www.nysba.org and click the Fastcase logo. And don't forget that Fastcase's free apps for iPhone, Android and iPad connect to your bar account automatically by Mobile Sync. All free as a benefit of membership in the NYSBA.

LTN #1
2014 Customer Satisfaction Survey

Content 100

Available on the iPhone App Store

Turn the page on write-downs and write-ups

...of the search
...occur over time, ho
...terms, how many times eac
...by all other cases, and how many time
...by the super-relevant cases within the searc
...search results). The visual map provides volumes mo
...than any list of search results – you have to see it to believe

From the NYSBA Book Store

Section
Members get
20%
discount*
with coupon code
PUB8145N

Entertainment Law

Fourth Edition



"The definitive text in the burgeoning field of entertainment law. It provides an in-depth analysis of the key issues currently confronting the practitioners of its various specialties. For both its breadth and depth, I highly recommend Entertainment Law to students, academics and professionals alike."

"This is a must for anyone who is seriously involved in the entertainment business."

EDITOR-IN-CHIEF

Howard Siegel, Esq.

PRODUCT INFO AND PRICES

2013 / 986 pp.,
looseleaf / PN: 40862

NYSBA Members	\$140
Non-members	\$175

Order multiple titles to take advantage of our low flat rate shipping charge of \$5.95 per order, regardless of the number of items shipped. \$5.95 shipping and handling offer applies to orders shipped within the continental U.S. Shipping and handling charges for orders shipped outside the continental U.S. will be based on destination and added to your total.

*Discount good until November 30, 2015

Entertainment Law, Fourth Edition, updates and expands the coverage of the previous edition, including the historical changes in the music industry, and features a new chapter on Exhibitions.

Edited by Howard Siegel, Esq., this book's 10 chapters cover the principal areas of entertainment law, including the Recorded Music Industry, Music Publishing, Television, Film, Commercial Theater, Book Publishing, Minors' Contracts, Personal Management, and Exhibitions.

The authors, from the New York, California and Nevada Bars, are some of the most successful entertainment law practitioners in the country.

Get the Information Edge

NEW YORK STATE BAR ASSOCIATION

1.800.582.2452 www.nysba.org/pubs Mention Code: PUB8145N





Finding Bliss

By Deborah Epstein Henry, Suzie Scanlon Rabinowitz and
Garry A. Berger

Reviewed by Janice Handler

Finding Bliss is subtitled “Innovative Legal Models for Happy Clients and Happy Lawyers.” As a professional cynic and someone who was never all that happy in any iteration of my legal career (which included a Wall Street law firm, Corporate General Counsel, SEC enforcement attorney, law professor and legal editor), I tended to doubt. Using the words “bliss” and “lawyer” in the same sentence sounded like an oxymoron to me.

OK, turns out that Bliss is a play on words alluding to Bliss Lawyers, a secondment firm that places lawyers in in-house positions and, of which, all the authors are principals. After starting with some personal memoirs of the authors’ individual roads to bliss, the book then explores alternatives galore to the billable hour, the law firm associate path, and corporate law department staffing. Not surprisingly, these paths to bliss often lead back to Bliss and the principle of secondment.

The authors begin by discussing their own legal careers, which began conventionally with judicial clerkships and large law firms, then veered to less traditional paths. Driven by women’s issues, work /life balance, and family responsibilities, the authors tried consulting, pro bono and virtual law practice before teaming up to form Bliss Lawyers, a firm combining secondment practice with a virtual law firm. From that platform, they explored innovative ways to provide more effective legal services by focusing on these key concepts:

- (1) Innovation,
- (2) Value,
- (3) Predictability and Trust,
- (4) Flexibility,
- (5) Talent Development,
- (6) Diversity and Inclusion, and
- (7) Relationship Building.

The book then focuses on each of these concepts, which the authors characterize as the means to maximize the talent pool’s performance and delivery of legal services. This discussion explores such questions as:

- How does innovation create new legal models?

- How do legal service providers offer more value to clients?
- How are multiple valued career paths for lawyers fashioned?
- How are services provided more flexibly?
- How is legal talent developed and supported?
- How are diverse and inclusive work environments created?

To answer these questions, the authors describe many alternative arrangements in the provision and pricing of legal services, many of which come back to secondment. In the chapter on Innovation, for example, the book extols the virtues of secondment and virtual firms, separately, but best all, jointly (while conceding that theirs is the only firm they know of that combines both). Secondment firms, they say, typically charge 1/3 to 1/2 of large law firms, and a virtual platform further reduces overhead and real estate costs, attracting high caliber talent while delivering cost savings to clients.

Similarly, the chapter on flexibility touts secondment firms as meeting the increasing need of in-house legal departments to bring in high caliber lawyers for temporary engagements without having long-term responsibility for these lawyers. Such assignments give in-house legal departments both economic and risk-sharing benefits. In discussing “Diversity and Inclusion,” the book praises the role of secondment in breaking through unconscious biases and promoting diversity in the workplace.

While there is nothing wrong with the authors liking and promoting what they do, a more interesting chapter for me was that on “Value,” which discusses alternatives for the traditional law firm billable hour and associate career trajectory. As someone who never wanted to be an entrepreneurial anything and who left a Wall Street law firm in less than a year, I read with interest of the newer career paths available today. In discussing “Value,” the authors point out the disconnect that exists between the traditional associate to partner path and the path many young lawyers desire—one that does not include the risks of equity partnership, the need to constantly pitch new business, and the 24/7 commitment to the business. They then discuss valued career alternatives for those who

are not reaching for the brass-ring, which include: non-equity partnerships, senior counsel positions and staff attorney slots. These paths for well credentialed young lawyers seeking to do interesting work without the responsibilities associated with partnership may make it easier for law firms to attract, retain and promote diverse talent (especially if there is flexibility in moving amongst these paths within the firm). Indeed, if such options had existed when I was a young associate, I might still be a private practitioner. (Doubt it!)

Finding Bliss is strongest as an encyclopedic compendium of every imaginable alternative in the provision and pricing of legal services, the training and development of legal providers and the structuring of career paths and workplace arrangements. It is at its weakest in the suggestion that this gets us to bliss.

Speaking as an ex-law school professor who left the profession because of the students' hysterical pre-occupation with grades and jobs, I feel this book overlooks over-riding societal and structural issues in the legal profession which are not solved by a re-arranging of deck chairs. The underlying construct—since the 60s, at least when I went to school—that more is better—more law schools, more students, more lawyers and that society

can only benefit from all of the above, needs to be challenged. It is time to ask what impact the medical malpractice system has had on the provision of caring cost-effective health care and whether the tort system has been hijacked by the greedy. It is time to question whether more law schools, more lawyers, more regulation and more litigation leads to any kind of bliss—personal, professional, or societal. This book does not address these issues.

Nor does it address the evolution in ethical and professional standards from the concept of law as a noble profession to the model of law as a business. In fact, by presenting so many of its suggestions in marketing terms, this book seems to fully embrace the business model.

In failing to address these fundamental issues, this book does not get this reader to bliss. However, while the profession awaits resolution of the bigger issues, the issues that this book does address, i.e., telecommuting, temporary opportunities, flexible work schedules, expanded career options and added value to clients, are not without benefit to lawyer and client alike.

Janice Handler is the former editor of *Inside* and retired General Counsel of Elizabeth Arden.

**Looking for Past Issues
of the
Corporate Counsel
Section Publication
Inside?**

<http://www.nysba.org/Inside>



Structuring for Success: Effective Compliance and Ethics Program Organization

By Rebecca Walker and Jeffrey M. Kaplan

Where compliance and ethics (“C&E”) programs should reside—in the legal department, as a separate function, or elsewhere—is a topic of continuous debate amongst C&E practitioners. Unfortunately, many C&E professionals have a fixed view on this question, leaving little room for genuine debate, which is that a wholly separate function is always the best (and for some, the only effective) structure. However, in our combined 40 years of practice in this field, we have seen some truly excellent C&E programs housed in law, internal audit and finance departments. In our view, the key to program effectiveness—regardless of where the program is housed—is maintaining an adequate level of independence and authority for the C&E function. We explore below:

- how organizations can create and maintain the level of authority and independence necessary for an effective C&E program;
- the advantages and disadvantages of housing a program in the legal department (still the most common program structure); and
- the value of charters and other documentation to developing and maintaining effective programs.

Authority and Independence

In order for a C&E program to function effectively, the C&E officer must possess the authority to, among other things:

- 1) understand and assess the organization’s C&E risks;
- 2) weigh in on company strategies and business practices;
- 3) help to ensure that the company’s policies, procedures and other aspects of its C&E program are adequate in light of its risks;
- 4) require employees to undergo C&E training;
- 5) take other steps to communicate company standards and policies, including through promulgation and dissemination of a code of business conduct and other appropriate policies;
- 6) weigh in on promotions (at least for key positions);
- 7) audit and monitor C&E controls (or have input into such auditing and monitoring by other functions);
- 8) escalate serious allegations of misconduct or other concerns to senior leadership and the board of directors, as necessary;

- 9) investigate allegations of misconduct, including having the ability to access any relevant company records or other evidence and to speak with any relevant employees or directors; and

- 10) help to ensure that discipline for violations is meted out in a way that adequately promotes ethical and law-abiding behavior at the company.

Independence from the business and other functions is also important in carrying out the above tasks, as independence permits the C&E function to audit, monitor, escalate and investigate the business and other functions more effectively. Attaining adequate authority and independence can be challenging, of course, but there are a few practices that can help make those two program attributes attainable regardless of where the C&E program is situated.

First, active board oversight of the C&E program, including unfettered access to the board by the C&E officer, is critical to both program authority and independence. Board oversight in this context contemplates both (1) the C&E officer’s ability to provide unfettered reports to the board regarding the C&E program on a periodic basis (e.g., quarterly) and (2) the C&E officer’s ability to escalate reports of suspected misconduct to the board, as appropriate. The importance of unfettered access to the board is discussed in several different legal standards. First, the Federal Sentencing Guidelines for Organizations—perhaps the most important of all official C&E-program-related standards in the U.S.—emphasize the importance of having the person with operational responsibility for a program provide reports to the board, including reporting regarding allegations of misconduct and periodic reporting on program implementation. Similarly, the Department of Justice and Securities and Exchange Commission’s *Resource Guide to the Foreign Corrupt Practices Act*; states that the compliance officer of an organization should possess adequate autonomy from management, and specifies that such autonomy generally includes direct access to an organization’s governing authority, such as the board of directors or a committee of the board of directors (e.g., the audit committee).¹ Meetings in executive session between the C&E officer and the board are another important means of enhancing program independence and authority. Yet another is a requirement that the duties or compensation of the C&E officer may not be diminished without prior approval of the board or a board committee.

Genuine C&E oversight of those employees who have important C&E-related duties is also important to the level of independence and authority of the program. Many C&E programs rely extensively on leveraging other functions (such as legal, internal audit, and human resources), and

on individuals in the businesses and other functions who have been assigned part-time responsibility for C&E. If C&E does not possess some means of exerting genuine oversight over such individuals (e.g., weighing in on performance evaluations), there can be a negative impact on effectiveness. And, if these individuals report solely to the businesses or functions for which they are performing the C&E role, their level of independence (with respect to the relevant business or function) may be compromised.

Advantages and Disadvantages of Housing C&E Within the Legal Department

While, as noted above, there is a perennial debate within the C&E community regarding the appropriateness of housing C&E in the legal department, a large number of programs continue to be located within the legal function. There are numerous advantages to such a structure, including that many of the activities of the C&E function are closely aligned with, and can, in most organizations, be effectively conducted by, the legal function, including compliance risk assessment; conducting due diligence on third parties; receiving reports of suspected misconduct; conducting investigations; and some forms of monitoring and auditing.

In addition, at many organizations, placing C&E within the ambit of the legal department enhances the level of authority and independence (from the businesses and all functions other than legal) of the C&E program. That is particularly true when a law department has a lot of “clout” in a company. Whether housing the C&E program within the legal department will enhance the authority and independence of the program is a function, in part, of the perception of the law department at the organization. Thus, while aligning these functions can enhance the program, it can also (depending on the particular organization) have the converse effect. If combining the functions has the impact of sidelining the C&E department or diminishing the credibility of the program, then the functions should be separated.

Another potential disadvantage of housing C&E within legal is that it can potentially create an actual or apparent conflict because of C&E’s role in serving as a check on the business and other functions. It is important, in considering this question, to consider whether the legal department is itself a foreseeable source of risk to the company—and hence would benefit from the “checks” that could be performed by C&E as a separate department. (Note that this determination will often depend on the industry a company is in—it is obviously not intended to be an occasion for considering whether an individual general counsel is law abiding.)

C&E Program Charters

C&E program charters or similar governance documentation can be important tools for helping to maintain the independence and authority of a C&E program. C&E

program charters typically document roles played by various individuals in the program, including both members of the C&E department and individuals in other functions that provide key support for the program (such as law, audit, human resources and procurement). They also set forth and describe the various components of the program, including, e.g., the C&E risk assessment process, C&E training and communications, and reporting and investigation procedures.

Having such documentation offers a number of practical benefits. Charters help ensure that key players know what their duties are; prevent turf battles; help demonstrate to employees and others how serious the company is about compliance; and provide a basis for program audits and assessments, as well as board oversight. They can also be useful if a company needs to “prove” its program in the context of litigation or a government investigation. Charters can and should be reviewed and approved by senior leaders and the board as a means of program oversight. And, perhaps most importantly, charters can help maintain the independence and authority of a program by documenting program structure and critical activities that create independence and authority, such as the reporting relationship of the C&E officer, including access of the C&E officer to the board.

Conclusion

While C&E has made great strides in recent years, many organizations continue to grapple with the question of how best to structure their programs. We hope that the suggestions in this article will help some companies in dealing with this complex and consequential issue.

Endnote

1. While the Resource Guide specifically discusses compliance with the Foreign Corrupt Practices Act, the extensive discussion of effective compliance programs is helpful guidance for any type of C&E program. (Available at <http://www.justice.gov/criminal-fraud/fcpa-guidance>.) Recent deferred prosecution agreements and corporate integrity agreements similarly highlight the importance of having the person with responsibility for the program report to the board. For example, in the deferred prosecution agreement between the Department of Justice and Total, S.A., entered into in 2013, Total agreed to assign responsibility for oversight of the anti-corruption compliance program to one or more senior corporate executives who have direct reporting obligations to independent monitoring bodies, including internal audit and the Board of Directors or any appropriate committee of the Board.

Rebecca Walker and Jeff Kaplan are partners in the law firm of Kaplan & Walker LLP, a law firm located in Santa Monica, California and Princeton, NJ, whose practice is devoted solely to compliance and ethics matters. Jeff Kaplan is co-editor of *Compliance Programs and the Corporate Sentencing Guidelines: Preventing Criminal and Civil Liability* (West 1993), and Rebecca Walker is the author of *Conflicts of Interest in Business and the Professions: Law and Compliance* (West 2005). Ms. Walker and Mr. Kaplan are also co-chairs of the Practicing Law Institute’s Compliance and Ethics Institutes.



THE NATIONAL ACADEMY OF DISTINGUISHED NEUTRALS

NEW YORK CHAPTER

www.NYMEDIATORS.ORG

NAME	BASED IN	PHONE	CALENDAR	NAME	BASED IN	PHONE	CALENDAR
David J. Abeshouse	Uniondale	(516) 229-2360	<input checked="" type="checkbox"/>	Irwin Kahn	New York	(212) 227-8075	
Prof. Harold I. Abramson	Central Islip	(631) 761-7110		Jean Kalicki	New York	(202) 942-6155	
Simeon H. Baum	New York	(212) 355-6527	<input checked="" type="checkbox"/>	Harold A. Kurland	Rochester	(585) 454-0717	<input checked="" type="checkbox"/>
Leona Beane	New York	(212) 608-0919	<input checked="" type="checkbox"/>	Lela Porter Love	New York	(212) 790-0365	<input checked="" type="checkbox"/>
David M. Brodsky	New York	(212) 906-1628	<input checked="" type="checkbox"/>	Richard Lutringer	New York	(917) 830-7966	<input checked="" type="checkbox"/>
William J.T. Brown	New York	(212) 989-2475		Robert E. Margulies	New York	(201) 207-6256	<input checked="" type="checkbox"/>
Mark J. Bunim	New York	(212) 683-0083		Michael Menard	Hamburg	(716) 649-4053	<input checked="" type="checkbox"/>
Steven Certilman	New York	(212) 956-3425	<input checked="" type="checkbox"/>	Peter Michaelson	New York	(212) 535-0010	
Douglas S. Coppola	Buffalo	(716) 852-4100	<input checked="" type="checkbox"/>	Charles J. Moxley Jr	New York	(212) 329-8553	<input checked="" type="checkbox"/>
Gail R. Davis	New York	(646) 246-8043		Phillip O'Neill	New York	(212) 308-4411	
Jacquelin F. Drucker	New York	(212) 688-3819	<input checked="" type="checkbox"/>	Shelley Rossoff Olsen	New York	(212) 607-2710	
Howard S. Ellen	New York	(516) 222-0888		Lawrence W. Pollack	New York	(212) 607-2792	
Eugene I. Farber	White Plains	(914) 761-9400		Ruth D. Raisfeld	New York	(914) 722-6006	<input checked="" type="checkbox"/>
Alfred Felio	New York	(212) 763-6802	<input checked="" type="checkbox"/>	Richard H. Silberberg	New York	(212) 415-9231	<input checked="" type="checkbox"/>
Ronnie Bernon Gallina	New York	(212) 607-2754		David C. Singer	New York	(212) 415-9262	<input checked="" type="checkbox"/>
David Geronemus	New York	(212) 607-2787		Steven Skulnik	New York	(646) 231-3457	<input checked="" type="checkbox"/>
Eugene S. Ginsberg	Garden City	(516) 746-9307	<input checked="" type="checkbox"/>	Norman Solovay	New York	(646) 278-4295	<input checked="" type="checkbox"/>
Krista Gottlieb	Buffalo	(716) 218-2188	<input checked="" type="checkbox"/>	Hon. Joseph P. Spinola	New York	(212) 967-6799	<input checked="" type="checkbox"/>
George L. Graff	Briarcliff Man.	(914) 502-2552		Stephen S. Strick	New York	(212) 227-2844	
Richard F. Griffin	Buffalo	(716) 845-6000		Edna Sussman	New York	(212) 213-2173	<input checked="" type="checkbox"/>
James E. Hacker	Albany	(518) 783-3843	<input checked="" type="checkbox"/>	Irene C. Warshauer	New York	(212) 695-1004	<input checked="" type="checkbox"/>
A. Rene Hollyer	New York	(212) 706-0248	<input checked="" type="checkbox"/>	Hon. Leonard Weiss	Albany	(518) 447-3200	<input checked="" type="checkbox"/>
David R. Homer	Albany	(518) 649-1999	<input checked="" type="checkbox"/>	Peter H. Woodin	New York	(212) 607-2761	
Hon. Allen Hurkin-Torres	New York	(212) 607-2785		Michael D. Young	New York	(212) 607-2789	



Check preferred available dates or
schedule appointments online
directly with the state's top neutrals

Visit www.NYMediators.org/quicksearch

This free web service funded by our New York members

The National Academy of Distinguished Neutrals is an invitation-only professional association of over 900 litigator-rated mediators & arbitrators throughout the US and Neutral Database Partner to the national trial bar (AAJ) & defense bar (DRI). For more info, please visit www.NADN.org/about

(paid advertisement)

Corporate Counsel Section Committee Chairpersons

CLE and Meetings

Steven G. Nachimson
Compass Group USA, Inc.
3 International Drive, 2nd Floor
Rye Brook, NY 10573
steven.nachimson@compass-usa.com

Howard S. Shafer
Shafer Glazer LLP
125 Maiden Lane, Room 16AB
New York, NY 10038-4949
hshafer@shaferglazer.com

Diversity

David S. Rothenberg
Goldman Sachs Family Office
The Ayco Company L.P.
200 West Street, 40th Floor
New York, NY 10282
david.rothenberg@gs.com

INSIDE/Publications

Jessica D. Thaler
410 Benedict Ave.
Tarrytown, NY 10591
jthaleresq@gmail.com

Elizabeth Jean Champnoi
Stout Risius Ross, Inc. (SRR)
120 West 45th Street, Suite 2800
New York, NY 10036
eshampnoi@srr.com

Membership

Thomas A. Reed
1172 Park Ave., Suite 15 C
New York, NY 10128
tareed1943@gmail.com

Joy D. Echer
Foot Locker, Inc.
Law Department
112 West 34th Street
New York, NY 10120
jecher@footlocker.com

Jana Springer Behe
NYSTEC
540 Broadway, 3rd Floor
Albany, NY 12207-2708
behe@nystec.com

Pro Bono

Steven R. Schoenfeld
DelBello Donnellan Weingarten Wise
& Wiederkehr, LLP
One North Lexington Avenue, 11th Fl.
White Plains, NY 10601
SRS@ddw-law.com

Technology and New Media

Fawn M. Horvath
Macy's, Inc.
11 Penn Plaza, 11th Floor
New York, NY 10001
fawn.horvath@macys.com

Natalie Sulimani
Sulimani & Nahoum P.C.
116 West 23rd Street, Suite 500
New York, NY 10011
natalie@sulimanilawfirm.com

Hanging on by a thread?

You are not alone. When life has you frazzled, call the New York State Bar Association's Lawyer Assistance Program.

We can help.

Unmanaged stress can lead to problems such as substance abuse and depression.

NYSBA's LAP offers free, confidential help and has been a trusted resource for thousands of attorneys, judges and law students since 1990. All LAP services are confidential and protected under Section 499 of the Judiciary Law.

Call 1.800.255.0569

NEW YORK STATE BAR ASSOCIATION
LAWYER ASSISTANCE PROGRAM

www.nysba.org/lap
nysbalap@hushmail.com



From the NYSBA Book Store



Business/Corporate and Banking Law Practice



PRODUCT INFO AND PRICES*

2014-2015 / 886 pp., softbound
PN: 405194

NYSBA Members	\$120
Non-members	\$135

Order multiple titles to take advantage of our low flat rate shipping charge of \$5.95 per order, regardless of the number of items shipped. \$5.95 shipping and handling offer applies to orders shipped within the continental U.S. Shipping and handling charges for orders shipped outside the continental U.S. will be based on destination and added to your total.

*Discount good until November 30, 2015

Authors

Michele A. Santucci, Esq.

Attorney at Law, Niskayuna, NY

Professor Leona Beane

Professor Emeritus at Baruch College and Attorney at Law, New York, NY

Richard V. D'Alessandro, Esq.

Richard V. D'Alessandro Professional Corporation, Albany, NY

Professor Ronald David Greenberg

Larchmont, NY

Thomas O. Rice, Esq.

Attorney at Law, Garden City, NY

This practice guide covers corporate and partnership law, buying and selling a small business, the tax implications of forming a corporation and banking law practice. It covers many issues including the best form of business entity for clients and complicated tax implications of various business entities.

Updated case and statutory references and numerous forms following each section, along with the practice guides and table of authorities, make this edition of *Business/Corporate and Banking Law Practice* a must-have introductory reference.

The 2014–2015 release is current through the 2014 New York legislative session and is even more valuable with the inclusion of **Forms on CD**.

Get the Information Edge

NEW YORK STATE BAR ASSOCIATION

1.800.582.2452 www.nysba.org/pubs

Mention Code: PUB8157N





NEW YORK STATE BAR ASSOCIATION
CORPORATE COUNSEL SECTION
One Elk Street, Albany, New York 12207-1002

ADDRESS SERVICE REQUESTED

PRST STD
U.S. POSTAGE
PAID
ALBANY, N.Y.
PERMIT NO. 155



Inside is a publication of the Corporate Counsel Section of the New York State Bar Association. Members of the Section receive a subscription to the publication without charge. Each article in this publication represents the author's viewpoint and not that of the Editors, Section Officers or Section. The accuracy of the sources used and the cases, statutes, rules, legislation and other references cited is the responsibility of the respective authors.

Accommodations for Persons with Disabilities:

NYSBA welcomes participation by individuals with disabilities. NYSBA is committed to complying with all applicable laws that prohibit discrimination against individuals on the basis of disability in the full and equal enjoyment of its goods, services, programs, activities, facilities, privileges, advantages, or accommodations. To request auxiliary aids or services or if you have any questions regarding accessibility, please contact the Bar Center at (518) 463-3200.

© 2015 by the New York State Bar Association.
ISSN 0736-0150 (print) 1933-8597 (online)

Inside

Section Officers

Chairperson

Natalie Sulimani
Sulimani & Nahoum P.C.
116 West 23rd Street, Suite 500
New York, NY 10011
natalie@sulimanilawfirm.com

Chairperson-Elect

Jeffrey P. Laner
77-10 34th Avenue
Jackson Heights, NY 11372
jlaneresq@nyc.rr.com

Vice-Chairperson

Joy D. Echer
Foot Locker, Inc.
Law Department
112 West 34th Street
New York, NY 10120
jecher@footlocker.com

Treasurer

Jeffrey P. Laner
77-10 34th Avenue
Jackson Heights, NY 11372
jlaneresq@nyc.rr.com

Secretary

Yamicha Stephenson
Deloitte
1633 Broadway
New York, NY 10019
yamicha.stephenson@gmail.com