

NY Business Law Journal



A publication of the Business Law Section
of the New York State Bar Association



Inside

- Email: Ethics and Security
- Cybersecurity
- The Active Response Continuum
- Banking Law
- Recent Employment Laws
- The Loser Pays Rule
- Can Bad Legal Precedent Just Be Wished Away?
- Benefit Corporations and Certified B Corporations

From the NYSBA Book Store



Business/Corporate and Banking Law Practice



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

PRODUCT INFO AND PRICES

2014-2015 / 912 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 February 13, 2015.

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, makes 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: PUB2864N



NY BUSINESS LAW JOURNAL

Winter 2014

Vol. 18, No. 2

THE BUSINESS LAW SECTION
NEW YORK STATE BAR ASSOCIATION

in cooperation with

NEW YORK LAW SCHOOL

© 2014 New York State Bar Association
ISSN 1521-7183 (print) ISSN 1933-8562 (online)

Business Law Section Officers

Chair	James William Everett, Jr. P.O. Box 7303 Albany, NY 12224 everettlaw@juno.com
First Vice-Chair	David W. Oppenheim Greenberg Traurig LLP 200 Park Avenue New York, NY 10166 oppenheimd@gtlaw.com
Second Vice-Chair..... and Fiscal Officer	Howard Dicker Weil, Gotshal & Manges LLP 767 Fifth Avenue New York, NY 10153 howard.dicker@weil.com
Secretary.....	Sarah E. Gold Gold Law Firm 1843 Central Avenue #187 Albany, NY 12205 sg@goldlawny.com

Business Law Section Committees

	Chair
Banking Law	Kathleen A. Scott Fulbright & Jaworski LLP 666 Fifth Avenue New York, NY 10103-3198 Kathleen.scott@nortonrosefulbright.com
Bankruptcy Law	Scott H. Bernstein McCarter & English, LLP Four Gateway Center 100 Mulberry Street Newark, NJ 07102 sbernstein@mccarter.com
Corporations Law	Richard De Rose Houlihan Lokey 245 Park Avenue New York, NY 10167-0002 rderose@hl.com

Derivatives and Structured Products Law	Ilene K. Froom Jones Day 222 East 41st Street, 4th Floor New York, NY 10017 ifroom@jonesday.com
Franchise, Distribution and Licensing Law	Richard L. Rosen The Richard L. Rosen Law Firm, PLLC 110 East 59th Street, 23rd Floor New York, NY 10022 rlr@rosenlawpllc.com
Legislative Affairs	Thomas M. Pitegoff LeClairRyan 885 Third Avenue, 16th Floor New York, NY 10022 Tom.Pitegoff@leclairryan.com
Membership	Sarah E. Gold Gold Law Firm 1843 Central Avenue #187 Albany, NY 12205 sg@goldlawny.com
Not-For-Profit Corporations	Frederick G. Attea Phillips Lytle LLP One Canalside 125 Main Street Buffalo, NY 14203-2887 fattea@phillipslytle.com
Public Utility Law	Bruce V. Miller Cullen & Dykman LLP 100 Quentin Roosevelt Blvd Garden City, NY 11530-4850 bmiller@cullenanddykman.com
Securities Regulation	Peter W. LaVigne Goodwin Procter LLP 620 Eighth Avenue The New York Times Building New York, NY 10018 plavigne@goodwinprocter.com
Technology and Venture Law	Shalom Leaf Shalom Leaf, PC 600 Madison Avenue, 22nd Floor New York, NY 10022 sleaf@leaflegal.com

NY BUSINESS LAW JOURNAL

Editor-in-Chief

David L. Glass, Division Director, Macquarie Group Ltd., New York City

Managing Editor

James D. Redwood, Professor of Law, Albany Law School

Editorial Advisory Board

Chair

Professor Ronald H. Filler,
Director, Center on Financial Services Law, New York Law School

Advisor Emeritus

Stuart B. Newman, Salon Marrow Dyckman Newman & Broudy LLP

Members

Frederick G. Attea, Phillips Lytle LLP
Adjunct Professor David L. Glass, Macquarie Group Ltd.
Richard E. Gutman, Exxon Mobil Corporation
Guy P. Lander, Carter Ledyard & Milburn LLP
Howard Meyers, Visiting Professor and Associate Director
of the Center on Business Law & Policy,
New York Law School
Raymond Seitz, Phillips Lytle LLP
Houman Shadab, Associate Professor, New York Law School
C. Evan Stewart, Cohen & Gresser LLP
Clifford S. Weber, Hinman Howard & Kattell, LLP

Lead Research Assistant

Alexis Kim

Research Assistants

Kaytlin Iapocce
Michelle Miltner
Jeffrey Pritchard
Breanna Staffon
Paul Williamson

Table of Contents

	Page
HeadNotes (David L. Glass)	6
Lawyers and Email: Ethical and Security Considerations (Scott Aurnou)	9
Cybersecurity: A New Approach Is Necessary (Jennifer Juste)	12
What Is Active Response Continuum, and What Does It Cover?..... (Wesley Paisley)	14
Banking Law Update..... (Sabra M. Baum)	23
Recent Employment Laws Impacting Private Employers in New York (Sharon Parella and Leah Ramos)	29
Inside the Courts (Prepared by Attorneys at Skadden, Arps, Slate, Meacher & Flom, LLP)	33
America's Tweak to the Loser Pays Rule: A Board-Insulating Mechanism?..... (Nithya Narayanan)	45
Squaring the Circle: Can Bad Legal Precedent Just Be Wished Away? (C. Evan Stewart)	49
Benefit Corporations and Certified B Corporations: Hybrid Corporate Options for Entrepreneurs and Socially Enterprising Business Owners Forming For-Profit Companies (Aaron Boyajian)	54
Committee Reports	57

HeadNotes

New York's highest court has (finally) handed a significant victory to the much-maligned banking community and its counsel. In a decision on a question certified to it by the Second Circuit Court of Appeals, the New York Court of Appeals has confirmed, to paraphrase Mark Twain, that reports of the death of the "separate entity" rule, which historically has applied to New York branches of foreign banks, have been greatly exaggerated. While a bank's branches, including those in different jurisdictions, are part of the parent bank for most purposes, historically U.S. branches of foreign banks—which predominantly are located in New York—have been treated as separate entities for certain specific purposes. Under New York law foreign bank branches are "ringfenced"—walled off from the parent—to protect New York depositors and creditors if the branch becomes insolvent. However, in the 2009 case *Koehler v. Bank of Bermuda*, the New York Court of Appeals held that a judgment creditor could enforce a judgment against assets of the debtor held by a foreign bank against the bank's New York branch—even though none of the assets in question were held in New York. Although it did not directly address the separate entity rule, *Koehler* called into question whether the doctrine had, in fact, been overruled.

The Court's October 2014 holding in *Motorola Credit Corp. v. Standard Chartered Bank* clarified that it had not. In the *Motorola* case the plaintiff, a judgment creditor, obtained a freeze order and served restraining notices pursuant to New York CPLR § 5222 on the New York branch of Standard Chartered Bank (SCB), a non-U.S. bank. Although SCB had no assets of the judgment debtor at its New York branch, a search revealed that its United Arab Emirates branch held about \$30 million in assets belonging to the debtor. SCB froze the \$30 million, but the UAE Central Bank took the view that SCB was not permitted to dishonor its obligation to repay the debtor's UAE deposits based on an order originating from a non-UAE court, and debited \$30 million from SCB's account with it.

Faced with the potential of double liability under U.S. and UAE law, SCB requested relief from the freeze order. The bank argued that the restraining notice served on its New York branch was ineffective as to the assets held in the UAE branch under New York's separate entity rule. The creditor argued that the separate entity rule had been overruled in *Koehler*. This was the question certified to the New York Court of Appeals. Noting that the separate entity rule was based in New York common law dating from early in the last century, the Court identified three principal policy reasons for maintaining the separate entity rule: first, as a matter of international comity; second, to protect banks from unfair financial and regulatory repercussions abroad and eliminate the potential for double liability; and third, that directing banks to process freeze

orders with respect to foreign assets would impose an "intolerable burden" by requiring them to identify and monitor assets in potentially numerous foreign branches. An important factor was that computer systems at New York branches generally do not allow them to access account information at head office or branches outside the United States. Finally, and perhaps most significantly, the Court noted that the separate entity doctrine had been an important stimulus to foreign banks opening branches in New York in the first place, and thus was vital to the State's "status as the preeminent commercial and financial nerve center of the Nation and the world."



Expressing scorn for the separate entity rule as a relic from an earlier age, however, the dissent in the 5-2 decision pointed to the trend of "banks...being held more accountable than ever for their actions vis-à-vis their customers," and characterized the majority holding as an unwelcome "deviation" and a "step in the wrong direction." So while the doctrine lives to fight another day, it seems that future cases will be very much fact-driven and banks cannot afford to view it as a shield.

The attention of businesses of all types and their counsel has been increasingly focused on the emerging risks to computer systems and the sensitive and valuable data they hold. Concerns about data security dominate the news, with major retailers as well as financial institutions being victimized by hackers and criminal networks. As such, it is increasingly essential for all attorneys involved in advising businesses to be up to speed on the latest developments in this area. The first three articles in this issue all deal with various ramifications of cybersecurity.

Attorneys are not known for being in the vanguard of new technology. But while most of us have progressed beyond quill pens, we remain insufficiently attentive to the risks of new ways of doing things. Case in point: Some ninety percent of law firms use email for privileged and confidential client communications. But the great majority of us take no measures to protect the confidentiality of those communications, other than attaching the words "privileged and confidential." In this issue's lead article, "Lawyers and Email: Ethical and Security Considerations," Scott Aurnou, an attorney and data security consultant, shows how the failure to use encryption, or other methods of data protection, not only compromises

the security of the communications, but can also result in violating ethics rules that mandate protection of client information. Mr. Aurnou explains the basics of how email and data encryption work, and discusses several methods lawyers can use to better assure the security of email communications.

In “Cybersecurity: A New Approach Is Necessary,” Jennifer Juste outlines the elements of a strong cybersecurity program. She notes that the traditional approach of directing resources to protecting against the largest known threats is insufficient in the current environment, and offers practical guidance on the elements of an effective program. Ms. Juste, a Compliance Manager at Interactive Data Pricing and Reference Data LLC, is a graduate of Fordham Law School and a member of the Business Law Section’s Securities Regulation Committee.

The third cybersecurity article conducts an in-depth exploration of all of the measures that can be undertaken in response to a cyber attack—collectively referred to as an “active response continuum,” or ARC. In “What Is Active Response Continuum and What Does It Cover?” Wesley Paisley reviews both U.S. and foreign legal precedents and the current state of technology. Mr. Paisley, a candidate for the JD degree at New York Law School, explains that ARC can take both aggressive and passive forms. The former include various means of counterattacking against the hackers’ software and hardware; the latter include such measures as marking data in order to detect when it is used illegally (analogous to marking money stolen from a bank). The means that can be deployed become especially problematical in the international context, as local laws in various jurisdictions may preclude or limit the use of some of these measures. Mr. Paisley makes clear that the law is only beginning to come to grips with the technology. For example, Congress has considered, but not enacted, the Stop Online Piracy Act, which would have allowed companies to aggressively hack into user computers to retrieve stolen data. So while building a strong system to protect computer systems and the data they contain remains essential, businesses and their counsel must also remain cognizant of developing legal trends in terms of what measures are and are not permissible.

While cybersecurity is a concern for all businesses, the banking industry finds itself especially dealing with other ramifications of technological change not contemplated by the law, such as the proliferating use of “virtual currencies” such as Bitcoin. In “Banking Law Update,” adapted from a talk given at the Business Law Section’s Fall Meeting held in September, Sabra Baum provides a concise update of key 2014 developments in laws and regulations affecting New York banks with respect to a host of payment-related issues—from virtual currency and cybersecurity to remittance transfers and payroll cards, along with key regulations relating to payday lend-

ing and new rules requiring identification of the ultimate beneficial owners of client companies, as part of the due diligence mandated by the Bank Secrecy Act to combat money laundering and other financial crimes. Ms. Baum is Senior Counsel of M&T Bank in Buffalo and a member of the Section’s Banking Law Committee.

The editors are pleased to announce that, beginning with this issue, attorneys Sharon Parella and Leah Ramos, who are respectively a partner and senior counsel in the Labor & Employment Group of Thomson Hine LLP, will be providing readers of the *Journal* with regular and timely updates on developments in New York and federal employment law that impact upon businesses. In this issue’s edition of “Recent Employment Laws Impacting Private Employers in New York,” Ms. Parella and Ms. Ramos focus on a range of 2014 enactments by the New York State Legislature and the New York City Council, dealing with matters such as including unpaid interns under anti-discrimination protections; mandatory provision of paid sick time; including electronic cigarettes under anti-smoking prohibitions; and prohibition of discrimination based upon pregnancy or a person’s status as being unemployed. They also note that the State Legislature is considering anti-bullying or “abusive work environment” legislation; businesses and their counsel are well advised to remain abreast of these and other developments.

Another regular feature of the *Journal* that has proven invaluable to practitioners is “Inside the Courts,” a comprehensive survey by the attorneys of Skadden Arps LLP of current litigation pertaining to securities and corporate matters in the federal courts. The current issue contains the usual clear and concise summaries of a wide range of current matters, ranging from shareholder derivative suits, to fiduciary duties, to current developments in Madoff-related litigation.

Our next article highlights a potential game-changer for corporate and securities litigation. In May 2014 the Delaware Supreme Court upheld a corporate by-law provision that shifts the cost of unsuccessful shareholder derivative suits to the plaintiff shareholders. But unlike the “loser pays” rule prevalent in the United Kingdom, whereby the losing party pays the litigation costs of the winner, the version upheld in Delaware is one-sided—the plaintiffs are liable for legal costs if they lose, but do not recover legal costs if they win. Not surprisingly, more than 20 corporations have adopted similar bylaws since the May 2014 decision. In “America’s Tweak to the Loser Pays Rule: A Board-Insulating Mechanism?” Ms. Nithya Narayanan, a candidate for the LLM degree at Harvard Law School, explains the so-called “tweaked loser pays rule” and explores its ramifications.

No issue of the *Journal* would be complete without Evan Stewart’s witty and insightful commentary on various aspects of legal ethics, and this issue is no excep-

tion. In “Squaring the Circle: Can Bad Precedent Just Be Wished Away?” Mr. Stewart, a partner at Cohen & Gresser LLP, takes umbrage with a recent opinion of the New York County Lawyers’ Association’s Professional Ethics Committee, which in his view attempts to accomplish exactly that. In an earlier article in the *Journal*, “Just When Lawyers Thought It Was Safe to Go Back in the Water” (Winter 2011), Mr. Stewart discussed the no-contact rule—which generally bars a lawyer from communicating with a party he knows to be represented by other counsel in the matter. In a 1990 case, the New York Court of Appeals held that the rule was not violated if an attorney representing an injured worker contacted *ex parte* other employees of the worker’s employer, as long as those employees were not acting as “alter egos” of the corporation. In the earlier article Mr. Stewart illustrated, and in this article reviews, the many troublesome ramifications of this holding. He then critiques the County Lawyers’ Professional Ethics Committee for, in effect, stating that the worst of these ramifications may be ignored. Along the way, Mr. Stewart provides his usual array of clever and amusing references to popular culture, from Lewis Carroll to The Godfather.

Concluding this issue is an article that should be of interest to all New York corporate practitioners. In

“Benefit Corporations and Certified B Corporations,” attorney Aaron Boyajian, a partner at Goetz Fitzpatrick LLP, provides a useful overview of New York’s Benefit Corporation Law, enacted in 2012. The law provides for creation of a new corporate form, the Benefit Corporation or B Corp, which can define its corporate purpose as serving the public interest in one of a number of defined ways, such as promoting human health or the environment, as well as earning a profit. The directors of the B Corp will have an explicit duty to fulfill the public interest purpose, thereby overcoming the primary obstacle to social responsibility missions within traditional corporate structures—the concern that directors and officers might breach their fiduciary duty to shareholders by placing social objectives ahead of maximizing profits. Mr. Boyajian clarifies that a B Corp is not necessarily the same thing as a Certified B Corporation. The latter is not a legal corporate form, but rather a status conferred by a non-profit organization dedicated to promoting corporate social responsibility. And while noting that law firms are “not traditionally thought of as socially responsible” (I beg your pardon!), Mr. Boyajian suggests that they, too, may be good candidates for B Corp status.

David L. Glass

Request for Articles



If you have written an article you would like considered for publication, or have an idea for one, please contact the *NY Business Law Journal* Editor-in-Chief:

David L. Glass
NY Business Law Journal
Macquarie Holdings (USA) Inc.
125 West 55th Street
New York, NY 10019
david.glass@macquarie.com

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

www.nysba.org/BusinessLawJournal

Lawyers and Email: Ethical and Security Considerations

By Scott Aurnou

The specter of attorney-client privilege has a long and well-respected history in litigation...but means nothing at all to a hacker. "Delete this email if you are not the intended recipient" or similar language theoretically sounds imposing, but essentially does nothing to protect firm or client data from any nefarious actors who view it (though they may get a good chuckle before reading the "forbidden" email).

In May 2014, LexisNexis published a study pertaining to law firm security awareness versus actual practices with respect to communications and file sharing with clients.¹ Almost 90% of those surveyed used email to communicate with clients and privileged third parties. The vast majority of attorneys surveyed also acknowledged the increasingly important role of various file sharing services and the inherent risk of someone other than a client or privileged third party gaining access to shared documents. Yet only 22% used encrypted email and 13% used secure file sharing sites, while 77% of firms relied upon the effectively worthless "confidentiality statements" within the body of emails to secure them.²

Relevant Ethical Standards

The effect of changes to the Model Rules: The ABA Model Rules of Professional Conduct were updated in 2012 specifically to address the effect of technology upon the legal profession, and a number of those changes directly pertain to the need for confidential communications.

The language in Comment 8 to Rule 1.1 (Competence) was amended to emphasize a duty for attorneys to stay up-to-date on technical matters pertaining to the practice of law, generally speaking: "[A] lawyer should keep abreast of changes in the law and its practice, *including the benefits and risks associated with relevant technology.*"³

Paragraph (c) of Rule 1.6 (Confidentiality of Information) states:

(c) A lawyer shall make reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client.⁴

Comment 18 to Rule 1.6 relates to the need for a lawyer to "act competently" to prevent the disclosure of "information relating to the representation of a client." It offers a safe harbor provision and factors to determine the reasonableness of an attorney's conduct in protecting the information at issue:

Factors to be considered in determining the reasonableness of the lawyer's efforts include, but are not limited to, the sensitivity of the information, the likelihood of disclosure if additional safeguards are not employed, the cost of employing additional safeguards, the difficulty of implementing the safeguards, and the extent to which the safeguards adversely affect the lawyer's ability to represent clients (e.g., by making a device or important piece of software excessively difficult to use).⁵

In addition, Comment 19 to Rule 1.6 specifically relates to electronic communications with clients, stating, "When transmitting a communication that includes information relating to the representation of a client, the lawyer must take reasonable precautions to prevent the information from coming into the hands of unintended recipients."⁶ It also offers a safe harbor provision: "This duty, however, does not require that the lawyer use special security measures if the method of communication affords a reasonable expectation of privacy."⁷

Therein lies the rub. What is reasonable, given the state of modern snooping technology? Moreover, from whom do the communications need to be kept private? Commercial competitors? Cyber criminals? Government actors? Other interested parties? Comment 19 specifically notes a pair of factors to consider when determining the reasonableness of the expectation of privacy. They are: (1) the sensitivity of the data itself, and (2) the extent to which the privacy of the communication is protected by law or by a confidentiality agreement.⁸ A client may also give informed consent to a method not otherwise permitted, though that approach may be asking for trouble if a client changes his or her mind later or disputes whether he or she was properly apprised of the relevant risks.

In addition to the Model Rules, failure to reasonably secure communications with clients can run afoul of state privacy laws⁹ and potentially provide an effective basis for a colorable legal malpractice claim.

Pertinent Technology Basics

How does email actually work? By its nature, email is not a terribly secure way to share information. When you send out an email, it goes through a more powerful, centralized computer called a server on its way to a corresponding email server associated with the recipient's computer or mobile device. It passes through any number of servers along the way from sender to recipient, like a

flat stone skipping along the top of a pond. And if that email isn't encrypted, anyone with access to any one of those servers can read it.

What is encryption? Encryption is the use of an algorithm to scramble normal data into an indecipherable mishmash of letters, numbers and symbols (referred to as "ciphertext"). An encryption key (essentially a long string of characters) is used to scramble the text, pictures, videos, etc. into the ciphertext. Depending on how the encryption is set up, either the same key (symmetrical encryption) or a different key (asymmetrical encryption) is used to decrypt the data back into its original state (called "plaintext"). Under most privacy and data breach notification laws, encrypted data is considered secure and typically doesn't have to be reported as a data breach if it's lost or stolen (so long as the decryption key isn't taken as well).

A Few Methods to Secure Email

(1) Encrypted email. Properly encrypted email messages should be converted to ciphertext before leaving the sender's computer or mobile device and stay encrypted until they are delivered to the recipient (remaining indecipherable as they pass through each server along the way). This is referred to as *end-to-end encryption*.

There are plenty of encrypted email offerings from larger commercial companies, as well as a number of new and interesting email encryption services that have become available in the wake of disclosures made by Edward Snowden.¹⁰

When choosing one, be mindful of where the service you use is located (including where the servers handling the emails on the system actually are). Mr. Snowden used a well-regarded U.S.-based encrypted email provider called Lavabit. Not long after Mr. Snowden's revelations came to light, federal law enforcement officials forced Lavabit to secretly turn over the encryption keys safeguarding its users' private communications. Lavabit's founder tried to resist, but was overwhelmed in federal court.¹¹ As a result, he shut down the service. Another well-regarded service called Silent Mail followed suit shortly thereafter, as it felt it could no longer ensure its customers' privacy.¹² Both have since relocated to Switzerland and are planning to introduce a new encrypted email service called Dark Mail.¹³

Larger companies offering encrypted email services typically control the encryption keys and will decrypt data before turning it over in response to a warrant or subpoena (including one coupled with a gag order). In addition, email service providers can legally read any email using their systems under Title II of the Electronic Communications Privacy Act, referred to as the Stored

Communications Act.¹⁴ Moreover, emails remaining on a third party server for over 180 days are considered abandoned.¹⁵ Any American law enforcement agency can gain access to them with a simple subpoena.¹⁶

Accordingly, if you choose to use a service based in the United States or another jurisdiction with similar privacy protections, be mindful of who controls the encryption keys.

(2) Secure cloud storage. Another way to securely communicate or share files with a client or privileged third party is to place the communication and/or files in encrypted cloud storage and allow the client or third party to have password-protected access to them. Rather than a direct email with possible attachments, the client or third party would receive a link to the securely stored data. The cloud service you select should be designed for security. Before you ask, DropBox and Google Drive would not be suitable options. There are a number of services offering well-protected cloud storage and it's important to do your due diligence before selecting one. If it all seems a bit much to figure out, two services I would recommend looking into are Cubby¹⁷ and Porticor.¹⁸

(3) Secure Web portal. A third approach is to place the communications and/or files in a secure portion of your firm's network that selected clients and/or privileged third parties can access. As with the secure cloud storage option noted above, the email sent to the client or third party would have a link back to the secure Web portal's log-in page. An advantage to this approach is that the communications and files do not actually leave your computer network and should be easier to protect.

An additional consideration. A government snoop or competent hacker doesn't necessarily have to target a message while it's encrypted. A message that is protected by strong encryption when it's sent or held in secure cloud storage can still be intercepted and read once it has been opened or accessed using a mobile device or computer that has been compromised. The same holds true for intercepting a message before it's encrypted initially. What steps can you take to protect them?¹⁹ The software on any computer or other device that can potentially access confidential data should be kept as up-to-date as possible; it should be protected against possible data loss if lost or stolen; and all firm personnel should have regular security awareness training with respect to social engineering²⁰ and other threats.

At the end of the day, there is no single silver bullet to provide "perfect security." But there are genuinely helpful steps (including those noted above) that you can take to comply with pertinent ethical standards and better protect your electronic communications with clients and privileged third parties.

Endnotes

1. LexisNexis Software Division, *LexisNexis Survey of Law Firm File Sharing in 2014*, SLIDESHARE (May 28, 2014), <http://www.slideshare.net/BusinessofLaw/lexisnexis-2014-survey-of-lfile-sharing-survey-report-final>.
2. *Id.*
3. MODEL RULES OF PROF'L CONDUCT R. 1.1, cmt. 8 (2014) (emphasis added).
4. MODEL RULES OF PROF'L CONDUCT R. 1.6.
5. *Id.* at cmt. 18.
6. *Id.* at cmt. 19.
7. *Id.*
8. *Id.*
9. See, e.g., MASS. GEN. LAWS, ch. 93H, § 2(a) (regulations at 201 CMR 17.00 *et seq.*) (2014); NEV. REV. STAT. § 603A.215 (2014).
10. See, e.g., Richard Stiennon, *Various Email Security Solutions Post Snowden*, SECURITY CURRENT (June 25, 2014), http://www.securitycurrent.com/en/news/ac_news/various-email-security-solutions-post-snowden.
11. Ladar Levinson, *Secrets, Lies and Snowden's Email: Why I Was Forced to Shut Down Lavabit*, THE GUARDIAN (May 20, 2014), <http://www.theguardian.com/commentisfree/2014/may/20/why-did-lavabit-shut-down-snowden-email>.
12. Parmy Olson, *Encryption App Silent Circle Shuts Down E-Mail Service 'To Prevent Spying'*, FORBES (Aug. 9, 2013, 12:41 PM), <http://www.forbes.com/sites/parmyolson/2013/08/09/encryption-app-silent-circle-shuts-down-e-mail-service-to-prevent-spying/>.
13. See DARK MAIL TECHNICAL ALLIANCE, <http://darkmail.info/> (last visited Nov. 20, 2014).
14. 18 U.S.C. § 2701(c)(1) (2014).
15. *Id.* at §§ 2701(c)(3), 2703.
16. *Id.* at § 2703(b).
17. See CUBBY, [HTTPS://WWW.CUBBY.COM/](https://www.cubby.com/) (last visited Nov. 20, 2014).
18. See PORTICOR, <https://www.porticor.com/> (last visited Nov. 20, 2014).
19. See Scott Aurnou, *What Is Endpoint Security?*, THE SECURITY ADVOCATE (Aug. 27, 2013), <http://www.thesecurityadvocate.com/2013/08/27/what-is-endpoint-security/>.
20. See Joan Goodchild, *Social Engineering: The Basics*, CSO ONLINE (Dec. 20, 2012, 7:00 AM), <http://www.csoonline.com/article/2124681/security-awareness/social-engineering-the-basics.html>.

Scott Aurnou is an information security consultant, attorney and Vice-President of SOHO Solutions, an IT consulting and managed services firm based in New York City. He regularly lectures on security, computer forensics and ethics relating to security and technology (particularly for legal professionals) and maintains a website called TheSecurityAdvocate.com.

NEW YORK STATE
BAR ASSOCIATION

CONNECT WITH NYSBA

Visit us on the Web:
www.nysba.org

Follow us on Twitter:
www.twitter.com/nysba

Like us on Facebook:
www.facebook.com/nysba

Join the NYSBA
LinkedIn group:
www.nysba.org/LinkedIn



Cybersecurity: A New Approach Is Necessary

By Jennifer Juste

With the plethora of high-profile data breaches and related regulatory focus, cybersecurity is on everyone's radar. Rightly so, companies are scrambling to understand the emerging threats to the security of their IT systems and the cyber-regulatory efforts in an attempt to create effective cybersecurity programs. One of the most problematic issues of cybersecurity is the quickly and constantly evolving nature of security risks.

To deal with the current environment, creating a strong cybersecurity program requires that companies evolve their approach to risk and data security. In order to do this, organizations must do the following three things: (1) Understand what cybersecurity is, (2) Determine which individuals and groups within the organization need to be involved in creating a cybersecurity program, and (3) Understand how to conduct a proper risk assessment to determine the vulnerabilities in an organization. Without an examination of these elements, a cybersecurity program is likely to lack in critical areas.

"[C]ompanies are scrambling to understand the emerging threats to the security of their IT systems and the cyber-regulatory efforts in an attempt to create effective cybersecurity programs."

First, an organization must determine what the term "cybersecurity" means. Broadly speaking, cybersecurity focuses on protecting computers, networks, programs and data from unintended or unauthorized access, change or destruction.¹ At one extreme, cybersecurity refers to national cyber-defense strategy against concerted cyber attacks by foreign powers or terrorists. At the other extreme, the term refers to persistent, sophisticated cyber-hacking events, large and small, that target government agencies and private corporations for purposes of sabotage or to acquire sensitive intelligence information.

These incidents do not only target Fortune 500 businesses, but also small to medium-sized businesses.² Therefore, organizations must have a strong understanding of how cybersecurity is defined and how it applies to their specific organization. Because of the evolving nature of cybersecurity, the best way for organizations to ensure they understand it is to educate their employees about cybersecurity through classes or by working with consulting firms.

Second, organizations must determine which individuals and groups need to be involved in creating an organization's cybersecurity program. The emerging threats to the security of an organization's IT systems and related cyber-regulatory efforts by governments pose unique business and legal challenges to companies. Because cybersecurity issues not only cut across traditional legal disciplines—but also, different business functions—too often companies lack an all-inclusive understanding of cybersecurity and the interrelationship of all critical teams necessary to create a strong program. Specifically, technology departments alone cannot address the legal compliance issues arising from cyber-regulatory efforts, and likewise, legal and compliance departments cannot address the emerging threats to the security of a company's IT systems.

Therefore, in order to implement an effective cybersecurity program, it is essential that organizations communicate across different business departments in a way that permits information technology and information systems employees to communicate the organization's current information systems and vulnerabilities to the organization's legal and compliance departments.

The adoption of written cybersecurity policies, which are one of the foundations of a strong program, cannot occur without the input of the departments that understand the threats to the security of an organization's systems. Ultimately, the coordination of efforts across business groups is the only way to protect an organization from cyber risk while also ensuring compliance with applicable rules and regulations.

Third, the foundation of cybersecurity preparedness is a complete risk assessment. Risk assessments need to be driven by the rules and regulations that apply to a particular organization and the organization's liability exposures.

Historically, the approach has been to focus most resources on the most crucial system components and protect against the biggest known threats, which necessitated leaving some less important system components undefended and some less dangerous risks not protected against. Such an approach is insufficient in the current environment.³

The current environment calls for organizations to conduct risk assessments to identify risks and the creation of measures to mitigate as many of those risks as possible. An effective risk assessment should uncover what

information the organization needs to protect and why. A strong risk assessment will also quantify the risk of a cyber attack occurring and the specific vulnerabilities an organization faces in light of its current infrastructure. The assessment should conclude with a plan of action to remedy any issues or vulnerabilities that were discovered during the assessment.

In short, a new approach is necessary to create strong cybersecurity programs. Although the task is not impossible, it will require organizations to take a critical look at how they currently handle cybersecurity and incorporate new measures that will ensure that organizations: (1) understand the evolving meaning of cybersecurity, (2) achieve collaboration and input across departments, and (3) conduct risk assessments that uncover an organization's valuable assets and cyber risks related to those assets.

Endnotes

1. *Cyber Security Primer*, UNIVERSITY AT MARYLAND UNIVERSITY COLLEGE, <http://www.umuc.edu/cybersecurity/about/cybersecurity-basics.cfm> (last visited Nov. 20, 2014).
2. *Cybersecurity and Privacy*, WIGGIN & DANA, LLP, <http://www.wiggin.com/12280> (last visited Nov. 20, 2014).
3. *Definition: Cybersecurity*, WHATIS.COM, [HTTP://WHATIS.TECHTARGET.COM/DEFINITION/CYBERSECURITY](http://whatis.techtarget.com/definition/cybersecurity) (last updated Dec. 2010).

Jennifer Juste is a Compliance Manager at Interactive Data Pricing and Reference Data LLC. She spent six years in private practice focusing on regulatory compliance for investment advisers before assuming her current role. She has served on the drafting committee of the New York State Bar Association Business Law Section Securities Regulation Committee to produce comment letters in response to rules proposed by the Securities and Exchange Commission.

Career Center Opportunities at www.nysba.org/jobs

Hundreds of job openings. Hundreds of attorneys.
All in one place.

Job Seekers:

- Members post resumes for FREE
- Members get 14-days advance access to new job postings
- Post your resume anonymously
- Hundreds of jobs already available for review
- Easy search options (by categories, state and more)

Find what you're looking for
at www.nysba.org/jobs.



What Is Active Response Continuum, and What Does It Cover?

By Wesley Paisley

In the wake of findings from the National Bureau of Asian Research,¹ companies need an active defense to protect their intellectual property from cyber thieves, cyber terrorists, and other miscreants. Governments and non-governmental organizations are not the only targets for cyber espionage.² When the proper authorities are unable to intervene in a timely fashion, an active offense is necessary to defend one's property.

This article differentiates between certain forms of Active Response Continuum (ARC) that are legal and illegal by looking at U.S. laws, case law, foreign legal analysis, and current technology. It also illustrates why some forms of ARC fail to help companies. Furthermore, the reader will learn policy reasons for why businesses and some private actors need to employ ARC.

Active Response Continuum encompasses all passive/aggressive activities that an actor will take to respond to a cyber offensive action,³ such as self-help, self-defense, and cooperation. Cooperation is a combination of self-help and self-defense. Self-help is when a private individual decides to recover property and alleviate his present situation without the help of the government.

Self-defense is an old concept tracing back to the thirteenth century, in which an urgent risk to an individual enabled her to defend herself if she did not have enough time to appeal to the proper authorities or retreat.⁴ Critics say it is difficult to transfer this concept to the cyber world because a computer network cannot retreat.⁵ However, the concept of retreat is possible: turn off the computer, shut down the network, or even simply isolate part of the server to prevent access. When a hacker learns he is getting hacked back, he cuts off his connections. Businesses cannot always afford to turn off their networks, or in other cases it might cause more harm to third parties. In that scenario, self-defense would be necessary.

Examples of ARC Can Be Divided Into Passive and Aggressive

ARC is broken into two different classifications, passive and aggressive. Some aggressive examples are: (1) halting the attacker's resources by disabling its zombie victim computers; (2) destroying the bots of a distributed denial of service (DDoS) attack; (3) reverse engineering the attacker's software (i.e., Remote Access Tools (RATs)) against the attacker;⁶ or (4) enabling the assets to self-destruct once they leave their original location, similar to the exploding bank money concept, a.k.a. "time-bomb."⁷

Passive ways include: (1) utilizing a honeypot, a program that replicates a vulnerable operating system in order to lure an intruder and log his information; (2) marking data in order to detect when it is re-used illegally;⁸ and (3) using community self-help.

As Neal Kaytal notes in his paper, *Community Self-Help*, a group of users on a network can work together to police a server or user group to weed out or alert others about the attacker or malware.⁹ This is quite similar to the non-cyber concept of NYC's MTA *If You See Something, Say Something*TM policy, which was later adopted by the Department of Homeland Security.¹⁰

"Active Response Continuum encompasses all passive/aggressive activities that an actor will take to respond to a cyber offensive action, such as self-help, self-defense, and cooperation."

Both policies encourage ordinary citizens to be on constant watch. Sometimes private actors prefer just to police their own network¹¹ rather than work with a community. Combining both approaches of policing the network and community self-help potentially solves problems such as less cooperation among international agencies.¹² Steve Chabinsky, Chief Officer of Crowd Strike, discussed a possible solution for companies: "[I]f we put together a group of international companies to police their networks we could reduce the risk of cyber harm, because most international companies own the very networks where the illegal cyber activity occurs."¹³ Just as cyber criminals work without borders, so do international companies, although there are some restrictions placed by civil procedure.¹⁴ However, this proposal is experimental, because it might violate anti-trust laws,¹⁵ privacy policies, and quite possibly international treaties.

What Is the Policy of ARC in the International Landscape?

Generally, international law governs only state actors.¹⁶ However, local foreign laws control companies that operate in the respective country, either by custom or by the black letter of the law. Some have stated foreign laws, such as Germany's criminal code, which makes hack back illegal,¹⁷ but in reality the law does not govern it all. For example, the law criminalizes illegal capture of data "that were not intended for him [and] were especially protected

against unauthorised access,”¹⁸ not data that the victim previously owned. Furthermore, since it is not a crime, you cannot be prosecuted under it.¹⁹ Some countries’ cyber laws are just developing, so they do not address ARC.²⁰

However, other countries have more developed cyber laws and try to entwine ARC within other existing frameworks of the law. In February 2013, the Canadian government abandoned the Protecting Children from Internet Predators Act (Bill C-30). This bill would allow private telecommunication companies to collect information on their users and send it to the police without a warrant. Private actors surmount privacy laws and keep information on customers who they suspect could be cyber criminals.²¹ However, some countries take a step further in the other direction and penalize the intrusion and changing of data packets on a computer.²²

In the European Union (EU), one court decision pushed the concept of the “right to be forgotten.”²³ Although this does not directly affect cyber criminal laws, it does tip the scales on the debate of privacy versus criminal acts. Usually when privacy has more support, ARC tends to have weaker support.²⁴ However, in countries where privacy laws are not heavily enforced, such as China,²⁵ the government actively encourages its agents to hack into other companies, and turns a blind eye when they hack into company networks from other countries to retrieve intellectual property.²⁶

Recently, the EU Committee on Civil Liberties, Justice and Home Affairs issued possible amendments to its policy on cybercrime. The commission wanted to impose tougher mandatory practices that would ensure at least two to five years in jail for those who hacked into other computers without authorization or on representatives of companies that benefitted from such attacks. However, the amended language states, “[t]his Directive does not intend to impose criminal liability where the objective criteria of the crimes listed in this Directive are met but the offences are committed without criminal intent, such as for...[protection of information systems].”²⁷ Therefore, hack back would be allowed because hack back lacks the criminal intent to harm. The member states have not fully adopted this legislation as of yet, but it shows that the EU is thinking about protecting companies that are hacking back for protection and not for criminal intent.²⁸ However, it should be noted that this type of language has been absent from the 2014 EU meeting.²⁹

Most academic communities usually analyze international defensive cyber measures under treaties of armed conflict.³⁰ This approach misconstrues the private sector, as private sectors do not act for the state but rather for their own profit. However, not every country follows that ideal, as China, for example, feels there is no difference between the private and government sector.³¹ With more cooperation between the private sector and government

to battle intellectual property theft,³² it is harder to argue against China’s position.

Foreign Legal Concepts Can Be Applied to ARC

EU’s tort theory of secondary liability for trademark infringement allows for more cooperation from the victims and service providers that are being used for cyber criminal activity. In the *L’Oreal v. eBay* case,³³ the European Court of Justice (ECJ) held that eBay was accordingly liable for allowing online shop owners to sell infringing material when they received proper notice. The EU can impose a similar type of duty that requests computer users or even hosting providers to remove malware, stolen goods, or vulnerable networks from their system once they receive notice. Recently, the EU considered adding such a duty in a recent Parliament meeting.³⁴ The infringing party would be more likely to remove the malware or stolen property rather than face litigation.

What Is the U.S. Policy on Hack Back?

Congress has mixed views on how ARC should be applied. Presently, there is no one comprehensive bill that fully answers ARC.³⁵ The Stop Online Piracy Act (SOPA),³⁶ allowed companies to aggressively hack into users’ computers and remove stolen items, but the Act failed to pass.³⁷ Under H.R. 624, the Cyber Security and Intelligence Act, the House wanted to provide more information sharing between government actors and private actors to stop cyber threats. However, this bill was amended to prevent hack back.³⁸ The Computer Fraud and Abuse Act (CFAA) has always been the definitive guide against hacking back into your neighbor’s computer: however, case law and different opinions state otherwise.³⁹ Moreover, unless the damage is above \$5,000, a civil claim will not lie under the CFAA.⁴⁰

The judicial branch has no particular answer to ARC, although many cases allow for individual areas of ARC under a specific fact-based analysis.⁴¹ Generally, the courts allow self-help as long as it isn’t violent and is done in good faith, and as long as contractual privity exists.⁴²

In 2013, President Obama issued Executive Order 13636⁴³ when Congress failed to pass a comprehensive cybersecurity bill.⁴⁴ However, Steve Chabinsky criticized 13636 by stating, “it’s not that good cyber hygiene is not good...it’s ultimately ineffective...or effective only at the margins.”⁴⁵ Chabinsky criticized the presidential order for not providing relief to stem cyber terrorism. It is merely a rhetorical statement. However, the aftermath of 13636 has been marginally more productive, because the order assigned the National Institute of Standards and Technology (NIST) the task of finding ways for private actors to build up cybersecurity.⁴⁶ This has created the potential for ARC. However, the Department of Justice has stated that companies that have been hacked should

not hack back into other computers to retrieve their files,⁴⁷ although the Department of Justice is silent on honeypots and other passive ARC.

ARC Can Be Used as a Defense Under NY Penal Law

The New York Penal Law allows for ARC when authorization is not an issue.⁴⁸ Under § 156.50[2], a reasonable defense to §§ 156.20, 156.25, 156.26 or 156.27 is that a party believes that it has the authority to delete computer data or programs.⁴⁹ The private actor can delete its files on its own server or another party's property using RATs in combination with honeypot.⁵⁰ However, when the private actor decides to intrude upon another person's computer or server it violates §156.10.⁵¹ Although the user might lack the *intent* to cause a felony, he is *knowingly* causing a felony,⁵² which is enough for the statute.

However, § 156.10 is a law of trespass, and trespass traditionally requires deprivation of enjoyment of the property.⁵³ If the private actor merely destroys the contraband, takes a picture of the attacker, or even just logs on to the zombie's computer IP address and methods, there is no trespass. However, if at any time the private actor denies the victim use of its services, this raises an issue under §156.10.⁵⁴ Courts will usually grant dismissal of charges when there is no damage.⁵⁵

However, if one takes apart the computer tampering section, one can see that different degrees support ARC as a defense. Computer tampering in the fourth degree allows the defendant to state in defense that he reasonably believed that he had the right to alter or destroy that data, because the statute relies upon the concept of *authorization*.⁵⁶

Section 156.25, computer tampering in the third degree, requires one to violate 156.20, and (1) commit or attempt a felony; (2) be previously convicted of a crime under §165.15 or §156; (3) intentionally alter computer material; (4) or take a financial amount from a victim.⁵⁷ If the private actor *only* destroys her property through RATs, there is no violation under (1), (2), and (4). Taking the financial amount from the private actor's own personal property would be a stretch of the law, because it would be the equivalent of arresting someone for destroying his own birthday balloon as it floated over a neighbor's yard. However, (3) doesn't define whose computer material has to be destroyed.⁵⁸ It can be inferred that this requires destruction of the true owner's property, but that would be a stretch. In *In re Shubov*,⁵⁹ the court required a commercial advantage to the party committing the cyber intrusion to satisfy the element of *mens rea*.⁶⁰ There is no commercial advantage for the party using ARC. One might argue that destroying trade secrets on the thief's computer would provide commercial advantage as it would prevent others from knowing the private actor's business secrets. However, a look at the civil field may clarify this problem. In the civil context, the plaintiff has

the burden of proving her financial loss.⁶¹ In this case ARC would be allowed. Furthermore, since §156.20 is not violated, the prosecutor cannot bring a fourth degree charge.

Computer tampering in the first and second degree is more problematic, because the *mens rea* requirement is satisfied by mere recklessness.⁶² An individual must be conscious of the risk to satisfy *mens rea*. If Party A merely hacks back into a computer to retrieve her data when she solely operates in the music industry, there is no risk that she might go through a medical server to damage a medical record. However, if there is a risk of damaging medical records, Party A has to be careful not to damage any data outside of her own. Furthermore, Party A must implement a time-bomb to destroy her own data to escape liability. However, the court could impose a misdemeanor penalty under § 156.05 since it is such a broad statute. The only way to avoid liability is by asking your neighbor if you can simply come onto his network and retrieve your property.⁶³

However, this begs the question to the critics: *how do you solve a problem when the attacker uses the host computers of one hospital to attack users of an ISP at another hospital?* Which user is more important in a cyber attack? And does this violate §156.25? Waiting for the government to act is one solution, but what if real lives are in danger? The problem blossoms into a larger disaster when the attacker is using a foreign hospital's network to attack.

Why §1080 of the CFAA Should Allow for ARC

Section 1080 should allow for ARC because it will enable actors to retrieve billions of dollars lost in revenue from intellectual property theft.⁶⁴ We already require companies to make sure that their physical/cyber space is secure,⁶⁵ so why not impose a duty to have their cyber space secure in an offensive manner?⁶⁶ If not an outright duty, there should exist reasonable regulation to allow individuals to use ARC, just as we already regulate the security profession.⁶⁷ Furthermore, as many commenters have said, the law under CFAA is quite ambiguous towards ARC.⁶⁸

A private company that partners with the government to locate a dangerous hacker could receive immunity to hack back and retrieve files.⁶⁹ In *Filarsky v. Delia*,⁷⁰ a lawyer partnering with the government to do an investigation was granted immunity in analogous circumstances, although the *Delia* case did not involve cyber information. Furthermore, companies are more successful when they have the ability to thwart DDoS attacks under the government's approval.⁷¹

Self-help Laws Can Be Applied

Self-help is allowed under the civil legal system through repossession of secured goods under Article 9 of the UCC, which supersedes the tort of trespass.⁷²

Under the UCC, the creditor has to adhere to a breach of the peace standard, which the debtor can overcome by a simple verbal utterance. However, criminals will rarely cry out because they fear criminal prosecution. This can be applied to the cyber element by allowing private actors to place time-bombs on their applications or at least watermarks to prevent unauthorized usage, especially if there is a contractual relation between the parties. Furthermore, the Restatement (Second) of Torts § 103 allows an individual in hot pursuit to retrieve his goods without civil penalty.⁷³ However, the criminal side is still in flux over self-help as a remedy for theft.⁷⁴

U.S. Police Obligations

Over the years the U.S. court system has eroded the liability of police officers to prevent frivolous lawsuits. However, some police officers have taken this as a hall pass to do whatever they like and whenever they like. For example, in *DeShaney v. Winnebago County*,⁷⁵ the Supreme Court found that state actors do not have a duty “to protect the life, liberty, and property of [their] citizens against invasion by private actors.”⁷⁶ The Court found that the failure to protect citizens did not operate as a denial of life, liberty, or property under due process.⁷⁷ The Court construed the duty that officers have to the public in general to mean that they do not have a duty to individual citizens. Furthermore, many courts have used this decision to excuse police officers who were not able to assist citizens in times of trouble.⁷⁸ Moreover, most of the principles in these cases can easily apply to the cyber world.⁷⁹ Accordingly, self-defense is still needed for people to properly defend themselves in times of immediate cyber danger.⁸⁰

Officers are overwhelmed with the number of cyber crimes that are present today. As one Assistant District Attorney has noted,⁸¹ nearly every case that comes into the Manhattan D.A.’s office has a cyber element to it. Furthermore, jurisdictional problems make it quite difficult for officers to cross foreign boundaries and find and prosecute cyber criminals located abroad.⁸² Even the royals are subject to cyber attacks.⁸³ Sometimes it is difficult for officers to get help from technically proficient professionals because of salary or internal policy issues.⁸⁴

Is ARC Really That Bad?

The Executive Branch is against ARC. However, without it, the Executive Branch would not be able to execute many arrests or engage in successful deterrence.⁸⁵ As much as passive ARC is a deterrent, hackers generally think of it as a challenge and will keep trying to attack a system no matter how many times they lose. Aggressive ARC is a better deterrent because it gives the hacker an incentive to not hack.

Community self-help solves the problem when government does not have all the resources to find and

deter a cyber attacker.⁸⁶ Cyber self-help is analogous to the non-cyber situation where police officers are unable to police every New York City transit train.⁸⁷ The private sector believes in the virtue of community monitoring, yet an even better remedy would consist in going after and forcibly deterring the cyber attacker.⁸⁸ At the very least, however, a constant sense of monitoring by communities can lead to the group creating its own moral code.

For example, Neal Katyal compares how some non-cyber stores illegally restrict access to their establishment based on race to how some cyber communities might legally restrict users who they believe are suspicious. A bigger group would be able to eliminate the invidious discrimination that plagues smaller groups by virtue of their size and the larger group’s common goal to protect each individual within the bounds of the law.⁸⁹

ARC Can Lead to an Arms Race or Even an International Incident

Unfortunately, ARC could place the private actor in a cyber arms race, because the most sophisticated cyber attacks are government-sponsored.⁹⁰ One party keeps upping the devastation on the cyber realm to the point where too much damage occurs.⁹¹ By attacking the criminal, the private actor might be vicariously attacking its own government, leading to an arms race.⁹²

Under the Law of Armed Conflict (LOAC), the idea of an *attack* is defined as a physical force, so a cyber attack is not classified as an attack.⁹³ However, if a cyber attack leads to physical harm, there could be a cause for action under LOAC. Furthermore, under the *Tallinn Manual*,⁹⁴ a cyber attack that is not injurious can be countered as long as it is illegal under the state’s sovereign law. Once the attacker becomes a “terrorist or hostile group,” it is open to physical strikes.⁹⁵ However, the *Tallinn Manual* is a non-binding study on international law and does not hold the same weight as a signed treaty. However, many foreign laws allow for government agencies to defend themselves in a cyber attack.⁹⁶

The Georgian government successfully used the honeypot method to hack into an intruder’s computer and infiltrate his web cam to take pictures of him.⁹⁷ Furthermore, had the person been a government agent, depending on what further actions Georgia took, it could have led to a full cyber war. Even if a party is not a government body, a contractor for the government is considered an agent of the government so as to warrant a defensive measure.⁹⁸

Furthermore, even if it does not escalate into a governmental arms race, ARC can still lead to an arms race between the company and the attacker. Cyber attackers that are not government sponsored do not give up easily.⁹⁹ Attackers that receive counterstrikes might escalate their attacks, leading to a cycle of internet violence.

ARC Can Open the Vigilante to Civil Liability

Hack back can open the individual to civil liability if done wrong. As this article has looked into a non-cyber ARC when it is successful, let us now look at what happens when ARC goes bad and opens the individual up to civil liability. One example, in a Louisiana case,¹⁰⁰ occurred when a store clerk gave chase to a shoplifter, and the shoplifter fled and knocked a customer on his back. The customer sued the store, and the court of appeals asserted that the thief was 40% and the store 60% liable for negligence. The court reasoned that the store had a duty to mitigate harm to its customers while apprehending the criminal.

This is quite analogous to the cyber world if a hacker leaves a path of destruction in order to prevent herself from being apprehended. However, the dissent in the Louisiana case was better reasoned, finding that the store did nothing wrong and the criminal was the “but for” cause¹⁰¹ of the customer’s injury. Analogously, service providers that use ARC should not be held liable for supervening criminal activity.

ARC Can Open the Vigilante to Conviction Under Other Cyber Criminal Laws

One commenter has posted a chilling scenario of aggressive ARC leading to child pornography, as highlighted below:¹⁰²

- (1) Hacker takes over Computer A.
- (2) Hacker uses Computer A to hack into Computer B.
- (3) User of Computer B notices hack attempt from Computer A.
- (4) User B installs covert software to snap a pic from the webcam of Computer A to catch evil hacker.
- (5) User A happens to be a teenage girl who’s changing clothes at the time.
- (6) User B gets 50 years in PMITA prison for child porn.

However, this commenter referred only to the most aggressive form of ARC, which would violate the CFAA and child pornography statutes by creating a significant harm of trespass. This does not apply to honeypots, or communal self-help.

No One Likes You When You Violate His Privacy

Honeypots create a different danger such as inadvertently violating privacy laws when honeypots gather information about the attacker. Although one can limit the type of information that the honeypot collects,¹⁰³ if the attacker uses a group of victim computers to attack a system, the honeypot will most likely log the personal

information of these computers. This can be easily overcome by making an agreement with any user that enters the network, giving him or her notice that his or her information has been logged. The service provider can create response messages that state the user’s information has been logged. We sometimes allow this in the non-cyber world when a person who comes onto property is given notice he or she is being recorded by a security camera.

New York State¹⁰⁴ and other jurisdictions¹⁰⁵ have a strong policy against underhanded surveillance by private and state actors. Others might state that this is the equivalent of a burglar caught on a security camera, except that the criminal is using an unwitting person to do her dirty deeds. Imagine your grandmother unwittingly breaking into a bank, while the criminal is controlling her. Poor granny thinks she is simply doing her job, like exchanging pennies for dollars, but she is also committing money laundering. Would granny feel violated if personal information was gathered by the bank and then used against her in a shame campaign or, worse, criminal investigation? However, most companies are prudent in that they don’t publicize the pictures or information of users they find while using ARC. Furthermore, companies can aggregate the data they collect and make sure it is not personal when shared with the government¹⁰⁶ or any other entity. Furthermore, by utilizing the terms of service (TOS), service providers can dictate what is considered a breach of privacy. In one case,¹⁰⁷ Microsoft used its TOS to subvert privacy laws to catch a criminal by looking through the attacker’s emails to track his illegal activity. Furthermore, the privacy debate can be eroded by understanding there is no expectation of privacy on the internet.¹⁰⁸ However, if consumers and private actors work together, they can maintain a level of privacy for the consumer while protecting the very networks from intrusion, rather than having to resort to the TOS.

Privacy Watchdog Groups Would Be in an Uproar

However, there is some expectation of privacy on the internet partly due to the Wiretap Act of the U.S.,¹⁰⁹ EU directives,¹¹⁰ and data encryption. When companies look to the government as a resource for sharing information on cyber attacks, privacy watchdog groups are wary that the companies must be sharing personal information on customers.¹¹¹ However, these privacy groups are protecting the very information that companies want to retrieve or remove from the possession of criminals. Private actors need to work more with privacy watchdog groups.¹¹²

Too Much ARC Can Slow the Economy of the Internet

If you overprotect your castle, it will be harder to allow people in. For example, one bank created fake bank user names¹¹³ to lure intruders. The bank will block the

intruder's internet protocol (IP) address and remove the fraudulent accounts when the intruder attempts to withdraw funds. The problem lies when the attacker uses a victim's IP address, which prevents the innocent victim from logging into her account because her IP address is blocked. Furthermore, unless the bank can successfully weed out the spurious IP addresses¹¹⁴ the victim will be re-victimized. On the other hand, this type of problem-solving can resolve a major computer crisis,¹¹⁵ but at the cost of their customers' comfort.

"ARC is a great resource for companies and regular everyday people like you and me to deter cyber attacks or assist law enforcement."

Another problem occurs when aggressive ARC leads to a slow or defunct network. When a business disrupts bots of DDoS, it takes a toll on the network. First, for every bot the attacker deploys, the more server services must be used to accommodate all that information. Second, the target company uses those same services on the network to do business. Third, the business uses these same services to combat those bots. Finally, with all these resources using the same network, eventually the server will crash due to a bottleneck of information. The attacker loses its bots, the company commerce website is offline, and the attacker ultimately wins since it has denied your service to your site. There is no win for the company here. Maybe the attacker is deterred, but it would have been better if the company had simply logged the attacker's information and sent it to the proper authorities.

Conclusion

ARC is a great resource for companies and regular everyday people like you and me to deter cyber attacks or assist law enforcement. Furthermore, ARC is very much legal in the U.S. because of statutes, case law, and policy reasons. However, some forms are outright illegal. Due to the debate on privacy, the internet is becoming increasingly difficult to regulate to stop cyber criminals, let alone deter them. However, this is not an argument against privacy. To the contrary, the lack of privacy leads to more problems and requires the even greater use of ARC.

Furthermore, international conflict of laws rules place certain actions in a gray area. In some countries ARC is clearly defined as illegal. Furthermore, where ARC is not clearly defined as a legal concept, it is seen as contrary to privacy law, although some jurisdictions see the need for it and will allow it for policy reasons.

Endnotes

1. See THE NATIONAL BUREAU OF ASIAN RESEARCH, IP COMMISSION REPORT, 6-7 (May 2013), available at http://www.ipcommission.org/report/IP_Commission_Report_052213.pdf.
2. See Comm. on Civil Liberties, Justice and Home Affairs, AMENDMENTS 20 - 147, EUR. PARL. DOC. (COM(2013)0048-C7-0035/2013-2013/0027(COD)), at 3, Jan. 7, 2014. [hereinafter EU Cybercrime].
3. David Dittrich, [Excerpted from] *The Active Response Continuum: Ethical and Legal Issues of Aggressive Computer Network Defense*, UNIVERSITY OF WASHINGTON STAFF (May 27, 2013), <http://staff.washington.edu/dittrich/arc/book/definitions.html>.
4. Shane McGee et al., *Adequate Attribution: A Framework for Developing a National Policy for Private Sector Use of Active Defense*, 8 J. BUS. & TECH. L. 1, 13 (2013).
5. *Id.* at 15.
6. STEPTOE, *The Hackback Debate*, STEPTOE CYBERBLOG (Nov. 2, 2012), <http://www.steptoecyberblog.com/2012/11/02/the-hackback-debate/> (exemplifying that the debate on legality of hackback speakers includes law professors, private attorneys, and bloggers).
7. Robbin Rahman, *Electronic Self-Help Repossession and You: A Computer Software Vendor's Guide to Staying Out of Jail*, 48 EMORY L.J. 1477, 1484-85 (1999).
8. Paul Rosenzweig, *International Law and Private Actor Active Cyber Defensive Measures*, 50 STAN. J. INT'L L. 103, 106 (2014).
9. Neal Kaytal, *Community Self-Help*, 1 J.L. ECON. & POL'Y J33-67, 45 (2005), available at <http://scholarship.law.georgetown.edu/facpub/533/>.
10. DEP'T OF HOMELAND SECURITY, *If You See Something, Say Something™ Campaign | Homeland Security*, <http://www.dhs.gov/if-you-see-something-say-something%E2%84%A2-campaign> (last visited Nov. 20, 2014).
11. Nick Wingfield & Nick Bilton, *Microsoft Software Leak Inquiry Raises Privacy Issues*, N.Y. TIMES, Mar. 20, 2014, at B1; *USA v. Kibkalo*, Docket No. 2:14-cr-00087, (W.D. Wash. Mar 28, 2014); Victoria Slind-Flor, *Daily Briefing: Green Cross Drug, Microsoft, Twitter, Patent Trademark & Copyright Law Daily*, BNA, June 26, 2014, <https://www.bloomberglaw.com/ms/search/results/dbd5d841f2142be91f9a20bd55d05a78/document/XBIR92D8000000> (Kibkalo was deported after being detained for 84 days).
12. Wcsnyder, *U.S. Secret Service Calls for Increased Penalties Under CFAA*, CROSSROADS BLOG (Feb. 6, 2014), <http://blog.cybersecuritylaw.us/2014/02/06/us-secret-service-calls-for-increased-penalties-under-cfaa/>.
13. Conversation at 1:05:16-01:15:00, *23rd Annual Review of the Field of National Security Law Conference*, ABA (Nov. 2013), available at http://www.americanbar.org/content/dam/aba/events/law_national_security/panel_5.mp3.
14. See generally, *J. McIntyre Mach., Ltd. v. Nicastro*, 131 S. Ct. 2780, 2800-02 (2011) (stating that companies that do business in a foreign jurisdiction are subject to that country's laws).
15. *FTC, DOJ Issue Antitrust Policy Statement on Sharing Cybersecurity Information*, FED. TRADE COMMISSION (Apr. 10, 2014), <http://www.ftc.gov/news-events/press-releases/2014/04/ftc-doj-issue-antitrust-policy-statement-sharing-cybersecurity>.
16. Rosenzweig, *supra* note 8, at 107.
17. *Id.* at 114.
18. Prof. Dr. Michael Bohlander, *GERMAN CRIMINAL CODE*, 2013, http://www.gesetze-im-internet.de/englisch_stgb/englisch_stgb.html#p1710 (English translation).

19. *Id.*
20. See OFFICIAL GAZETTE OF THE REPUBLIC OF PHILIPPINES, *Republic Act No. 10175* (Sept. 12, 2012), <http://www.gov.ph/2012/09/12/republic-act-no-10175/> (criminalizing illegal computer access).
21. Michel Leclerc, *The End of a Controversed Canadian "Government-Spying" Bill*, NYU PRIVACY RESEARCH GROUP BLOG, <http://blogs.law.nyu.edu/privacyresearchgroup/2013/03/the-end-of-a-controversed-canadian-government-spying-bill/> (last visited Nov. 20, 2014).
22. See generally UNITED STATES AGENCY FOR INTERNATIONAL DEVELOPMENT, INTRODUCTION TO NEWS MEDIA LAW AND POLICY IN JORDAN (2011), available at [http://www.irex.org/sites/default/files/Media%20Law%20and%20Policy%20Primer%20\(English\).pdf](http://www.irex.org/sites/default/files/Media%20Law%20and%20Policy%20Primer%20(English).pdf); Drew Mitnick & Jon Fox, *Turkish government passes harsh new internet law*, ACCESS (February 20, 2014, 12:05am), <https://www.accessnow.org/blog/2014/02/20/turkish-government-passes-harsh-new-internet-law> (advocating that punishment under the Turkish internet laws are not proportional to the crime).
23. Press Release, Court of Justice of European Union, Press Release No 70/14 (May 13, 2014), available at <http://curia.europa.eu/jcms/upload/docs/application/pdf/2014-05/cp140070en.pdf>.
24. We can also see in the United States, specifically in New York, that when privacy of a document is limited, criminalization of intrusion is weaker. *People v. Klapper*, 28 Misc. 3d 225, 228–30, 902 N.Y.S.2d 305, 309–11 (Crim. Ct., N.Y. Co. 2010) (discussing the penal law's legislative intent to criminalize intrusions where the owner placed protections on the property in question.).
25. See generally AMERICAN BAR ASSOCIATION STANDING COMMITTEE ON LAW AND NATIONAL SECURITY, A PLAYBOOK FOR CYBER EVENTS 42 (1st ed. 2013) (noting that Asia-Pacific has nonbinding agreements for privacy).
26. Michael S. Schmidt & David E. Sanger, *5 in China Army Face U.S. Charges of Cyberattacks*, N.Y. TIMES, May 19, 2014, http://www.nytimes.com/2014/05/20/us/us-to-charge-chinese-workers-with-cyberspying.html?_r=0; see Ellen Nakashima, *U.S. said to be target of massive cyber-espionage campaign*, WASH. POST, Feb. 10, 2013, at 1.
27. EUROPEAN PARLIAMENT, AMENDMENTS 34 – 128 9–10 (COM(2010)0517 – C7-0293/2010 – 2010/0273(COD) 2012), available at [http://www.europarl.europa.eu/RegData/commissions/libe/amendments/2012/480665/LIBE_AM\(2012\)480665_EN.pdf](http://www.europarl.europa.eu/RegData/commissions/libe/amendments/2012/480665/LIBE_AM(2012)480665_EN.pdf).
28. See EUROPEAN PARLIAMENT, AMENDMENTS 20 - 147 10 (COM(2013)0048 – C7-0035/2013 – 2013/0027(COD)), available at <http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-%2F%2FEP%2F%2FNONSGML%2BCOMPARL%2BPE-521.696%2B02%2BDOC%2BPDF%2BV0%2F%2FEN>.
29. See generally *id.*
30. See Dittrich, *supra* note 3.
31. *23rd Annual Review of the Field of National Security Law Conference*, 01:16:33–01:18:27, AMERICA BAR ASSOCIATION (Nov. 2013), http://www.americanbar.org/groups/leadership/office_of_the_president/cybersecurity/resources.html.
32. See EUROPEAN PARLIAMENT, AMENDMENTS 20 - 147 at 49–50.
33. *L'Oreal SA v. eBay International AG* [2012] (C-324/09) Bus. L.R. 1369.
34. See EUROPEAN PARLIAMENT, AMENDMENTS 20 - 147 at 16–17.
35. Ellen Nakashima, *Senate intelligence panel leaders draft cyber legislation*, WASH POST, Apr. 28, 2014, http://www.washingtonpost.com/world/national-security/senate-intelligence-panel-leaders-draft-cyber-legislation/2014/04/28/fe7387bc-cf03-11e3-a6b1-45c4dfb85a6_story.html.
36. Declan McCullagh, *RIAA Wants to Hack Your PC*, WIRED, Oct. 15, 2001, <http://archive.wired.com/politics/law/news/2001/10/47552?currentPage=all>.
37. Grant Gross, *SOPA and PIPA: What went wrong?*, COMPUTERWORLD (Jan. 23, 2012 02:29 PM), http://www.computerworld.com/s/article/9223645/SOPA_and_PIPA_What_went_wrong_?taxonomyId=70&pageNumber=2.
38. Permanent Select Committee on Intelligence, Committee Report, Cyber Intelligence Sharing and Protection Act, H.R. 624, 113th Cong. (2013) (statement of Rep. Langevin).
39. Benson Richards, *A Legal Defense of Counter-Hacking*, 28 BYU Prelaw Rev. 33, 40 (2014).
40. See *In re Google Inc. Cookie Placement Consumer Privacy Litig.*, 988 F. Supp. 2d 434, 448 (D. Del. 2013) (“[T]he court conclude[d] that plaintiffs have not sufficiently alleged the threshold loss of \$5,000 required by the CFAA,” therefore dismissing their claim.).
41. Richards, *supra* note 39, at 44–46; Robbin Rahman, *Electronic Self-Help Repossession and You: A Computer Software Vendor's Guide to Staying Out of Jail*, 48 EMORY L.J. 1477, 1484–85 (1999).
42. See generally, *Am. Computer Trust Leasing v. Jack Farrell Implement Co.*, 763 F. Supp. 1473, 1493–1495 (D. Minn. 1991), *aff'd and remanded, sub nom. Am. Computer Trust Leasing v. Boerboom Int'l, Inc.*, 967 F.2d 1208 (8th Cir. 1992); Adam B. Badawi, *Self-Help and the Rules of Engagement*, 29 YALE J. ON REG., vol. 1, no. 43 (2012).
43. Executive Order 13636—Improving Critical Infrastructure Cybersecurity, 78 Fed. Reg. 33 (Feb. 19, 2013).
44. Jaikumar Vijayan, *Obama to Issue Cybersecurity Executive Order This Month*, COMPUTER WORLD (Feb. 1, 2013), http://www.computerworld.com/s/article/9236438/Obama_to_issue_cybersecurity_executive_order_this_month.
45. *Cybersecurity: Future Challenges (23rd Annual Review of the Field of National Security Law Conference)*, ABA (Nov. 2014), http://www.americanbar.org/content/dam/aba/events/law_national_security/panel_5.authcheckdam.mp3.
46. *The Cybersecurity Partnership Between the Private Sector and Our Government: Protecting Our National and Economic Security*, http://www.commerce.gov/sites/default/files/documents/2013/april/gallagher_030713.pdf (last visited Nov. 20, 2014); DEPARTMENT OF COMMERCE, NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, *Incentives To Adopt Improved Cybersecurity Practices*, 78 FR 18954-01 (March 28, 2013).
47. Gerry Smith, *'Hacking Back' Could Deter Chinese Cyberattacks*, *Report Says*, HUFFINGTON POST (March 22, 2013 7:39 PM), http://www.huffingtonpost.com/2013/05/22/hacking-back-chinese-cyberattacks_n_3322247.html; see U.S. DEP'T OF JUSTICE, CRIMINAL DIVISION, COMPUTER CRIME AND INTELLECTUAL PROPERTY SECTION, PROSECUTING COMPUTER CRIMES MANUAL, available at <http://www.justice.gov/criminal/cybercrime/docs/ccmanual.pdf> (last visited Nov. 20, 2014).
48. Under New York law, the term *without authorization* is defined as “the use or access of a computer, computer service or computer network without the permission of the owner.” N.Y. PENAL LAW § 156.00 (McKinney 2014); see Daniel B. Prieto & Evan Wolff, *A Playbook for Cyber Events*, A.B.A. STANDING COMMITTEE ON L. & NAT'L SECURITY (2014); see also *People v. Klapper*, 902 N.Y.S.2d 305, 309 (N.Y. Crim. Ct. 2010).
49. N.Y. PENAL LAW § 156.00.
50. Rahman, *supra* note 41, at 1504.
51. N.Y. PENAL LAW § 156.00 (McKinney 2014).
52. *Id.*
53. *People v. Puesan*, 973 N.Y.S.2d 121, 126 (App. Div. 2013); cf. *Bose v. Interclick, Inc.*, No. 10 Civ. 9183, 2011 U.S. Dist. LEXIS 93663, (S.D.N.Y. Aug. 17, 2011) (The court granted dismissal because the trespass did not create any damages.); see also *Del Vecchio v. Amazon.com, Inc.*, No. C11-366RSL, 2012 U.S. Dist. LEXIS 76536, (W.D. Wash. June 1, 2012).

54. See *Puesan*, 973 N.Y.S.2d at 126.
55. Cf. *Bose*, 2011 U.S. Dist. LEXIS at 93663 (S.D.N.Y. Aug. 17, 2011) (The court granted dismissal because the trespass did not create any damages).
56. See *Puesan*, 973 N.Y.S.2d at 126-28.
57. N.Y. PENAL LAW § 156.25 (McKinney 2014).
58. *Id.*; 1 Charges to Jury & Requests to Charge in Crim. Case in N.Y. § 21:6.50 (2013).
59. *In re Shubov*, 802 N.Y.S.2d 437 (App. Div. 2005).
60. *Id.* at 440.
61. *Del Vecchio v. Amazon.com, Inc.*, C11-366RSL, 2012 WL 1997697 (W.D. Wash. June 1, 2012).
62. *Id.*
63. See AMERICAN BAR ASSOCIATION STANDING COMMITTEE ON LAW AND NATIONAL SECURITY, A PLAYBOOK FOR CYBER EVENTS 72-73 (Evan Sills, October 2013).
64. THE NATIONAL BUREAU OF ASIAN RESEARCH, IP COMMISSION REPORT, 6-7 (May 2013), available at http://www.ipcommission.org/report/IP_Commission_Report_052213.pdf.
65. See FTC, Financial Institutions and Customer Information: Complying with the Safeguards Rule, April 2006, <http://www.business.ftc.gov/documents/bus54-financial-institutions-and-customer-information-complying-safeguards-rule> ("Monitoring the websites of your software vendors and reading relevant industry publications for news about emerging threats and available defenses.").
66. See *supra* note 4.
67. *Id.*
68. *Id.*
69. Zach, *Hackback Sunday: Skating on Stilts/ Cyberdialogue*, CYBER SEC. L. & POL'Y (Mar. 3, 2013), <http://blog.cybersecuritylaw.us/2013/03/03/hackback-sunday-skating-on-stiltscyberdialogue/>.
70. Amy Howe, *In Plain English: Recent Decisions*, SCOTUSBLOG (Apr. 23, 2012, 11:41 AM), <http://www.scotusblog.com/2012/04/in-plain-english-recent-decisions/>.
71. AM. BAR ASSOC. STANDING COMM. ON LAW AND NAT'L SEC., *supra* note 25, at 77.
72. Badawi, *supra* note 42, at 43.
73. *Id.* at 32; RESTATEMENT (SECOND) OF TORTS § 103 cmt. b (1979).
74. Badawi, *supra* note 42, at 33; see also *People v. Tufunga*, 987 P.2d 168, 169 (Cal. 1999) ("At common law, a claim of right was recognized as a defense to larceny because it was deemed to negate the animus furandi, or intent to steal, of that offense.").
75. *DeShaney v. Winnebago Cnty. Dep't of Soc. Servs.*, 489 U.S. 189 (1989).
76. *Id.* at 195-96.
77. *Id.*
78. See *McDonald v. City of Chicago*, 561 U.S. 742 (2010) (holding that the right to self-defense was incorporated into the Second Amendment); *Warren v. D.C.*, 444 A.2d 1, 3 (D.C. 1981) (holding an officer had no duty to victims of rape who called for the police); *Bowers v. DeVito*, 686 F.2d 616, 619 (7th Cir. 1982) ("But the only duties of care that may be enforced in suits under section 1983 are duties founded on the Constitution or laws of the United States; and the duty to protect the public from dangerous madmen is not among them."); *Archie v. City of Racine*, 847 F.2d 1211, 1215 (7th Cir. 1988) ("The government need not provide services, and...if it does provide services it need not provide them competently.").
79. *Id.*
80. See *McDonald v. City of Chicago, Ill.*, 561 U.S. 742 (2010) (the right to self-defense is incorporated into the Second Amendment).
81. Danny Yadron, *Police Grapple With Cybercrime*, WALL ST. J. (April 20, 2014 7:50 PM), <http://online.wsj.com/news/articles/SB10001424052702304626304579508212978109316>; see generally Ass'n of Chartered Certified Accountants, *Cybercrime in the World Today: 2014 | ACCA Official*, YouTube (Apr. 3, 2014) (3:52-3:55; 4:40-5:00), <http://www.youtube.com/watch?v=LifiaNnaxJl&feature=youtu> ("Nearly every case handled by our [Manhattan] office has a cyber crime element... Identity theft is the fastest growing crime that exists in the country [US].").
82. See Debarati Halder, *Book Review of Policing Cyber Hate, Cyber Threats and Cyber Terrorism*, 7 INT'L J. OF CYBER CRIMINOLOGY 169, 170 (2013).
83. *Phone-hacking Trial: Kate Middleton 'Hacked 155 Times'*, BBC (May 14, 2014 5:02 PM), <http://www.bbc.com/news/uk-27413632>.
84. Leo Kelion, *FBI 'Could Hire Hackers On Cannabis' to Fight Cybercrime*, BBC (May 22, 2014 6:20 AM), <http://www.bbc.com/news/technology-27499595>.
85. See AM. BAR ASSOC. STANDING COMM. ON LAW AND NAT'L SEC., *supra* note 25, at 77.
86. See Kaytal, *supra* note 9, at 50.
87. See *See Something, Say Something*, MTA, http://transittrax.mta.info/audio/ttx_transcripts/SeeSomethingSaySomething.htm (last visited Nov. 20, 2014).
88. Ron Ross, ESTABLISHING A SECURE FRAMEWORK, FEDTECHMAGAZINE.COM (2012), available at http://csrc.nist.gov/groups/SMA/fisma/ron_ross_continuous_monitoring_article_july2012.pdf.
89. AM. BAR ASSOC. STANDING COMM. ON LAW AND NAT'L SEC., *supra* note 25, at 77.
90. See cf. McGee, *supra* note 4, at 4-5 ("[A] digital 'arms race' determining absolute attribution can be difficult if not near impossible; the retaliatory or defensive strike may cause more harm than the original attack and could easily impact innocent bystanders. Furthermore, legal uncertainties exist as to whether active defense as a form of [self-defense] would be permitted.").
91. *Id.*
92. *Id.*
93. LAURIE R. BLANK, *CYBERWAR: LAW & ETHICS FOR VIRTUAL CONFLICTS*, 21 (forthcoming 2015).
94. Michael N. Schmitt, *The Law of Cyber Warfare: Quo Vadis?*, 25 STANFORD L. & POL'Y REV. 7 (forthcoming 2014) (discussing the *Tallinn Manual on the International Law Applicable to Cyber Warfare* remedies).
95. BLANK, *supra* note 93, at 29.
96. *Telecompaper, Belgium has laws in place to fight cyberterrorism*, (January 10, 2012 | 15:10 CET), <http://www.telecompaper.com/news/belgium-has-laws-in-place-to-fight-cyberterrorism--848893>.
97. Jeremy Kirk, *Irked by Cyberspying, Georgia Outs Russia-based Hacker—withPhotos*, IT WORLD, <http://www.itworld.com/308638/irked-cyberspying-georgia-outs-russia-based-hacker-photos?page=0,2> (last visited May 21, 2014).
98. Michael N. Schmitt, *The Law of Cyber Warfare: Quo Vadis?*, (September 4, 2013) (unpublished manuscript), http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2320755.
99. Benson Richards, *A Legal Defense of Counter-hacking*, 28 BYU PRELAW REV. 36, 40 (2014).
100. *Brock v. Winn Dixie Louisiana, Inc.*, 617 So. 2d 1234, 1239 (La. Ct. App. 1993), *aff'd*, 620 So. 2d 848 (La. 1993).
101. *Id.* at 1239 (Stoker, J., dissenting).
102. Mike Masnick, *Rep. Gohmert Wants A Law That Allows Victims To Destroy The Computers Of People Who Hacked Them*, TECHDIRT.COM (Tuesday, Mar 19th 2013 7:30 am), <http://www.techdirt.com/articles/20130316/01560522347/rep-gohmert-wants-law-that-allows-victims-to-destroy-computers-people-who-hacked-them.shtml#c77>.

NYSBA's CLE Online

))) ONLINE | iPod | MP3 PLAYER

Bringing CLE to you... anywhere, anytime.

NYSBA is proud to present the most flexible,
"on demand" CLE solutions you could ask for.

With **CLE Online**, you can now get the valuable
professional learning you're after

...at your convenience.

- > Get the best NY-specific content from the state's **#1 CLE provider**.
- > Take "Cyber Portable" courses from your laptop, at home or at work, via the Internet.
- > Download CLE Online programs to your iPod or MP3 player.
- > Everything you need to obtain full MCLE credit is included **online!**



Come click for CLE credit at:
www.nysbaCLEonline.com



Features

Electronic Notetaking allows you to take notes while listening to your course, cut-and-paste from the texts and access notes later – (on any computer with Internet access).

Audio Seminars complement the onscreen course texts. You control the pace, and you can "bookmark" the audio at any point.

Bookmarking lets you stop your course at any point, then pick up right where you left off – days, even weeks later.

MCLE Credit can be obtained easily once you've completed the course – the form is part of the program! Just fill it out and mail it in for your MCLE certificate.

103. Lance Spitzner, *Honeypots*, TRACKING-HACKERS.COM, <http://www.tracking-hackers.com/papers/honeypots.html> (last Modified: May, 29 2003).
104. See *People v. Capolongo*, 85 N.Y.2d 151, 160 (1995); CLE: Kenneth Citeralla, *Divorce in the Digital Age: A Primer for Practitioners* (2014) (on file with author).
105. See Deborah Brown, *Spotlight on Internet Governance Part Four: NetMundial* (April 14, 2014, 12:49 PM), <https://www.accessnow.org/blog/2014/04/14/spotlight-on-internet-governance-part-4-netmundial>; Katherine Maher, *The Day The World Fought Back* (Feb. 11, 2014, 12:03 AM), <https://www.accessnow.org/blog/2014/02/11/the-day-the-world-fought-back>.
106. AM. BAR ASSOC. STANDING COMM. ON LAW AND NAT'L SEC., *supra* note 25, at 66.
107. See Nick Wingfield & Nick Bilton, *Microsoft Software Leak Inquiry Raises Privacy Issues*, N.Y. TIMES (March 20, 2014), http://www.nytimes.com/2014/03/21/technology/microsofts-software-leak-case-raises-privacy-issues.html?_r=0; *USA v. Kibkalo*, Docket No. 2:14-cr-00087 Bloomberg Law (W.D. Wash. Mar 28, 2014).
108. See CLE: Kenneth Citeralla, *Divorce in the Digital Age: A Primer for Practitioners*, at 3 (2014) (on file with author) (finding that passwords do not seal the contents of the email as that account is disclosed as it travels through different networks); *People v. Kucharski*, 2013 IL App (2d) 120270, 987 N.E.2d 906, 921–22 *appeal denied*, 996 N.E.2d 19 (Ill. 2013) (holding that encryption is not considered the same as changing a password, so one can simply remotely change the password to an account without violating a state cyber statute); *but see United States v. Jones*, 132 S. Ct. 945, 955–957 (2012) (discussing the fear of the government's unfettered data mining of individuals); see Brown, *supra* note 105 (advocating for more privacy rights); Maher, *supra* note 105 ("[T]housands of websites will let the world's governments know that we reject global mass surveillance at home and overseas.... Mass surveillance violates our fundamental rights").
109. See 18 U.S.C. §§ 2510-2522.
110. EUROPEAN COMMISSION, *Progress on EU data protection reform now irreversible following European Parliament vote* (March 12, 2014), http://europa.eu/rapid/press-release_MEMO-14-186_en.htm.
111. AM. BAR ASSOC. STANDING COMM. ON LAW AND NAT'L SEC., *supra* note 25, at 65.
112. See Conversation, *23rd Annual Review of the Field of National Security Law Conference*, ABA (November 2013), available at http://www.americanbar.org/content/dam/aba/events/law_national_security/panel_5.mp3 (providing commentary from Laurie Donahue to the effect that privacy is a factor we must configure when deciding against cyber attacks).
113. *Bankers go undercover to catch bad guys*, THE ECONOMIST (April 5, 2014), <http://www.economist.com/news/finance-and-economics/21600148-bankers-go-undercover-catch-bad-guys-hacking-back?fsrc=scn/tw/te/bl/ed/hackingback>.
114. Internet Systems Consortium Inc., *Mitigating DNS Denial of Service Attacks* (March 29, 2012, 17:17), <https://www.dns-oarc.net/wiki/mitigating-dns-denial-of-service-attacks>.
115. Brandon Mercer, *HeartBleed Counter Attack Via Honey Pot Could Snag Hackers Who Compromised Millions Of Passwords* (Apr. 15, 2014 2:39 PM), <http://sanfrancisco.cbslocal.com/2014/04/15/heartbleed-counter-attack-via-honey-pot-could-snag-hackers-who-compromises-millions-of-passwords/>.

Wesley Paisley is a JD candidate at New York Law School.

Banking Law Update

By Sabra M. Baum

The financial services industry in New York and beyond saw a number of regulatory changes during 2014. Now that the year has drawn to a close, it is a good time to provide an update on some of those changes. I have chosen the following topics for this update: (i) virtual currencies, (ii) cybersecurity, (iii) payday lending, (iv) BSA “beneficial owner” rules, (v) remittance transfers, and (vi) payroll cards.

1. NY Issues Proposed Regulations for Virtual Currencies

On July 17, 2014, the New York Department of Financial Services (“NYDFS”) published proposed “BitLicense” regulations.¹ The NYDFS’s proposal is the first comprehensive regulatory regime proposed in the U.S. and will likely have a large impact on the industry, and the development of regulations in other jurisdictions. Comments on the proposed regulations were due on September 6, 2014; however, the NYDFS recently extended that deadline to October 21, 2014. In recent years, there has been increasing concern with virtual currencies in light of the failure of several virtual currency exchanges (such as the once-largest Bitcoin exchange, Mt. Gox²), concerns over the use of Bitcoin for potential money laundering and fraud (such as with respect to the Silk Road marketplace),³ the lack of a single comprehensive regulatory regime for virtual currency businesses, and the increasing popularity of Bitcoin and virtual currencies.⁴

Under the NYDFS’ proposed regulations, businesses that operate virtual currencies (e.g., Bitcoin) must be licensed in order to engage in business with customers in New York (whether retail or institutional), or if they otherwise operate in New York. There are numerous consumer protections in the proposed regulations, such as requirements for upfront and per-transaction disclosures of terms and risks, complaint procedures and advertising restrictions. Virtual currency businesses will be required to meet certain capital requirements, and submit quarterly financials and annual audited GAAP financials to the NYDFS. There are also numerous requirements to help mitigate cybersecurity risk, including annual reporting to the NYDFS, annual penetration testing/audits and board-approved security policies and procedures. The proposed regulations include comprehensive anti-money-laundering (“AML”) requirements that are largely consistent with federal AML requirements, including obligations on virtual currency businesses to put in place an AML program, keep transaction records for 10 years, report to the NYDFS any transactions of \$10,000 or more per person/per day, SAR reporting, a customer identification program, OFAC checks and internal/external audits. The NYDFS will examine virtual currency businesses at least every two years.

It is clear from the proposed regulations that the cost of compliance for regulated businesses will be high. The regulations would appear to be aimed at creating a high barrier to entry and more legitimacy with respect to virtual currency businesses. Ben Lawskey, of the NYDFS, has said, “We have sought to strike an appropriate balance that helps protect consumers and root out illegal activity—without stifling beneficial innovation.”⁵

The Financial Crimes Enforcement Network (“FinCen”) also has recently confirmed its regulatory oversight of the virtual currency industry. On October 27, 2014, FinCen issued two rulings regarding virtual currency payment systems and trading platforms. Under the first ruling, FinCen ruled that a company planning to establish a virtual currency payment system would be a “money transmitter” subject to FinCen rules regarding money services businesses (“MSBs”).⁶ In the second ruling, FinCen ruled that a company that set up a virtual currency trading and booking platform would be a “money transmitter” and subject to regulation by FinCen as a MSB.⁷

Other regulators in the U.S. also are increasingly focusing on virtual currencies. The Consumer Financial Protection Bureau (“CFPB”) issued a consumer advisory on August 11, 2014 warning consumers about the risks of virtual currencies, such as Bitcoin, and began taking complaints about virtual currencies.⁸ The Conference of State Bank Supervisors (“CSBS”) issued the “Model State Consumer and Investor Guidance on Virtual Currency” on April 23, 2014⁹ to assist state regulatory agencies in providing consumers with information about virtual currency and factors consumers should consider when transacting with or investing in virtual currency. Nevada and Maryland have already issued guidance based on that model. The Securities and Exchange Commission (“SEC”) issued an investor alert on May 7, 2014 regarding the risks of investments in Bitcoin and virtual currency,¹⁰ and the Internal Revenue Service (“IRS”) issued guidance in March 2014 to the effect that general property tax principles will apply to virtual currency transactions.¹¹

2. Increasing Regulatory Focus on Cyber Security

Cyber security is now one of the most critical risks affecting financial institutions. In September 2014, Home Depot announced a credit and debit card breach affecting some 56 million cardholders and 53 million email addresses of customers¹²—an even larger breach than the high profile 2013 hack on Target’s payment system which affected 40 million cardholders.¹³ However, the banking industry was put on high alert when J.P. Morgan discovered a breach of its servers in July 2014 and subsequently

announced that 76 million accounts and seven million small business accounts had been compromised.¹⁴ This hack comes in the wake of increasing attention by hackers of bank systems, including a number of large denial-of-service attacks against major banks in the last several years.¹⁵

In response to these hacks, financial institutions have been bolstering their cybersecurity resources and expenditure in an effort to stay a step ahead of the hackers.¹⁶ In addition, regulators have increased their focus on cybersecurity in the financial services industry. In New York, the NYDFS released a report in May 2014 entitled "Report on Cyber Security in the Banking Sector,"¹⁷ in which it announced its plans to expand its IT examination procedures to focus more fully on cybersecurity. The NYDFS said its exam procedures will now include additional questions in the areas of IT management and governance, incident response and event management, access controls, network security, vendor management and disaster recovery—aimed at taking a more holistic view of an institution's cyber readiness, but still tailored to the institution's unique risk profile. The report is based on a survey conducted by the NYDFS in 2013 of 154 banks and credit unions in New York. Survey participants were questioned about industry trends, their own security framework, cybersecurity breaches and future plans. The NYDFS's report largely concludes that smaller institutions are less prepared than larger banks to handle cyber threats.

The Federal Financial Institutions Examination Council ("FFIEC") also is attempting to raise awareness of cybersecurity in the financial services industry. In June 2014, the FFIEC launched a new web page dedicated solely to current and future FFIEC-related cybersecurity materials.¹⁸ The FFIEC held a webinar in May 2014 for approximately 5000 CEOs and senior managers of financial institutions to highlight the pervasiveness of cyber threats, discuss the role of executive leadership in managing those risks, and to share actions being taken by the FFIEC. Earlier in the year, the FFIEC had issued a statement to financial institutions regarding risks associated with cyber attacks on ATMs and payment card authorization systems, including steps financial institutions should be taking to mitigate those risks.¹⁹

A number of other financial institution regulators also have increased their attention on cybersecurity in 2014. On May 16, 2014, Thomas Curry, the Comptroller of the Currency, expressed his view before The New England Council that the Office of the Comptroller of the Currency ("OCC") is concerned with cybersecurity and, in particular, with the increasing reliance by banks on vendors, especially foreign vendors, to support critical activities.²⁰ The SEC had previously announced that its 2014 Examination Priorities would include a focus on cybersecurity preparedness, and issued a Risk Alert in April 2014 to announce that the SEC's Office of Compliance Inspections and Examinations ("OCIE") will examine more than 50

registered broker-dealers and investment advisors, focusing on cybersecurity governance, risks, protections and experiences.²¹ The OCIE has issued a sample questionnaire for that initiative. In September 2014, the Federal Trade Commission ("FTC") submitted a comment letter to the CFPB in response to the CFPB's request for information on mobile financial systems.²² The FTC identified privacy and security of consumers' personal and financial data as a critical consumer protection concern with mobile financial systems, and noted that it is addressing these issues through enforcement, policy initiatives and education.²³ The government's concern with cybersecurity has even culminated in President Obama issuing an Executive Order on October 27, 2014 focused on the security of consumer financial transactions.²⁴ The Executive Order deals with three issues—government payments, identity theft remediation and online federal transactions. With respect to government payments, for example, the Executive Order requires agencies to enhance security measures, such as CHIP and PIN technology for payment processing terminals and cards.

In a turn of events, while regulators focus on financial institutions' systems, the Government Accountability Office ("GAO") took a closer look at the CFPB's security systems. Following concern raised by several members of Congress, the GAO published a report on September 22, 2014 regarding the CFPB's collection of sensitive consumer data and information. The GAO concluded that the CFPB generally satisfied its legal privacy requirements; however, it recommended a number of additional steps for the CFPB to implement in order to enhance security and privacy controls.²⁵

3. Regulators' Continued Focus on Payday Lending

Regulators across the U.S., including in New York, continue to put pressure on financial institutions to help "choke off" payday lenders' access to the banking systems—dubbed "Operation Choke Point" by the Department of Justice ("DOJ") and several other regulators. The DOJ has now sent subpoenas to more than 50 banks. In January 2014, Four Oaks Bank agreed to a \$1.2 million settlement with the DOJ regarding allegations that it allowed a third party payment processor to use the Fed in connection with unlawfully debiting consumer bank accounts.²⁶ U.S. prosecutors have now opened criminal and civil probes into at least 15 banks and payment processors as part of Operation Choke Point. On June 23, 2014, Attorney General Eric Holder announced that the DOJ would continue to aggressively investigate financial institutions that knowingly facilitate transactions for payday lenders engaging in fraudulent transactions.²⁷ Mr. Holder made clear, however, that the DOJ had no interest in pursuing lawful conduct. The CFPB also is currently researching and considering whether rulemaking is warranted in the area of payday lending.²⁸

In New York, the NYDFS sent cease and desist letters in August 2013 to 35 companies offering illegal payday loans to New York consumers, as well as a letter to the National Automated Clearing House Association (“NACHA”) and 117 financial institutions requesting that they assist the NYDFS to “choke off” ACH system access by the payday lending industry.²⁹ Since then, NACHA issued a Request for Comment in November 2013 on proposed rules to improve ACH network quality in light of the focus on payday lending issues.³⁰ However, in a subsequent letter sent to NACHA in January 2014, the NYDFS said that while the NACHA proposal was a positive step, the NYDFS believed the proposal did not adequately address some of the abuses of the ACH network by payday lenders who made illegal loans in New York.³¹ NACHA continued to take comments through 2014 and, on August 22, 2014, approved a number of new rules to help reduce illegal payday lenders’ use of the NACHA system.³² In particular, effective September 18, 2015, two new NACHA rules will (i) reduce the “return threshold” for unauthorized debits from 1% to 0.5% and (ii) establish a return rate threshold for account data quality returns at 3% and an overall debit return rate threshold of 15%. In addition, the new rules will impose quality fees and fines on originating banks in order to incent them to improve the quality of originated ACH transactions.

The NYDFS also is looking into other payment networks used by payday lenders. The NYDFS announced, in a press release on April 30, 2014, that in response to mounting regulatory pressure to curb payday lenders’ abuse of the ACH network, some lenders are now using debit card transactions to deduct funds from New York consumers’ bank accounts.³³ The NYDFS said, in its press release, that it had sent cease and desist letters to another 20 companies engaging in illegal payday loans (12 of which are using debit card tactics) and that the NYDFS had reached a settlement agreement with Visa and Mastercard to take a series of steps to help stop the processing of debit card payments towards illegal payday loans over the Visa and Mastercard networks. Under the settlement agreement, Visa and Mastercard will be required to work with financial institutions to ensure they are not processing illegal debit card transactions on behalf of payday lenders and to notify banks about New York’s laws prohibiting payday lenders.

There appears, however, to be mounting criticism of the regulators’ running of Operation Choke Point. In May 2014, the U.S. House of Representatives Committee on Oversight and Government Reform (chaired by Republican Darrell Issa) issued a report that concluded that the DOJ lacks legal justification for Operation Choke Point and that the DOJ is targeting payday lenders in a deliberate attempt to deny them access to banking services.³⁴ On June 26, 2014, Missouri Republican Blaine Luetkemeyer introduced a bill to end Operation Choke Point.³⁵ The Community Financial Services Association of America also filed a lawsuit on June 5, 2014 in the U.S.

District Court for District of Columbia against several regulators (the FDIC, OCC and the Fed) alleging that regulatory guidance issued by them relating to Operation Choke Point is “arbitrary and capricious” and intended to drive payday lenders out of business.³⁶ In July 2014, the Committee on Financial Services of the U.S. House of Representatives held a hearing regarding Operation Choke Point, calling witnesses from both sides of the fence to discuss their views on the operation.³⁷ Most recently, on October 6, 2014, six senators from the Committee on Banking, Housing and Urban Affairs sent a letter to Attorney General Eric Holder to express concern over the creation of lists of “high risk merchants” in regulatory guidance, and to request that the DOJ and other agencies limit the scope of Operation Choke Point and cease using subpoenas and political action to unfairly target business merchants engaged in legal commerce.³⁸ Another coalition of members of the House of Representatives also sent letters to the DOJ and FDIC in October 2014 criticizing the DOJ and FDIC’s “abuse” of authority to advance political and/or moral agendas, and requesting that they initiate investigations into Operation Choke Point.³⁹

Possibly in reaction to this mounting criticism of Operation Choke Point, the FDIC, on July 28, 2014, issued a letter to confirm that it would be removing the list of high-risk merchants from certain of its supervisory guidance of third party payment processors, and explained that its inclusion of lists of examples of high-risk merchants in FDIC guidance had created a misperception that those merchants were prohibited or discouraged.⁴⁰

4. New FinCen Proposed Rules to Identify Beneficial Owners

On July 30, 2014, FinCen issued its much anticipated Notice of Proposed Rulemaking (“NPR”)⁴¹ to amend existing Bank Secrecy Act (“BSA”) regulations to help prevent the use of anonymous companies to engage in or launder the proceeds of illegal activity in the U.S. financial sector. Comments on the NPR were due by October 3, 2014, and numerous comments were received.⁴² The proposed rule clarifies and strengthens customer due diligence (“CDD”) obligations of covered financial institutions that are subject to customer identification programs (“CIP”), such as banks.⁴³ In particular, the proposed rule focuses on what FinCen describes as the four core elements of CDD. The first element of CDD will be to identify and verify customers—FinCen notes that this is already addressed in existing CIP regulations.

The second element of CDD, however, will require covered financial institutions to identify and verify the identity of beneficial owners of legal entity customers. This is a new requirement of the BSA regulations. Currently, BSA regulations only require financial institutions to take reasonable steps to identify beneficial owners in two limited situations—first, with respect to private banking accounts in the U.S. for non-U.S. persons⁴⁴ and, second, with respect to correspondent accounts for cer-

tain foreign financial institutions.⁴⁵ Under the proposed rule, covered financial institutions will have to identify any individual who, directly or indirectly, owns 25% or more of the equity interests of the legal entity customer (the “ownership prong”) as well as at least one individual who “controls” the legal entity (the “control prong”). An individual identified under the “control prong” might also be one of the same persons who meets the “ownership prong.” A legal entity customer will include corporations, LLCs, partnerships or similar business entities (but will not include trusts not formed through a filing). Certain legal entity customers will be exempt from the beneficial owner requirements, such as publicly held companies traded on a U.S. stock exchange, domestic government agencies, and financial institutions regulated by a federal regulator (*e.g.*, a bank, broker-dealer etc.). FinCen also may consider some other exemptions, such as certain SEC or other registered entities. In addition, there is an exemption for issuers of prepaid cards and financial institutions that hold funds in omnibus or intermediated accounts—in particular, if the covered financial institution has no CIP obligations with respect to the intermediary’s underlying client, then the intermediary can be treated as the legal entity customer. Under the proposed rule, the covered financial institution will be required to obtain, at the time a new account is opened, a standard certification form from the legal entity customer setting out its beneficial owners. The covered financial institution then will be required to verify the identity of those beneficial owners using their existing risk-based CIP practices, although the institutions generally can rely on representations of their customers when answering questions about the owners of the entity.

The proposed rule also will amend FinCen’s AML requirements to expressly state the third and fourth element of CDD set out in the proposed rules. The third element of CDD in the proposed rules is that covered financial institutions must understand the nature and purpose of customer relationships. FinCen notes that such information should already be getting obtained, so this requirement should not change an institution’s existing practices. The fourth element of CDD is that covered financial institutions conduct ongoing monitoring of customer relationships—again, FinCen notes that institutions should already be conducting ongoing customer reviews under existing AML guidance.

5. Changes to Remittance Transfer Regulations

On August 22, 2014, the CFPB issued a final rule⁴⁶ to revise the remittance transfer regulations that became effective in October 2013.⁴⁷ In particular, the rule extends by five years (to July 21, 2020) the expiration date for the “temporary exception” under the regulations that allows a remittance transfer provider to disclose reasonable estimates of the exchange rate, transfer amount, covered third party fees, and the total amount to be received by the recipient. The rule also made a number of clarifica-

tions to the remittance transfer regulations—for example, that U.S. military installations abroad are considered to be located in a State for purposes of the regulations, and that whether an account is a consumer account can be determined by looking at the primary purpose of the account, etc.

In addition, on September 12, 2014, the CFPB also finalized a rule to expand its coverage of large non-depository financial service companies (*i.e.*, nonbanks) for international money transfers.⁴⁸ Section 1024 of the Dodd-Frank Act provided the CFPB with authority to supervise certain nonbanks, such as large participants in a market for consumer financial services. Under the new rule, the CFPB can supervise companies that provide at least one million international money transfers a year for compliance with the remittance transfer regulations (found in Subpart B of Regulation E), as well as for compliance with other consumer financial laws, such as privacy and unfair, deceptive and abusive acts and practices (UDAAP) laws. The CFPB said that the new rule will affect approximately 25 nonbanks that provide approximately 90% of the transfers in the nonbank market for international money transfers. For example, companies such as Western Union and MoneyGram International will be affected. The CFPB said that it plans to coordinate examinations of such companies with state regulatory authorities that generally have the authority to license and examine these nonbanks under money transmitter and similar laws.

6. NY Bill to Regulate Payroll Cards

On June 10, 2014, a bill was introduced by New York State Assembly Majority Leader Joseph Morelle and State Senator Patrick Gallivan to regulate payroll cards in New York.⁴⁹ The bill follows a report issued by New York Attorney General Eric Schneiderman on June 13, 2014 that highlighted the impact of payroll cards on low-wage workers and proposed a Payroll Card Act to prevent the reduction of workers’ wages through payroll card fees.⁵⁰ Mr. Schneiderman’s report notes that “virtually all payroll card programs charge fees for card related activities, and these fees can add up, reducing the meager take-home pay received by the lowest paid workers in the state.”

If enacted, the bill will add new provisions to New York’s labor laws. For example, employers must obtain the employee’s written consent in order to pay wages or salary by direct deposit to a payroll card (and that consent can be withdrawn at any time by the employee), and employers must offer employees the option of receiving payment by check or deposit to a bank account. Employers also must provide certain notices to the employee before obtaining consent—those notices include fees that may be assessed by the payroll card issuer or third parties. Importantly, an employer is restricted from paying employees with payroll cards unless certain requirements are met—such as at least one network of ATMs within reasonable proximity to the cardholder’s place of employment or

residence that allows unlimited cash withdrawals and balance inquiries at no cost. Payroll card accounts must be FDIC or NCUA insured and must comply with Regulation E and not be linked to a credit product. Finally, payroll card programs also cannot charge fees for account initiation, participation, closing, etc.

Endnotes

1. <http://www.dfs.ny.gov/about/press2014/pr1407171-vc.pdf>.
2. Mt. Gox (based in Tokyo, Japan) was a Bitcoin exchange that commenced business in July 2010 and filed for a form of bankruptcy protection in February 2014. In 2013, it handled 70% of all Bitcoin transactions. Mt. Gox announced, at that time, that about 850,000 Bitcoins (valued at \$450 million) were missing and likely stolen (although some of those Bitcoins were later recovered). <http://www.reuters.com/article/2014/02/28/us-bitcoin-mtgox-insight-idU.S.BREA1R06C20140228>.
3. In October, 2013, the FBI shut down “Silk Road,” an online market founded in 2011. It was alleged that Silk Road was an anonymous Internet marketplace that facilitated purchases of illegal drugs, money laundering and murder-for-hire using Bitcoin payments. <http://www.nytimes.com/2013/10/03/nyregion/operator-of-online-market-for-illegal-drugs-is-charged-fbi-says.html?pagewanted=all&r=0>. Since then, it has been reported that a Silk Road 2.0 marketplace has been opened.
4. The Government Accountability Office (“GAO”) released a report on June 26, 2014 on virtual currencies. The report notes that, as of March 31, 2014, approximately 12.6 billion Bitcoins were in circulation, having a total value of \$5.6 billion. The report identifies key challenges with virtual currencies and highlights regulatory actions relating to virtual currencies, such as FFIEC guidance, enforcement actions, etc. The report also recommends that the CFPB take steps to address virtual currencies. <http://www.gao.gov/products/GAO-14-496>.
5. <http://www.dfs.ny.gov/about/press2014/pr1407171.html>.
6. http://www.fincen.gov/news_room/rp/rulings/html/FIN-2014-R012.html.
7. http://www.fincen.gov/news_room/rp/rulings/html/FIN-2014-R011.html.
8. <http://www.consumerfinance.gov/newsroom/cfpb-warns-consumers-about-bitcoin/>.
9. <http://www.csbs.org/legislative/testimony/Documents/ModelConsumerGuidance--Virtual%20Currencies.pdf>.
10. http://www.sec.gov/oiea/investor-alerts-bulletins/investoralertsia_bitcoin.html#.U--M4fldXhs.
11. <http://www.irs.gov/uac/Newsroom/IRS-Virtual-Currency-Guidance>.
12. <http://online.wsj.com/articles/home-depot-breach-bigger-than-targets-1411073571>. On September 14, 2014, Home Depot announced that 56 million debit and credit cards had been hacked during a five-month period between April and September 2014. Shortly afterwards, on November 7, Home Depot announced that the hackers had also stolen 53 million email addresses of customers.
13. <http://krebsonsecurity.com/2014/05/the-target-breach-by-the-numbers/>. Target announced, on December 19, 2013, that a security breach had occurred. Over 40 million credit and debit card numbers were stolen, and 70 million customers’ names and other records were stolen. In addition to regulatory scrutiny, over 100 class action lawsuits have been filed against Target—those suits have now been transferred to the U.S. District Court for the District of Minnesota for consolidated proceedings.
14. <http://dealbook.nytimes.com/2014/10/02/jpmorgan-discovers-further-cyber-security-issues/>.
15. <http://money.cnn.com/2012/09/27/technology/bank-cyberattacks/>. Numerous banks, including Bank of America, JPMorgan Chase, Wells Fargo, U.S. Bank and PNC Bank, have all suffered denial-of-service attacks since 2012.
16. In October 2014, J.P. Morgan CEO, James Dimon, said the bank would double its spending on cybersecurity in the next five years. J.P. Morgan’s 2014 annual budget for cybersecurity was \$250 million. <http://online.wsj.com/articles/j-p-morgans-dimon-to-speak-at-financial-conference-1412944976>.
17. http://www.dfs.ny.gov/about/press2014/pr140505_cyber_security.pdf.
18. <http://www.ffiec.gov/cybersecurity.htm>.
19. <https://www.ffiec.gov/press/pr040214.htm>.
20. <http://www.occ.gov/news-issuances/speeches/2014/pub-speech-2014-73.pdf>.
21. <http://www.sec.gov/ocie/announcement/Cybersecurity+Risk+A+lert++%2526+Appendix++4.15.14.pdf>.
22. http://www.ftc.gov/system/files/documents/advocacy_documents/ftc-staff-comment-consumer-financial-protection-bureau-regarding-use-mobile-financial-services/140912mobile_financialservices_update.pdf.
23. For example, in March 2014, the FTC settled actions against Fandango and Credit Karma for failing to secure their mobile apps. <http://www.ftc.gov/news-events/press-releases/2014/03/fandango-credit-karma-settle-ftc-charges-they-deceived-consumers>.
24. <http://www.whitehouse.gov/the-press-office/2014/10/17/executive-order-improving-security-consumer-financial-transactions>.
25. <http://www.gao.gov/assets/670/666000.pdf>.
26. <http://www.justice.gov/usao/nce/press/2014/2014-apr-29.html>.
27. <http://www.justice.gov/opa/pr/attorney-general-holder-vows-justice-department-will-continue-look-banks-help-payment>.
28. <http://www.consumerfinance.gov/blog/category/payday-loans/>. In July 2014, the CFPB reached a \$10 million settlement with one of the country’s largest payday lenders (ACE Cash Express) over illegal debt collection tactics. <http://www.forbes.com/sites/laurengensler/2014/07/10/cfpb-moves-against-payday-loan-industry-orders-ace-cash-express-to-pay-10-million/>.
29. <http://www.dfs.ny.gov/about/press2013/pr1308061.htm> and <http://www.dfs.ny.gov/about/press2013/pr130806-link1.pdf>.
30. https://www.shazam.net/pdf/ach_networkQuality_propRules_1113.pdf.
31. <http://www.dfs.ny.gov/about/press2014/pr1401131-letter-nacha.pdf>.
32. <https://www.nacha.org/rules/ach-network-risk-and-enforcement-and-improving-ach-network-quality>.
33. <http://www.dfs.ny.gov/about/press2014/pr1404301.htm>.
34. <http://oversight.house.gov/release/report-doj-operation-choke-point-secretly-pressured-banks-cut-ties-legal-business/>.
35. H.R. 4986.
36. <http://online.wsj.com/articles/trade-group-sues-u-s-bank-regulators-over-payday-crackdown-1402020003>.
37. <http://financialservices.house.gov/calendar/eventsingle.aspx?EventID=387064>.
38. <http://www.crapo.senate.gov/issues/banking/documents/RepublicanLettertoHolderDOJOperationChokePoint10-06-14.pdf>.
39. http://luetkemeyer.house.gov/uploadedfiles/10_16_14_doj_letter.pdf and http://luetkemeyer.house.gov/uploadedfiles/10_23_14_fdic_letter.pdf.
40. Financial Institution Letter FIL-41-2014 (July 28, 2014), <https://www.fdic.gov/news/news/financial/2014/fil14041.pdf>.

41. <http://www.treasury.gov/press-center/press-releases/Pages/jl2595.aspx>. FinCen had published an Advanced Notice of Proposed Rulemaking ("ANPR") in March 2012 and, thereafter, received about 90 comments and held five public hearings.
42. For example, Global Financial Integrity's comments can be found at: <http://www.gfintegrity.org/press-release/gfi-comments-fincen-notice-proposed-rulemaking-customer-due-diligence-requirements-financial-institutions/>.
43. FinCen notes in the NPR that it may consider expanding the proposed rule to cover other financial institutions not currently subject to CIP requirements, such as money services businesses.
44. 31 C.F.R. § 1010.620(b)(1).
45. 31 C.F.R. § 1010.610(b)(1)(iii)(A).
46. <http://www.consumerfinance.gov/newsroom/cfpb-finalizes-revisions-to-rule-protecting-consumers-sending-money-internationally/>.
47. Regulations governing "remittance transfers" (consumer international electronic transfers of funds) became effective on October 28, 2013. Those regulations implemented Section 1073 of the Dodd-Frank Act, and are found in Subpart B of CFPB Regulation E (which implements the Electronic Funds Transfer Act).
48. <http://www.consumerfinance.gov/newsroom/cfpb-finalizes-rule-to-oversee-larger-nonbank-international-money-transfer-providers/>.
49. Similar bills have been introduced in other States. On May 5, 2014, for example, the Hawaii legislature passed a bill to allow employers to use payroll cards to pay employees, provided certain conditions are met to protect the employee. Haw. Rev. Stat. Section 388-2.
50. <http://www.ag.ny.gov/pdfs/Pinched%20by%20Plastic.pdf>.

Sabra M. Baum is senior counsel at M&T Bank, focusing largely on bank depository related matters. She is a member of the Executive Committee of the Business Law Section of the NYSBA.

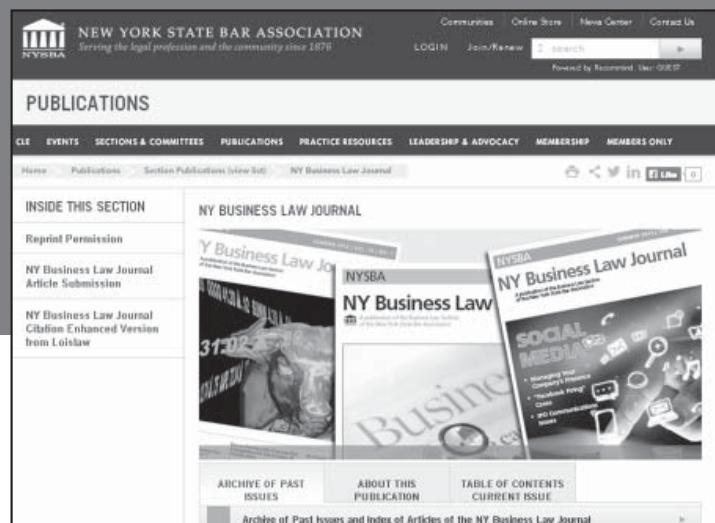
The *NY Business Law Journal* is also available online

Go to www.nysba.org/BusinessLawJournal to access:

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

*You must be a Business Law 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.



Recent Employment Laws Impacting Private Employers in New York

By Sharon Parella and Leah Ramos

Introduction

During 2014, the New York City Council and New York State Legislature enacted several laws that are particularly impactful on private employers and their workplaces. In addition, significant legislation regulating “abusive conduct” in the workplace (commonly referred to as “workplace bullying”) is currently under consideration by the New York State Senate and Assembly, and is being closely watched by employers, employees, lawyers and advocates.

A summary of these laws is set forth below.

New York City Council Enactments

Prohibition of Discrimination Against Unpaid Interns

Effective June 14, 2014, an amendment to the New York City Human Rights Law both extended current prohibitions against workplace discrimination to unpaid interns and clarified that the current prohibitions are indisputably applicable to paid interns despite the generally short-term nature of their employment.

The New York City Human Rights Law (NYCHRL)¹ provides, among other things, that it is unlawful for an employer with four or more employees to discriminate against its employees on the basis of race, creed, color, age, national origin, gender (including gender identity and sexual harassment), disability (including pregnancy), marital status, partnership status, sexual orientation, alienage or citizenship status, arrest or conviction record, status as a victim of domestic violence, stalking and sex offenses or unemployment status in hiring, compensation or the terms, conditions or privileges of employment. The new law mandates that interns, both paid and unpaid, are covered by the foregoing protected categories, and defines an “intern” as follows:

The term “intern” shall mean an individual who performs work for an employer on a temporary basis whose work: (a) provides training or supplements training given in an educational environment such that the employment of the individual performing the work may be enhanced; (b) provides experience for the benefit of the individual performing the work; and (c) is performed under the close supervision of existing staff. The term shall include such individuals without regard to whether the employer pays them a salary or wage.²

In addition, a New York City Council press release indicates that the new law “would require employers to make reasonable accommodations for interns in certain circumstances.”³

This amendment to the NYCHRL was largely in response to the 2013 decision in *Wang v. Phoenix Satellite Television US, Inc.*,⁴ in which the court held that an unpaid intern could not sue her employer for sexual harassment under the NYCHRL because she was unpaid and, therefore, not intended to be a covered person within the meaning of the statute. Ms. Wang, then a 22-year-old master’s degree student, had alleged that she had been subjected to a hostile work environment, quid pro quo sexual harassment and retaliation by her supervisor. The court granted the employer’s motion to dismiss these claims, concluding that:

The plain meaning of the NYCHRL, the case law, interpretations of analogous wording in Title VII [of the Civil Rights Act of 1964] and the [New York State Human Rights Law], as well as the legislative history of the NYCHRL all confirm that the NYCHRL’s protection of employees does not extend to unpaid interns.⁵

Ms. Wang also had asserted that Phoenix Satellite Television (“Phoenix”) failed to hire her for full-time employment based on the discriminatory animus of her supervisor; these claims (brought under both the NYCHRL and the New York State Human Rights Law) survived Phoenix’s motion to dismiss the second amended complaint.

Regulation of Electronic Cigarettes

Effective April 29, 2014, an amendment to New York City’s Smoke-Free Air Act prohibits the use of electronic cigarettes in all locations where smoking is prohibited, including in places of employment.⁶ Employers are required to modify their no smoking policies to include electronic cigarettes.

Provision of Paid Sick Time to Employees

Effective April 1, 2014, under New York City’s Earned Sick Time Act (“Paid Sick Leave Law”), employers with five or more employees who are hired to work more than 80 hours each calendar year must provide employees with up to 40 hours of paid sick leave each calendar year.⁷ Employers with fewer than five employees must provide an equal amount of sick leave on an unpaid basis. Employers with one (or more) domestic worker who has been employed for at least one year and works more

than 80 hours each calendar year must provide two days of paid sick leave (in addition to the three days of paid rest provided under the New York State Labor Law⁸). Employees accrue sick leave at the rate of one hour for every 30 hours worked, up to a maximum of 40 hours of sick leave per calendar year (accrual differs for domestic workers, as well as for employees who are covered by collective bargaining agreements). Employees begin to accrue sick leave on April 1, 2014 or on their first day of employment, whichever is later (the date accrual begins differs for certain employees covered by collective bargaining agreements).

In addition, employers must provide employees with written notice of their rights to sick leave, and maintain records reflecting compliance with the law. A "Notice of Employee Rights" may be obtained on the NYC Department of Consumer Affairs website and is available in 26 languages.⁹

An employee may use sick leave when he or she:

- (i) has a mental or physical illness, injury, or health condition; needs to get a medical diagnosis, care, or treatment of his or her mental or physical illness, injury or condition; or needs to get preventive medical care.
- (ii) must care for a family member who needs medical diagnosis, care, or treatment of a mental or physical illness, injury or health condition, or who needs preventive medical care.
- (iii) works for an employer whose business is closed due to a public health emergency, or needs to care for a child whose school or child care provider is closed due to a public health emergency.

Under the law, "family members" are defined as a:

- (i) child (biological, adopted or foster child; legal ward; child of an employee standing *in loco parentis*)
- (ii) grandchild
- (iii) spouse
- (iv) domestic partner
- (v) parent
- (vi) grandparent
- (vii) child or parent of an employee's spouse or domestic partner
- (viii) siblings (including half, adopted or step sibling).

If the need for sick leave is foreseeable, an employer may require up to seven days' advance notice of the employee's intention to use sick leave. If the need is un-

foreseeable, the employer may require notice as soon as practicable.

Up to 40 hours of unused sick leave can be carried over to the next calendar year. An employer is only required, however, to allow an employee to use up to 40 hours of sick leave per calendar year.

Finally, employers may not retaliate against employees who (i) request and use sick leave, (ii) file complaints with the Department of Consumer Affairs for alleged violations of the law, (iii) communicate with any person, including coworkers, about any violation of the law, (iv) participate in an administrative or judicial action regarding an alleged violation of the law, or (v) inform another person of that person's potential rights. Retaliation includes any threat, discipline, discharge, demotion, suspension or reduction in hours, or any other adverse employment action for exercising or attempting to exercise any right under the law.

Prohibition of Discrimination Based on Pregnancy, Childbirth or a Related Medical Condition

Effective January 30, 2014, the New York City Pregnant Workers Fairness Act makes it illegal for an employer with four or more employees to refuse to provide reasonable accommodations to pregnant women and those who suffer medical conditions related to pregnancy and childbirth.¹⁰ Reasonable accommodations may include bathroom breaks, breaks to facilitate increased water intake, periodic rest if the employee is required to stand for long periods of time, assistance with manual labor, changes to the employee's work environment and unpaid medical leave.¹¹ In addition, employers must provide written notice to their employees regarding the right to be free from this type of discrimination. In this regard, a poster which satisfies this written notice requirement, entitled "Pregnancy & Employment Rights," may be obtained on the NYC Commission on Human Rights website and is available in seven languages.¹²

Prohibition of Discrimination Based on an Individual's Status as Unemployed

Although this amendment to the New York City Human Rights Law was effective June 11, 2013, it is important to remember that employers with four or more employees are prohibited from considering an applicant's status as being unemployed when making employment decisions with regard to hiring, compensation or the terms, conditions or privileges of employment, unless there is a substantially job-related reason for doing so.¹³ Employers are also prohibited from posting job advertisements that require applicants to be currently employed or that state that the employer will not consider applicants based on their unemployment status. Under the law, "unemployed" is defined as "not having a job, being available for work, and seeking employment."¹⁴ In addition to providing that an employer may consider an applicant's

unemployment based on a substantially job-related reason, express exemptions contained in the law permit employers to (i) inquire into the circumstances surrounding an applicant's separation from prior employment, (ii) decide that only applicants who are its current employees will be considered for employment or given priority for employment or with respect to compensation, terms, conditions or privileges of employment, or (iii) publish an advertisement for a job vacancy that requires or takes into consideration certain job-related qualifications (such as a current and valid professional or occupational license, a minimum level of education or training, or a minimum level of occupational or field experience).

New York State Legislature

Protection of Unpaid Interns from Workplace Discrimination and Sexual Harassment

On July 22, 2014, Governor Andrew Cuomo signed into law an amendment to the New York State Human Rights Law which extends protections against workplace discrimination and harassment to unpaid interns.¹⁵ The amendment was effective immediately upon signing.

The new law defines an "intern" as follows:

[A] person who performs work for an employer for the purpose of training under the following circumstances:

- a. the employer is not committed to hire the person performing the work at the conclusion of the training period;
- b. the employer and the person performing the work agree that the person performing the work is not entitled to wages for the work performed; and
- c. the work performed: (1) provides or supplements training that may enhance the employability of the intern; (2) provides experience for the benefit of the person performing the work; (3) does not displace regular employees; and (4) is performed under the close supervision of existing staff.¹⁶

Pending Legislation Prohibiting Abusive Conduct in the Workplace

"Workplace bullying" is indisputably a hot topic in New York and throughout the United States. Nonetheless, although illegal in many countries, there is currently no law prohibiting workplace bullying alone in the United States. Federal and state courts prohibit workplace bullying only in cases where the bullying conduct relates to acts of discrimination and/or harassment based on

protected categories under federal, state or local discrimination laws and/or retaliation based on the target of the bullying making a report of discrimination or harassment. In addition, in cases where discrimination or sexual harassment did not occur, New York courts may protect against workplace bullying under tort laws (such as laws prohibiting the intentional infliction of emotional distress) or pursuant to an employer's policies on professional conduct (finding a breach of contract if a policy prohibits workplace bullying and the employer does not take steps to correct a bullying situation).

New York was the ninth state to introduce legislation to prohibit "abusive conduct" in the workplace. The currently pending Senate and Assembly bills are based on a template that was created by Professor David Yamada of Suffolk University School of Law. Specifically, in 2001 Professor Yamada proposed legislation, entitled the "Healthy Workplace Bill" ("HW Bill"), with the intent that it would be enacted in each state throughout the United States. The text of this original bill was based on Professor Yamada's extensive research on workplace bullying and conclusion that there is a need for "status blind" harassment laws (i.e., protection from harassment in the workplace regardless of whether the harassment is based on one of the protected categories under federal, state or local discrimination laws). The text of the bill was later revised in 2009.

In 2010, a HW Bill was passed in the New York Senate.¹⁷ This bill was subsequently "held" and extinguished in the New York Assembly. A new 2011 Assembly HW Bill was filed on February 2, 2011 by Assemblymember Steve Englebright.¹⁸ The companion Senate HW Bill¹⁹ was introduced by Senator Diane J. Savino and was referred to the Labor Committee on March 28, 2011. On February 13, 2013, Assemblymember Englebright reintroduced the HW Bill for the 2013-2014 Legislative Session.²⁰ On February 25, 2013, Senator Savino reintroduced the Senate version of the HW Bill,²¹ and it was referred to the Senate Labor Committee. The Senate Labor Committee passed the HW Bill on June 3, 2013, and it is now before the Senate Finance Committee.

The proposed New York HW Bill establishes a civil cause of action for employees who are subjected to an "abusive work environment," and provides, among other things, that:

- (1) It is unlawful to subject an employee to an "abusive work environment." Affected employees may bring legal actions in court against their employers and/or the bullies who target them.
- (2) "Abusive conduct" is conduct (acts and/or omissions) that "a reasonable person would find abusive." The severity, nature and frequency of the behavior at issue are relevant when determining whether such conduct is "abusive." "Abusive conduct" includes (i) repeated verbal abuse (such as derogatory remarks, insults and epithets);

(ii) verbal or physical conduct that a reasonable person would find threatening, intimidating or humiliating; and/or (iii) the sabotage or undermining of an employee's work performance. Conduct that exploits an employee's known psychological or physical illness or disability is considered an aggravating factor.

- (3) A single act will not constitute "abusive conduct," unless such single act is especially severe or egregious.
- (4) An "abusive work environment" is a workplace where an employer or one or more of its employees, acting with intent to cause pain or distress to an employee, subjects that employee to "abusive conduct" that causes physical and/or psychological harm to the employee.
- (5) One possible remedy is that employers must remove the bullies from their workplaces.
- (6) Additional remedies include reinstatement, reimbursement for lost wages, front pay and medical expenses, compensation for pain and suffering, compensation for emotional distress, punitive damages and attorneys' fees.
- (7) Affirmative defenses are available to both employers and purported bullies, and retaliation against an employee who complains about "abusive conduct" is prohibited.
- (8) Any action in court must be commenced by the targeted employee within one year of the last incident of "abusive conduct" which is the basis of the allegation of an "abusive work environment."

It is noteworthy that neither the New York State Legislature nor the New York City Council has enacted a law requiring sexual harassment training by employers. By contrast, California law currently mandates that employers with 50 or more employees must provide at least two hours of sexual harassment training and education to all supervisory employees in California within the first six months of the employee's assumption of a supervisory role and every two years thereafter.²² Moreover, in September 2014, California enacted a new law, effective January 1, 2015, which requires employers with 50 or more employees to include "prevention of abusive conduct" as part of the sexual harassment training that is provided to supervisory employees.²³

Endnotes

1. N.Y.C. ADMIN. CODE §§ 8-101 *et seq.*
2. *Id.* § 8-102(28).
3. Press Release, The Council of the City of New York Office of Communications, Council Votes to Protect Interns against Discrimination (Mar. 6, 2014), <http://council.nyc.gov/html/pr/032614stated.shtml>.
4. 976 F. Supp. 2d 527 (S.D.N.Y. 2013).
5. *Id.* at 537.
6. N.Y.C. ADMIN. CODE §§ 17-501 *et seq.*
7. *Id.* §§ 20-911 *et seq.*
8. See N.Y. LABOR LAW § 161(1).
9. NYC's Paid Sick Leave Law, N.Y.C. DEP'T OF CONSUMER AFF., <http://www.nyc.gov/html/dca/html/law/PaidSickLeave.shtml> (last visited Nov. 20, 2014).
10. N.Y.C. ADMIN. CODE § 8-107(22).
11. See N.Y.C. LOCAL LAW INT. NO. 974-A, available at <http://legistar.council.nyc.gov/View.ashx?M=F&ID=2633222&GUID=F483E5BC-9A79-4704-B38B-063FA005267A> (last visited Nov. 20, 2014).
12. *Pregnancy & Employment Rights Posters*, N.Y.C. COMMISSION ON HUM. RTS., <http://www.nyc.gov/html/cchr/html/publications/pregnancy-employment-poster.shtml> (last visited Nov. 20, 2014).
13. N.Y.C. ADMIN. CODE § 8-107(21).
14. *Id.* § 8-102(27).
15. N.Y. EXEC. LAW § 296-c.
16. *Id.* § 296(c)(1).
17. S. 1823, 2009 Leg., Reg. Sess. (N.Y. 2009).
18. Assemb. 4258, 2013 Leg., Gen. Assemb. (N.Y. 2013).
19. S. 2489, 2011 Leg., Reg. Sess. (N.Y. 2011).
20. Assemb. 4965, 2013 Leg., Gen. Assemb. (N.Y. 2013).
21. S. 3865, 2014 Leg., Reg. Sess. (N.Y. 2013).
22. CAL. GOV. CODE § 12950.1(a).
23. *Id.* § 12950.1(g) (as amended).

Sharon Parella is a partner and Leah Ramos is senior counsel in the Labor & Employment group at Thompson Hine LLP. Their practices focus on representing employers, including domestic and foreign financial institutions, in all aspects of employment law, and they are based in Thompson Hine's New York office. They are also Executive Editors of the Advance@Work blog on workplace innovators (www.advanceatwork.com), and have published an e-book on workplace bullying, entitled *Workplace Bullying (The Inside Story): FAQs About Workplace Bullying*.

Inside the Courts

Prepared by Attorneys at Skadden, Arps, Slate, Meagher & Flom LLP

CLASS CERTIFICATION

E.D.N.Y. Denies Class Certification in Investment Marketing Materials Dispute

***Goodman v. Genworth Fin. Wealth Mgmt. Inc.*, No. 09-CV-5603(JFB)(GRB), 300 F.R.D. 90 (E.D.N.Y. Apr. 15, 2014).**

Judge Joseph F. Bianco of the U.S. District Court for the Eastern District of New York denied class certification of claims that a financial services company violated Section 10(b) of the Securities Exchange Act by allegedly misrepresenting the company's investment approach in its marketing materials. The plaintiffs alleged that Genworth misrepresented that its investment approach would be guided by a particular investment manager's recommendations concerning mutual fund and asset allocation selections. The court determined that the plaintiffs failed to allege a common theory of reliance as required under Federal Rules of Civil Procedure 23(b)(3). The plaintiffs did not identify an efficient market for the securities at issue, so they were not entitled to a presumption of reliance under the fraud-on-the-market theory. The plaintiffs also were not entitled to a presumption of reliance under *Affiliated Ute Citizens of Utah v. United States*, 406 U.S. 128 (1972), which applies to material omissions, because the plaintiffs' claims actually were based on Genworth's affirmative representations concerning an investment manager's role in mutual fund selection and asset allocation, not any alleged omissions. In addition, the court rejected the plaintiffs' purported expert on class-wide reliance because plaintiffs could not prove class-wide reliance by showing that the representations and omissions at issue were uniform and material.

DEMAND FUTILITY

Ninth Circuit Reverses District Court's Dismissal, Holds Plaintiffs Adequately Alleged Demand Futility in Shareholder Derivative Action

***Rosenbloom v. Pyott*, No. 12-55516 (9th Cir. Sept. 2, 2014).**

The U.S. Court of Appeals for the Ninth Circuit reversed the dismissal of a derivative action brought by shareholders of Allergan, Inc., concluding that the plaintiffs had adequately alleged demand futility.

Allergan makes Botox, a cosmetic and therapeutic drug. Botox has been prescribed for both on-label and off-label uses. While a doctor may prescribe an approved drug for an off-label use, federal law imposes limits on whether and how a drug manufacturer can promote off-

label uses. In 2010, Allergan faced allegations it had acted illegally in marketing and labeling Botox. The company settled several *qui tam* suits and pleaded guilty in a criminal case. Allergan ultimately paid over \$600 million in fines.

Shortly thereafter, plaintiff shareholders filed a derivative action alleging that Allergan's directors were liable to the company for violations of various state and federal laws, and for breaches of their fiduciary duties. The plaintiffs, however, did not make a demand on Allergan's board requesting that Allergan bring the claims in its own name. The plaintiffs argued that demand was excused for two reasons. First, the board decided to pursue a business plan premised on unlawful conduct. Second, the board remained consciously inactive despite actual or constructive knowledge of wrongdoing at the company. The district court dismissed the action, concluding that the plaintiffs failed to allege particularized facts that demand was excused.

On review, the Ninth Circuit first explained the different standards under which demand may be excused. For the plaintiffs' claim that the board pursued a business plan premised on unlawful conduct, the two-part, disjunctive *Aronson* test applies. See *Aronson v. Lewis*, 473 A.2d 805, 814 (Del. 1984). Under that standard, demand is excused if, under the particularized facts alleged, *either* a reasonable doubt is created that the directors are disinterested and independent, *or* there is a reasonable doubt that the challenged transaction was otherwise the product of a valid exercise of business judgment. Under that standard, the court noted, a director has a "disabling interest for pre-suit demand purposes when the potential for liability...may rise to a substantial likelihood."

For the plaintiffs' claim that the board remained consciously inactive when it knew (or should have known) about the illegal conduct, the court acknowledged that the demand standard is "less settled." Some courts have employed the *Aronson* test for the claim. Other courts classify the claim as a theory of oversight liability, as set forth in *In re Caremark Int'l.*, 698 A.2d 959, 971 (Del. Ch. 1996). Demand futility for *Caremark* claims is tested under the *Rales* standard, which requires a plaintiff to allege facts that create a reason to doubt that the board "could have properly exercised its independent and disinterested business judgment in responding to a demand." *Rales v. Blasband*, 634 A.2d 927, 934 (Del. 1993). Despite the uncertainty regarding the appropriate demand standard, the court explained that demand is excused under either approach if a plaintiff alleges particularized facts that create a reasonable doubt as to whether a majority of a board

faces a substantial likelihood of personal liability for breaching the duty of loyalty. The court also noted that, “[w]hen appropriate, courts may evaluate demand futility by looking to the whole board of directors rather than by going one by one through its ranks.”

The panel first analyzed the plaintiffs’ claim that the board remained consciously inactive despite actual or constructive knowledge of wrongdoing at the company. The court recognized, as Allergan argued, that it was entirely possible for off-label sales to increase on their own, without any illegal promotion by a drug manufacturer. Here, however, the plaintiffs provided “a battery of particularized factual allegations that strongly support an inference” that the board knew of illegal activity and yet did nothing. First, the plaintiffs alleged that the board closely and regularly monitored off-label Botox sales. Second, the board received data directly linking Allergan’s sales programs to fluctuations in off-label sales. Third, the board received repeated FDA warnings about illegal promotion of Botox. Fourth, Botox was one of Allergan’s most important drugs. Fifth, the conduct “was unquestionably of significant magnitude and duration.”

The court concluded that, taking these allegations together, the district court abused its discretion in determining that they did not create a reasonable inference of conscious inaction. The panel highlighted three specific errors by the district court. First, the district court considered the allegations in isolation rather than in combination, “even though in cases like this one an inference of Board involvement or knowledge may depend on a combination of factual allegations.” Second, the district court drew inferences in the board’s favor, rather than in the plaintiffs’ favor. Third, “the district court essentially insisted on a smoking gun of Board knowledge, even though precedent holds that plaintiffs can show demand futility by alleging particular facts that support an *inference* of conscious inaction.”

Having already determined that demand was excused, the panel still proceeded to briefly analyze demand futility under the plaintiffs’ claim that the board pursued a business plan premised on unlawful conduct. Taking the same factual allegations, the court concluded that it was a reasonable inference that the “red flags of illegal conduct” were not “signs that the marketing team had gone off the rails.” Rather, as the plaintiffs alleged, it was reasonable to infer that “they were welcome indicators that a massive, Board-approved push for off-label sales of Botox was going according to plan.” The court reasoned that an inference that the board decided to break the law can be drawn even without a “Board-approved document stating, ‘we’re all going to go promote Botox off-label now and do so in a way that violate[s] the FDA’s regulations.’” Rather, it is sufficient if the allegations create a reasonable doubt that the board adopted a plan premised on illegal, off-label marketing of Botox, and therefore faces a substantial likelihood of liability for breaching the duty of loyalty.

District of Nevada Dismisses MGM Mirage Shareholder Derivative Action, Citing Issue Preclusion

***In re MGM Mirage Derivative Litig.*, No. 2:09-cv-01815-KJD-RJJ, 2014 WL 2960449 (D. Nev. June 30, 2014).**

Judge Kent J. Dawson of the U.S. District Court for the District of Nevada granted defendant MGM Resorts International’s (MGM) motion to dismiss a shareholder derivative action.

The plaintiff alleged that MGM officers and directors made false representations regarding MGM’s “construction of CityCenter, a massive, multi-billion dollar high rise on the Las Vegas strip.” The plaintiff failed to make a demand on MGM’s board, but alleged that demand was not required because it would have been futile.

Meanwhile, two other MGM shareholders filed a derivative suit in Nevada state court in 2011, alleging the same misleading conduct on the part of MGM directors and officers, and alleging the same issues of demand futility. The Nevada state court granted MGM’s motion to dismiss that action, and the Nevada Supreme Court affirmed the judgment in December 2013.

Given the state court ruling, MGM argued here that the plaintiff was precluded from relitigating the same issue. Judge Dawson first explained that, in applying Nevada issue preclusion law, four elements must be satisfied: (1) the issue decided in the prior litigation must be identical to the issue presented here; (2) the initial ruling must have been on the merits and final; (3) the party against whom the judgment is asserted must have been a party in privity with a party in the prior litigation; and (4) the issue was actually and necessarily litigated. The plaintiffs here based their arguments on elements (1) and (3).

As to whether the issues here and in the prior state court action were identical, the plaintiff argued that the facts supporting the demand futility issue were different because the plaintiff here had access to internal MGM documents and the benefit of a court order in a related securities action. The court disagreed, reasoning that “[d]emand futility is the ‘common issue’ in both proceedings.” Thus, “additional facts supporting demand futility are irrelevant.”

As to whether the party here was the same as, or in privity with, the parties in the prior action, the plaintiff argued that the actions were brought by different shareholders. The court acknowledged a “dearth of Nevada state law” on this point. However, the court noted that a derivative action allows a shareholder to “step into the corporation’s shoes,” and found persuasive a recent District of Nevada opinion that concluded “plaintiffs in a shareholder derivative action represent the corporation, and therefore the question of whether demand on the board of directors would have been futile is an issue that is the same no matter which shareholder serves as plaintiff.” The court allowed for the possibility that the

plaintiff may have merely been in privity with the state court shareholder plaintiffs, but “it is clear that Plaintiff is one or the other.” Therefore, element (3) was satisfied. Accordingly, because all four elements of Nevada’s issue preclusion law were met, the court dismissed the complaint.

District Court Dismisses Derivative Claims Over Parent Company’s Actions Regarding Struggling Subsidiary

***Gordon v. Bindra*, No. 2:14-cv-01058-ODW(ASx), 2014 U.S. Dist. LEXIS 77620 (C.D. Cal. June 5, 2014).**

Judge Otis D. Wright II of the U.S. District Court for the Central District of California dismissed, for failure to allege demand futility, a shareholder derivative action alleging that board members of Edison International (EIX), in violation of their fiduciary duties, caused subsidiary Energy Mission Energy (EME) to pay \$924 million in dividends and \$183 million under a tax-sharing agreement while EME was insolvent. According to the complaint, these actions forced EME into bankruptcy.

The plaintiff attempted to demonstrate that the directors were not disinterested by alleging that they faced a serious threat of liability based on the allegations. The court concluded that the plaintiff failed to make that showing.

First, the court noted that, under California law, “there is no indication” of a duty owed by directors of a parent corporation to a subsidiary. Moreover, California courts have held that there is “no broad, paramount fiduciary duty of due care or loyalty that directors of an insolvent corporation owe the corporation’s creditors solely because of a state of insolvency.” Given that, the parent company directors would also not owe a fiduciary duty to the subsidiary’s creditors because “the parent’s directors...are even further removed.” Therefore, the plaintiff cannot establish demand futility based on a likelihood of director liability.

Second, EIX’s articles of incorporation include an exculpation clause that relieves directors of liability to the extent allowed under California law. Thus, the plaintiff would have to allege that the directors acted intentionally, knowingly, or in bad faith.

Third, even if the court were to find that the EIX board owed EME some fiduciary duty on the basis that EME was insolvent, the plaintiff still failed to adequately plead that EME was, in fact, insolvent. The complaint contained numerous statements regarding EME’s “financial crisis” or “looming debt problems,” but those descriptive phrases, the court ruled, could not substitute for well-pleaded allegations regarding EME’s insolvency.

Fourth, the plaintiff failed to allege on a “director-by-director” basis why each did not meet the test of independence or disinterest. Rather, “she lumps all Individual Defendants together or simply references the ‘EIX

Board.” Such “generalized allegations preclude the Court from making findings” regarding each director.

Finally, the plaintiff failed to allege that the transactions in question were not a valid exercise of business judgment. The plaintiff based her argument on the claim that the directors acted in bad faith by forcing EME to violate a provision of the U.S. Bankruptcy Code. However, the allegedly fraudulent transfer occurred before EME was insolvent, even under the plaintiff’s allegations. Further, as noted above, the plaintiff failed to plead sufficient facts that EME was, in fact, insolvent.

ERISA

Seventh Circuit Reverses District Court Decision Granting Defendant Summary Judgment in ERISA Action for Breach of Fiduciary Duty

***Fish v. Greatbanc Trust Co.*, 749 F.3d. 671 (7th Cir. 2014).**

The U.S. Court of Appeals for the Seventh Circuit reversed the district court’s grant of summary judgment in favor of the defendants in an action brought under the Employee Retirement Income Security Act of 1974 (ERISA). The plaintiffs, participants in The Antioch Company’s employee stock ownership plan, alleged that the plan trustee breached its fiduciary duties in connection with a leveraged buyout of Antioch stock that ultimately left the company bankrupt. The defendants contended that the plaintiffs’ claims were time-barred under ERISA’s three-year statute of limitations because the plaintiffs gained actual knowledge of the alleged ERISA violations from proxy statements describing the transaction and the company’s subsequent financial decline more than three years before they filed suit.

In reversing the district court’s decision, the Seventh Circuit held that a plaintiff does not have “actual knowledge” of a breach of fiduciary duty, for purposes of triggering ERISA’s three-year statute of limitations, until the plaintiff has knowledge of “all material facts.” However, the court explained that this standard does not require that plaintiffs have knowledge of every detail of a transaction or knowledge of illegality. The court further ruled that where a plaintiff alleges a “process-based” fiduciary duty claim, knowledge of the transaction terms alone is not enough to trigger the three-year statute of limitations. Rather, the court explained, the plaintiff must have actual knowledge of the procedures the fiduciary used or failed to use.

Applying this standard, the Seventh Circuit concluded that neither the proxy materials nor plaintiffs’ knowledge of Antioch’s financial problems gave them actual knowledge of the inadequate processes the fiduciaries used to evaluate the buyout transaction more than three years before filing suit. Thus, the court ruled the

plaintiffs' claims were not time-barred under ERISA's three-year statute of limitations.

EXCHANGE ACT

Ninth Circuit Holds Company's Alleged False and Misleading Statements Were Nonactionable Puffery and That Plaintiffs Failed to Adequately Plead Scienter

***Police Ret. Sys. of St. Louis v. Intuitive Surgical, Inc.*, No. 12-16430, 2014 WL 3451566 (9th Cir. July 16, 2014).**

The U.S. Court of Appeals for the Ninth Circuit affirmed the dismissal of a federal securities action brought under Section 10(b) of the Exchange Act and SEC Rule 10b-5. In affirming the district court, the panel held that the company's purportedly false and misleading statements were actually nonactionable puffery. In addition, the plaintiffs failed to adequately allege that executives made false statements with knowing or reckless disregard for the truth.

The plaintiffs alleged that Intuitive executives, in the company's 2007 annual report and in four analyst calls in 2008, painted an overly optimistic picture of the company's prospects for continued growth despite internal data showing Intuitive was headed for a slowdown.

The Ninth Circuit disagreed, holding that the plaintiffs failed to adequately plead falsity or scienter. As to falsity, the panel concluded that the alleged misstatements—which the court characterized as “classic growth and revenue projections”—either were forward-looking statements covered by the safe harbor provision of the PSLRA or mere corporate puffery. For the statements concerning future economic performance or “assumptions underlying those projections,” Intuitive provided disclaimers accompanying each purported misstatement. Those disclaimers contained cautionary language that was “virtually identical to the cautionary language approved in *Cutera*,” referring to *In re Cutera Sec. Litig.*, 610 F.3d 1103 (9th Cir. 2010), the preeminent Ninth Circuit case on statements protected by the PSLRA's safe harbor provision.

As to scienter, the plaintiffs attempted to establish scienter through three different avenues: (1) the core operations theory, (2) witness accounts and (3) evidence of insider trading. Under the core operations theory, the plaintiffs failed to allege specific facts showing the individual defendants' involvement in day-to-day operations, or that the individual defendants accessed reports that purportedly showed a grim financial outlook for the company. The witness account consisted of the impressions of a single low-level employee, amounting to “an unsubstantiated statement without substance or context.” Finally, as to insider trading, “the complaint contains no allegations regarding the defendants' prior trading history, which are necessary to determine whether the sales

during the Class Period were ‘out of line with’ historical practices.”

Third Circuit Affirms Dismissal of 10b-5 Claims Against Pfizer Over Alzheimer's Drug

***City of Edinburgh Council v. Pfizer, Inc.*, 754 F.3d 159 (3d Cir. 2014).**

The U.S. Court of Appeals for the Third Circuit affirmed the dismissal of claims brought against Pfizer, as successor-in-interest to Wyeth, under Section 10(b) of the Securities Exchange Act and SEC Rule 10b-5.

The plaintiff investors alleged that Wyeth made false and misleading statements regarding interim Phase 2 clinical trial data for its Alzheimer's drug, including that the company's decision to initiate a Phase 3 trial was based, in part, on the “‘encouraging’” Phase 2 interim data. In addition, the plaintiffs alleged that Wyeth's statements and actions triggered a duty to disclose full and complete material information about the Phase 2 interim results.

In denying the plaintiffs' appeal and affirming the district court's dismissal, the Third Circuit first explained that the plaintiffs' “own pleading demonstrates the accuracy of defendants' statement.” Indeed, the plaintiffs' allegations of falsity were “based on a selective reading” of Wyeth's purportedly misleading press release. A complete reading of the press release revealed no false or misleading statements. Second, the allegedly misleading statements “explicitly cautioned investors that ‘[n]o conclusion’ could be drawn about the Phase 2 interim results until the completion of Phase 2.” Third, the affirmative statements the company made regarding the Phase 2 interim results referred to them in ways such as “encouraging.” Such expressions, the court held, were mere inactionable puffery.

The panel next addressed the allegations supplied by two confidential witnesses, described as “former Wyeth executives” who were involved in the development of the Alzheimer's drug. According to the confidential witnesses, there was internal disagreement regarding how to interpret the Phase 2 interim results, and whether they supported the decision to proceed to Phase 3. The Third Circuit held that these allegations were also insufficient to state a claim. “Interpretations of clinical data are considered opinions. Opinions are only actionable under the securities laws if they are not honestly believed and lack a reasonable basis. [Plaintiffs] have failed to adequately allege defendants did not honestly believe their interpretation of the interim results or that it lacked a reasonable basis.”

Finally, the court held that the company was under no duty to disclose the full Phase 2 interim results. According to the court, because Wyeth did not “place the strength or nature of the Phase 2 interim results ‘in

play,'...it was under *no* duty to provide additional details about those results."

Northern District of California Dismisses with Prejudice Claims Against Hewlett-Packard Arising Out of Allegations Regarding Former CEO's Relationship with Ex-Adult Film Actress

***Retail Wholesale & Dep't Store Union Local 338 Ret. Fund v. Hewlett-Packard Co.*, No. 12-cv-04115-JST, 2014 WL 2905387 (N.D. Cal. June 25, 2014).**

Judge Jon S. Tigar of the U.S. District Court for the Northern District of California dismissed with prejudice claims brought by Hewlett-Packard shareholders alleging that the company and its former chairman, president and CEO, Mark Hurd, made false and misleading statements and omissions regarding Hurd's compliance with HP's Standards of Business Conduct (SBC) policy. The plaintiffs alleged that HP and Hurd made statements regarding the importance of the SBC policy and, in so doing, implied that Hurd "was in fact in compliance with them."

Instead, according to the Second Amended Complaint (SAC), Hurd hired ex-adult film actress Jodie Fisher, with whom he had a personal relationship, as an independent consultant to host executive events and introduce Hurd to important HP customers. A later investigation by HP's board revealed that Fisher received compensation or expense reimbursement where there was not a legitimate business purpose, and that Hurd submitted inaccurate expense reports that were intended to or had the effect of concealing his relationship with Fisher. Thus, the plaintiffs alleged, statements implying Hurd's compliance with the SBC policy were materially misleading, and Hurd's failure to disclose his conduct was a material omission.

The district court disagreed, concluding that "[b]oth claims fail because they do not adequately plead materiality or falsity." While the SAC adequately alleged that Hurd violated the SBC, plaintiffs failed to plead that any of HP or Hurd's representations amounted to a warranty of ethical compliance with the SBC. The court explained "a code of ethics is inherently aspirational; it simply cannot be that every time a violation of that code occurs, a company is liable under federal law for having chosen to adopt the code at all, particularly when the adoption of such a code is effectively mandatory." Judge Tigar distinguished cases in which courts found actionable various companies' misrepresentations about their compliance with corporate policy because those cases "related either to compliance with the law (as opposed to a purely company policy) or to a company's core product or service."

Finally, the court found that Hurd's concealment of his noncompliance with the SBC was not a materially false omission. As an initial matter, the plaintiffs' theory effectively would create an actionable omission any time

an executive is "involved in misconduct that might lead to his or her resignation or termination." More to the point, however, for an omission to be actionable, there must be a duty to disclose the underlying non-compliance or misconduct. Here, because the representations about corporate ethics did not constitute a warranty of compliance, Hurd had no duty to disclose his misconduct to make those representations not misleading.

District Court Dismisses Section 10(b) and 20(a) Claims Against Tempur-Pedic for Failure to Adequately Plead a Material Misrepresentation or Omission

***Norfolk Cnty. Ret. Sys. v. Tempur-Pedic Int'l, Inc.*, No. 5:12-CV-195-KKC, 2014 U.S. Dist. LEXIS 70859 (E.D. Ky. May 23, 2014).**

Judge Karen K. Caldwell of the U.S. District Court for the Eastern District of Kentucky dismissed an investor class action for securities fraud alleging that Tempur-Pedic, a company that manufactures premium mattresses, and two of its officers misled investors about the financial impact of a competitor's new product line in violation of Sections 10(b) and 20(a) of the Securities Exchange Act and SEC Rule 10b-5. The court ruled that the plaintiffs had not adequately pled a material misrepresentation or omission and that many of the statements at issue also fell within the PSLRA's "safe harbor" provision.

The plaintiffs claimed that while Tempur-Pedic's CEO and CFO were aware that the introduction and expansion of the competing line had encroached on its market share, they overstated Tempur-Pedic's performance after its debut and made overly optimistic statements about the company's future growth opportunities. The complaint also alleged that the officers exercised thousands of stock options for a gain of over \$5.7 million before releasing a series of press releases lowering projections and expectations, after which Tempur-Pedic's share price dropped dramatically.

The court determined that most of the statements at issue were immaterial because they were so vague and generally optimistic that they communicated nothing at all and that the officers' representations about past performance were not misleading because they were accurate statements of historical fact. The court also concluded that the officers were not liable for any material omissions because disclosures about the competing product were not necessary to correct any otherwise misleading prior statements. Finally, the court explained that if any of the officers' forward-looking statements did constitute material misrepresentations or involve material omissions, they were accompanied by meaningful cautionary language and thus protected under the "safe harbor" provision of the PSLRA. Accordingly, the court dismissed the plaintiffs' complaint and denied as futile the plaintiffs' request for leave to amend.

EXPERT WITNESSES

S.D.N.Y. Excludes Plaintiffs' Expert Testimony in Pfizer Stock Price Litigation

***In re Pfizer Inc. Sec. Litig.*, No. 04 Civ. 9866, 2014 WL 2136053 (LTS) (HBP) (S.D.N.Y. May 21, 2014).**

Judge Laura Taylor Swain of the U.S. District Court for the Southern District of New York excluded the expert testimony of Daniel R. Fischel proffered in support of the plaintiffs' claims concerning the effect of a pharmaceutical company's alleged misrepresentations on its stock price. Fischel's report utilized an event study to purportedly demonstrate that the company's stock price was inflated by the allegedly false public statements. The court previously had granted summary judgment to the defendant with respect to two of the alleged misstatements and statements by a nonparty, and in response, Fischel reduced his overall stock price inflation findings by 9.7 percent. However, Fischel provided little analysis or explanation as to how he reached the new amount of stock price inflation, and failed to disaggregate his computations to identify inflation caused by the dismissed misstatements. The court determined that "Fischel's failure to account in any way for the impact of the excluded [] statements render[ed] his opinions unhelpful to the jury," and excluded his testimony.

FIDUCIARY DUTIES

Books and Records

Delaware Supreme Court Finds *Garner v. Wolfenbarger* Exception to Privilege Applies in Stockholder/Corporation Plenary Proceedings and Section 220 Actions

***Wal-Mart Stores, Inc. v. Ind. Elec. Workers Pension Trust Fund IBEW*, 95 A.3d 1264 (Del. 2014).**

Defendant Wal-Mart Stores, Inc. appealed from a Court of Chancery judgment that identified specific steps Wal-Mart had to take in searching for documents and categories of documents that had to be produced in response to a books and records demand pursuant to 8 Del. C. § 220. Plaintiff IBEW made a books and records demand seeking information regarding alleged bribery of Mexican officials and Wal-Mart's internal investigation of such bribery. After a trial to determine whether Wal-Mart had produced all responsive documents in response to the demand, the Court of Chancery entered an order requiring production of a wide variety of additional documents, including, among others, officer-level documents, documents spanning a seven-year period and documents from recovery tapes. The Court of Chancery also ordered the production of documents that ordinarily would be protected by the attorney-client and work product privileges, applying the privilege exceptions elaborated by the U.S. Court of Appeals for the Fifth Circuit in *Garner v. Wolfenbarger*, 430 F.2d 1093 (5th Cir. 1970).

The Delaware Supreme Court affirmed the Court of Chancery's judgment with respect to the scope of document production, the range of dates of documents and the requirement that documents be collected from backup tapes, finding the Court of Chancery properly exercised its discretion. As for the production of privileged documents, the Delaware Supreme Court determined that the doctrine elaborated in *Garner v. Wolfenbarger* should be applied in plenary stockholder/corporation proceedings, as well as in a Section 220 action. In *Garner*, the Fifth Circuit recognized a fiduciary exception to the attorney-client privilege, permitting stockholders of a corporation to "invade the corporation's attorney-client privilege in order to prove fiduciary breaches by those in control of the corporation upon showing good cause." The Supreme Court held that, in a Section 220 proceeding, the inquiry into whether documents are "necessary and essential" to the stockholder's proper purpose in making a demand should precede any privilege inquiry, "because the necessary and essential inquiry is dispositive of the threshold question — the scope of document production to which the plaintiff is entitled under Section 220." After holding that the *Garner* standard applies in plenary stockholder proceedings and in Section 220 actions, the Supreme Court found that the Court of Chancery properly applied the *Garner* exception in ordering the production of documents protected by the attorney-client and work-product privileges.

Bylaws

Delaware Supreme Court Upholds the Facial Validity of Fee-Shifting Bylaw in Nonstock Corporation

***ATP Tour, Inc. v. Deutscher Tennis Bund (German Tennis Fed'n)*, 91 A.3d 554 (Del. 2014).**

Justice Carolyn Berger of the Delaware Supreme Court issued an opinion holding that fee-shifting provisions in a Delaware nonstock corporation's bylaws are not *per se* invalid. The bylaw at issue shifted all litigation expenses to an unsuccessful plaintiff in intracorporate litigation who did "not obtain a judgment on the merits that substantially achieves, in substance and amount, the full remedy sought."

The Supreme Court answered four certified questions from the U.S. District Court for the District of Delaware: (1) Fee-shifting bylaws may be lawfully adopted under Delaware law; (2) If otherwise valid and enforceable, the bylaw could shift fees if a plaintiff obtained no relief in the litigation (given the difficulty in applying a "substantially achieves" standard); (3) The bylaws would be unenforceable if adopted for an improper purpose (notably, the court remarked that the "intent to deter litigation would not necessarily render the bylaw unenforceable"); and (4) The bylaw generally would be enforceable against members who joined the corporation before the provision's enactment.

The court also noted it was not deciding whether the specific bylaw at issue was adopted for a proper purpose or enforceable under the circumstances.

The Corporation Law Section of the Delaware Bar is actively considering legislation that might limit *ATP*'s holding in some fashion.

Rights Plans

Delaware Court of Chancery Upholds Discriminatory Rights Plan

***Third Point LLC v. Ruprecht*, Nos. 9469-VCP et al., 2014 WL 1922029 (Del. Ch. May 2, 2014).**

Vice Chancellor Donald F. Parsons, Jr. of the Delaware Court of Chancery issued an opinion denying a preliminary injunction and allowing Sotheby's annual meeting to proceed and refused to enjoin the use of its rights plan. In response to an apparent threat posed by increasing activity in Sotheby's stock by hedge funds, including plaintiff Third Point, Sotheby's adopted a rights plan that would be triggered at a lower percentage of ownership for those stockholders who filed a Schedule 13D (10 percent trigger threshold) than those filing a Schedule 13G (20 percent trigger threshold). Third Point, an activist hedge fund, claimed that the Sotheby's board violated its fiduciary duties by adopting the rights plan and refusing to provide Third Point with a waiver from the 10 percent trigger, allegedly to give the board an impermissible advantage in an ongoing proxy contest.

The court refused to issue a preliminary injunction, noting "[t]he substantive issue on the plaintiffs' motion is not whether the defendants have breached their fiduciary duties or whether the corporation's rights plan is invalid. Rather, the question is whether plaintiffs have made a sufficient showing to warrant my granting a preliminary injunction." The court found that the plaintiffs had not stated a reasonable likelihood of success on the merits and that *Unocal* was the appropriate standard of review, and it was "possible, but unlikely, that [the] *Blasius* [standard of review] may be implicated within the *Unocal* framework in this case."

First, applying *Unocal*, the court found that Third Point presented an objectively reasonable and legally cognizable threat to the corporation by its "creeping control." The court also held that the plaintiffs did not demonstrate a reasonable probability of success on their *Blasius* claim that the board adopted the rights plan for the primary purpose of interfering with the franchise of any stockholder, including Third Point, several months later. Second, the court found that the plaintiffs had not shown a reasonable likelihood that they would be able to demonstrate that the rights plan was either coercive or preclusive. Third, the court found that the board would likely be able to show that the rights plan was a reasonable and proportionate response to the threat of creeping control.

With respect to the board's refusal to grant Third Point a waiver from the 10 percent trigger in March 2014 to allow it to acquire up to 20 percent of the corporation's stock, the court noted, "[t]his presents a much closer question than the Board's original decision to adopt the Rights Plan in October 2013." The court held it was not clear that the board "did or should have had the exact same concerns in March 2014 that it did in October 2013 when it adopted the Rights Plan. As a result, I am skeptical that there is a reasonable probability that the Board could establish that when it rejected the request for a waiver, it had an objectively reasonable belief that Third Point continued to pose a 'creeping control' risk to the Company, either individually or as part of a 'wolf pack.'" Nevertheless, the court held that the Sotheby's board "made a sufficient showing as to at least one objectively reasonable and legally cognizable threat: negative control."

On the other elements of injunctive relief, the court found that "[a]lthough it is a close question, I find that Third Point's reduced odds of winning the proxy contest due to the Rights Plan likely would have qualified as a threat of irreparable harm, if Third Point had established a likelihood of success on the merits." Also, the balance of the equities weighed "slightly in favor" of plaintiffs, but since there was not a showing of likelihood of success on the merits, an injunction was not warranted.

FOREIGN CORPORATIONS

Second Circuit Affirms Dismissal of Claims That Financial Services Firm Violated the Commodities Exchange Act Because the Plaintiff Did Not Allege a Domestic Transaction

***Loginovskaya v. Batratchenko*, No. 13-1624-cv (2d Cir. Sept. 4, 2014).**

The U.S. Court of Appeals for the Second Circuit affirmed the dismissal of claims that a financial services company allegedly violated the Commodities Exchange Act because the plaintiff did not allege a domestic transaction. The court held that the transactional test of *Morrison v. National Australia Bank Ltd.*, 561 U.S. 247 (2010), applied to the Commodities Exchange Act's private right of action because the act did not contain a clear statement that it had extraterritorial effect. In addition, because the act limits private rights of action to suits over four specific types of transactions, those transactions must occur in the United States. Although the company that the plaintiff invested in was incorporated in New York, the plaintiff resided in Russia and negotiated and signed her investment contracts in Russia, and so the transactions were deemed to have occurred outside the United States. In sum, the court held that the Commodities Exchange Act "creates a private right of action for persons anywhere in the world who transact business in the United States," but it does not provide a right of action for those "who choose to do business elsewhere."

Second Circuit Affirms Dismissal, Holding Plaintiffs Failed to Allege Facts to Overcome *Morrison*'s Presumption Against Extraterritoriality

***Parkcentral Global Hub Ltd. v. Porsche Automobile Holdings SE*, No. 11-447-cv (2d Cir. Aug. 15, 2014).**

The U.S. Court of Appeals for the Second Circuit affirmed the dismissal of claims that Porsche violated Section 10(b) of the Securities Exchange Act by allegedly claiming that it did not intend to acquire a controlling interest in Volkswagen and concealing its accumulation of Volkswagen's stock. The plaintiffs (international hedge funds with U.S.-based investment managers) purchased in the United States securities-based swap agreements tied to Volkswagen's stock trading only on foreign exchanges. These synthetic swap agreements were an "unusual security" according to the court, and those transactions were argued by the plaintiffs to be economically equivalent to short sales of Volkswagen's stock sufficient to invoke Section 10(b). Relying on *Morrison v. National Australia Bank, Ltd.*, 561 U.S. 247 (2010), and *Absolute Activist Value Master Fund Ltd. v. Ficeto*, 677 F.3d 60 (2d Cir. 2012), the court held that, while a domestic securities transaction is necessary to invoke Section 10(b), it is not always sufficient to state a claim. The court reasoned that the plaintiffs' domestic purchase of the swap agreements at issue in this case was predominately foreign under *Absolute* because Porsche's alleged false statements were made primarily in Germany with respect to a German company traded only on a foreign exchange. The court thus held that the plaintiffs failed to allege facts to overcome *Morrison*'s presumption against extraterritoriality. According to the court, "the imposition of liability under § 10(b) on these foreign defendants with no alleged involvement in plaintiffs' transactions, on the basis of defendants' largely foreign conduct, for loss incurred by the plaintiffs in securities-based swap agreements based on the price movements of foreign securities would constitute an impermissibly extraterritorial extension of the statute." It remanded the case to allow the district court to entertain motions to amend the complaints, if any, in light of the opinion.

INTERPRETING *JANUS*

Fourth Circuit Holds That *Janus* Does Not Apply in Criminal Actions

***Prousalis v. Moore*, 751 F.3d 272 (4th Cir. 2014).**

On May 7, 2014, the U.S. Court of Appeals for the Fourth Circuit addressed the applicability of the U.S. Supreme Court's decision in *Janus Capital Group, Inc. v. First Derivative Traders*, 131 S. Ct. 2296 (2011), to the criminal context, holding that *Janus* applies only to private suits; it does not extend to the criminal context. Thomas Prousalis, a securities lawyer, was convicted after pleading guilty under Rule 10b-5 to knowingly including false and misleading information in IPO registration materials that he

prepared and which his client signed and filed. Prousalis appealed his conviction and lost. Thereafter, the Supreme Court issued its decision in *Janus*, holding that "the maker of a statement" for purposes of Rule 10b-5 is "the person or entity with ultimate authority over the statement, including its content and whether and how to communicate it." Prousalis filed a *habeas* petition, arguing that the conduct for which he was convicted—merely preparing the registration materials that were signed and filed by others—no longer was illegal after the Supreme Court's decision in *Janus*. The Fourth Circuit rejected Prousalis' argument and affirmed the district court's dismissal of his petition. The Fourth Circuit held that *Janus* was rooted in the implied private right of action of Rule 10b-5 and that the decision is therefore "inapplicable outside the context of the 10b-5 implied private right of action." The Fourth Circuit noted that "the *Janus* Court gave no indication that it intended to curtail the government's criminal enforcement, nor did the opinion suggest that it even contemplated the issue." The Fourth Circuit thus declined to broaden *Janus*' holding beyond the domain of implied private rights.

LOSS CAUSATION

Ninth Circuit Holds Announcement of Investigation Insufficient to Plead Loss Causation

***Loos v. Immersion Corp.*, No. 12-15100, 2014 WL 4073061 (C.C.H.) (9th Cir. Aug. 7, 2014).**

The U.S. Court of Appeals for the Ninth Circuit affirmed the dismissal of claims brought under Section 10(b) of the Exchange Act and SEC Rule 10b-5, holding that "the announcement of an investigation, standing alone, is insufficient to establish loss causation."

The plaintiff, purporting to represent a class of Immersion shareholders, alleged that Immersion "'cooked the books'" in response to mounting pressure from investors to become profitable. Specifically, the plaintiff claimed that Immersion violated GAAP principles by recognizing revenue earlier than permitted under the guidelines. The plaintiff alleged that this fraud was revealed to the market through a series of "'partial disclosures'" consisting of (i) disappointing earnings results for four out of five quarters and (ii) the subsequent announcement of an internal investigation into prior revenue transactions.

The district court dismissed the complaint, concluding that the plaintiff failed to adequately allege scienter or loss causation. The Ninth Circuit affirmed on loss causation grounds, without reaching the issue of scienter.

As to the quarterly results, the court held that disappointing earnings reports "are merely indicative of poor financial health; they do not tend to suggest that the company had engaged in fraudulent accounting practices. At bottom, these disclosures simply reveal that Immersion failed to meet its revenue goals."

On the issue of the investigation, the panel first noted that the Ninth Circuit has “never squarely addressed whether the disclosure of an internal investigation can satisfy the loss causation element of a § 10(b) and Rule 10b-5 claim.” The court then proceeded to analyze a recent U.S. Court of Appeals for the Eleventh Circuit decision, *Meyer v. Greene*, 710 F.3d 1189 (11th Cir. 2013). In that case, the Eleventh Circuit held that “the commencement of an SEC investigation, without more, is insufficient to constitute a corrective disclosure for purposes of § 10(b). The announcement of an investigation reveals just that—an investigation—and nothing more.” *Meyer*, 710 F.3d at 1201. The Ninth Circuit agreed with the Eleventh Circuit’s reasoning. The panel explained that the “announcement of an investigation does not ‘reveal’ fraudulent practices to the market. Indeed, at the moment an investigation is announced, the market cannot possibly know what the investigation will ultimately reveal.... Consequently, any decline in a corporation’s share price following the announcement of an investigation can only be attributed to market speculation about whether fraud has occurred. This type of speculation cannot form the basis of a viable loss causation theory.”

First Circuit Upholds Decision in Favor of Investment Bank in AOL Shareholder Dispute

***Bricklayers & Trowel Trades Int’l Pension Fund v. Credit Suisse Sec. (USA) LLC*, 752 F.3d 82 (1st Cir. 2014).**

The U.S. Court of Appeals for the First Circuit affirmed summary judgment to an investment bank in an action brought by a class of AOL shareholders claiming that the investment bank violated Section 10(b) of the Securities Exchange Act by allegedly misrepresenting information about AOL in its analysts’ research reports. To attempt to satisfy their burden regarding loss causation, the plaintiffs introduced event studies and expert testimony allegedly showing that the investment bank’s purported alleged misstatements or omissions concerning AOL’s financial strength, the severity of AOL’s layoffs and AOL’s unconventional accounting caused AOL’s stock price to artificially inflate. The court held that the plaintiffs’ expert’s event study was methodologically flawed, and consequently determined that there was no triable issue on loss causation. The event study contained several problems, including the selection of event dates based on unreliable data and the failure to properly consider previously disclosed information and other confounding factors. As a result, the court concluded that the district court did not abuse its discretion in excluding the plaintiff’s expert testimony on loss causation. Because the plaintiffs failed to introduce admissible evidence on loss causation, summary judgment in favor of the investment bank was appropriate.

MISREPRESENTATIONS

Second Circuit Affirms Dismissal of ARS-Related Claims Against Investment Bank

***La. Pac. Corp. v. Merrill Lynch & Co.*, No. 13-1980-cv, 2014 WL 2870146 (2d Cir. June 25, 2014).**

The U.S. Court of Appeals for the Second Circuit affirmed in a summary order the dismissal of claims that an investment bank violated Section 10(b) of the Securities Exchange Act by allegedly manipulating and misrepresenting the market for auction rate securities (ARS). The plaintiffs alleged that the investment bank’s bidding affected the clearing rate of the auctions and that the investment bank’s ARS activities inflated the market prices of ARS. The Second Circuit held that the liquidity risks inherent in ARS auctions and the investment bank’s bidding were adequately disclosed in both an SEC cease-and-desist order and the investment bank’s online disclosure of its ARS practices and procedures. In addition, the investment bank’s disclosure that it routinely placed support bids was not misleading, even though it allegedly placed support bids in every single auction and knew that each auction would fail if it did not place these bids. Lastly, the Second Circuit compared the plaintiffs’ allegations to two previously dismissed complaints against the same investment bank alleging similar claims and concluded that, like the insufficient allegations in those cases, the plaintiffs’ allegations were too generalized and conclusory to support a claim.

PSLRA

Safe Harbor Provision

Fifth Circuit Denies Safe Harbor Protection to Mixed Present/Future Statements

***Spitzberg v. Houston Am. Energy Corp.*, 758 F.3d 676 (5th Cir. 2014).**

The U.S. Court of Appeals for the Fifth Circuit joined the First, Third and Seventh Circuits in holding that a “‘mixed present/future statement is not entitled to the safe harbor with respect to the part of the statement that refers to the present.’” In *Spitzberg*, investors brought a securities fraud class action against an oil and gas exploration company and certain of its employees and directors, alleging that the defendants made material misrepresentations regarding the amount of oil in an oil-and-gas concession. The plaintiffs alleged that, based on the definition of “reserves” commonly used in the industry and in SEC regulations, the defendants’ use of the word “reserves” in communications with investors suggested that certain production or geological testing had been completed when, in fact, no such production or testing had been done. The district court granted the defendants’

motion to dismiss the complaint. On appeal, the plaintiffs argued, among other things, that one of their challenged statements regarding “reserves” was not entitled to safe harbor protection. Examining the statement in context, the Fifth Circuit concluded that although the defendants’ use of the term “reserves” communicated a forward-looking thought in one part of the statement, their use of the term elsewhere in the statement was undoubtedly backward-looking. Noting the absence of any authority to the contrary, the Fifth Circuit followed the decisions of its sister circuits in holding that a statement that contains both forward-and backward-looking aspects is not entitled to safe harbor protection with respect to that part of the statement that concerns the present.

RULE 10B-5 OMISSION LIABILITY

First Circuit Affirms Dismissal of Claims in Drug Development Dispute

In re Genzyme Corp. Sec. Litig., 754 F.3d 31 (1st Cir. 2014).

The U.S. Court of Appeals for the First Circuit affirmed the dismissal of claims that a pharmaceutical company allegedly violated Section 10(b) of the Securities Exchange Act by concealing manufacturing difficulties that purportedly delayed the company’s efforts to obtain FDA approval for a drug. The court held that the plaintiffs’ complaint was an “ill organized and convoluted collection of 364 paragraphs” and failed to plead a strong inference of scienter as required by the Private Securities Litigation Reform Act. The company’s decision not to disclose the FDA’s preliminary findings after a factory inspection was not fraudulent because the findings were merely observational in nature and did not bear an explicit relation to whether the drug would receive FDA approval. The company’s delay in disclosing certain difficulties with contamination in one of its factories also was not fraudulent because the company did not immediately know the cause of the problems and thereafter disclosed its investigation in due course. In addition, statements made to investors about the prospects of receiving FDA approval were inactionable forward-looking projections, and the company appropriately disclosed information about the negative developments in manufacturing the drug as it became available.

D.C. Circuit Holds That Accurate, “Snapshot” Disclosures Made During Volatile Market Cycles Are Not Actionable Under Federal Securities Law

Wu v. Stomber, 750 F.3d 944 (D.C. Cir. 2014).

The U.S. Court of Appeals for the D.C. Circuit dismissed the plaintiffs’ Section 10(b) and Rule 10b-5 claims challenging snapshot disclosures made by an investment fund. The court held that no fraud had occurred because the disclosures, which were issued during a period of unusual market volatility, accurately reflected the portfo-

lio’s performance as of the date they purported to represent. Carlyle Capital Corporation was an investment fund heavily exposed to residential mortgage-backed securities (RMBS). Beginning in 2007, as the real estate and financial sectors took a sharp downturn, Carlyle’s RMBS assets experienced substantial losses and increased volatility. When Carlyle conducted a private offering with accredited investors in June 2007, it disclosed a “snapshot” of “the latest, updated figure[s]” reflecting its RMBS losses and warned investors that the real estate securities market was “highly volatile” and “difficult to predict.” Carlyle’s losses grew following the financing, and investors brought class action suits alleging material misstatements and omissions in the June 2007 offering memorandum. The district court dismissed the complaints. On appeal, the plaintiffs alleged that Carlyle’s financials as of June 13, 2007 were inaccurate, relying on an email from a Carlyle director regarding the portfolio’s much lower market valuation as of June 11. The D.C. Circuit rejected the plaintiffs’ argument, noting that the initial offering memorandum purported to reflect Carlyle’s balance sheet as of June 13, 2007, and had warned investors against relying on the stability of RMBS valuations due to volatile market conditions. Further, Carlyle postponed the pricing of its shares and issued a supplemental memorandum nine days later, which further updated the market regarding its portfolio’s poor performance through June 26, 2007. Because Carlyle’s disclosures in the offering memorandum and supplemental memorandum were accurate and “did not suggest [in either document] that the snapshot...was anything other than just that—a snapshot,” the D.C. Circuit held that dismissal of the plaintiffs’ securities fraud claims was proper.

SCIENTER

Second Circuit Upholds Dismissal of 10(b) Claims Against Telecommunications Company

Shemian v. Research In Motion Ltd., No. 13-1602-cv, 2014 WL 2766173 (2d Cir. June 19, 2014).

The U.S. Court of Appeals for the Second Circuit affirmed the dismissal of claims that a telecommunication and wireless equipment company violated Section 10(b) of the Securities Exchange Act by allegedly issuing false and misleading statements about its projected financial results, sales of its existing product line, and the introduction of both a new operating system and new tablet. The Second Circuit held that the plaintiffs’ claims did not adequately allege scienter. The plaintiffs failed to plead any cognizable motive to commit securities fraud because the plaintiffs did not allege specific facts supporting an inference that defendants “knew, when speaking, that their statements regarding product quality and release deadlines were false.” Although the company’s projections may have been unduly optimistic based on its history of product setbacks, such allegations were insufficient to show recklessness. The Second Circuit further held that the plaintiffs failed to adequately allege materiality. The

court determined that the statements made by the company were at most puffery and any alleged omissions were not material in light of the total mix of information available. The court also dismissed arguments that the company failed to disclose information about its products as a “‘known trends or uncertainties’” within the management discussion and analysis section of its SEC filings. The plaintiffs failed to allege any trend that was either not disclosed or not already known to the market. In addition, the court affirmed the trial court’s denial of leave to amend.

Scienter May Be Imputed to Corporation from Employee Who Does Not “Make” a Statement Within the Meaning of *Janus*

***Lee v. Active Power, Inc.*, No. A-13-CA-797-SS, 2014 WL 3010679 (W.D. Tex. July 2, 2014).**

Judge Sam Sparks of the U.S. District Court for the Western District of Texas denied a motion to dismiss a securities fraud complaint, holding that the plaintiffs adequately alleged corporate scienter by pleading knowledge of an employee that could be imputed to the corporation. The plaintiffs sued Active Power, Inc., its CEO and CFO for alleged violations of Section 10(b) of the Securities Exchange Act and Rule 10b-5. The plaintiffs alleged that, based on false information provided by another employee, Active Power made false public statements regarding its China operations. The defendants moved to dismiss, arguing that the employee’s scienter (which was undisputed) could not be imputed to the corporation because, under the U.S. Supreme Court’s definition of “make” as articulated in *Janus Capital Group, Inc. v. First Derivative Traders*, 131 S. Ct. 2296 (2011), the employee never actually made the statements on which the suit was based. The defendants argued that *Janus* overruled the Fifth Circuit’s decision in *Southland Securities Corp. v. INSpire Insurance Solutions, Inc.*, 365 F.3d 353 (5th Cir. 2004), which held that corporate scienter may be imputed from an employee who “makes” a false statement or one who “furnish[es]” information used in a false statement. The court rejected the defendants’ argument, holding that while *Janus* excludes from the definition of the “maker” of a false statement someone who merely furnishes information, *Janus* did not overrule the Fifth Circuit’s controlling precedent in *Southland*. The court reasoned that *Janus* “defined who ‘makes’ a statement; the ‘furnished information’ language from *Southland* defined from whom scienter may be imputed for the purposes of corporate liability.”

SEC ENFORCEMENT ACTIONS

Second Circuit Reverses Jury Verdict in Favor of SEC in Section 17 Claims Against Financial Broker

***S.E.C. v. Ginder*, 752 F.3d 569 (2d Cir. 2014).**

The U.S. Court of Appeals for the Second Circuit reversed a jury verdict in favor of the SEC in a civil en-

forcement action claiming that a financial broker violated Section 17 of the Securities Act by allegedly engaging in marking timing despite directives from certain mutual funds and the broker’s employer to cease those activities. The jury found that the broker did not intentionally or recklessly violate Section 17, but that he had acted negligently. The district court ruled that the jury’s verdict was supported by evidence that the broker did not read and heed emails from his supervisors directing him not to engage in market timing. The Second Circuit held that the broker was entitled to judgment as a matter of law based on the insufficiency of the evidence. The court determined that the SEC failed to present any evidence of the appropriate standard of care from which a jury could determine whether the broker acted negligently toward the mutual funds. In addition, the record evidence established that the mutual funds’ prohibition on market timing was unclear and contradictory and that the broker’s employer condoned the broker’s market timing activities.

The dissent disagreed with the majority’s analysis on this point, noting that the plaintiff “does not allege that she suffered any loss due to the Barclays Defendants’ purported deceptive conduct, nor does she allege that any loss is traceable to a misrepresentation related to the LIBOR-rate manipulation or to the LIBOR-rate manipulation itself.” The dissent pointed out that the plaintiff’s payments were never affected by the defendants’ alleged conduct. Therefore, according to the dissent, the plaintiff’s “alleged injury is far too attenuated to establish Article III standing.”

SECURITIES FRAUD PLEADING STANDARDS/STANDING

District Court Denies Motions to Dismiss Securities Action Against Former Dewey & LeBoeuf Managers

***Aviva Life & Annuity Co. v. Davis*, No. 4:12-cv-00603-JEG, 2014 WL 2069640 (S.D. Iowa May 19, 2014).**

Judge James E. Gritzner of the U.S. District Court for the Southern District of Iowa refused to dismiss claims brought against three former Dewey & LeBoeuf LLP managers for alleged violations of Sections 10(b) and 20(a) of the Securities Exchange Act, SEC Rule 10b-5, and state securities laws. The plaintiffs claimed that the defendants used materials containing misrepresentations and omissions to convince institutional investors to purchase Dewey-issued notes. In denying the motion to dismiss, the court rejected the argument that the plaintiffs, who had sold their notes and some of their related rights, lacked standing to bring the securities claims. The court reasoned that even though the plaintiffs had expressly assigned their rights to bring claims against the defendants, the U.S. Supreme Court’s holding in *Blue Chip Stamps v. Manor Drug Stores*, 421 U.S. 723 (1975) rendered such assignment inoperable as a matter of law. Accordingly, the assignee’s release of all claims against Dewey during bankruptcy

proceedings did not bar the plaintiffs' claims because their assignment never had been valid.

The court further held that the plaintiffs sufficiently pled a claim under Section 10(b), even though the complaint did not identify which defendant made which statement, where a state court indictment and SEC complaint set forth specific statements made by each individual defendant tying him to a conspiracy to commit a fraudulent act. Moreover, the court clarified that the group pleading doctrine, an exception to the heightened pleading requirement, survived both the passage of the PSLRA and the U.S. Supreme Court's decision in *Janus Capital Group, Inc. v. First Derivative Traders*, 131 S. Ct. 2296 (2011). The plaintiffs also sufficiently pled their Section 20(a) claim, even though Dewey, the primary violator, was not a named defendant. The court determined that a primary violator is not a required party to a Section 20(a) action. Rather, the primary violator's liability is merely a required element of the claim.

SETTLEMENTS

Second Circuit Reverses District Court's Order Refusing to Approve MBS-Related Settlement Between SEC and Bank

***S.E.C. v. Citigroup Global Mkts., Inc.*, 752 F.3d 285 (2d Cir. 2014).**

The U.S. Court of Appeals for the Second Circuit reversed an order of a district court judge refusing to approve a settlement agreement between the SEC and a large bank arising from the bank's alleged short positions against mortgage-backed securities that it participated in selling. The district court ruled that it lacked sufficient information about the alleged conduct to determine if the consent agreement was not only fair and reasonable, but also adequate and in the public interest. The Second Circuit clarified that the proper standard for review of a proposed consent agreement is only whether the agreement is fair and reasonable. Applying that standard, the Second Circuit held that the district court abused its discretion in refusing to approve the agreement because the court needed only to establish some factual basis "supported by factual averments by the SEC, neither admitted nor denied by the wrongdoer," not "'cold, hard, solid facts established either by admissions or by trials.'" The record below supported such a finding. In addition, the district court's invocation of the public interest was error. The SEC is squarely responsible for determining if a proposed agreement serves the public interest, and a district court may only consider whether the agreement would disserve the public in some way, such as by barring potential litigants from receiving separate relief. Likewise, the SEC has the exclusive right to determine which claims to assert against a particular defendant, and the district court erred in questioning the SEC's decision not to assert fraud claims.

SLUSA

First Circuit Vacates District Court's Dismissal of State Law Claims Against Investment Fund

***Hidalgo-Vélez v. San Juan Asset Mgmt., Inc.*, 758 F.3d 98 (1st Cir. 2014).**

The U.S. Court of Appeals for the First Circuit vacated a district court's dismissal of state law claims pursuant to the Securities Litigation Uniform Standards Act (SLUSA) and reversed the denial of the plaintiffs' motion to remand the case to state court. The plaintiffs alleged that an investment fund did not comply with the investment policies it promised in the prospectus, and that its investment strategy was contrary to Puerto Rico law. The district court ruled that SLUSA barred the plaintiffs' state law class action claims against the investment fund and its adviser because, although the securities held by the plaintiffs were not "covered securities," the fund's anticipated investments included several covered securities. Relying on the U.S. Supreme Court's recent opinion in *Chadbourne & Parke LLP v. Troice*, 134 S. Ct. 1058 (2014), which limited SLUSA's reach, the First Circuit held that SLUSA did not preclude the plaintiffs' claims. Although the fund's prospectus "suggested" that the fund might hold covered securities, the main investment allocation—at least 75 percent of the fund's assets—contained offerings of uncovered securities, the alleged misrepresentations concerned uncovered securities (shares in the fund), and the plaintiffs primarily sought ownership of uncovered securities. Thus, unlike other cases where the investors' intent was to own covered securities, the alleged misrepresentations and any connection to covered securities in the fund's portfolio were too attenuated to support SLUSA preclusion.

Second Circuit Denies Petition Seeking Rehearing of Dismissal of SLUSA Claims Against Madoff Securities

***In re Herald, Primeo, and Thema*, 753 F.3d 110 (2d Cir. 2014).**

The U.S. Court of Appeals for the Second Circuit denied a petition seeking rehearing of an opinion affirming the dismissal of state law claims pursuant to the Securities Litigation Uniform Standards Act (SLUSA). The district court previously had determined that SLUSA barred the plaintiffs' state law class action claims against Madoff Securities because they were predicated on fraudulent transactions in nationally traded securities. After reviewing the U.S. Supreme Court's recent opinion in *Chadbourne & Park LLP v. Troice*, 134 S. Ct. 1058 (2014), the Second Circuit determined that SLUSA applied and denied rehearing, even though the *Chadbourne* opinion arguably limited the scope of SLUSA. The court held that in the case at hand, Madoff Securities had fraudulently induced the plaintiffs' investment in nationally traded securities, "albeit through feeder funds (not alleged in the instant complaints as anything other than intermediaries)," and thus SLUSA barred those claims in the class action format.

America's Tweak to the Loser Pays Rule: A Board-Insulating Mechanism?

By Nithya Narayanan

At first blush, the year 2014 might seem no different for corporate America than any other; like a preordained folklore, it witnessed a host of new and exciting developments in corporate and securities litigation. One issue, which initially got lost in the shuffle but is now the cynosure of debate amongst regulators and academicians, is the adoption of the “loser pays” or “fee-shifting” rule (Loser Pays Rule) by public companies in the United States. The Loser Pays Rule is no novelty; it originated and has been in existence in the United Kingdom since time immemorial. As per this rule, the loser of the litigation pays for the winner’s legal costs, which is an exception to the quintessential American rule, where each party bears its own litigation costs.¹ It is not the rule, but its application by U.S. public companies that is disconcerting. The obligation of incurring the costs and risks arising out of corporate litigations is being shifted onto the shareholders. Hence, unlike the United Kingdom, the approach in the United States has been one-sided. Since the Delaware Supreme Court’s May 2014 ruling in *ATP Tour, Inc. v. Deutscher Tennis Bund* (ATP Tour Case),² there has been a surge of more than twenty companies which have adopted bylaws for incorporating a rather tweaked version of the Loser Pays Rule (to distinguish this from the original Loser Pays Rule, it is hereinafter referred as the “Tweaked Loser Pays Rule”).³ The Tweaked Loser Pays Rule has been *unilaterally* adopted by the board of directors of companies requiring shareholder plaintiffs to mandatorily bear the defendant’s costs and expenses of litigation, should such plaintiffs be unsuccessful in shareholder litigations against the company. However, they stand to gain nothing should they be successful; the corporation and its officers do not bear a similar liability. This makes the rule prejudiced against the shareholders, having a resultant effect of impeding shareholder suits.

The Tweaked Loser Pays Rule came under the scanner, especially when different courts started taking diverging positions on the validity of its unilateral adoption. While the Oregon County Circuit Court, in *Roberts v. TriQuint Semiconductor, Inc.*, found its adoption contrary to public policy,⁴ the Delaware Supreme Court in the ATP Tour Case held the Tweaked Loser Pays Rule adopted by the board of ATP Inc. to be enforceable against all shareholder plaintiffs, even though it was adopted without their approval. Though ATP Inc. was a non-stock company, there is nothing that prevents courts from extending this decision to stock corporations. The fee-shifting provision in the ATP Tour Case was preposterously one-sided because it requires the plaintiff to pay fees, costs

and expenses incurred by all of the defendants, should the plaintiff fail to “obtain a judgment on the merits that substantially achieves, in substance and amount, the full remedy sought.”⁵ Thus, even if the plaintiff wins on the merits of the case, but subsequently loses on technicalities, he would be saddled with reimbursement costs. This could inhibit not only small stockholders, but also those with a significant financial interest in the company to pursue litigation. The Delaware Supreme Court sanctified ATP Inc.’s bylaw by holding that it was intended to deter unwanted litigation, and the burden was on the shareholders to prove that the bylaw was adopted for an “improper purpose.”⁶

“The Loser Pays Rule is no novelty; it originated and has been in existence in the United Kingdom since time immemorial. As per this rule, the loser of the litigation pays for the winner’s legal costs, which is an exception to the quintessential American rule, where each party bears its own litigation costs.”

This decision created a huge uproar and induced animated debates on policy considerations surrounding a board’s powers to unilaterally increase the monetary liabilities of its shareholders. On May 22, 2014, Delaware’s Corporate Law Council proposed an amendment to Title 8 of the Delaware General Corporation Law blocking public companies from shifting defense costs to investors.⁷ The proposal stated that it “intended to limit the applicability of [the Delaware Supreme Court decision in *ATP Tours, Inc. v. Deutscher Tennis Bund*] to non-stock corporations, and to make clear that such liability may not be imposed on holders of stock in stock corporations.”⁸ However, the Delaware state legislature has tabled this proposal until January 2015, upon requests received from the U.S. Chamber Institute for Legal Reform, which opposed this amendment on the basis that it would only protect frivolous lawsuits intended to “line the pockets of the plaintiffs’ trial bar at the expense of national and Delaware companies and their shareholders.”⁹

The following sections of the article discuss the legality and viability of the Tweaked Loser Pays Rule and whether the rule has been formulated by companies as a board-insulating mechanism.

I. Should Directors Be Permitted to Unilaterally Adopt Fee-Shifting Provisions?

Per se, the Loser Pays Rule is an efficient model for keeping out unmeritorious suits, which are resource-draining nightmares for publicly traded companies. Such a rule has a three-fold benefit: (i) shareholders would exercise greater caution while bringing suits without lawful basis, thereby reducing frivolous litigation; (ii) this, in turn, would not only save judicial resources, but also the funds of the corporate treasury (from expenses incurred in connection with defending those claims); and more importantly (iii) this could be an incentive for shareholders to gain from a win. Shareholders initiate company related suits with the intention of obtaining the relief they seek thereunder. But they do not get reimbursed for the exorbitant expenditures they incur for undertaking such legal proceedings. An application of the Loser Pays Rule would enable them to recoup these expenses in case they win such suit. However, the Tweaked Loser Pay Rule deprives shareholders of this gain. This is in addition to permitting the board of directors to unilaterally adopt this rule, without consulting the shareholders—the parties whose rights are directly affected.

The basic principles of contract law govern the relationship between the company and its shareholders; the charter documents and bylaws of a company are essentially contracts between them. In absence of a contractual or statutory provision to the contrary, amendment of the terms of such contracts, modifying the extent or nature of either party's obligations, should necessarily require the express consent of such party.¹⁰ What is disturbing about the *ATP Tour* Case is that the Delaware Supreme Court conceded that bylaws are "contracts among a corporation's shareholders," and held that the Tweaked Loser Pays Rule would fall within the contractual exception to the American Rule.¹¹ The court chose to ignore the fact that a contract's most essential characteristic is *consensus ad idem*¹² between the parties, which is evidently absent in the unilaterally board-embraced bylaws. Moreover, the plaintiffs in this case contended that they became aware of such bylaw only after the commencement of the litigation. The court thus conveniently relied on those facts and aspects of contract law that supported its position of upholding the validity of the bylaw.

A shareholder's right to initiate a derivative action, on behalf of the corporation, enables him to seek enforcement and redressal of a breach of fiduciary duties by the corporate insiders. This forms part of the basic structure of the constitution of a corporation. An amendment to the bylaw of the corporation, which has the effect of altering or affecting the exercise of such right, should not be singly decided by the board of the company. Incorporating a fee-shifting rule in the corporation's bylaws has a direct bearing on the shareholder's fundamental right to sue, and thus embracing it should necessarily require shareholder approval.

II. A Potential for the Race to the Bottom?

Managing the business and affairs of a corporation is the core function of the board of directors of a company. Even though shareholders might be restricted or limited in their rights, to the extent of the shares they own in the corporation, they still have a say by way of voting on important matters of the company, including the election of the directors. The directors owe fiduciary duties to the corporation and to its ultimate beneficiaries, the shareholders. This is the underpinning of such relationship. The directors act as trustees of the corporation, while exercising their judgment, and manage the corporation's assets for the sole benefit of the shareholders. A violation of such duties results in liabilities. Derivative suits and class actions are the fora for shareholders to voice their concerns, seek enforcement of, redress for, a breach of such fiduciary duties. This limited, but indirect, right of shareholders to control corporate affairs, and the common law theory of the fiduciary duties of the directors and officers, enable the smooth functioning of a company.

Delaware courts are infamous for adopting a management-friendly approach in their decisions, and the Tweaked Loser Pays Rule is no exception. It is alarming that the Delaware Supreme Court in the *ATP Tour* Case did not analyze the potential impact of its decision on board comportment. Eliminating or reducing shareholder litigation could lead to moral hazard problems and also increase the incidence of inappropriate action by the board members. With the board being fully cognizant of the fact that shareholders are limited in their means to challenge the company's actions, owing to the onerous fee-shifting provisions, they would clearly lack the incentive to conduct themselves in compliance with their fiduciary duties.

Consecrating a bylaw which appeases the manager frustrates the shareholders, who would then presumptively prefer investing in corporations outside Delaware. This could severely impact Delaware, which thrives on shareholder litigation. That said, the Delaware Supreme Court confronted a rare clash of interests in this case, between preferring the interests of the directors and managers of the corporation and preventing the outflow of Delaware's clientele. At the end, the court chose to render a management friendly decision; by shifting the liability onto the shareholders to bear the defendant's costs, it has throttled the shareholders' right to initiate litigation. The upshots of this decision are already being felt in Delaware. In *Kastis v. Carter*,¹³ the stockholders of Hemispherx Biopharma, Inc. (Hemispherx) brought a derivative action in the Delaware chancery court challenging payments made to certain Hemispherx employees.¹⁴ During the pendency of the case, Hemispherx notified the plaintiffs that it had retroactively adopted a bylaw which would allow the company to recoup litigation costs from unsuccessful shareholders and was invoking the same in the pending proceedings. The plaintiffs challenged the

validity of the bylaw, but expressed their reluctance to move forward in the case until the chancery court first declared the bylaw invalid. However, the parties to the suit thereafter mutually agreed and notified the court that Hemispherx would not apply the bylaw to the present litigation, as a result of which the issue of whether Hemispherx's bylaw is valid or enforceable is no longer an issue in the litigation.¹⁵ Though it remains to be seen if the Delaware courts would follow the ruling in the *ATP Tour* Case, it is evident that the decision has sent shockwaves of apprehension into the shareholder community.

"...America's move toward the Tweaked Loser Pays Rule could have some disastrous consequences on corporate and securities litigation."

III. The Tweaked Rule and Capital Raising Transactions

In capital raising transactions, such as an initial public offering (IPO), the issuer raises capital from the public on the basis of the disclosures made in the prospectus and other regulatory filings. So long as such fee-shifting provisions are publicly and sufficiently disclosed in the offering documents *before* investors subscribe to the company's shares, they cease to be a cause of disquiet from a corporate-contract law point of view. Recently, on October 29, 2014, Senator Richard Blumenthal (D-CT) wrote to the Securities and Exchange Commission (SEC) Chairman, Ms. Mary Jo White, requesting SEC investigation of Alibaba Group Holding, Ltd. (Alibaba), for its failure to disclose the existence of provisions "limiting private citizen suits" at the time of the offering.¹⁶ Alibaba had included a fee-shifting provision in its articles of incorporation requiring the shareholders to recompense Alibaba in any suit against the company, unless the same is "100 percent successful."¹⁷ However, this clause received no mention in the prospectus of the company, which was the basis on which Alibaba raised \$25 billion from investors and began trading on the New York Stock Exchange. Alibaba is a non-U.S. company incorporated in the Cayman Islands. Its fee-shifting provision applies to any claim made against the corporation by its shareholders. The situation gets a bit convoluted when U.S. incorporated companies adopt these fee-shifting provisions in their bylaws or charters. Depending on the dialect of the Loser Pays Rule used by the company, the repercussions differ. For example, when the Delaware incorporated grocery chain Smart & Final Stores, Inc. went public, it included a form of the Loser Pays Rule,¹⁸ the contours of which are not entirely

clear.¹⁹ The reading of the relevant article of its charter suggests that the language is wide enough to cover not only state claims, but also those arising out of the federal securities laws.²⁰

IV. What Lies Ahead?

Columbia Law School professor John Coffee and Widener Law professor Larry Hamermesh testified before Securities and Exchange Commission's Investor Advisory Committee on why the SEC should get involved in the debate over fee-shifting bylaws.²¹ Though acknowledging that it was a matter of concern for the state legislature and judiciary, Professor Coffee advocated that the SEC should step in at the earliest moment and take immediate measures toward discouraging adoption of fee-shifting provisions by public companies.²² However, others have noted that this could "forestall experimentation and choice"²³ and that individual states should be allowed to determine whether or not, and in what form, the Loser Pays Rule should be adopted for companies incorporated within their jurisdiction. Having said that, the State of Oklahoma has been criticized for having "upset" the American rule by going ahead and enacting legislation (which came into effect on November 1, 2014), under which the non-prevailing party in shareholder derivative litigation would pay the legal fees and costs of the prevailing party.²⁴ This author commends Oklahoma for having statutorily adopted the correct and complete version of the Loser Pays Rule, according to which if the shareholder loses the suit, he pays, but upon winning, he can recover all his fees and costs associated with such litigation.²⁵ However, it has been recognized that derivative suits not infrequently get dismissed on procedural grounds, despite being factually meritorious.²⁶ Thus, the potential remains for exorbitant monetary liabilities of shareholders despite the two-way application of the fee-shifting provision.

In light of the aforementioned deliberations, America's move towards the Tweaked Loser Pays Rule could have some disastrous consequences for corporate and securities litigation. It is a board-insulating mechanism which frustrates the established economic theory behind bifurcating the role of the owner-shareholders and that of the director-officers of a corporation. Whether the SEC will respond to the requests made by Senator Blumenthal and legal academicians is something we should know by early 2015. Until then, the Tweaked Loser Pays Rule may continue to be adopted by U.S. corporations. With regard to Delaware, the manager-centric view propounded by the *ATP Tour* Case could cause the management of out-of-state companies to relocate to Delaware to take advantage of its position on the fee-shifting bylaw. And so the race to the bottom continues.

Endnotes

1. Arthur L. Goodhart, Costs, 38 YALE LJ. 849, 851-78 (1929) (providing lengthy discussion of history of attorney's fees award in England and brief discussion of American Rule).
2. 91 A. 3d 554 (2014).
3. According to Professor John Coffee, twenty-four companies have adopted fee-shifting bylaws since May 2014. See Professor John C. Coffee Jr., Adolf A. Berle Professor of Law, Columbia University Law School And Director of its Center on Corporate Governance, *Fee-Shifting Bylaws: Can They Apply in Federal Court?—The Case For Preemption*, Testimony before SEC Investor Advisory Committee, Securities and Exchange Commission, Washington, D.C. (October 9, 2014), http://www.law.columbia.edu/null/download?&exclusive=filemgr.download&file_id=623364.
4. C.A. No. 1402-02441 (Cir. Ct. Or. Aug. 14, 2015).
5. 91 A. 3d at 555.
6. *Id.* at 560.
7. See <http://www.delawarelitigation.com/files/2014/05/2014DGCLBillIII.pdf>.
8. *Id.*
9. Jonathan Starkey, *Fee-shifting bylaw bill tabled until 2015*, The News Journal Delawareonline (June 19, 2014), <http://www.delawareonline.com/story/money/business/2014/06/19/delaware-general-assembly-tables-legal-fee-shifting-bylaw-bill/10946611/>.
10. Lawrence A. Hamermesh, *Consent in Corporate Law*, Business Lawyer (forthcoming).
11. 91 A.3d 554.
12. An agreement of the parties to the same thing; a meeting of the minds, Black's Law Dictionary (9th ed. 2009).
13. C.A. No. 8657-CB, available at <http://www.delawarelitigation.com/files/2014/09/2104SEPTBLOG-U01137891.pdf>.
14. *Id.* July 21, 2004 Motion to Invalidate Retroactive Fee-Shifting and Surety Bylaw or, in the Alternative, to Dismiss and Withdraw Counsel.
15. *Id.* September 16, 2014 letter to Chancellor Bouchard.
16. Letter from Richard Blumenthal to Mary Jo White, Chairman, SEC, *Blumenthal Calls On SEC To Protect Critical Check On Corporate Malfeasance*, Press Release, Office of Richard Blumenthal (October 30, 2014), <http://www.blumenthal.senate.gov/newsroom/press/release/blumenthal-calls-on-sec-to-protect-critical-check-on-corporate-malfeasance>.
17. *Id.*
18. Second Amended and Restated Articles of Incorporation of Smart & Final Stores, Inc. (September 19, 2014), http://www.sec.gov/Archives/edgar/data/1563407/000104746914007771/a2221499zex-3_1.htm [hereinafter Amended and Restated Articles].
19. *Id.* Article Sixteen of the Amended and Restated Articles *inter alia* states that if: "... (i) any current or prior stockholder or anyone on their behalf (a 'Claiming Party') initiates any action, suit or proceeding, whether civil, criminal, administrative or investigative or asserts any claim or counterclaim (each, a 'Claim') or joins, offers substantial assistance to or has a direct financial interest in any Claim against the Corporation (including any Claim purportedly filed on behalf of any other stockholder) and/or any director, officer, employee or affiliate thereof (each, a 'Company Party'), and (ii) the Claiming Party (or the third party that received substantial assistance from the Claiming Party or in whose Claim the Claiming Party had a direct financial interest) does not obtain a judgment on the merits that substantially achieves, in substance and amount, the full remedy sought, then each Claiming Party shall be obligated jointly and severally to reimburse the applicable Company Party for all fees, costs and expenses of every kind and description (including, but not limited to, all reasonable attorneys' fees and other litigation expenses) that the applicable Company Party may incur in connection with such Claim... Any person or entity purchasing or otherwise acquiring any interest in the shares of capital stock of the Corporation shall be deemed to have notice of and consented to the provisions of this Article SIXTEENTH." Many other Delaware companies have incorporated similar clauses after the ATP Tour Case, including ATD Corporation, which announced an IPO in August of 2014, see <http://www.nasdaq.com/markets/ipos/filing.ashx?filingid=9714197>.
20. The provision applies to "any action, suit or proceeding, whether civil, criminal, administrative or investigative" filed by "any current or prior stockholder or anyone on their behalf." One can reasonably presume that such a provision could apply even to claims arising under the Securities Act of 1933.
21. "Fee-Shifting Bylaws: Can They Apply in Federal Court?—The Case For Preemption," Testimony of Professor John C. Coffee Jr., Adolf A. Berle Professor of Law, Columbia University Law School and Director of its Center on Corporate Governance before SEC Investor Advisory Committee, Securities and Exchange Commission, Washington, D.C. October 9, 2014, available at http://www.law.columbia.edu/null/download?&exclusive=filemgr.download&file_id=623364.
22. *Id.* Professor Coffee wants the SEC to require companies to specifically preclude the application of such provisions in cases involving the federal securities laws, not grant acceleration of registration statements for companies having such onerous one-sided fee-shifting provision in their charters or bylaws, and he further recommends that the SEC begin to collect data to show the amount of fee recovery that could be involved.
23. Keith Paul Bishop, *Why The SEC Should Stay Out Of The Fee-Shifting Charter Debate*, The National Law Review (October 15, 2014), <http://www.natlawreview.com/article/why-sec-should-stay-out-fee-shifting-charter-debate>.
24. Cydney Posner, *Will the SEC intercede in the battle over fee-shifting bylaws?*, PubCo@ Cooley, Cooley LLP (October 13 2014), <http://cooleypubco.com/2014/10/13/will-the-sec-intercede-in-the-battle-over-fee-shifting-bylaws/>.
25. See <https://www.sos.ok.gov/documents/legislation/54th/2014/2R/SB/1799.pdf>.
26. J Robert Brown Jr., *Fee Shifting in Derivative Suits and the Oklahoma Legislature*, TheRacetotheBottom.org (September 24, 2014), <http://www.theracetothebottom.org/home/fee-shifting-in-derivative-suits-and-the-oklahoma-legislatur.html>.

Nithya Narayanan is an LL.M. Candidate, 2015, at Harvard Law School.

Squaring the Circle: Can Bad Legal Precedent Just Be Wished Away?

By C. Evan Stewart

Squaring the circle is a conundrum that has vexed mathematicians dating back to Ancient Babylon; in 1862, a solution was proven to be impossible by Ferdinand von Lindemann (because pi is a transcendental rather than an algebraic irrational number), and subsequent attempts have not moved the dial.¹ Unconstrained by notions of mathematical certitude, some lawyers are not so easily stopped, thinking that when they pronounce a cow to be a pig they can in fact make it so. Add the New York County Lawyers' Association's Professional Ethics Committee (the "NYCLA Committee") to that group.

But before we get to the NYCLA Committee, let's properly set the stage.

"[I]n 1862, a solution was proven to be impossible by Ferdinand von Lindemann (because pi is a transcendental rather than an algebraic irrational number), and subsequent attempts have not moved the dial. Unconstrained by notions of mathematical certitude, some lawyers are not so easily stopped, thinking that when they pronounce a cow to be a pig they can in fact make it so."

Rivera: The Outlier of Outliers (The Prequel)

Faithful readers of this august journal may remember that several years ago I introduced them to a truly wacky decision: *Rivera v. Lutheran Medical Center*.² For those who do not have photographic memories, as well as for our new readers, a recap of *Rivera* and the judicial bad apples that laid the groundwork for its wackiness is in order.

It all started in 1990, when the New York Court of Appeals decided *Niesig v. Team I*.³ In that case, the Court held that a lawyer representing an injured worker suing his company could interview, *ex parte*, employees of the company. New York's "no-contact" rule⁴ was held to apply only to those current employees "whose acts or omissions in the matter under inquiry are binding on the corporation (in effect, the corporation's 'alter egos') or important to the corporation for purpose of its liability, or employees implementing the advice of counsel." Believing that the "alter ego" test it created would "become relatively clear in application," the Court concluded that its ruling would further the "informal discovery of information" and

"serve both the litigants and the entire judicial system by uncovering relevant facts, thus promoting the expeditious resolution of disputes."

In adopting its definition for what constitutes a party for purposes of the "no-contact" rule, the Court considered and rejected not only a standard based upon that which had been determined by the U.S. Supreme Court in *United States v. Upjohn* (where each corporate employee was deemed to be a client for purposes of the attorney-client privilege),⁵ but also a "control group" test (i.e., only those who "control" a company may not be contacted) because of "practical and theoretical problems." With respect to the *Upjohn* decision, the New York Court of Appeals determined that the attorney-client privilege was "an entirely different subject" from the "no-contact" rule, and that "a corporate employer who may be a 'client' for purposes of the attorney-client privilege is not necessarily a 'party' for purposes of the ['no-contact' rule]."

No sooner had the *Niesig* decision been handed down than it was clear that there were a number of problems/issues with the "relatively clear" decision. The first concerned the risk of disqualification or professional sanctions. How is an attorney who wants to interview a current employee going to know in advance whether he or she is a corporate "alter ego"? As one California court looking at this quandary expressed: an attorney in such circumstances would be forced to make a "unilateral decision...based upon expectations or predictions."⁶

An obvious illustration of this quandary is posed by the hearsay exceptions set forth in Rule 801(d)(2)(D) of the Federal Rules of Evidence. A statement is not hearsay if it is "offered against a party and is...a statement by his agent or servant concerning a matter within the scope of his agency or employment, made during the existence of the relationship." Before conducting an *ex parte* interview, however, an attorney will be at risk as to whether the employee's knowledge of relevant facts comes from outside the scope of his or her employment.

The *Niesig* Court brushed this issue to one side because the hearsay rule in New York is different from Rule 801(d)(2)(D); in New York, very few employees are in a position to bind their companies by their statements.⁷ But what about jurisdictions that do not have an evidentiary rule similar to New York's but which nonetheless choose (or have chosen) to follow *Niesig*?⁸ Or what about a New York court sitting in diversity, seeking to apply *Niesig*'s substantive rule, while being bound to apply the Federal Rules of Evidence—once having allowed the interviews,

the New York federal court would also have to allow into evidence any statements made by the employee within the scope of her employment, pursuant to Rule 801(d)(2)(D).⁹

Another concern relates to whether the “alter ego” test is in fact “relatively clear in application” (as the New York Court of Appeals prophesized) or whether it leads to another procedural/litigation layer, with lawyers uncertain on how best to proceed. One look at the federal courts in New Jersey would suggest a not-so-sanguine answer.¹⁰ And the disparate treatment in just that one federal district is only the tip of the iceberg as to the satellite litigation that has been spawned in this area.¹¹

Niesig also represents the diminishment of the attorney-client privilege. Notwithstanding the New York Court of Appeals’ declaration that the privilege has nothing whatever to do with the “no-contact” rule, just saying so does not make it so. In fact, one of the basic policies underlying that rule is the need to protect communications and information covered by the privilege and the attorney work product doctrine.¹² And as the U.S. Supreme Court made clear in *Upjohn*, “the privilege exists to protect not only the giving of professional advice to those who can act on it but also the giving of information to the lawyer to enable him to give sound and informed advice.”¹³ Consistency with *Upjohn* would therefore require that an employee who is a “client” for privilege purposes (i.e., one who gives information and receives advice) should also be a “party” for purposes of the “no-contact” rule.¹⁴

The Court of Appeals subsequently compounded its error by expanding the “yes” to the “no contact” rule,¹⁵ but it was others who really grabbed the *Niesig* precedent and ran with it (into bad places). First came *Gidatex v. Campaniello Imports, Ltd.*¹⁶ In that case, a plaintiff’s lawyer in a trademark enforcement case sent undercover investigators into the defendant’s furniture showroom in order to prove that the defendant had engaged in “bait and switch” tactics. Wearing hidden wires, the investigators taped their discussions with the defendant’s employees; the plaintiff’s lawyer then sought to introduce the tapes at trial to impute liability to the defendant. An outraged defendant moved to preclude the tapes on the ground that a lawyer cannot send a non-lawyer to do that which a lawyer is ethically barred from doing (e.g., be deceptive, violate the “no-contact” rule, etc.).¹⁷

The *Gidatex* court, in the Southern District of New York, relying upon *Niesig*’s non-“bright-line rule” and “informal discovery” policy goal, as well as a New Jersey federal court decision that had applied *Niesig* in a similar situation,¹⁸ ruled that the tapes were admissible. Although the judge found that plaintiff’s counsel had “technically” violated applicable ethics rules (i.e., he engaged in deception; he violated the “no-contact” rule; etc.), she also found that the lawyer had not “substantively” violated those rules “because his actions simply

do not represent the type of conduct prohibited by the rules.”¹⁹ Huh?!

The NYCLA Committee (Part I)

On May 23, 2007, the NYCLA Committee decided to join in on the fun, issuing Formal Opinion 737. Inspired by the *Gidatex* decision, the NYCLA Committee embraced the plaintiff’s lawyer’s conduct and explicitly endorsed an ethical safe harbor for lawyers who employ “dissemination” in the evidence-gathering process; in other words, this ethics group opined that there should be formal exceptions to the broad admonition against lawyers engaging in “dishonesty, fraud, deceit, or misrepresentations”—so long as *Niesig*’s policy goal of “informal discovery of information” is promoted.

As if this was not bad enough, as we will soon see, the NYCLA Committee’s creative juices were only just getting started.

Rivera: The Outlier of Outliers (Part Deux)

In *Rivera*, a prominent, international law firm was retained by a hospital to defend against an employment discrimination claim. Shortly thereafter, the firm did what every experienced lawyer I know (including me) would do: it contacted the hospital’s current and former employees with first-hand knowledge of the facts, assured them that the firm could ethically represent them (i.e., there were no conflicts of interest), and offered to represent them at the hospital’s expense; four current and former employees accepted the offer. Thereafter, the plaintiff moved to disqualify the law firm from representing those four individuals, citing various purported ethics violations.

The trial judge did not agree that the law firm had violated any conflict of interest rule (there was in fact no evidence whatever that the multiple representations constituted a potential or actual conflict of interest). But the judge did find that the firm had violated the “non-solicitation” rule. That rule bars lawyers from “soliciting” clients directly (e.g., in person), unless the prospective client “is a close friend, relative, former client or current client.”²⁰

The judge’s legal authority for this unusual finding? *Niesig*:

[The employees] were clearly solicited by [the law firm] on behalf of [the hospital] to gain a tactical advantage in this litigation by insulating them from informal contact with plaintiff’s counsel. This is particularly egregious since [the law firm], by violating the Code in soliciting these witnesses as clients, effectively did an end run around the laudable policy

consideration of *Niesig* in promoting the importance of informal discovery practices in litigation, in particular, private interviews of fact witnesses. This impropriety clearly affects the public view of the judicial system and the integrity of the court.²¹

As I have previously opined,²² the *Rivera* decision is simply dead wrong. Unfortunately, the Appellate Division, Second Department did not agree with me, affirming the trial judge in a terse opinion: “the record supports the Supreme Court’s determination” that the law firm violated the non-solicitation rule.²³ Equally unfortunate is that a federal magistrate judge in New York has cited *Rivera* with approval;²⁴ of not much use to New York lawyers is the fact that a federal judge in Oklahoma agrees with me and expressly rejected *Rivera*.²⁵

Faced with this state of play (which is still the state of play today),²⁶ I publicly explored in this distinguished journal a number of possible ways to deal with this crazy precedent: (i) pretend it does not exist; (ii) have non-lawyers engage in the non-solicitation efforts; and/or (iii) enact a corporate policy that would permit the non-solicitation/representation arrangement. None of these I found to be terribly useful or likely to be successful.²⁷ One other alternative—which would clearly work—was put forward by the Committee on Professional Responsibility for the Association of the Bar of the City of New York: change the “non-solicitation” rule so it would not trip up lawyers in *Rivera* type situations; unfortunately, that proposal went nowhere.²⁸

The NYCLA Committee (Part Deux)

On June 9, 2014, the NYCLA Committee weighed in to save the day with Formal Opinion 747. Employing the same keen analysis it utilized when it endorsed lawyer “dissemination” in civil litigation (Formal Opinion 737), the group purportedly “solved” the *Rivera* problem by basically opting for the first alternative I identified several years ago.

Evidently (according to the NYCLA Committee), the problem with the law firm’s conduct in *Rivera* was that the firm’s “primary, if not exclusive, purpose...from its inception” was to “insulate the witnesses from opposing counsel’s informal contact.” Where the NYCLA Committee divined that “primary, if not exclusive, purpose” is a bit unclear, since evidence thereof does not exist in either of the *Rivera* decisions (or in the litigation record). But having constructed that Trojan Horse, the NYCLA Committee then rode it into the city of Troy, opining that all will be well *so long as* “the primary purpose of the in-person meeting at its inception is not to offer the lawyer’s services to the employee, but to interview the employee as a potential witness.” After that, it will then be perfectly okay to offer to represent the individual (in addition

to representing the company) *so long as* the “lawyer’s ‘primary purpose’ is not to secure legal fees” from that individual. This two-step scenario, according to the NYCLA Committee, is “meaningfully distinguishable” from *Rivera* and thus hunky dory from an ethics standpoint. Really?

The solution proffered by the NYCLA Committee actually runs afoul of the same “problem” that concerned the trial court in *Rivera*; it merely delays it by a matter of minutes. In other words, the same “tactical advantage” will accrue to the company’s lawyer—she will still be able to block *ex parte* communications with the individual.²⁹ But because that lawyer will act with “purer” motives the first time she speaks with the individual, and has no pecuniary interest in representing the individual (a factor *not* in play in *Rivera* or in *any* of the corporate multiple representation situations of which I am aware), somehow her conduct will not fall on the wrong side of *Rivera*. If you buy that one, there is a bridge that spans the East River that is up for sale at a very attractive price.

“For Rivera to truly ‘sleep with the fishes,’ it either must be expressly rejected by the New York Court of Appeals, or there must be an amendment to the ‘non-solicitation’ rule. Until then, caution remains the watchword for New York lawyers addressing multiple representation situations.”

Conclusion

Neither wishing away bad legal precedent, nor constructing non-substantive “steps” that do not alter reality, works in the real world. For *Rivera* to truly “sleep with the fishes,”³⁰ it either must be expressly rejected by the New York Court of Appeals, or there must be an amendment to the “non-solicitation” rule. Until then, caution remains the watchword for New York lawyers addressing multiple representation situations.

Endnotes

1. See J.J. O’Connor & E.F. Robertson, *Squaring the Circle* (Apr. 1999), http://www-history.mcs.st-andrews.ac.uk/HistTopics/Squaring_the_circle.html. Those who have tried to solve this problem (or mused upon it) include: Charles Lutwidge Dodgson (“Lewis Carroll”), Dante, Alexander Pope, Gilbert and Sullivan, O’Henry, and James Joyce. FRANCINE F. ABELES, CHARLES L. DODGSON’S GEOMETRIC APPROACH TO ARCTANGENT RELATIONS FOR π , 153–54 (*Historia Mathematica* 20, 1993), available at http://ac.elsa-cdn.com/S031508608371013X/1-s2.0-S031508608371013X-main.pdf?_tid=2bbfc544-6628-11e4-a625-00000aacb35f&acdnt=1415328524_56da8a44378397fad3a2b68517062a21; Peter Kalkavage, *In the Heaven of Knowing: Dante’s Paradiso*, THE IMAGINATIVE CONSERVATIVE (Aug. 10, 2014), <http://www.theimaginativeconservative.org/2014/08/heaven-knowing-dantes-paradiso.html>; GEORGE GILFILLAN, THE POETICAL WORKS OF ALEXANDER POPE 288; see

- Princess Ida, INTERNET ARCHIVE, available at http://archive.org/stream/princessidaorcas00sulliala/princessidaorcas00sulliala_djvu.txt; O'Henry, *Squaring the Circle*, available at <http://www.readbookonline.net/readOnline/14958/>; see JAMES JOYCE, ULYSSES (1922). Stevie Wonder released his "In Square Circle" album in 1985, for which he won the Grammy Award for Best Male R&B Vocal Performance. *Stevie Wonder Biography*, Rolling Stone, <http://www.rollingstone.com/music/artists/stevie-wonder/biography> (last visited Nov. 20, 2014). And for film aficionados, you can watch Bollywood's *The Square Circle* (1996), starring Nirmal Pandey, Sonali Kulkarni, and Faiyaz. *The Square Circle*, IMDB, <http://www.imdb.com/title/tt0116002/> (last visited Nov. 20, 2014).
2. 22 Misc. 3d 178, 866 N.Y.S.2d 520 (Sup. Ct., Kings Co. 2008), *aff'd*, 73 A.D.3d 891, 899 N.Y.S.2d 859 (2d Dep't 2010). See C. Evan Stewart, *Just When Lawyers Thought It Was Safe to Go Back into the Water*, N.Y. BUS. L.J., vol. 15, no. 2, at p. 24 (Winter 2011).
 3. 76 N.Y.2d 363, 559 N.Y.S.2d 493, 558 N.E.2d 1030 (1990).
 4. The "no-contact" protocol under the ABA's Model Rules is Model Rule 4.2, which provides that "a lawyer shall not communicate... with a person the lawyer knows to be represented by another lawyer in the matter." MODEL RULES OF PROF'L CONDUCT R. 4.2 (2014) (Communication with Person Represented by Counsel). This rule, which many (but not all) states have adopted in whole or in part, was clarified in 1995, when the word "person" was substituted for "party" so as to ensure that the *ex parte* ban covered, inter alia, pre-litigation contexts. *Id.* Unlike ABA Model Rule 4.2, New York's "no-contact" rule has always applied to a "party," as opposed to a "person." NEW YORK CITY BAR, FORMAL OP. 2002-3, available at http://www2.nycbar.org/Publications/reports/show_html_new.php?rid=125 (last visited Nov. 20, 2014).
 5. 449 U.S. 383 (1981). In *Upjohn*, the Supreme Court recognized that "[m]iddle-level—and indeed lower level—employees can, by actions within the scope of their employment, embroil the corporation in serious legal difficulties, and it is only natural that their employees would have relevant information needed by corporate counsel if he is adequately to advise the client with respect to such actual or potential difficulties." *Id.* at 391.
 6. *Mills Land & Water Co. v. Golden West Refining Co.*, 189 Cal. App. 3d 116, 130, 230 Cal. Rptr. 461, 468 (1986).
 7. See Comm. on Prof'l Ethics of the Ass'n. of the Bar of the City of N.Y., Inquiry Ref. No. 46 (1980).
 8. See, e.g., *Messing, Rudavsky & Weliky v. President and Fellows of Harvard Coll.*, 764 N.E.2d 825, 832–33 (Mass. 2002); *Strawser v. Exxon Co. U.S.A.*, 843 P.2d 613, 621 (Wyo. 1992); *Dent v. Kaufman*, 406 S.E.2d 68, 72–73 (W. Va. 1991).
 9. See *Polycast Tech. Corp. v. Uniroyal Inc.*, 129 F.R.D. 621, 626–27 (S.D.N.Y. 1990).
 10. *Compare Pub. Serv. Elec. & Gas Co. v. Assoc. Elec. Gas Ins. Serv. Ltd.*, 745 F. Supp. 1037, 1042–43 (D. N.J. 1990) (*ex parte* communication barred with present or former employees) with *Curley v. Cumberland Farms Inc.*, 134 F.R.D. 77, 82–83 (D. N.J. 1990) (*ex parte* communications allowed with former employees, unless they played a central role in the controversy in dispute) with *In re Prudential Ins. Co. of Am. Sales Practices Litig.*, 911 F. Supp. 148, 154 (D. N.J. 2000) (*ex parte* communications allowed with former employees, except for those in the company's "litigation control group").
 11. *Compare Orlowski v. Dominick's Finer Foods Inc.*, 937 F. Supp. 723, 735 (N.D. Ill. 1996); *Valasses v. Samuelson*, 143 F.R.D. 118, 126 (E.D. Mich. 1992); *Dubois v. Gradco Sys. Inc.*, 136 F.R.D. 341, 347 (D. Conn. 1991) with *Amsey v. Medshores Mgmt. Servs. Inc.*, 184 F.R.D. 569, 574 (W.D. Va. 1998); *Lang v. Reedy Creek Improvement Dist.*, 888 F. Supp. 1143, 1149–50 (M.D. Fla. 1995); *Midwest Motor Sports Inc. v. Arctic Cat Sales Inc.*, 144 F. Supp. 2d 1147, 1160 (D. S.D. 2001); *Palmer v. Pioneer Inn Assocs., Ltd.*, 59 P.3d 1237, 1248–49 (Nev. 2002), BNA U.S. Law Week 1411 (Jan. 14, 2003).
 12. See *Blanchard v. Edgemark Fin. Corp.*, 175 F.R.D. 293, 302, n.10 (N.D. Ill. 1997); *Candler v. Md.*, 910 F. Supp. 115, 119–20 (D. Md. 1996); see also ABA Comm. on Ethics & Prof'l Responsibility, Formal Op. 396 (1995); S. Miller & A. Cairo, *Ex Parte Contact with Employees and Former Employees of a Corporate Adversary; Is It Ethical?* 42 BUS. LAW. 1053, 1054–55, 1060–65 1071 (1987). Another reason for the rule is to protect unknowledgeable people from unscrupulous lawyers.
 13. 449 U.S. at 390.
 14. See GEOFFREY C. HAZARD & W. WILLIAM HODES, LAW OF LAWYERING 437 (1985) (an employee covered by the privilege, as per *Upjohn*, should be considered a "party" under the ethical rules). Indeed, the *Niesig* court's client/party dichotomy does not stand up to scrutiny because the status, knowledge, and/or responsibility of an employee should be irrelevant for purposes of whether an *ex parte* contact is permissible. An employee who can bind the company may be just as much in possession of underlying facts as one who cannot. Moreover, if "uncovering relevant facts" is the uppermost policy goal, should there be any difference as to which type of employees may invoke this protection? Finally, as indicated above, the policies served by the privilege and the "no contact" rule are, in fact, aligned.
 15. The Court first pushed ahead in *Muriel Siebert & Co. v. Intuit Inc.*, 8 N.Y.3d 506, 836 N.Y.S.2d 527, 868 N.E.2d 208 (2007). In that case, the chief operating officer of Siebert, who was directly involved in ongoing litigation with Intuit, was contacted and interviewed by Intuit's lawyers immediately upon their hearing of his termination by the company. Notwithstanding that the COO had indisputably been a Siebert "alter ego" for purposes of the *Niesig* test, the Court reasoned that because he was no longer an employee at the time of the *ex parte* interview that meant that Intuit's lawyers had done nothing wrong.
- The Court further reasoned that because Intuit's lawyers had been careful not to elicit privileged information from the ex-COO, the interview had merely served to facilitate *Niesig*'s policy goal of furthering the "informal discovery of information," and thus there were no other ethical issues of any kind implicated by their actions.
- Just months after *Siebert*, the New York Court of Appeals struck again in *Arons v. Jutkowitz*, 9 N.Y.3d 393, 880 N.E.2d 831, 850 N.Y.S.2d 345 (2007). There, the Court held that defense lawyers in a medical malpractice action could conduct *ex parte* interviews with the plaintiff's doctor. After reviewing its prior rulings in *Niesig* and *Siebert*, the Court determined that there was no reason why there should not be informal discovery in this context, as well. As to whether doctors would be "gulled into making an improper disclosure," the Court was unmoved, having previously rejected such a concern for corporate employees (*Niesig*) and former corporate big-wigs (*Siebert*).
16. *Gidatex v. Campaniello Imports, Ltd.*, 82 F. Supp. 2d 119 (S.D.N.Y. 1999).
 17. See ABA Formal Op. 95-396 (1995); see also MODEL RULES OF PROF'L CONDUCT, R. 5.3(c) & 8.4(a); DR 1-102(A)(1), DR 1-102(A)(4), & DR 1-104(D) (New York's then-existing, applicable ethics rules).
 18. See *Apple Corp. Ltd., MPC v. Int'l Collectors Society*, 15 F. Supp. 2d 456 (D. N.J. 1998).
 19. For contrary authority on this point, see *Midwest Motor Sports v. Arctic Sales Inc.*, 347 F.3d 693 (8th Cir. 2003).
 20. The "non-solicitation" rule in play when the *Rivera* judge ruled was DR 2-103(A)(i). When New York State revamped its ethics rules, the rule became Rule 7.3, with no substantive change.
- The rationale for the "non-solicitation" rule is to deal with ambulance-chasing behavior and is best expressed in Comment 1 to ABA Model Rule 7.3: "There is a potential abuse inherent in direct in-person, live telephone or real-time electronic contact by a lawyer with a prospective client known to need legal services. These forms of contact between a lawyer and a prospective client subject the layperson to the private importuning of the trained

advocate in a direct interpersonal encounter. The prospective client, who may already feel overwhelmed by the circumstances giving rise to the need for legal services, may find it difficult fully to evaluate all available alternatives with reasoned judgment and appropriate self-interest in the face of the lawyer's presence and insistence upon being retained immediately. The situation is fraught with the possibility of undue influence, intimidation, and over-reaching." MODEL RULES OF PROF'L CONDUCT, R. 7.3 cmt. 1.

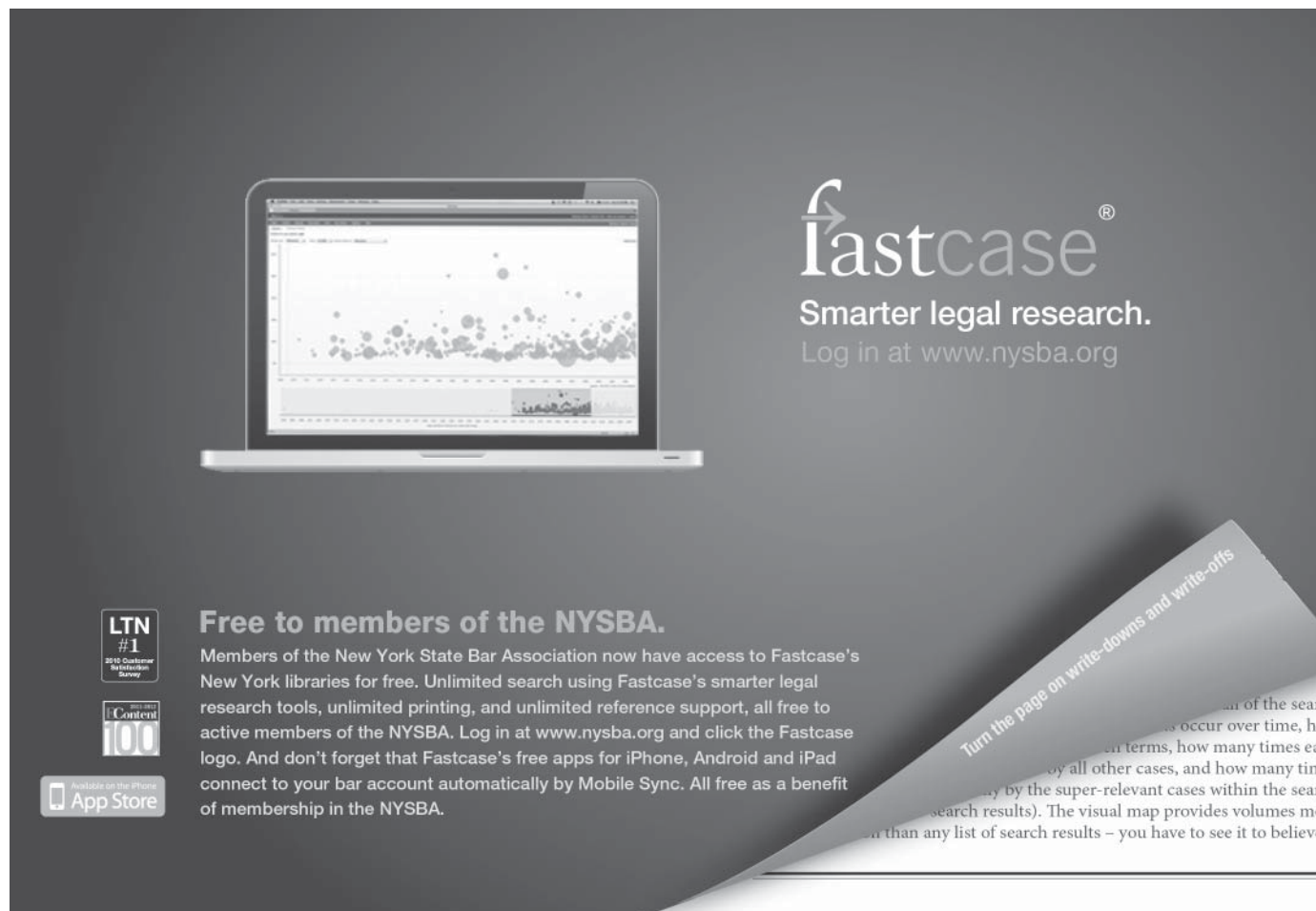
This rationale is obviously not present in the *Rivera* case—the law firm was chasing no ambulance; furthermore, it told the four individuals that their decisions were completely voluntary and there would be no impact on the two employees' employment status if they declined representation.

21. The *Rivera* judge also reported the law firm's "misconduct" to the New York State Disciplinary Committee. *Rivera v. Lutheran Medical Center*, 866 N.Y.S.2d 520, 526. (Sup. Ct., Kings Co. 2008).
22. *Id.*
23. *Rivera v. Lutheran Medical Center*, 73 A.D.3d 891, 891 (2010).
24. *See Matusick v. Erie County Water Authority*, 2010 WL 2431077 (W.D.N.Y. Feb. 22, 2010).
25. *See Wells Fargo Bank, N.A. v. LaSalle Bank Nat'l Ass'n*, 2010 WL 1558554 (W.D. Okla. Apr. 19, 2010).
26. *See Michael J. Dell, Ethical Considerations in the Representation of Multiple Clients*, PRACTICING LAW INSTITUTE (Aug. 21 2014), [http://](http://www.pli.edu/Content/Seminar/Ethics_in_Banking_and_Financial_Services/_/N-4kZ1z12evy?ID=173702)

www.pli.edu/Content/Seminar/Ethics_in_Banking_and_Financial_Services/_/N-4kZ1z12evy?ID=173702.

27. C. Evan Stewart, *supra* note 2.
28. *Id.*
29. The "tactical advantage" concern of the *Rivera* judge just underscores how wacky the ruling truly is. Of course the law firm was seeking a tactical advantage in the litigation—that is what lawyers are supposed to do. *See* Simon H. Rifkind, *The Lawyer's Role and Responsibilities in Modern Society*, 10 RECORD (1975).
30. A la Luca Brasi in GODFATHER (Paramount 1972) (done in by Bruno Tattaglia, son of Philip Tattaglia, head of the Corleone's rival crime family). All of life's important lessons can be learned from GODFATHER and GODFATHER PART II (Paramount 1974); none can be learned from GODFATHER PART III (Paramount 1990), which is a terrible movie.

C. Evan Stewart is a partner in the New York City office of Cohen & Gresser LLP, focusing on business and commercial litigation. He has published over 200 articles on various legal topics and is a frequent contributor to the *New York Law Journal* and this publication.



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 2010 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 tim
...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

Benefit Corporations and Certified B Corporations: Hybrid Corporate Options for Entrepreneurs and Socially Enterprising Business Owners Forming For-Profit Companies

By Aaron Boyajian

Benefit Corporations

In recent years, entrepreneurs and business owners are taking corporate responsibility and social enterprise into consideration more than ever when forming new companies. Until recently, in New York,¹ when determining which corporate structure to utilize when forming socially conscious entities, these entrepreneurs would be pigeonholed into using the standard corporate forms of corporations and limited liability companies. However, the use of the standard corporate form did not ultimately mesh with the purposes proffered by these emerging companies because there is an inherent tension created between a socially responsible mission and the rigid strictures of corporate law, which require officers and directors to maximize profits for shareholders above and beyond any other goal. This tension has traditionally forced socially enterprising companies to eschew their original purposes in order to adhere to the bottom-line profit margin which is a guiding principle of corporate law. One of the oft-cited examples of this is the sale of Ben & Jerry's ice cream to Unilever in 2000.²

However, on February 10, 2012, a new era for entrepreneurs and business owners dawned in New York when the Benefit Corporation Law³ was enacted, which bridged the gap to allow corporations⁴ to both focus on profit maximization while at the same time allowing them to operate with social and economic benefits and goals in mind. The Benefit Corporation Law offers a new, hybrid form of corporation to be formed, known as Benefit Corporations ("B-Corp").⁵

A B-Corp, unlike standard S-Corporations or C-Corporations, combines the features of for-profit and non-profit corporations by allowing management to consider the corporation's impact on the environment, community and its employees, in addition to considering the profit returned to shareholders. Therefore, since the purpose of a B-Corp is to create a positive impact on society and the environment, the likelihood of claims being brought by investors and shareholders for failure to maximize profit will be greatly decreased when directors seek to uphold the stated corporate mission over generating profit.

While New York was not the first state in the country to adopt this new corporate form, it was in the forefront of the initiative and is now one of only 23 states which

allow the formation of Benefit Corporations,⁶ including, New Jersey, Pennsylvania, Massachusetts and Delaware.

B-Corps are formed in the same way as traditional New York corporations. However, there are two main differences of note. Specifically, B-Corps are formed for a public benefit purpose, and they must be accountable and transparent with respect to such benefit purpose.

Purpose

All Benefit Corporations are formed for the purpose of creating "general public benefit." As defined in Section 1702 of the BCL, a general public benefit is one that provides a material positive impact on society and the environment, taken as a whole, assessed against a third-party standard, from the business and operations of a benefit corporation.

A Benefit Corporation can go one step further and identify one or more "specific public benefits" for which it intends to operate. Examples of specific public benefits are (a) providing low-income or underserved individuals or communities with beneficial products or services; (b) promoting economic opportunity for individuals or communities beyond the creation of jobs in the normal course of business; (c) preserving the environment; (d) improving human health; (e) promoting the arts, sciences or advancement of knowledge; (e) increasing the flow of capital to entities with a public benefit purpose; and (f) the accomplishment of any other particular benefit for society or the environment.

While there are many obvious types of products and services which fit nicely under the auspice of what a Benefit Corporation should be (e.g., eco-friendly cleaning products, organic and raw sourced foods and solar energy firms), there are other businesses, like law firms, architecture firms and investment firms, which, while not traditionally thought of as socially responsible, make very good candidates to be formed as B-Corps.

Transparency

After a B-Corp is formed, in addition to the usual corporate filing requirements, it will have to file an annual report showing how its performance benefited social and environmental goals. This benefit report must contain, among other things, (1) a narrative description

of the ways in which the benefit corporation pursued the general public benefit during the year and the extent to which that general public benefit was created; (2) the ways in which the benefit corporation pursued any specific public benefit that the certificate of incorporation states is the purpose of the benefit corporation to create, and the extent to which that specific public benefit was created; and (3) any circumstances that have hindered the creation by the benefit corporation of general or specific public benefit; (4) an assessment of the performance of the Benefit Corporation, relative to its general public benefit purpose assessed against a third-party standard applied consistently with any application of that standard in prior benefit reports, or accompanied by an explanation of the reasons for any inconsistent application and, if applicable, assessment of the performance of the benefit corporation, relative to its specific public benefit purpose or purposes; (5) the compensation paid by the benefit corporation during the year to each director in that capacity; and (6) the name of each person who owns beneficially or of record five (5%) percent or more of the outstanding shares of the benefit corporation.

The benefit report must be sent annually to each shareholder within one hundred twenty (120) days following the end of the B-Corp's fiscal year. Additionally, the benefit report must be posted on the public portion of the B-Corp's website and delivered to the New York State Department of State for filing. The exception to this requirement is that compensation paid to directors and any financial or proprietary information which is included in the shareholder benefit report may be omitted from what is shown to the public. As of now, in New York, the annual benefit reports are not required to be verified, certified, or audited by a third-party standard organization.

Accountability

New York's Benefit Corporation Law statute sets forth that "the purpose to create general public benefit shall be a *limitation* on the other purposes of the benefit corporation, and *shall control* over any inconsistent purpose of the benefit corporation." Therefore, wherever there is a trade-off between seeking profits and creating general public benefit, there is a legal mandate which demands that the B-Corp pursue the latter.

To accomplish the stated goals of the B-Corp, directors are given an expanded fiduciary duty which requires them to take into consideration various other factors over and above the financial benefits of the shareholders. To that end, directors must not only consider the effects of any corporate action on whether such action or inaction will accomplish the general and any specific public benefit purposes of the B-Corp, but they must also consider how the corporate action will impact (a) its shareholders; (b) its employees and workforce (and those of its suppliers); (c) its customers; (d) the community and society, including any community in which offices or facilities

of the benefit corporation or its subsidiaries or suppliers are located; (e) the local and global environment; and (f) its short-term and long-term interests, including benefits which may accrue from its long-term plans and the possibility that these interests may be best served by the continued independence of the benefit corporation. The statute does not provide any order or priority by which the directors must consider the interests of the B-Corp.

Additionally, when determining if a proposed purchase of the business is in the B-Corp's best interest, the directors may consider the (a) resources, intent and conduct (past, stated and potential) of any person or entity seeking to acquire control of the corporation; and (b) any other pertinent factor or the interest of any other group that they deem appropriate.

The ability for directors to focus on sustaining the purposes of the corporation while not being required to maximize shareholder profit makes B-Corps, in essence, double-bottom line businesses, whereby they can seek to treat both their purpose and their capital in a sustainable manner.⁷

Certified B Corporations

A B-Corp is not the same as a "Certified B Corporation." A Certified B Corporation status is a certification, which companies with an operating history apply to attain. This certification is conferred by the nonprofit known as B Lab,⁸ which charges annual fees of \$500-\$25,000 for companies to keep the Certified B Corporation status current. B-Corps and Certified B Corporations are often confused, and while primarily similar, they have a few important differences which are discussed below.

B-Corps are legal entities which are administered by individual states, like New York. A company may choose to incorporate as a benefit corporation in a state which recognizes it as a legal entity and may also seek to become certified as a "Certified B Corporation." In the alternative, a corporation which has not been formed under a statutory benefit corporation law may seek to obtain Certified B Corporation status while retaining the customary corporate form.

There is no requirement that B-Corps obtain certification as a Certified B Corporation. However, certification as a Certified B Corporation means that a company has met a high overall standard of social and environmental performance, accountability and transparency, and as a result, has access to a portfolio of services and support from B Lab that non-certified companies and B-Corps do not. As of the date of this article, there are 999 Certified B Corporations, including well-known brands such as Warby Parker (warbyparker.com), Greystone Bakery (New York's first Certified B Corporation) (greystonbakery.com), Etsy (etsy.com) and Uncommon Goods (uncommongoods.com).

Certification

Each Certified B Corporation must achieve a verified minimum score of 80 points out of a possible 200 points from B Lab on the B Impact Assessment.⁹ This assessment is tailored to a company's size, sector and geography and takes around 1-3 hours to complete. The assessment seeks to determine a multitude of information relating to realigning the social and economic performance by the company, including its corporate governance, accountability and transparency, compensation, benefits and training, community practices, and environmental practices.

Since the B Impact Assessment asks about what a company has done in the past, a newly formed company will find it difficult to answer the questions unless it has an operating history. Therefore, B Lab suggest that companies wait to seek certification until after the first 6 months of full operations and revenue generation.

Once certified as a Certified B Corporation, a company can attract investors, generate press, and allow like-minded companies to partner with it. Members of the public will have confidence that they are purchasing from companies which are seeking to address social challenges.

Conclusion

The movement to increase corporate responsibility quickly, and all entrepreneurs and business owners should give consideration to whether a B-Corp would be the proper form of entity for their new ventures. We anticipate that B-Corp formations will dramatically increase over the next few years as business owners will want to show investors and consumers that they intend to be, and will be held to be, good corporate citizens. Therefore, any for-profit business which is or intends to provide a benefit to the public through charitable activities, sustainable operations practices or by promoting economic opportunity for individuals or communities beyond the creation of jobs in the normal course of business, should consider utilizing this new form of entity offered by New York State, and should also consider seeking certification as a Certified B Corporation.

Endnotes

1. This article will focus on New York law. However, it should be noted that most states have general corporate laws similar to New York, which makes much of this discussion germane relating to the implementation of statutes akin to the New York Benefit Corporation Law.
2. In its official announcement with respect to the deal, Ben & Jerry's noted that it would keep the firm's "social mission" intact. However, at the end of the day, the determining factor which overrode all others was that Ben & Jerry's simply could not pass on the deal because of the financial windfall which its shareholders stood to gain, http://www.slate.com/articles/business/moneybox/2000/04/the_scoop_on_ben_jerrys_sellout.html.
3. McKinney's Business Corporation Law §§ 1701 *et seq.*
4. New York does not allow for the formation of a low-profit limited liability company (LLC), which is the LLC variant of the Benefit Corporation.
5. The formation of a benefit corporation is not limited to new entities. If an existing corporation believes that it may be able to operate as a Benefit Corporation, it can elect to do so under Section 1704 of the new BCL. In order for an existing corporation to make this election, in addition to complying with the Benefit Corporation law, it must: (a) amend its certificate of incorporation so that it contains a statement that the corporation is a benefit corporation; and (b) adopt the amendment by a least a 75% vote of all shareholders.
6. In addition to New York, the following states provide for the use of benefit corporations: Arizona (effective December 31, 2014), Arkansas, California, Colorado, Delaware, Hawaii, Illinois, Louisiana, Maryland, Massachusetts, Nebraska (effective July 17, 2014), Nevada, New Jersey, Oregon, Pennsylvania, Rhode Island, South Carolina, Utah (effective May 13, 2014), Vermont, Virginia, and West Virginia (effective July 1, 2014). The District of Columbia also allows for the formation of benefit corporations.
7. Ben & Jerry's famously called this double bottom line of profits and people the "double dip."
8. B Lab is a 501(c)3 nonprofit whose stated mission is to serve a global movement of entrepreneurs using the power of business to solve social and environmental problems. B Lab envisions that all businesses in the world will measure and manage their impact as readily as they do profitability. bcorporation.net.
9. bimpactassessment.net.

Aaron Boyajian is a Partner at Goetz Fitzpatrick LLP (goetzfitz.com) and can be reached at aboyajian@goetzfitz.com.

**Looking for Past Issues
of the
NY Business Law Journal?**

Go to www.nysba.org/BusinessLawJournal





Banking Law Committee

A meeting of the Banking Law Committee was held during the Business Law Section Fall Meeting, on September 11, 2014. Committee member Sabra Baum discussed some of the pressing regulatory matters she has followed, highlighting cybersecurity, virtual currency (bitcoin), payday lenders, and proposed Bank Secrecy Act regulations that would require customer due diligence to be performed on beneficial owners of legal entity customers, as well as on the customers themselves. The theme for the panel discussion was “An Inside Look at the Regulators” with Sara Kelsey, former General Counsel at the FDIC and former Deputy Superintendent and Counsel at the former New York State Banking Department (predecessor of the current Department of Financial Services), and Barbara Kent, former Acting Superintendent of Banks and former Director of Consumer Affairs and Financial Products at the New York State Banking Department. They each provided their views on various regulatory and enforcement issues using the backdrop of recent events in the banking industry such as the mortgage crisis. A lively discussion among the attendees and the speakers ranged over a host of issues about regulations and regulators. The discussion lasted far beyond the time allotted, and many attendees wished it could have gone on far longer. So Ms. Kelsey and Ms. Kent may be appearing again at another committee meeting in the foreseeable future.

The next Banking Law Committee meeting was scheduled to be held during the Annual Meeting of the New York State Bar Association on January 28, 2015. The agenda has not yet been decided, but the members of the committee will be contacted with information once it is available.

Kathleen A. Scott, Chair

Bankruptcy Law Committee

The Bankruptcy Law Committee held a well-attended panel discussion regarding the interplay of Bankruptcy and Intellectual Property Law as part of the Section’s Fall Meeting in Manchester Village, Vermont. The Bankruptcy Law Committee planned a CLE class for the Annual Meeting and is soliciting topics for a CLE class for the Spring Meeting. For copies of the materials from the Committee meeting in Manchester Village or to suggest topics, contact Scott Bernstein at sbernstein@mccarter.com.

Scott Bernstein, Chair

Corporations Law Committee

The Corporations Law Committee affords practitioners who specialize in advising corporations and/or alternative business entities an opportunity to learn about and discuss with their colleagues in the New York Bar the latest developments in mergers and acquisitions, corporate governance and other related matters. In that regard, the Committee endeavors to provide its members with educational opportunities for CLE credit.

One of the key functions of the Committee is to review pending legislation that affects corporations and other legal entities. The Committee reviews pending and proposed legislation and court cases involving the New York Business Corporation Law (the “BCL”) and other New York laws affecting corporations and other business entities, including partnerships, limited partnerships, and limited liability companies. It takes an active role in proposing legislation which affects corporations and alternative business entities.

In the past, the Committee has successfully led the effort to revise the New York Not-For-Profit Corporation Law, and to amend the Business Corporation Law to facilitate majority voting for New York corporations and to allow the payment of dividends out of net profits. The Committee has also submitted legal memoranda in opposition to various bills that did not become law, including bills requiring remote access and voting at shareholder meetings and requiring disclosure of, among other things, the duties and responsibilities of members of limited liability companies.

The next meeting of the Committee was scheduled to be held in conjunction with the Annual Meeting of the NYSBA. Richard De Rose will provide an overview of key recent trends and developments in M&A and Delaware law. The Committee is also looking for volunteers to make presentations at future committee meetings. Please contact Richard De Rose (212-49-7867 or rderose@hl.com) to volunteer to make a presentation, to provide suggestions about future topics to discuss at Committee meetings, or for other information regarding Committee activities.

Richard De Rose, Chair

Derivatives and Structured Products Law Committee

The Derivatives and Structured Products Law Committee meets on a monthly basis from September through June of each year. The committee's members are diverse and include lawyers from law firms, banks and hedge funds. The committee's monthly meetings are generally hosted by law firms. The host firm provides a presentation, which usually includes CLE credit, on an area in derivatives. Past meeting topics include the 2014 Credit Derivatives Definitions, UCC and bankruptcy issues that relate to cleared derivatives, position limits, SEFs and the Volcker rule. In addition to being a source of education for current topics in the derivatives industry, these meetings provide a forum for dialogue on the changing legal landscape of derivatives. As many of those who attend these meetings are experienced derivatives attorneys, participants often raise thought-provoking questions and comments with the panelists. As new rules and regulations pertaining to derivatives continue to be issued, the Derivatives and Structured Products Law Committee continues to be an important resource for its members.

Ilene K. Froom, Chair

Franchise, Distribution and Licensing Law Committee

The Business Law Section held its Fall meeting at the beautiful Equinox Golf Resort and Spa in Manchester, Vermont between September 10 and September 12, 2014. In conjunction with the Fall meeting, the Franchise, Distribution and Licensing Law Committee participated in a CLE program and offered a seminar exploring and explaining various ways for a franchisor to structure its franchise offering and to implement the development of its franchise program. Your Chairman served as moderator for the program, and committee member Thomas Pitegoff, together with Edward (Ned) Levitt, from Toronto, Canada, made presentations regarding the topic.

Despite the relatively compact time frame available for presentation, both the session and the paper which accompanied it were widely encompassing, covering a variety of general domestic franchise issues (e.g., Advertising Fund contributions, transfer issues, term and renewal issues, venue and applicable law). The program also explored multi-unit development deals, both domestically and internationally, and, in that context, examined topics such as territorial exclusivity, the types of entities that area developers would utilize, the types of agreements with respect to these development arrangements, and the particular issues attendant on the expansion of franchise systems internationally.

The session, which was offered for full CLE credit, was well attended and provided the attendees a variety of insights into the various ways to implement and expand

a franchise system, both domestically and internationally, at a level usually reserved for those attorneys who are sophisticated practitioners in the field. As such, the attorneys present had an opportunity to hear about and assess the typical (and atypical) means by which franchisors expand their systems, as well as the pitfalls that might attend some of those expansion methods.

During the last several months, our Committee has continued to work on the proposed modifications to the New York State Franchise Sales Act. The proposed modifications, which are presently on the legislature's calendar for consideration, are intended to be coordinated with the views of the New York State Attorney General's Office and, by the time this report "goes to press," a meeting will likely have been held with that Office in order to discuss the Attorney General's views with respect to the proposed legislation and, in all likelihood, to incorporate those views into the proposed legislation. Our Committee is seeking to make the New York law consistent with the Federal Trade Commission Rule, the federal statute which regulates franchise offerings, and to make the law of our state more "franchise friendly."

For further information regarding the Committee and its activities or with respect to the next Committee meeting, please contact Committee Chair Richard L. Rosen (rlr@rosenlawpllc.com or at 212-644-6644).

Richard L. Rosen, Chair

Insurance Law Committee

No report submitted.

Legislative Affairs Committee

The Legislative Affairs Committee continues to work on two active projects. The Nonprofit Revitalization Act of 2013 became effective July 1, 2014, after a ten-year effort by the committee. Members of the Not-for-Profit Corporation Law Committee now plan to make recommendations to the New York Attorney General's Office to clarify certain points in the Act and provide guidance to the non-profit community with respect to the Attorney General's enforcement policies.

Second, Richard Rosen, David Oppenheim and I are continuing our discussions with key staff in the Attorney General's Office and with legislators in Albany with the intention of introducing our proposed bill in the 2015 legislative session and hopefully seeing it through to enactment. (See the Report of the Franchise, Distribution and Licensing Law Committee.)

Kevin Kerwin, Associate Director in the NYSBA's Department of Governmental Relations, continues to work closely with us in our dealings with the legislature and the Attorney General's Office.

We continue to monitor bills that may affect business in New York State and we welcome new ideas for legislative changes from all interested members of the Business Law Section.

The next Committee meeting was scheduled to take place January 28, 2015, at the NYSBA's Annual Meeting. All Section members are welcome.

Thomas M. Pitegoff, Esq., Chair

Public Utility Law Committee

On October 17, 2014, the Public Utility Law Committee of the New York State Bar Association Business Law Section hosted the Public Utility Law Institute, an all-day continuing legal education program dedicated exclusively to current issues affecting public utility law. The program, which was well attended, included several panels covering a wide range of topics, including:

- A discussion of the legal issues affecting the New York State Public Service Commission's Reforming the Energy Vision proceeding in which the Commission is considering a substantial transformation of electric utility practices to improve system efficiency, empower customer choice, and encourage greater penetration of clean generation and efficiency technologies;
- Legal considerations associated with the increasing reliance on natural gas by electric generating facilities;
- Recent developments in the telecommunications industry; and
- The jurisdictional line between federal and state utility regulation.

Each panel included top practitioners in the energy field from both the public and private sectors who were able to provide varying perspectives on each topic. The program's keynote speaker was New York State Public Service Commissioner Gregg Sayre, who spoke about net neutrality.

Bruce Miller, Chair

Securities Regulation Committee

The Securities Regulation Committee is made up of experienced securities practitioners, newer securities lawyers and business lawyers who want to know more about securities regulation. The Committee holds dinner meetings generally on the third Wednesday of every month. The proceedings, which start with cocktails, continue with dinner and finish with two hours of topical presentations, provide opportunities for lawyers to network with one another and then participate in what are often lively

discussions. A conference call option is available upon request for members who are outside of the New York City area.

A sampling of recent topics includes:

- Crowdfunding, Regulation A, and the challenges of Rule 506(c);
- The SEC's crackdown on Section 16 late filers;
- The evolution of OTC Markets;
- The SEC's Money Market Fund Reform amendments;
- Implications of Halliburton II;
- The SEC's actions regarding equity market structure;
- FINRA Rule amendments;
- The new Municipal Advisor Rule and updated FAQs;
- Peer-to-peer lending and real estate crowdfunding; and
- The conflict minerals rule and the First Amendment.

The Committee continues to attract top-level speakers who are knowledgeable in their field and deal daily with the aspects they address. Recent speakers have come from the following firms and other organizations, among others: McCarter & English; OTC Markets Group; Dechert; Goodwin Procter; Fried, Frank, Harris, Shriver & Jacobson; SEC3 Compliance Consultants, Inc.; Carter, Ledyard & Milburn; Pepper Hamilton; and Simpson Thacher & Bartlett.

The Committee's Private Investment Funds Subcommittee, chaired by Anastasia Rockas, meets periodically, examining timely topics such as cybersecurity for investment advisers, and significant developments in the Cayman Islands.

Where appropriate, the Committee issues comment letters on proposed legislation and regulation, giving members an opportunity to have a voice in the issues that affect their practice.

The Committee welcomes new members, and invites you to get involved. For information about upcoming meetings, visit our Committee's page at www.nysba.org/Business, or contact businesslaw@nysba.org.

Peter LaVigne, Chair

Technology and Venture Law Committee

No report submitted.

Publication Policy and Manuscript Guidelines for Authors

All proposed articles should be submitted to the *Journal's* Editor-in-Chief. Submissions should be e-mailed or sent on a disk or CD in electronic format, preferably Microsoft Word (pdfs are not acceptable). A short author's biography should also be included.

The editors reserve the right to edit the manuscript to have it conform to the *Journal's* standard in style, usage and analysis. All citations will be confirmed. Authors should consult standard authorities in preparing both text and footnotes, and should consult and follow the style presented in *Bluebook: A Uniform System of Citation*. An *Author's Guide* can be obtained by contacting the Editor-in-Chief. The revised manuscript will be submitted to the author for approval prior to publication.

The views expressed by the authors are not necessarily those of the *Journal*, its editors, or the Business Law Section of the New York State Bar Association. All material published in the *Journal* becomes the property of the *Journal*. The *Journal* reserves the right to grant permission to reprint any articles appearing in it. The *Journal* expects that a manuscript submitted to the *Journal*, if accepted, will appear only in the *Journal* and that a manuscript submitted to the *Journal* has not been previously published.

A manuscript generally is published five to six months after being accepted. The *Journal* reserves the right (for space, budgetary, or other reasons) to publish the accepted manuscript in a later issue than the issue for which it was originally accepted.

Manuscripts are submitted at the sender's risk. The *Journal* assumes no responsibility for the return of the material. Material accepted for publication becomes the property of the Business Law Section of the New York State Bar Association. No compensation is paid for any manuscript.

The Section's Committees are also encouraged to submit for publication in the *Journal* notices of committee events, Annual Meeting notices, information regarding programs and seminars and other news items of topical interest to the members of the Business Law Section.

Manuscripts are to be submitted to:

David L. Glass
Editor-in-Chief
NY Business Law Journal
Macquarie Group Ltd.
125 West 55th Street
New York, NY 10019
telephone: (212) 231-1583
e-mail: david.glass@macquarie.com

Subscriptions

Subscriptions to the *Journal* are available to non-attorneys, universities and other interested organizations. The 2015 subscription rate is \$135.00. Please contact the Newsletter Department, New York State Bar Association, One Elk Street, Albany, NY 12207 or call (518/487-5671/5672) for more information.

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.

Business Law Section



ANNUAL STUDENT WRITING COMPETITION

The Business Law Section sponsors an annual Student Writing Competition, open to all students who are candidates for the J.D. or LL.M. degree at an accredited law school during the year in which the article is submitted. The student articles submitted in a given year that are judged first and second best, provided they are of publishable quality and otherwise meet the criteria of the Competition, will receive cash prizes of \$1,500 and \$1,000, respectively. At the discretion of the editors, they also will be published in the *NYSBA NY Business Law Journal*, which is sponsored by the Section in cooperation with New York Law School. Additional cash prizes may be awarded in the discretion of the Section. Entries that do not qualify for cash prizes may also be considered for publication in the *Journal*.

Articles submitted will be judged on the following criteria:

- Relevance to the *Journal's* audience (New York business lawyers)
- Timeliness of the topic
- Originality
- Quality of research and writing
- Clarity and conciseness

The manuscript should follow Bluebook cite format (using endnotes rather than footnotes) and be a minimum of 3,000 words (there is no maximum). All submissions become the property of the NYSBA and the *NY Business Law Journal*. By submitting an article, the student is deemed to consent to its publication, whether or not a cash prize is awarded.

To enter, the student should submit an original, unpublished manuscript in Word format to David L. Glass, Editor-in-Chief, *NYSBA NY Business Law Journal* (david.glass@macquarie.com). The student should include a brief biography, including law school attended, degree for which the student is a candidate, and expected year of graduation.



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

ADDRESS SERVICE REQUESTED

NON PROFIT ORG.
U.S. POSTAGE
PAID
ALBANY, N.Y.
PERMIT NO. 155



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

