



COMMITTEE NEWS

Professional Liability Insurance

The Unexpected Impact Judge Kavanaugh's Appointment to the Supreme Court Could Have on U.S. Securities Laws

After a lengthy and highly controversial confirmation process, Judge Brett M. Kavanaugh, a former United States Circuit Judge for the United States Court of Appeals for the District of Columbia, has replaced Justice Anthony M. Kennedy as the newest Justice on the Supreme Court of the United States. Judge Kavanaugh's appointment has obvious significance, as conservatives now comprise the majority of the U.S. Supreme Court. Less obvious, however, is the impact Judge Kavanaugh's appointment will likely have on U.S. securities laws. Due to the timing of the nomination, Judge Kavanaugh will be faced with an important decision: whether to recuse himself from a securities fraud case that he recently heard as D.C. Circuit Court Judge.

[Read more on page 18](#)

Adam S. Katz

*Partner, Goldberg Segalla LLP
Corporate Services and Commercial
Litigation Group*

Ryan W. McNagny

*Associate, Goldberg Segalla LLP
Corporate Services and Commercial
Litigation Group*

Any commentary or opinions do not necessarily reflect the views of Goldberg Segalla LLP. © 2018 Adam S. Katz and Ryan W. McNagny.



In This Issue

- The Unexpected Impact Judge Kavanaugh's Appointment... 1
- Chair Message 2
- Defrosting Shareholder Actions for Cyber-Insecurity: 8
- Law Firms' Liability Exposure 9
- Gone Phishing – Legal Malpractice in the Age of the Cyber-Attack 10

**Chair Message**

Dear Members of the Professional Liability Insurance Committee:

For those of you continuing as members of the PLIC, welcome back! For all you new members, welcome! This is a letter of introduction from this year's co-chairs, Peter Biging and Tim Rowan, and a heads up about the year ahead.

Peter Biging is a holdover as Chair of this Committee from last year. A partner in the law firm of Goldberg Segalla LLP, Peter heads up the New York metro area professional liability and D&O practice of the firm, and also functions as the Vice Chair of the firm's nationwide Management and Professional Liability Practice group.

Tim Rowan is Managing Director of Marsh USA Inc., where he heads up the company's Professional Firms practice. Tim and Peter decided to work together this year so there would be some continuity as Tim steps into this new role.

We look forward to working with you in the year ahead, and look forward to your active participation.

For those of you who were not able to participate in person or by phone during our meeting at the Fall Leadership Conference on October 13th, the following is a summary of what was discussed.

First, one of the things we're extremely proud of is this publication, our Quarterly Newsletter. The newsletter is filled with timely articles on issues of interest to our members, and presents not only an opportunity for our members to keep up to date with the latest key issues as they arise, but also an opportunity for our members to show off their expertise to our other members and burnish their credentials. We are incredibly excited about this issue, which includes articles discussing the D&O risks presented by the failure to procure adequate cyber liability coverage, the anticipated impact Justice Kavanaugh will have on U.S. securities laws, and the risks of legal malpractice in the age of cyber-attacks. They are incredibly timely, and tackle a number of cutting edge issues. While we are extremely excited about this issue, we still need articles for the next newsletter. Please think about getting involved and sending us drafts to review. If you have something you are working on, or you have an idea in mind for an article you think would be of interest to the PLIC community, please feel free to reach out to either of us or Jennifer Feldscher, this year's article's editor. Also, if you have an article you did for your firm or company publication and you think it would benefit a wider audience, please consider suggesting that as well. We can be reached through the ABA website, or by sending emails to Pbiging@goldbergsegalla.com and Tim.Rowan@marsh.com. You can also send the articles to our articles editor, Jennifer Feldscher. She



Peter J. Biging, Esq.

*Chair, Professional Liability
Insurance Committee*

pbiging@goldbergsegalla.com



Timothy Rowan

Marsh USA Inc

tim.rowan@marsh.com



can be reached at jfeldscher@goldbergsegalla.com. We will need draft articles to review by mid-December.

Second, we want to remind folks of the opportunity to get yourself published in the Tort Trial & Insurance Practice Law Journal's Year in Review Issue. Each year, this Committee contributes to this special issue with a section discussing recent developments in professional liability and D&O, including coverage issues. This is a law review caliber publication, and the articles are unfailingly of extremely high quality. We will be looking for folks to write articles on the most recent developments over the past year in lawyer's professional liability, accountant's E&O, insurance agent/broker E&O, real estate professional E&O, and management liability/D&O, as well as miscellaneous professional. Please help us continue to contribute to this annual issue, and let us know what topics you would be most interested in writing on. Because the entire submission can't be 50 pages in length, the goal here is quality over length. So preparation of each part of our submission should be extremely manageable from a time commitment standpoint. We need to receive submissions on this by mid-November.

Third, we want to provide you with an early reminder to block out time to attend the ABA Tort Trial & Insurance Practice Section (i.e., "TIPS") Conference, scheduled to be held next year on May 1-5, 2019 at the Westin Hotel in New York City. Last year's Section Conference contained a host of timely and terrific presentations, and the 2019 conference promises to be no exception. In addition to the availability of useful practice guidance and CLE afforded by the conference, it offers unparalleled networking opportunities as well. We know you have a lot of options for your CLE, but this is a conference we believe you should make every effort to block out time for.

Fourth, we want to invite you to join us for our monthly calls, during which we will talk about committee business, discuss upcoming programs we are looking to develop or participate in (including our annual participation in the D&O insurance coverage min-conference held each year at St. John's University Law School's New York City campus in late January on the eve of the PLUS D&O conference, as well as joint mini-conferences with PLUS in development), and on occasion hear from guest speakers. This past year, we were treated to presentations on how to understand and advocate to the Millennial Juror, how to manage the overwhelming morass of electronically stored information now presented in each professional liability and D&O matter, and how to approach the issue of lost profits from an accounting expert's perspective. We are planning on having a number of guest speakers again this coming ABA year, and look forward to hearing from you regarding any ideas you have for specific topics and speakers.



Lastly, we want to invite people to participate more actively by becoming a member of a sub-committee. If you are interested, we are looking for folks to participate in the following sub-committees:

- **Management Liability/D&O**
- **Lawyer and Accountant Professional Liability**
- **Financial Services E&O**
- **Miscellaneous Professional Liability** (Consultants, Architects and Engineers, Technology, etc.)

If you are interested in getting involved in a sub-committee, please contact us and copy our Chair Elect, Scott Slater, who can be reached at sslater@slatergrant.com.

As you may have guessed by now if you've read this far, this is a very active Committee, and a committee we are very proud of. We look forward to working with you in the year ahead, and getting a chance to get to know you and spend time with you! ➤

Sincerely,
Peter and Tim

**Connect with
Professional Liability
Insurance** [website](#)



**Stay Connected
with TIPS**



We encourage you to stay up-to-date on important Section news, TIPS meetings and events and important topics in your area of practice by following TIPS on [Twitter](#) @ABATIPS, joining our groups on [LinkedIn](#), following us on [Instagram](#), and visiting our [YouTube](#) page! In addition, you can easily connect with TIPS substantive committees on these various social media outlets by clicking on any of the links.

©2018 American Bar Association, Tort Trial & Insurance Practice Section, 321 North Clark Street, Chicago, Illinois 60654; (312) 988-5607. All rights reserved.

The opinions herein are the authors' and do not necessarily represent the views or policies of the ABA, TIPS or the Professional Liability Insurance Committee. Articles should not be reproduced without written permission from the Copyrights & Contracts office copyright@americanbar.org.

Editorial Policy: This Newsletter publishes information of interest to members of the Professional Liability Insurance Committee of the Tort Trial & Insurance Practice Section of the American Bar Association — including reports, personal opinions, practice news, developing law and practice tips by the membership, as well as contributions of interest by nonmembers. Neither the ABA, the Section, the Committee, nor the Editors endorse the content or accuracy of any specific legal, personal, or other opinion, proposal or authority.

Copies may be requested by contacting the ABA at the address and telephone number listed above.



Member Roster

Chair

Peter Biging

Goldberg Segalla LLP
711 3rd Ave., Ste 1900
New York, NY 10017-4043
(646) 292-8711
Fax: (646) 292-8701
pbiging@goldbergsegalla.com

**Co-Chair,
Membership
Vice-Chair**

Timothy Rowan

Marsh USA Inc
540 W Madison St, Ste 1200
Chicago, IL 60661-7608
(312) 627-6000
tim.rowan@marsh.com

Chair-Elect

Scott Slater

Slater Grant
2818 Cypress Ridge Blvd, Ste 230
Wesley Chapel, FL 33544
(813) 995-6444
Fax: (813) 221-6445
sslater@slatergrant.com

**Immediate Past
Chair, Council
Representative**

Ari Magedoff

Axis Insurance
300 Connell Dr, Ste 8000
Berkeley Heights, NJ 07922-2820
(908) 508-4353
ari.magedoff@axiscapital.com

**Diversity
Vice-Chair**

Blaise Chow

Ropers Majeski Kohn & Bentley
750 3rd Ave, Rm 2500
New York, NY 10017-2708
(646) 454-3244
bchow@rmkb.com

**Technology
Vice-Chair**

Michael Brown

Adler Pollock & Sheehan P.C.
175 Federal St, 10th Fl
Boston, MA 02210
(617) 603-0534
Fax: (617) 737-1191
mbrown@apslaw.com

Scope Liaison

David Becker

Freeborn & Peters LLP
311 S Wacker Dr, Ste 3000
Chicago, IL 60606-6679
(312) 360-6391
Fax: (312) 360-6594
dbecker@freeborn.com

**Newsletter &
Publications
Editor**

Jennifer H Feldscher

Goldberg Segalla LLP
711 3rd Ave Fl 19
New York, NY 10017-4043
Phone: (646) 292-8712 (Work)
jfeldscher@goldbergsegalla.com

Vice-Chairs

William Bila

Walker Wilcox Matousek LLP
1 North Franklin St, Ste 3200
Chicago, IL 60606
(312) 244-6700
Fax: (312) 244-6800

Patrick Boley

Patrick Boley Law Firm, PLLC
879 Cheri Lane
Mendota Heights, MN 55120
(651) 245-5331
Fax: (651) 312-6618
pjboley@comcast.net

Carleton Burch

Anderson McPharlin & Connors LLP
707 Wilshire Blvd, Ste 4000
Los Angeles, CA 90017-3623
(213) 236-1649
Fax: (213) 622-7594
crb@amclaw.com

Edward Carleton

Skarzynski Black
1 Battery Park Plz, 32nd Fl
New York, NY 10004
(212) 820-7710
ecarleton@skarzynski.com

Kelly Castriotta

3407 S Aberdeen St
Chicago, IL 60608-6510
(201) 646-2261
castriok@gmail.com

Robert Chesler

Anderson Kill & Olick PC
1 Gateway Ctr, Ste 1510
Newark, NJ 07102-5320
(973) 642-5828
rchesler@andersonkill.com

Michael Chester

Skarzynski Black LLC
1 Battery Park Plz, Fl 32
New York, NY 10004-1405
(212) 820-7752
Fax: (212) 820-7740
mchester@bswb.com

Charles Coffey

The Bar Plan Mutual Insurance
Company
1717 Hidden Creek Ct
Saint Louis, MO 63131-1826
(314) 288-1027
Fax: (314) 965-8122
cscoffey@thebarplan.com

Barbara Costello

Kaufman Borgeest & Ryan LLP
120 Broadway, Fl 14
New York, NY 10271-1600
(212) 980-9600
Fax: (212) 980-9291
bcostello@kbrlaw.com

Jason Cronic

Wiley Rein LLP
1776 K St NW
Washington, DC 20006-2304
(202) 719-7175
Fax: (202) 719-7049
jcronic@wileyrein.com

Jason Ederer

Mound Cotton Wollan
& Greengrass LLP
1 New York Plaza, 44th Fl
New York, NY 10004
(212) 804-4507
jederer@moundcotton.com

Ommid Farashahi

BatesCarey LLP
191 N Wacker Dr, Ste 2400
Chicago, IL 60606-1886
(312) 762-3205
Fax: (312) 762-3200

Perry Granof

1147 Longmeadow Ln
Glencoe, IL 60022-1022
(847) 242-9932
pgranof@granofinternational.com

Angela Iannacci

Supreme Court of Nassau County
100 Supreme Court Dr
Mineola, NY 11501-4802
(516) 493-3196
aiannacc@nycourts.gov

Seth Laver

Goldberg Segalla LLP
1700 Market St, 1418
Philadelphia, PA 19103
(267) 519-6877
Fax: (267) 519-6801
slaver@goldbergsegalla.com

Melissa Lessell

Deutsch Kerrigan LLP
755 Magazine St
New Orleans, LA 70130-3629
1 (504) 5930689
Fax: (504) 566-4022
mlessell@deutschkerrigan.com

Amber Locklear

Ropers Majeski Kohn Bentley
750 3rd Ave, 25th Fl
New York, NY 10017
(212) 668-5927
alocklear@rmkb.com

Teresa Milano

46 Randlett St
Quincy, MA 02170
(914) 474-6351
tmilano21@gmail.com

Joseph Monteleone

One Crossroads Dr, Ste 102A
Bedminster, NJ 07921
(973) 242-1630
jmonteleone@wglaw.com

John Muller

Sompo International Insurance
1221 Avenue of The Americas, Fl 19
New York, NY 10020
(917) 421-4961
jmuller@sompo-intl.com

Nicholas Novak

BatesCarey LLP
191 N Wacker Dr, Ste 2400
Chicago, IL 60606
(312) 762-3266
nnovak@batescarey.com

John Rogers

Carlock Copeland & Stair
191 Peachtree St NE, Ste 3600
Atlanta, GA 30303-1757
(404) 221-2204
jrogers@carlockcopeland.com

Member Roster | continued

Andrew Sachs

4515 Greenwood Ave N, #101,
Seattle, WA 98103

Nilam Sharma

Nilam Sharma Limited
22A Brechin Place
London, SW74QA
447539770012
Fax: 44 442074814968
nilam.sharma@nrsharmaltd.com

Michael Skoglund

BatesCarey LLP
191 N Wacker, Ste 2400
Chicago, IL 60606
(312) 762-3173
mskoglund@batescarey.com

Daniel Standish

Wiley Rein LLP
1776 K St NW
Washington, DC 20006-2304
(202) 719-7130
Fax: (202) 719-7207
dstandish@wileyrein.com

Jonathan Walton

Cozen O'Connor
123 N Wacker Dr, Ste 1800
Chicago, IL 60606
(312) 474-1636
jwalton@cozen.com

Justin Wear

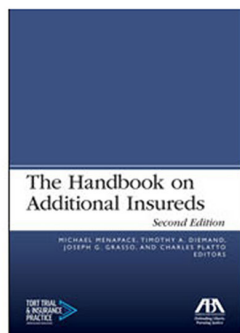
Manier & Herod
1201 Demonbreun St, Ste 900
Nashville, TN 37203
(615) 244-0030
Fax: (615) 242-4203
jwear@manierherod.com

Frederick Zauderer

AXIS Capital
1211 Avenue of The Americas,
24th Fl
New York, NY 10036
(908) 508-4370
Fax: (908) 508-4389
fred.zauderer@axiscapital.com

New Insurance Law Books from TIPS

TORT TRIAL
& INSURANCE
PRACTICE



The Handbook on Additional Insureds

Second Edition

Michael Menapace, Timothy A. Diemand, Joseph G. Grasso, and Charles Platto, Editors

Now completely updated, this handbook addresses all aspects involved when dealing with this complex coverage.

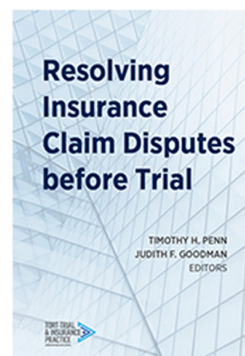
Order online
www.ShopABA.org

Order by email
orders@americanbar.org

Resolving Insurance Claim Disputes before Trial

Timothy H. Penn and Judith F. Goodman, Editors

Understand how to effectively use ADR mechanisms such as arbitration, mediation, settlement conferences, and appraisal to resolve insurance claim disputes without the cost and delay of trial.





TORT TRIAL
& INSURANCE
PRACTICE

Join us for the premier CLE conference for insurance, defense, corporate, and plaintiffs attorneys.

TIPS SECTION CONFERENCE

May 1-4, 2019 | The Westin New York at Times Square | New York, NY

LEARN:

CLE programs from distinguished panelists including prominent judges and leading in-house and corporate counsel.

NETWORK:

Expand your circle at our complimentary nightly networking receptions.

CELEBRATE:

Entertaining social events in the Big Apple.

JOIN:

Become involved with our over 30 practice-specific committees for professional development and leadership opportunities

ENJOY:

Explore New York City with colleagues, new and old.



americanbar.org/tips



Defrosting Shareholder Actions for Cyber-Insecurity: D&O Liability for Inadequate Insurance Coverage

The failure of the shareholder derivative litigation stemming from the hacking of data held by the Wyndham Hotel and Resorts led to a chilling of shareholder actions against directors and officers of companies arising from cyber losses. Recent evidence, however, reveals that the chilling effect of this failed litigation is all but over. The fact is that directors and officers' potential liability resulting from data breaches is growing. The soft cyber market for many industries, in conjunction with the lack of a standardized cyberinsurance policy, allows for policies to be fully customized with the elimination of certain broad exclusions. If companies fail to avail themselves of favorable policy provisions and instead allow cyberinsurance policies to contain sweeping exclusions, they will look to recover from their insurance brokers. But, as a company's response to a cyberattack, which necessarily includes obtaining insurance, is increasingly the C-suite's responsibility, shareholders may target the directors and officers of the company, particularly the Chief Information Security Officer or the head of risk management, for their failure to obtain the most favorable policy language available in the marketplace. Recent events reveal this scenario is hardly fear-mongering.

Prior to 2018, shareholder actions against directors and officers stemming from a data breach loss seemed to be a long shot. Following breaches suffered by Wyndham Hotel and Resorts between 2008 and 2010, shareholders brought a derivative action that was ultimately dismissed.¹ On three occasions, hackers had breached Wyndham Worldwide Corporation's ("WWC") main network and collected sensitive data. The Federal Trade Commission began its investigation in April 2010 and, in June 2012, filed suit against WWC for its inadequate security practices. Shareholders sent demands on two occasions to the WWC Board of Directors demanding that it bring a lawsuit based upon the breaches. The Board rejected the demands. The shareholder who sent the second demand filed suit in 2014 against WWC and numerous corporate officials, asserting they failed to implement adequate data security mechanisms, which allowed the hackers to steal customer data and, in turn, damaged WWC's reputation and resulted in a significant expenditure of legal fees.

WWC moved to dismiss the derivative suit arguing, in pertinent part, the refusal to pursue the shareholder's demand was a good-faith exercise of business judgment and further, the shareholder failed to plead with particularity that the decision was

Peter J. Biging

*Partner, Goldberg Segalla LLP
New York City*

Jonathan L. Schwartz

*Partner, Goldberg Segalla LLP
Chicago*

Colin B. Willmott

*Associate, Goldberg Segalla LLP
Chicago*

[Read more on page 21](#)



Discussion Paper: Limiting Law Firms' Professional Liability Exposure

How law firms can maintain client relationships while protecting themselves against malpractice claims

The relationship between law firms and their corporate clients is changing.

Corporate attorneys are increasingly bringing more work in-house and spreading the remaining work among a number of law firms. In the process, they are demanding more concessions from outside legal counsel in exchange for the opportunity to remain on the company's approved counsel list. These concessions can range broadly from data protection provisions to limits on working with the client's competitors, requests for statute of limitation waivers, broad indemnity agreements and more.

Many law firms feel pressure to yield to these requests in the interest of maintaining the client relationship. Further complicating matters is increased competition from both traditional rivals and new market entrants, such as accounting and consulting firms and technology-enabled providers offering legal services at reduced rates. Since these new competitors are not law firms, they are not bound by the same ethical rules that law firms operate under and can, therefore, require extensive contractual limitation of liabilities from clients. Meanwhile, where law firms utilize outside specialists and consultants to cut costs while maintaining service levels, they take on supervisory responsibility for the actions of these third-parties and increase their own liability exposure.

Against this backdrop, law firms are increasingly presented with engagement letters that open the door to greater professional and cyber liability exposure, often beyond the scope of their insurance coverage. Further, as the severity of professional liability claims continues to rise, law firms are increasingly viewed as deep pocket defendants. As a result, proactive risk management, beginning at the point of client engagement, has become an increasingly important part of the overall practice management strategies that law firms employ to protect their future viability.

This discussion paper takes a closer look at the importance for law firms to utilize engagement letters that are designed to limit their professional liability exposure. Proper attention to three components in the letter can assist in accomplishing this objective. In fact, many professional liability claims can be avoided by the judicious use of a well-thought-out engagement letter. Taking prudent steps to limit or guard

Stuart Pattison

Senior Vice President
U.S. Professional Lines
Sompo Pro
+1.917.281.0744
spattison@sompo-intl.com

John Muller

Vice President
U.S. Professional Lines
Sompo Pro
+1.917.421.4961
jmuller@sompo-intl.com

If you have additional questions about related issues beyond those outlined above, please feel free to contact us directly.

[Read more on page 26](#)



Gone Phishing – Legal Malpractice in the Age of the Cyber-Attack

In early June, news broke that local and federal law enforcement officials had arrested 74 people, including nearly 30 in Nigeria, in a “coordinated crackdown on people who convince correspondents to wire them money for fraudulent activities.”¹ The scam? We all know it of course – it’s the old “Nigerian prince needs help transferring his inheritance to the United States” email, the one where your account number, social security number and other personal information are “urgently” required to help assist the Prince with getting his money out of his country. Of course, after that information is provided, the victims watch as *their* money is slowly but surely siphoned off and out of *their* accounts never to be recovered or seen again. The Prince’s inheritance never does show up in the victim’s electronic coffer.

Legal professionals may scoff at the notion that they could ever be affected by this type of fraud, what has become known as the “man in the email” scam. Who could ever fall for that, right? Well, as it turns out, variations of this particular scam have begun to seep their way into sensitive and potentially confidential matters attorneys have with their clients in the legal profession. In fact, recently, certain fact patterns have emerged where *clients*, rather than attorneys are the ones fooled by the “man in the email” scam, leaving attorneys vulnerable to claims of malpractice as a result of a cyber-attack on their offices’ systems which may have yielded the confidential information alleged to have caused or contributed to the clients being exposed to the scam. While there is some debate as to what duty, if any, the attorney has to the client in this situation, the evolution of this area of potential exposure has been both interesting and worrisome to watch.

Developments in Case Law

In one of the first cases to examine these issues, *Shore v. Johnson & Bell, Ltd.*, 16-cv-04363 (N.D.Ill. 2016), the plaintiffs filed a class action complaint² against a Chicago-based law firm alleging that the firm’s computer systems suffered from “critical vulnerabilities in its internet-accessible web services[,]” the result of which was that confidential client information had been exposed and was allegedly at great risk of unauthorized disclosure. In fact, plaintiffs claimed that it was “only a matter of time until hackers learn[ed] of these vulnerabilities,” risking harm to their client’s information, communications and additional documents stored on the firm’s servers. Even more specifically, plaintiffs alleged that the lack of security surrounding the remote network utilized by the firm made a “man in the email” or, as they

Kenneth M. Labbate, Esq.
*Mound Cotton Wollan &
Greengrass LLP*

Jason L. Ederer, Esq.
*Mound Cotton Wollan &
Greengrass LLP*



characterized it, a “Man in the Middle” attack, a “serious concern.”³ Plaintiffs further alleged that, while they had expected that the firm would use unspecified “industry standard measures” to protect their confidential data, they would not have retained the firm or provided their confidential data had they known about the “lax” security protocols and insecure systems utilized by the firm.⁴ As a result of the foregoing, plaintiffs alleged that their confidential data had been exposed.⁵

The challenge with the allegations raised in the *Shore* complaint was fairly evident – it was not clear what, if any, damages were sustained. This may have been one of the primary reasons why the *Shore* case was diverted to pre-trial arbitration in February of 2017, never to be heard from again. Whereas that case seemed like a preemptive strike against a *possible* breach (indeed, the duty allegedly breached was that the firm “failed to implement industry standard data security measures, resulting in [potential] vulnerabilities and the exposure of confidential data”⁶), it was the next case which took this type of claim a step further, giving potential plaintiffs a clear template to utilize in suing law firms whose data breaches ended up costing them dearly.

In *Millard v. Doran*, No. 153262/2016 (Sup. Ct. N.Y. Cty.), plaintiffs, a husband and wife, alleged that defendant, their real estate lawyer, was liable for malpractice and breach of fiduciary duty arising out representation in connection with a real estate purchase in New York City. According to the complaint⁷, Doran, the defendant attorney, committed malpractice by “permit[ing]” cyber criminals to hack into her email system and to read and intercept communications that had purportedly been sent to the Millards by Doran. Apparently, after alerting the unnamed criminals that the Millards were about to transfer large sums of money to the seller as part of the real estate purchase, the cyber-criminals drafted fraudulent emails made to look like they were written and sent to the Millards by Doran herself. In those emails, the Millards were instructed to send funds by wire transfer to a bank account that purportedly belonged to the seller, but which, they later found out, was actually under the control of the criminals.⁸ The story is a familiar one after that -- following receipt of the instructions, the Millards wired the money (upwards of \$2 million) to the requested location, i.e., straight into to the criminals’ account.⁹ They did not speak with Doran before sending the money. In fact, the scheme was, apparently, plotted so meticulously that the criminals even sent fraudulent confirmation emails to *Doran* from the fake account, just to lull both sets of victims into a further sense of comfort that nothing was amiss. By the time either client or attorney realized that the email address in question did not, in fact, belong to the seller’s attorney, the \$2 million had vanished.¹⁰



Given that there was an ascertainable and verifiable loss involved, allowing the plaintiffs to allege damages that were beyond the mere speculative damages alleged in *Shore*, the *Millard* case appeared ripe for adjudication. Similar to *Shore* though, the *Millard* case appears to have been settled shortly after issue was joined. Why did these cases not move forward? Is such a malpractice claim viable? These questions have yet to be answered. However, the repetitive allegations in these lawsuits raise another important question lying at the heart of this issue: what is a law firm's duty in dealing with cyber security on the one hand, and protection of confidential client information on the other? Ethical considerations and an analysis under applicable law may shed some light on why plaintiffs appear more willing to resolve these claims early rather than undertaking the effort and cost associated with trying to establish a malpractice claim in these circumstances.

Ethical Considerations

An attorney's ethical responsibilities are now fairly well-defined when it comes to the protection of a client's confidential data. Following the ABA Ethics 2020 Commission's Report and Recommendation, the ABA House of Delegates approved the following amendments to the ABA's Rules of Professional Conduct:

- Paragraph 8 of the Comment to Rule 1.1 now states that "a lawyer should keep abreast of changes in the law and its practice, *including the benefits and risks of technology...*"; and
- Rule 1.6 imposed a duty on attorneys to use reasonable means to maintain the confidentiality of information relating to a client's representation. Pursuant to the 2020 Commission's Report, subpart (c) to Rule 1.6 was amended to add that:
- "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."¹¹

While these changes were certainly welcome, this initial report failed to outline what the changes in technology were that attorneys were to keep themselves abreast of, and what constituted "reasonable efforts" which attorneys needed to undertake to ensure that their clients' confidential information was, in fact, safely guarded.

In June of 2017, the ABA Standing Committee on Ethics and Professional Responsibility moved to clarify the report further, putting forward its [Formal Opinion 477R](#) on "Securing Communication of Protected Client Information."¹² In that



opinion, the ABA provided guidance or what can be better termed as “suggestions” as to what “reasonable efforts” may mean for attorneys going forward. These suggestions included: (1) that attorneys/firms should understand the nature of the potential cyber threat and make greater efforts to protect confidentiality with “higher risk scenarios”; (2) that attorneys/firms should understand how and where communications with clients are stored, with the recommendation that each method of transmission be assessed for its compliance; (3) that attorneys/firms should use reasonable electronic security measures to safeguard their clients’ information, with what is “reasonable” varying depending on the facts and circumstances of the case; (4) that attorneys/firms should protect certain electronic communications at different levels, depending on the sensitivity of the communications; (5) that attorneys/firms establish policies, procedures and training methods to help other attorneys/non-lawyers with the handling of this type of information; and (6) that attorneys/firms conduct due diligence on their email service providers prior to enlisting their services.¹³ However, besides creating what amounts to a cyber-security “arms race” among law firms, the “guidance” also fails to provide any insight as to how a sole practitioner can compete against a large firm in implementing and maintaining these “reasonable efforts” without bankrupting itself.

Practical Considerations

While not an exhaustive list, these “suggestions” bring to mind a number of practical questions and concerns. As these cases become more and more prevalent and of concern to large and small firms alike, questions arise as to what firms can do to best insulate themselves from this type of claim and when exposed to a claim of malpractice based upon an underlying cyber-attack, how attorneys are to handle these types of claims.

It starts with scrutiny of a complaint, itself, and the allegations made therein. For example, take the factual situation where a plaintiff (client or former client of a firm) asserts that its confidential information was obtained from the firm’s computer as a result of a “data breach” or “cyber-attack.” To the extent the firm was, in fact, a victim of a cyber-attack that resulted in a data breach, it must consider whether it has obligations under breach notification statutes, such as [N.Y. Gen. Bus. Law Section 899-aa](#), the New York State Information Security Breach and Notification Act, enacted in either the state of the action or other states/countries in which it is doing business or servicing clients. Any firm involved in this situation should seek counsel from their errors and omissions insurer (and any other insurers that may potentially



provide coverage to the firm such as property, general liability, and stand-alone cyber insurers) and with companies specializing in breach notification obligations to ascertain what exposure they may have and how to best respond to that exposure. Once an attorney learns of a claim from a client or former client that a loss may have been sustained as a result of a data breach to its system, that attorney should immediately place all applicable insurers on notice, so as to secure the maximum available coverage. Attorneys and firms alike *must* know and understand their policies' limitations at the outset, and make sure to safeguard themselves against a potential future malpractice claim, as well.

In responding to such a claim, an attorney or law firm must also be cognizant of, and make sure to preserve, all information stored electronically or on back-up media (tapes, hard drives, CDs, etc.), as well as all electronic systems and storage devices (whether physically located at the premises where the firm and/or attorney works, or remotely, e.g., in cloud storage on a home computing system). This is often a costly undertaking, but one that must be done in an effort to insulate the firm from sanctions that could be imposed by a court for the failure to preserve relevant evidence. The latter type of "system," residing on "the cloud" such as Gmail or AOL Mail, is the type of system often utilized by smaller firms and sole practitioners in an effort to balance expenses against revenues.

Attorneys sharing data with their clients face a related risk in that they may be doing business with clients that maintain inadequate security *of their own*, thereby exposing their firm's systems to infiltration. Certainly, an attorney can control their own systems, but how can an attorney control their clients' computer systems? At a minimum, attorneys should employ, and encourage their clients to implement, two-factor authentication on their electronic accounts, i.e., a password and a second form of identification (i.e., a numerical code sent by text), as a "reasonable measure" to protect against data loss through a cyber-attack. While limiting the use of third-party email, like Gmail, may not be feasible for either attorney/firm or client, other recommendations include utilizing free, downloadable antivirus protection, both in the home and remotely on smartphones, using password-protected, private Wi-Fi, as opposed to public Wi-Fi, when working or sending things remotely, allowing automatic security updates to download on all computer systems and, if possible, using encrypted means of exchanging information, rather than general, unprotected email, to communicate between attorney and client, especially if the information is particularly sensitive (such as confidential bank and transactional-related information). While an attorney/firm must stay vigilant in maintaining his own system, failure to advise the client about the simplest of



security measures for their confidential documents could also potentially leave the attorney at risk for claims of malpractice. Attorneys would be wise to gain a full understanding of these simple measures, both to be ethically compliant and to safeguard themselves against potential malpractice claims as these claims are anticipated to evolve and become more prevalent.

Data preservation by a firm after notification of a loss also preserves information for a forensic review, which may provide the best evidence upon which to defend against a claim of “malpractice” based upon inadequate electronic security. Indeed, something unique to this type of case that is emerging is the “*offensive*” forensic review done immediately to disprove allegations of hacking into a firm’s computer system. By undertaking a forensic review of a firm’s system, the firm may be able to *rule out* the possibility that it was the victim of a data breach, thereby negating upfront a claim that a client’s confidential information was exposed due to a breach of the firm’s systems.

Using your best defense offensively in this type of case, highlights the potential difficulties a plaintiff may experience in actually attempting to establish this type of claim. One of the challenges with this approach, and the reason why the *Millard* and *Shore* cases may have resolved early, is that the costs associated with an “offensive” forensic review may outweigh the actual or alleged exposure presented, thereby leaving a firm and its involved insurers to weigh the “costs and benefits” associated with undertaking a costly forensic review, particularly when the potential exposure is nominal.

In addition to a forensic review of a firm’s system to defend against a plaintiff’s claim of damages resulting from a breach, attorneys can rely upon other traditional defenses to a claim of “malpractice” to defend against such claims. Under New York law, for example, an action for legal malpractice requires proof of three elements: (1) that the attorney was negligent; (2) that such negligence was a proximate cause of plaintiff’s losses; and (3) proof of actual damages.¹⁴ The challenge that exists with the type of claim based on the factual situation presented by the *Millard* case is whether a client or former client can show in a claim for professional negligence arising from an alleged breach of the attorney’s computer system. In other words, “but for” the attorney’s alleged malpractice, the plaintiff must show he or she would not have sustained some actual ascertainable damages, as such a failure to establish proximate cause requires dismissal regardless of whether negligence is established.¹⁵



In a case like *Millard*, where it is the *client* who responds to a fraudulent email and wires money to a fraudulent bank account, where there are numerous third parties involved in the transaction (lender, broker, other attorneys, title companies, etc.), it would be very difficult to show that the loss of confidential information and damages that are alleged to flow therefrom were, in fact, caused by the attorneys' conduct in failing to secure the client's confidential information. In other words, the loss may be too attenuated to meet the requisite "but-for" element of causation required to maintain a malpractice claim against an attorney. If the client can establish that the information in the fraudulent email was obtained from a breach of the attorney's email system and/or electronic files, it may allow the claim to proceed, depending upon what evidence exists of security implemented by the firm to secure its clients' data and how that Court views those safeguards in light of the standard of care for similarly situated attorneys, using the "reasonable efforts" now required of firms to safeguard confidential client data.

Complicating matters further for potential plaintiffs is the fact that while maintaining "inadequate" security systems may give rise to an ethical violation, it is well-settled law in certain venues that an ethical violation does not, in and of itself, give rise to a legal malpractice claim.¹⁶ It has been noted that the Code of Professional Responsibility only provides for a public, disciplinary remedy, and does not set out rules for asserting private claims in a civil lawsuit.¹⁷ Thus, simply alleging a violation of the aforementioned ethical rules will only get a plaintiff so far, and often an appropriate Disciplinary Committee, and not a courtroom, is the appropriate forum for same.¹⁸ Even with a provable ethical violation, a plaintiff still needs more -- evidence that the ethical breach caused damages and violated the standard of care owed to the client -- to maintain a malpractice claim. The evidence to support such a claim is costly and may be hard to come by (IP hosts and email service and system providers will need to be subpoenaed) and even harder to utilize (i.e., did the information used come from the allegedly hacked counsel, or any of the other individuals/entities participating in the transaction? was it the disclosed information which *caused* the damages, or was it other information?).

Accordingly, there are many hurdles to a plaintiff's effort to establish a "man in the email" malpractice-based claim that may quell the desire of counsel to file such claims or lead to an early "cost efficient" settlement of such claims.



Conclusion

In the end, the legal profession continues to hold its breath while the courts wrestle with this issue and work to define the scope of the duty owed by counsel to their clients for the preservation of confidential client data in an environment where the cyber criminals are, and will, likely remain a step ahead of any technology that can be implemented, leaving aside the costs associated with implementing “state-of-the-art” protections, which themselves may be unaffordable to many or most firms and become outdated in very short periods of time. ➤

Endnotes

- 1 BBC News, “US arrests 74 in global email scam crackdown”, <https://www.bbc.com/news/business-44445436>.
- 2 See, Complaint, *Shore, et al. v. Johnson & Bell, Ltd.*, No. 16-cv-04363 (N.D. Ill. April 15, 2016), <https://www.datasecuritylawjournal.com/files/2016/12/Johnson-and-Bell-Complaint.pdf>.
- 3 *Id.*
- 4 *Id.*
- 5 *Id.*
- 6 *Id.*
- 7 See, Complaint, *Millard, et al. v. Doran*, No. 153262/2016 (Sup. Ct. N.Y. Cty. April 18, 2016), https://iapps.courts.state.ny.us/nyscef/ViewDocument?docIndex=DwYoLtNofB3D5sp/shG_PLUS_Aw==.
- 8 *Id.*
- 9 *Id.*
- 10 *Id.*
- 11 See, American Bar Association Commission on Ethics 20/20 Report to House of Delegates and Resolution (August 2012), https://www.americanbar.org/content/dam/aba/administrative/ethics_2020/20120808_revised_resolution_105a_as_amended.authcheckdam.pdf.
- 12 See, American Bar Association Formal Opinion 477R, May 11, 2017 (Revised May 22, 2017), https://www.americanbar.org/content/dam/aba/administrative/professional_responsibility/aba_formal_opinion_477.authcheckdam.pdf.
- 13 *Id.*
- 14 *Glob. Bus. Inst. v. Rivkin Radler LLP*, 958 N.Y.S.2d 41, 42 (1st Dep’t 2012); *Brooks v. Lewin*, 21 A.D.3d 731, 734 (1st Dep’t 2005); *lv. denied*, 6 N.Y.3d 713 (N.Y. 2006).
- 15 See, e.g., *Pellegrino v. Rubenstein*, 738 N.Y.S.2d 320 (1st Dep’t 2002); *Russo v. Feder, Kaszovitz, Isaacson, Weber, Skala & Bass, LLP*, 750 N.Y.S.2d 277 (1st Dep’t 2002). See also *Wo Yee Hing Realty Corp. v. Stern*, 99 A.D.3d 58, 63 (1st Dep’t 2012) (internal quotation marks omitted) (“[T]he failure to show proximate cause mandates dismissal of a legal malpractice action regardless of whether the attorney was negligent”).
- 16 See, e.g., *Drago v. Buonagurio*, 46 N.Y.2d 778 (1978) (holding that even if the claimed ethical violation violates the Code of Professional Responsibility, there is no legal malpractice cause of action unless the factual situation falls with an acknowledged category for tort of contract liability); see also, *Shapiro v. McNeill*, 92 N.Y.2d 91 (1998).
- 17 See, e.g., *Schafrann v. N.V. Famka, Inc.*, 2003 WL 25668486 (Sup. Ct. N.Y. Cty. 2003).
- 18 See, e.g., *Kristian SRB v. Fortelini*, 1993 WL 13715532 at *3 (Sup. Ct. N.Y. Cty. 1993).



The Unexpected... continued from page 1

The Case: *Lorenzo v. Securities and Exchange Commission*

Lorenzo v. Securities and Exchange Commission,¹ which the U.S. Supreme Court recently agreed to hear on appeal, involved an investment banker who, at the direction of his boss, copied and pasted fraudulent statements written by his boss into emails to two potential investors. The statements were intended to induce the investors to purchase bonds from Lorenzo's only investment banking client at the time, a start-up energy company. Despite Lorenzo's knowledge that the company had recently declared its assets devoid of any value, Lorenzo's emails informed the investors that the company had over \$10 million in confirmed assets and \$43 million in orders. However, Lorenzo's emails expressly indicated that they had been sent "at the request of" his boss, and Lorenzo claimed that he simply copied and pasted the emails at his boss's direction without any independent analysis of their contents.

In a split decision, the D.C. Circuit concluded that Lorenzo, by copying and disseminating his boss's words to potential investors, was not the "maker" of the fraudulent statements for the purposes of Rule 10b-5(b) under the Securities Exchange Act of 1934, which deems it unlawful "[t]o make any untrue statement of a material fact. . . in connection with the purchase or sale of any security."² However, the Court found that Lorenzo acted with the requisite intent in sending the emails and was therefore liable for participating in a "fraudulent scheme" under Rule 10b-5(a) and (c), as well as Section 17(a)(1) of the Securities Act of 1933, which deem it unlawful to "to employ any device, scheme, or artifice to defraud . . . in connection with the purchase or sale of any security."³

In so holding, the Court differentiated *Janus Capital Group, Inc. v. First Derivative Traders*,⁴ in which the Supreme Court articulated the rule that the "maker" of a statement for purposes of Rule 10b-5 is the individual or entity with ultimate authority over its content. In *Janus*, the Court found that an investment advisor that initially drafted false statements was not liable for violations of Rule 10b-5 where an independent entity disseminated the statements to investors in its own name because the investment advisor's role in preparing the statements was unknown to the investors. The D.C. Circuit found that, in contrast to the entity acting as an investment advisor in *Janus*, Lorenzo was significantly more culpable and acted as a participant in the scheme by sending the statements in his own name. The Court emphasized that, "Unlike in *Janus*, therefore, the recipients of Lorenzo's emails were not exposed to the false information only through the intervening act of 'another person.'"⁵

Judge Kavanaugh's Dissent

Judge Kavanaugh dissented from the D.C. Circuit's opinion in *Lorenzo*, asserting that holding Lorenzo liable for "scheme liability" under Rule 10b-5(a) and (c) and



Section 17(a)(1) blurred the line between primary liability and secondary liability (*i.e.*, aiding and abetting) for securities fraud violations. Instead, he stated that he would adopt the approach of other Circuit Courts that “scheme liability must be based on conduct that goes beyond a defendant’s role in preparing mere misstatements or omissions made by others.”⁶ In his view, this rule is intended to prevent those who would normally be only secondarily liable for aiding and abetting the making of fraudulent misstatements from being held primarily liable for the same conduct under a theory of scheme liability. In Judge Kavanaugh’s view, expanding the scope of scheme liability to hold individuals in Lorenzo’s position liable for primary violations of Rule 10b-5 will effectively eliminate secondary liability by making aiders and abettors primarily liable for securities fraud violations.

The distinction between primary liability and secondary liability is particularly important to the SEC, because it is easier to prove primary liability. This is because, in order to prove secondary liability, the SEC must prove not only a securities violation by the primary violator, but also knowledge of this violation and “substantial assistance” by the aider and abettor in committing the violation. It is also particularly significant to private plaintiffs, who are not permitted to bring claims for aiding and abetting securities fraud.⁷ For this reason, blurring the line between primary and secondary liability would make it much easier for the SEC and private plaintiffs to prove securities fraud claims against entities and individuals like Lorenzo, who did not “make” the fraudulent statement at issue.

The Potential Impact of Kavanaugh’s Appointment

What do Judge Kavanaugh’s dissent and appointment to the Supreme Court mean for the *Lorenzo* case? Due to his prior involvement in the case as a D.C. Circuit Judge, Judge Kavanaugh may be forced to recuse himself from the case, leaving the possibility of a split decision.⁸ In fact, in 2016, public interest group Fix the Court found that Supreme Court Justices recused themselves 180 times in a single session, with most of the recusals due to prior work on the case at issue.⁹ For this reason, it is not only possible, but is likely, that Judge Kavanaugh will be forced to sit on the sidelines when the Supreme Court hears the *Lorenzo* appeal.

If Judge Kavanaugh does recuse himself from the case, his recusal will leave only eight Justices to decide *Lorenzo*, and one less Justice who favors a more restrictive view of who can be considered the “maker” of a statement and held liable for violations of Rule 10b-5 under a theory of scheme liability. This is critical, because *Janus* was a 5-4 decision, with the four more liberal Justices—Justices Breyer, Ginsburg, Sotomayor, and Kagan—all of whom are still Supreme Court Justices—dissenting.



In their dissent, these Justices expressed their disagreement with the majority's view that only those with "ultimate authority" over a statement can be considered the "maker." Thus, a recusal by Judge Kavanaugh would create a significant likelihood that the Supreme Court will reach a 4-4 deadlock in *Lorenzo*.

A 4-4 deadlock would not only delay further clarification from the Supreme Court on the standard articulated in *Janus*, but would also leave the D.C. Circuit's ruling in *Lorenzo* intact. As a result of this deadlock, ultimately the SEC would have significantly expanded authority under the D.C. Circuit's ruling, allowing the SEC to sidestep the higher burden of proof for aiding and abetting claims and instead impose primary liability for violations of Rule 10b-5 on a defendant who was not the "maker" of a fraudulent statement using a theory of scheme liability. Perhaps most significantly, an affirmance of the D.C. Circuit's ruling would allow private plaintiffs to invoke scheme liability to bring claims against secondary violators like Lorenzo, who would otherwise be beyond the reach of private actions for violations of Rule 10b-5.

While it appears unlikely Judge Kavanaugh will participate in the *Lorenzo* appeal given his previous involvement and the strong opinion he has already articulated in the case, his appointment to the Supreme Court could have broader implications for U.S. securities laws. Even if a deadlock does prevent the Supreme Court from overruling the D.C. Circuit's holding in *Lorenzo* for the time being, a predominantly conservative Supreme Court is ultimately likely to expand the ruling of *Janus* to prevent individuals and entities who did not "make" the fraudulent statement at issue from being held liable under a theory of scheme liability, thereby significantly curtailing the ability of both the SEC and private parties to bring claims for primary violations of Rule 10b-5. ➤

Endnotes

1 [872 F.3d 578 \(D.C. Cir. 2017\)](#).

2 [17 CFR 240.10b-5\(b\) \(1951\)](#).

3 [17 CFR 240.10b-5\(a\) \(1951\)](#); [15 U.S. Code § 77q \(2010\)](#).

4 [564 U.S. 135 \(2011\)](#).

5 [872 F.3d at 591](#).

6 [Id. at 600](#).

7 [Id. at 590](#).

8 See [28 U.S.C. § 455 \(1990\)](#).

9 Debra Cassens Weiss, *Supreme Court Justices Recused Themselves 180 Times in Most Recent Term*, ABA Journal (Jul. 12, 2016), http://www.abajournal.com/news/article/supreme_court_justices_recused_themselves_180_times_in_most_recent_term/.

Defrosting... continued from page 8

either made in bad faith or based on an unreasonable investigation. In terms of bad faith, the shareholder argued both outside counsel and WWC's general counsel were conflicted. The court rejected both arguments.² The court also found the shareholder failed to show WWC's investigation to be unreasonable since the Board had reviewed ample information and took numerous steps to familiarize itself with the subject matter of the demand.³ This ruling understandably had a chilling effect on shareholder derivative actions with respect to data breaches, since shareholders likely noted that, under the auspices of the business judgment rule, the court gave substantial deference to the company concerning cybersecurity affairs.

Plaintiffs did not give up entirely, however, and recent events have shown their resolve may ultimately pay off. A prime example is the \$80 million settlement entered into by Yahoo in connection with securities class action lawsuits brought by its shareholders.⁴ As background, Yahoo had learned in 2014 that it had suffered a breach impacting 500 million of its users. However, it did not disclose the breach until 2016. Between the breach and the disclosure, Yahoo entered into negotiations to be acquired by Verizon. The gist of the class' allegations was that certain directors and officers failed to disclose and presented misleading information regarding Yahoo's cybersecurity practices. As a result of these subpar practices resulting in data breaches and the failure to promptly report and remedy the breaches, it was alleged that the company's stock price dropped, which caused Yahoo to be sold to Verizon for \$350 million less than it otherwise would have.⁵

Wendy's became embroiled in a similar scenario, albeit critically different in regards to the harm that could be identified. Wendy's had discovered a data breach in early 2016 and subsequently realized in June 2016 the breach was much greater than initially expected. In December 2016, a shareholder derivative action was filed.⁶ The case was settled in May 2018, which included an agreement to adopt better cybersecurity measures and, of course, pay the plaintiff's substantial attorneys' fees. Since the plaintiff shareholders could not point to a reduced share price or purchase price, there was no real opportunity for them to recover damages. Accordingly, Wendy's exposure was dramatically different than Yahoo's exposure.

Apparently emboldened by the success of the shareholders of Yahoo and Wendy's, shareholders of Equifax recently brought a class action complaint against Equifax and more than a dozen of its executives in connection with the massive data breach Equifax discovered in 2017.⁷ While it is uncertain how this litigation will be resolved, it is clear that it is a new day for shareholder suits following data breaches.

Potentially portending a greater number of class action lawsuits against companies following data breaches is the immature cyberinsurance marketplace. For most

industry classes, perhaps other than retailers and health insurers, the market for cyberinsurance policies is soft.⁸ Recent estimates indicate global cyberinsurance premiums collected in 2017 were approximately \$2.5 billion, and market experts continue to predict total annual premiums will grow to \$20 billion by 2025, which means cyberinsurance remains the “golden goose” for the insurance industry.⁹ As a result, policies are near-fully customizable and few policy exclusions are non-negotiable.¹⁰ Moreover, there is no accepted standardized cyberinsurance policy available, which allows for policyholders and their brokers to shop provisions from carrier to carrier.¹¹ And, there is a growing recognition that a company’s response to a cyberattack, including its insurance program, must be the focus of the C-suite.¹²

All of these factors taken together could prove significant for shareholders if and when their companies suffer a major data breach, which requires the involvement of the companies’ insurance carriers. If those carriers deny coverage outright, or limit coverage significantly, because of a policy provision that was capable of being negotiated out of the policy, the company can expect shareholder consternation and perhaps a lawsuit depending on the magnitude of the unavailability of coverage.

Indeed, glaring examples of coverage denials and litigation arising from policy provisions that could have been eliminated are out there. Perhaps the most illustrative example was a lawsuit filed by an insurer against its policyholder, Cottage Health System (“CHS”), in connection with a data breach that resulted in the release of private health care patient information.¹³ The underlying suit was a class action filed against CHS for violations of California’s Confidentiality of Medical Information Act. The underlying action was settled for \$4.125 million, which was paid by the insurer. The insurer then initiated a declaratory judgment action seeking reimbursement. It relied upon the policy’s Failure to Follow Minimum Required Practices Exclusion, which stated that the insurer was not liable for any loss arising out of any failure of the insured to “continuously implement the procedures and risk controls identified in the Insured’s application for this Insurance and all related information submitted to the Insurer in conduction with such application whether orally or in writing.” The insurer alleged CHS’ failure to abide by the minimum required practices resulted in the data breach and subsequent loss. The coverage litigation is ongoing.

Another example is the victory of Federal Insurance Company over P.F. Chang’s¹⁴ with regard to a claim under a cyberinsurance policy. The dispute arose when P.F. Chang’s suffered a data breach resulting in the compromise of approximately 60,000 customer credit card numbers. Federal initially reimbursed P.F. Chang’s for approximately \$1.7 million in response costs to the breach. However, Bank of American Merchant Services (“BAMS”) also suffered three assessments (Fraud



Recovery Assessment, Operational Reimbursement Assessment, and a Case Management Fee) by MasterCard in connection with the loss and demanded reimbursement from P.F. Chang's pursuant to contract. When Federal denied coverage for the losses, P.F. Chang's filed suit. The district court analyzed coverage for each of the assessments separately and concluded they either did not satisfy an insuring agreement or were barred pursuant to exclusions. The court also found compelling that P.F. Chang's had failed to purchase Payment Card Industry ("PCI") liability coverage. At the time P.F. Chang's purchased its cyberinsurance policy, PCI liability coverage was not a standard industry offering, although the more sophisticated policyholders were purchasing it. At bottom, P.F. Chang's failure to obtain this newer insurance offering cost it millions.

In a similar situation, New Hotel Monteleone ("Monteleone") suffered a greater loss than necessary because it purchased cyberinsurance with inadequate PCI liability limits.¹⁵ There, Monteleone had suffered a prior cyberattack and was seeking to purchase a cyberinsurance policy that would cover losses arising out of a subsequent attack. After a second cyberattack, for which Monteleone's payment card industry liability exceeded the limits of its coverage, the policyholder sued its insurer and retail agent. The decisions by Monteleone and its agent ultimately resulted in a substantial loss that could have been eliminated entirely, or at least mitigated, had they better prepared for the aftermath of a cyberattack.

We should see more coverage disputes arising from policy provisions that could have been deleted through pre-binding negotiation. One source of these disputes is the cyberterrorism exclusion found in some policies. State actors, non-state, and quasi-state continue to target companies for pecuniary or other purposes. A recent threat assessment by the Director of National Intelligence warns of continued cyberattacks from Russia, China, Iran, and North Korea, among others.¹⁶ While the War Exclusion in the cyberinsurance policies are unlikely to be deleted, the terrorism exclusion seems more fungible, especially given many policies are sold with affirmative cyber terrorism coverage. Also indicative of the fungibility of the terrorism exclusion is the reality that to qualify as terrorism, the act against the company must be so certified by the United States Secretary of the Treasury in concurrence with the Secretary of State and Attorney General, and no act has ever been certified an act of terrorism.¹⁷

Another potential source of coverage disputes is the insurability of fines and penalties assessed against U.S. companies as a result of their violation of the EU's General Data Protection Regulation ("GDPR"). The fines can range from €10 million to 4% of the company's turnover, whichever is greater and depending on the severity of



the violation. Some policies in the marketplace offer language that determines insurability of a fine or penalty in accordance with law that would be most favorable to the insured. Absent negotiation for such favorable language, the policyholder may find itself with a multi-million dollar uncovered loss and, in turn, angry shareholders. This novel question of the insurability of GDPR fines may ultimately yield an answer that no penalties and fines are ever insurable, irrespective of the jurisdiction, but failure to negotiate for the most favorable policy provisions may foreclose even the possibility of creative argument.

While shareholder actions so far have focused on inadequate cybersecurity measures and improper reporting of breaches, the failure of a company to obtain the best available cyberinsurance could be the rhythm shareholders next bang out on their drums of criticism. Given the lack of standardized cyber coverage and the competitiveness of the marketplace, companies typically have the opportunity to dig in their heels in the negotiation for cyberinsurance policies and negotiate for favorable terms. If they do not, they risk inadequate insurance coverage, or even none at all, in the aftermath of a data breach. This theory of liability against directors and officers is untested. But, as the cost of data breaches continues to increase exponentially, we can fully expect shareholders to avail themselves of any and all means to pursue recovery for the perceived failures of the company to have in place a robust response to a cyberattack, including a strong, comprehensive insurance program.

Companies should thus consult either a broker or an insurance coverage attorney particularly knowledgeable of cyberinsurance policies to review their insurance programs, and not just at renewal, to determine if any gaps in coverage exist. And, brokers better get with the program, as well. The fact is that it is not uncommon for brokers who sell cyber coverage to specifically tout their expertise in regards to cyber coverage issues and the efforts they will undertake to identify risks and prepare comprehensive risk management solutions for their customers specifically designed to protect them from their unique and individual cyber risks. While the law in the vast majority of states provides that brokers do not owe a duty to advise or guide their customers with respect to coverage to purchase (including types of coverage, limits, or specialized coverages available by endorsement), a duty to advise may arise where there are deemed to be “special circumstances” or the parties’ business dealings are determined to constitute a “special relationship.”¹⁸ Relevant factors in making this determination include where the broker represents itself as and is viewed by the customer as an expert in regards to a specific type of coverage, and where the broker should reasonably understand that its advice is being sought and specially relied upon.¹⁹ Because brokers looking to gain a



competitive advantage in selling cyber coverage will often make representations that can be cited as evidencing these critical factors, the absence of coverage for cyber related losses may provide the basis for failure to advise claims.²⁰ Further, these exposures can potentially be so significant, it opens up brokers to enormous potential risk if they talk the talk but don't walk it. ➤

Endnotes

- 1 [*Palkon ex. rel. Wyndham Worldwide Corp. v. Holmes*, No. 2:14-cv-234, 2014 WL 5341880 \(D.N.J. Oct. 20, 2014\)](#).
- 2 [*Id.* at *4-5](#).
- 3 [*Id.* at *6](#).
- 4 *In re Yahoo! Inc. Sec. Litig.*, 5:17-cv-000373 (N.D. Cal.).
- 5 Am. Compl., at ¶ 151 ("On February 20, 2017, Yahoo and Verizon amended the Stock Purchase Agreement, reducing the consideration to be paid by Verizon to Yahoo by \$350 million . . .").
- 6 *Graham ex. rel. The Wendy's Company v. Peltz, et al.*, 1:16-cv-1153 (S.D. Ohio).
- 7 *Teamsters Local 443 Health Servs. & Ins. Plan v. Gamble, et al.*, No. 1:18-cv-00577 (N.D. Ga.).
- 8 Jason Tashea, "'Confusing as Hell': Making Sense of Cyber Insurance," *ABA Journal*, March 9, 2018.
- 9 "5 Cyber Insurance Trends to Watch for in 2018," *Willis Towers Watson*, Dec. 12, 2017; Allianz Global Corporate & Specialty, "A Guide to Cyber Risk: Managing the Impact of Increasing Interconnectivity," Sept. 2015, p.5; see also Jonathan S. Ziss and Jonathan L. Schwartz, "Cyberinsurance 2015: A Robust and Rapidly Changing Market," *LegalTech*, December 30, 2015.
- 10 Sam Friedman & Adam Thomas, "Demystifying Cyber Insurance Coverage," *Deloitte*, Feb. 23, 2017.
- 11 *Id.*
- 12 Chris Esemplare, "As Cyber Risk Escalates, the C-Suite Must Take Action," *SecurityIntelligence*, Apr. 19, 2018.
- 13 *Columbia Cas. Co. v. Cottage Health Sys.*, 2:15-cv-3432 (C.D. Cal.).
- 14 [*P.F. Chang's China Bistro, Inc. v. Fed. Ins. Co.*, No. Cv-15-1322, 2016 WL 3055111 \(D. Ariz. May 31, 2016\)](#).
- 15 *New Hotel Monteleone, LLC v. Certain Underwriters at Lloyd's of London*, No. 2:16-cv-161-ILRL-JCW (E.D. La.).
- 16 Worldwide Threat Assessment of the US Intelligence Community, Feb. 13, 2018. According to the Assessment, cyber operations are a low-cost tool used by nefarious state actors, terrorist groups, and criminal organizations. In particular, terrorist groups are expected to focus primarily on disclosing personally identifiable information, website defacements, and denial-of-service attacks. Another potential issue with cyberattacks, especially in connection with the War Exclusion, is the blurring of the line between mere criminal activity and nation-state activity.
- 17 For a further discussion on insurance coverage for cyberterrorism, please see *Pop Quiz Hotshot! This Bus Is Now Under My Control: Cyberterrorism Risk for Commercial Vehicle Operators and Rental Agencies* by Thomas D. DeMatteo and Jonathan L. Schwartz.
- 18 See, e.g., [*Voss v. Netherlands Ins. Co.*, 8 N.E.3d 823 \(N.Y. 2014\)](#); [*Peter v. Schumacher Enter., Inc.*, 22 P.3d 481 \(Alaska 2001\)](#); [*AAS-DMP Mgmt., L.P. Liquidating Trust v. Acordia Northwest, Inc.*, 63 P.3d 860 \(Wash. Ct. App. 2003\)](#); [*Fitzpatrick v. Hayes*, 57 Cal. App. 4th 916 \(Cal. Ct. App. 1997\)](#).
- 19 [*Tiara Condo. Ass'n, Inc. v. Marsh USA, Inc.*, 991 F. Supp. 2d 1271 \(S.D. Fla. 2014\)](#); [*Meridian Title Corp. v. Gainer Grp., LLC*, 946 N.E.2d 634 \(Ind. Ct. App. 2011\)](#); [*Bush v. Mony Life Ins. Co. of Am.*, No. 3:07-cv-451, 2008 WL 4874137 \(D. Conn. Nov. 10, 2008\)](#); [*Southwest Auto Painting & Body Repair, Inc. v. Binsfeld*, 904 P.2d 1268 \(Ariz. Ct. App. 1995\)](#).
- 20 Biging, Peter, Schwartz, Jonathan, and Collins, Meghan, "Does Broker Know Best When Purchasing Cyberinsurance?," *Law360*, May 10, 2016.



Discussion Paper... continued from page 9

against potential liabilities can reduce the likelihood that clients will later file claims, as well as reducing the costs associated with these claims, which include loss of fees, self-insured retentions, the cost of insurance and damage to the firm's reputation.

Why Many Law Firms Do Not Attempt To Limit Their Liability In Engagement Letters...

Unlike accounting firms and other professional organizations, law firms typically do not attempt to limit their liability in their engagement letters. In fact, many firms do not secure formal letters of engagement from clients at all. Some law firms are concerned that clauses seeking to limit their liability are not enforceable due to ethical restrictions. Others fear that asking clients to agree to certain concessions could negatively impact the relationship, putting them at a disadvantage compared to more agreeable competitors. In addition, many law firms do not believe that putting these kinds of restrictions in place will significantly reduce liability to an extent that justifies the expense and resources necessary to implement them.

...And 5 Reasons Why They Should

While it is understandable why law firms may be reluctant to take steps to limit their liability in the engagement letter, there are a number of reasons why they should reassess this position:

- 1. Clients are now requiring their own engagement letters** and the clients' contract language typically seeks to impose and expand liability on law firms, often through boilerplate language that seems to run counter to the retained counsel's position as a trusted counselor and advisor.
- 2. Law firms are held to very high professional standards,** and even with the best quality controls in place, the professional liability exposure they face can result in claims in excess of their insurance policy limits, often from engagements in which the firm received very little compensation.
- 3. Law firms may be at a competitive disadvantage** as their subcontractors and other providers who take steps to limit their own liability can offer services at cheaper rates.
- 4. The American Bar Association ("ABA") recommends that lawyers communicate key terms of representation to clients,** preferably in writing, either before or within a reasonable time after the representation has begun (see ABA, Model Rules of Professional Conduct (hereinafter "MRPC"), "Client-Lawyer Relationship, Rule 1.5, Fees").



5. All experienced malpractice insurers recommend that law firms secure signed engagement letters that clearly state the responsibilities of the firm and include provisions that limit the firm's liability, where permitted.

Structuring Engagement Letters That Limit Law Firm Liability

While the vast majority of states permit agreements limiting a lawyer's liability, a few notable outliers unequivocally forbid a lawyer from entering into such an agreement.¹ Where permitted, the client must be independently represented by counsel, which can include in-house counsel (see MRPC, "Client-Lawyer Relationship, Rule 1.8 (h) (1), Current Clients: Specific Rules").

Despite differences in enforceability from state to state, there seems to be little dispute regarding three components of a well-structured engagement letter that can help law firms in their client relationships and provide possible protection against malpractice claims. The three key components to the letter are: (1) identifying the client, (2) defining the scope of engagement, and (3) handling conflicts of interest.

Identify the Client

Defining who is and who is not the client is one of the most critical components of an engagement agreement. Without a tightly drawn definition of clients and non-clients in their contracts, law firms may be more susceptible to claims of conflict of interest that can be difficult and costly to defend. For an example of an ambiguous engagement letter with a client that exposed the law firm to malpractice and fiduciary breach of claims by a non-client, see the case of [*Exeter Law Group LLP v. Wong*, 2016 NY Slip Op 32425\(U\) \(Sup Ct. NY County 2016\)](#).

- **Corporate Clients.** When representing a corporation, law firms should define precisely who the corporate client is, and seek to specifically exclude those persons or entities the firm does not represent. For example, if Company A is a client, the firm should designate Company A's officers, directors, employees, subsidiaries and assigns as non-clients.
- **Founders of a Company or Partnership.** If the firm's client is a partnership or company with partners, the founders or partners should be designated as non-clients. Conflict of interest claims have been alleged based on a believed attorney-client relationship between a law firm and one of the founders and minority partner of the client. Including language that clarifies what parties are included from those excluded in the attorney-client relationship can help



law firms minimize these kinds of risks. A case that illustrates the importance of clearly designating clients and non-clients alike in an engagement letter is [*Home Care Industries, Inc. v. Murray*, 154 F. Supp.2d 861 \(D.N.J. 2001\)](#).

- **Spouses and Domestic Partners or Parents and Children.**

Including language that clearly identifies the client and also designates non-clients is especially important when the law firm has a pre-existing relationship with one or more of the parties or their family members. [*Silberberg v. Meyers*, 885 N.Y.S. 2d. 713 \(Sup. Ct 2009\)](#) is an example of the effective use of clear engagement letter language to define which family members are included in the definition of client, and which ones are not.

Scope of the engagement

It's equally important to **define the scope of the engagement in the contract as clearly and specifically as possible**. MRPC Rule 1.2 (c), "Scope Of Representation And Allocation Of Authority Between Client And Lawyer," states that a lawyer may limit the scope of the representation if the limitation is reasonable under the circumstances and the client gives informed consent.

Law firms have traditionally shied away from narrowly defining the scope of engagement, believing that it is impractical to obtain frequent written amendments changing the scope of the engagement letter. Although a broadly worded scope of engagement section allows a firm to represent a client on a range of matters without the need for a new engagement letter, this could come with a price. In the event of a claim, a law firm's belief about what it was retained to do may differ greatly from its client. From a risk management standpoint, the more restrictive the description, outlining solely what that firm intends to do, the better. Further, more precision and certainty around what the firm has or has not agreed to do encourages more frequent client contact, and could have other benefits as well, especially with respect to activities falling under an alternative fee arrangement rather than traditional hourly billing.

The case [*AmBase Corp. v. Davis Polk & Wardwell*, 866 N.E. 2d 1033 \(N.Y. 2007\)](#) is an example where the law firm prevailed in a malpractice case, in part, because the engagement contract wording was limited in scope and, therefore, viewed by the court as precise and clear. In contrast, the law firm in [*Barack v. Seward & Kissell, LLP*, 2017 WL 4023141, 16-cv-09664 \(S.D.N.Y Sept.12, 2017\)](#) lost its motion to dismiss, because the court found the language in the retainer agreement to be too broad.

In drafting contract wording regarding the scope of the client engagement, attorneys should consider limitations on both the subject matter and the duration of their



representation. The following are sample disclaimers law firms should consider including when drafting this section of their client contracts:

- Where the firm represents the client in general litigation, and where insurance coverage is available to the client, the firm should consider stating that it *“is neither opining on the scope of any available insurance nor representing the client in notifying insurers of claims, or in any negotiating or settlement of claims.”*
- With litigation matters, it is particularly important to state that *“the firm does not provide any guarantee or promise as to the outcome of any client matters undertaken by the firm.”*
- Where relevant, the contact should explain *“that the firm does not act as an investment advisor, or accountant, appraiser, insurance consultant, or architect or engineer, and does not accept any liability or responsibility for their appointment, supervision or performance of such entities that have been retained to perform those services.”*
- Although clients may want their terms to control, the law firm’s contract should state, *“In the event of any conflict between the provisions of the firm’s engagement letter and any outside counsel guidelines, the provisions of the firm’s engagement letter shall control.”*
- Where the client has also retained another firm to handle an aspect of the engagement, it should be clearly specified what assignments the other firm will be handling, as claims have been brought by clients alleging that the firm had a broader role than the firm assumed. For example, specify if the firm will not make UCC filings in order to avoid any confusion (e.g., *“The firm will not be responsible for any UCC filings or patent annuity work.”*)
- In a merger and acquisition scenario, a firm may wish to specify that it has not been retained to give tax advice relating to the transaction. Even if another firm has given a tax opinion relating to the transaction, the firm may still want to consider including a provision that they have not been retained to review other counsel’s work.
- In the sale of a company, a firm may also want to specify whether their representation of the company will survive the transaction. If it does, new management will then have full access to the firm’s client files. In a case where a hostile takeover has occurred, new management could use this opportunity to comb through the firm’s files for communications relating to the defense of the takeover.



Conflicts of interest

Conflicts of interest cause a significant number of malpractice claims that are very difficult to defend. As such, many firms look to secure a blanket advanced conflict of waiver in the engagement letter.

An example of this kind of language is: *“The Firm represents a large number of other clients, and it is possible that during the course of such representation of the client by the firm, other clients may seek to assert or protect interests adverse to the client. These may constitute conflicts of interest that could prevent or otherwise inhibit the firm’s ability to represent such client. As a condition to the undertaking of this representation by the firm, the client agrees that the firm may continue to represent or undertake to represent existing or new clients even if those interests are directly adverse to or different from the clients, so long as such representation is not substantially related to work for the client.”*

While these kinds of waivers can be effective, they can also be challenged (see *Sheppard, Mullin, Richter & Hampton, LLP v. J-M Manufacturing Co., Inc.*, Case no S232946, a case currently under review by the California Supreme Court in which Sompco International and other malpractice insurance carriers have filed an amicus brief).¹

Challenges are normally based on the premise that in order for any conflict to be waived, the specific nature of the conflict and the identity of the other client should be disclosed, factors that may be impossible to identify at the time the engagement letter is signed.

Additional Disclosures to Consider

Depending on the situation, there are a number of additional disclosures and items law firms should consider when preparing engagement letters that can help limit professional liability exposure. These include:

- **Indemnification agreements that limit liability to specific amounts of damages.** While there are significant restrictions on a law firm’s ability to limit liability, they may be able to do so when retained to provide non-legal services, such as when retained to provide supervisory responsibility for outside providers. Services that can be handled by non-lawyers include certain trust and estate or other fiduciary work, tax advice, electronic discovery and patent annuity tasks.
- **Restrictions on the statute of limitations.** This protection can be achieved directly in states where it is allowed, or indirectly through a clause in



the engagement letter stating that any dispute is to be handled by arbitration or litigation in a specific state and in accordance with the laws of that state that has the shortest statute of limitations.²

- Firms can also include language stating the engagement is terminated when the service is complete in order to ensure that the firm's liability does not remain open-ended.
- **“Waiver of jury trial” provisions.** While this kind of provision does not directly impact a firm's ability to limit professional liability, it will allow the attorney to control the forum in which any disputes are to be resolved, thus potentially leading to a more predictable outcome. The firm should also consider including language stating that at the option of the firm, mediation or arbitration may be required in place of litigation for any client disputes, especially when the dispute involves fees.
- **Protections against third-party suits and liability.** Law firms should consider including the following types of statements in both their own engagement letters as well as on any documents a third party could potentially read:
 - “Any opinion provided to the client cannot be relied on by any third party without the specific agreement of the firm.”
 - “Clients are prohibited from assigning claims to third parties.”
- **Limiting the liability associated with supervising subcontractors.** In situations where a subcontractor is supervised by the law firm, retained counsel should take steps to guard against becoming fully responsible for any negligence of the subcontractor. For example, attorneys may request that subcontractors maintain certain minimum coverage in their insurance policies or request that a subcontractor indemnify the law firm for any claims brought by a client in response to actions taken by that subcontractor.
- **Disclosure regarding electronic communications.** For example:
“We may communicate with you and others via email. Such emails can be intercepted read, disclosed or otherwise used or communicated by an unintended third party. We cannot guarantee or warrant that emails from us will be properly delivered and read only by the addressee and may result in attorney client privilege being waived. We specifically disclaim any liability or responsibility whatsoever for such interception or unintentional disclosure, and you agree we shall have no liability for any loss or damage to any person or entity resulting from the use of email transmissions.”



How to Respond if a Client Asks for an Indemnity Agreement

Before finalizing or amending the terms of any engagement letter or indemnity agreement, a law firm should have its own general counsel review the contract. In fact, a firm should avoid entering into an indemnity agreement if possible, although many firms feel pressure to do so in the interest in maintaining a client relationship. If faced with this type of request, the following strategies can help law firms respond.

- **Attempt to persuade the client that an indemnity agreement is not appropriate for a professional service firm.** Law firms act in a professional role and are subject to ethical restrictions. As such, they are unlike other vendors who may serve simply as suppliers of products.
- **Explain that indemnity agreements were originally intended for bodily injury and property damage claims** brought by third parties, and therefore, should exclude professional services. Most law firms are protected for bodily injury and property damage claims in a commercial general liability insurance policy and against data breaches through the purchase of a cyber liability policy.
- **Remind the client that it is not in their best interest.** Entering an indemnity agreement can change the fundamental relationship between the client and its retained counsel. Doing so can potentially invalidate the law firm's professional liability insurance policy, thus reducing a source of recovery for any malpractice claims made against them. In addition, requiring these agreements could reduce the number of law firms available to the client, and firms who sign them may seek higher rates to counteract increased exposure under their professional liability insurance policy.
- **Request that the client waive any indemnity provisions to the extent they impair or conflict with the firm's malpractice insurance policy.** Signing an indemnity agreement could trigger a contractual liability exclusion in the firm's insurance policy and leave it unprotected, reducing a source of recovery to pay a client's malpractice claim against the firm.
- **If indemnification is agreed to, obtain reciprocal indemnification from the client.** If the firm indemnifies the client against claims based on negligence of the firm, require that the client, in turn, indemnify the firm for claims caused by client negligence.




- **If all else fails, assert the firm's right to proportionate liability.**

Include a clause similar to the following into the agreement: *"Without limiting the generality of the foregoing, the obligations undertaken by outside counsel do not impair outside counsel's ability to assert defenses of contributory or comparative negligence, or defenses otherwise applicable in professional negligence or negligent supervision claims."*

Conclusion

Changing client relationships, increased competition and a rise in claims severity underscore the imperative for law firms to take steps to limit their professional liability exposure. While the laws governing client agreements vary from state to state, the inclusion of provisions for identifying the client, defining the scope of engagement and handling conflicts of interest can play an important role in a firm's risk mitigation process.

Understandably, firms do not want to place demands on clients that could potentially jeopardize the relationship. However, as clients increasingly look to limit their own liability exposure, it is reasonable for them to expect that their retained counsel should do the same. In this context, a carefully crafted and thoughtfully presented engagement letter can be an important tool to help firms strike a successful balance between protecting the firm and preserving their client relationships. 

Sompo International does not make any representations or warranties as to the technical accuracy or compliance with any law or professional standards. We recommend retaining experienced counsel knowledgeable about engagement letters and ethical standards, your firm, and the laws of the jurisdiction where you practice.

Endnotes

1 Since we originally wrote this paper, the California Supreme Court has issued a decision in *Sheppard, Mullin, Richter & Hampton, LLP v. J-M Manufacturing Company, Inc.* In that case, the Court held (in part) that without full disclosure of existing conflicts known to the attorney, the client's consent was not informed for purposes of California's ethics rules. The court did not reach the issue of whether a blanket advance waiver would be permissible (p 28). As California still follows the Model Code, a different outcome may result under the Model Rules.

2 Hinshaw & Culbertson LLP has prepared a listing that shows how each state views this issue and provides details about the statute of limitations for commencing a legal malpractice action based on claims of negligence for each state.



Welcome to the New Diverse Speakers Directory Page!

Open to both ABA and
Non-ABA members.

The Directory is a great way
to build your resume and
expand your career!

[https://www.americanbar.org/
diversity-portal/SpeakersDirectors.html](https://www.americanbar.org/diversity-portal/SpeakersDirectors.html)



- Expand your speaking experience both nationally and internationally.
- Show off your past speaking engagements.
- Create a customized Speakers Bio.
- Show off your technical skills.
- Market yourself to more than 3,500 ABA entities seeking speakers around the country and the world

For more information or questions regarding the directory email: diversity@americanbar.org

Calendar

November 7-9, 2018	Fidelity & Surety Law Fall Conference Contact: Janet Hummons – 312-988-5656	Ritz Carlton Philadelphia Philadelphia, PA
January 16-18, 2019	Fidelity & Surety Law Midwinter Conference Contact: Juel Jones – 312-988-5597	Hilton San Diego Bayfront San Diego, CA
January 17-19, 2019	Midwinter Symposium on Insurance and Employee Benefits Contact: Janet Hummons – 312-988-5656	Hyatt Regency Coral Gables, FL
January 23-27, 2019	ABA Midyear Meeting Contact: Arthena Little – 312-988-5672	Las Vegas, NV
February 21-23, 2019	Insurance Coverage Litigation Midyear Conference Contact: Janet Hummons – 312-988-5656 Contact: Danielle Daly – 312-988-5708	Arizona Biltmore Resort & Spa Phoenix, AZ
March 20-22, 2019	Transportation MegaConference XIV Contact: Janet Hummons – 312-988-5656 Contact: Danielle Daly – 312-988-5708	Sheraton New Orleans New Orleans, LA
March 22-23, 2019	Admiralty and Maritime Law National Program Contact: Juel Jones – 312-988-5597	Sheraton New Orleans New Orleans, LA
April 4-5, 2019	Motor Vehicle Products Liability Conference Contact: Janet Hummons – 312-988-5656 Contact: Danielle Daly – 312-988-5708	Hotel Del Coronado Coronado, CA
April 5-6, 2019	Toxic Torts & Environmental Law Conference Contact: Janet Hummons – 312-988-5656	Hotel Del Coronado Coronado, CA
May 1-5, 2019	TIPS Section Conference Contact: Janet Hummons – 312-988-5656 Contact: Juel Jones – 312-988-5597 Speaker Contact: Arthena Little – 312-988-5672	Westin New York Times Square New York, NY

Hypertext citation linking was created with [Drafting Assistant](#) from Thomson Reuters, a product that provides all the tools needed to draft and review – right within your word processor. Thomson Reuters Legal is a Premier Section Sponsor of the ABA Tort Trial & Insurance Practice Section, and this software usage is implemented in connection with the Section's sponsorship and marketing agreements with Thomson Reuters. Neither the ABA nor ABA Sections endorse non-ABA products or services. Check if you have access to [Drafting Assistant](#) by contacting your Thomson Reuters representative.