In-house counsel, your help is needed!

We have had strong interest from young lawyers about participating in the corporate counsel mentor program - so much so that we have more mentees than mentors. If you are interested in serving as a mentor, or would just like to hear more about it, please email Stefan Palys at stefan.palys@stinson.com.

NAIC Insurance Data Security Model Law Emerges

On October 24, 2017, Version 6 (with technical corrections) of the NAIC Insurance Data Security Model law¹ ("Model") was granted final approval by the National Association of Insurance Commissioners (NAIC) Executive (EX) Committee and Plenary. The Model is now available for consideration and adoption by the states.

The final version of the Model — the sixth iteration of the proposal — has been in the works since late 2015. It incorporates significant changes from the first

Read more on page 12
Dear Corporate Counsel Committee Members,

Welcome to the Committee’s Winter 2018 newsletter. I hope everyone enjoyed some time off during the holidays and that you are staying warm during what thus far has been a frigid beginning to 2018. In this newsletter you will find several articles providing practical advice and tips on subjects ranging from data security and e-discovery to business party etiquette -- content that should be useful and relevant to all members, regardless of practice setting.

Thanks to all of you for contributing to the success of our 2017-2018 year. We have a new Technology vice-chair focusing on ways to improve our communications through social media, Membership vice-chairs helping us meet the Section Chair’s challenge to increase committee and TIPS overall membership, and many members committed to the continued success of our mentoring program, paring new in-house lawyers with seasoned practitioners to help navigate the early years of in-house practice. During our first few monthly calls we were privileged to hear from practitioners specializing in OSHA and employment law on the timely subjects of workplace injury and illness reporting compliance and best practices in implementing sexual harassment policies. We will continue to hold combined business and educational monthly calls through the remainder of the year.

Please reserve time to attend the TIPS Spring CLE Conference in Los Angeles May 2-6, 2018. The proposed agenda includes a number of great programs that will highlight topics relevant to corporate counsel, including a program based on former Corporate Counsel Committee Chair Bill Kruse’s recently published survival handbook, and will provide attendees with numerous networking opportunities. Bill Kruse also is preparing to host a corporate counsel talent development program at Gallup’s Irvine, California, offices to coincide with the Section Conference this Spring. I hope many of you will plan to attend that session too.

I look forward to seeing you in Los Angeles and to speaking even sooner during our next monthly call.

Best regards,

Beth M. Kramer

Lockheed Martin Corporation

Chair, ABA TIPS Corporate Counsel Law Committee
### Member Roster | continued

<table>
<thead>
<tr>
<th>Name</th>
<th>Company/Address</th>
<th>Phone</th>
<th>Fax</th>
<th>Email</th>
</tr>
</thead>
<tbody>
<tr>
<td>Maureen Manning</td>
<td>American Traffic Solutions, Inc.</td>
<td>(480) 719-7032</td>
<td>Fax: (602) 252-5339</td>
<td><a href="mailto:maureen.manning@atsol.com">maureen.manning@atsol.com</a></td>
</tr>
<tr>
<td>Matthew Moeller</td>
<td>The Moeller Firm LLC</td>
<td>(504) 702-6774</td>
<td><a href="mailto:matthew@moellerfirm.com">matthew@moellerfirm.com</a></td>
<td></td>
</tr>
<tr>
<td>Ndidi Moses</td>
<td>US Attorney’s Office</td>
<td>(203) 821-3700</td>
<td>Fax: (860) 275-8299</td>
<td><a href="mailto:ndidi.moses@usdoj.gov">ndidi.moses@usdoj.gov</a></td>
</tr>
<tr>
<td>Pamela Palmer</td>
<td>Morris Polich &amp; Purdy LLP</td>
<td>(213) 488-1178</td>
<td><a href="mailto:ppalmer@mpplaw.com">ppalmer@mpplaw.com</a></td>
<td></td>
</tr>
<tr>
<td>Stefan Palys</td>
<td>Stinson Leonard Street</td>
<td>(602) 212-8523</td>
<td>Fax: (602) 240-6925</td>
<td><a href="mailto:stefan.palys@stinson.com">stefan.palys@stinson.com</a></td>
</tr>
<tr>
<td>Gary Pappas</td>
<td>Carlton Fields</td>
<td>(305) 530-7230</td>
<td>Fax: (305) 530-0055</td>
<td><a href="mailto:gpappas@carltonfields.com">gpappas@carltonfields.com</a></td>
</tr>
<tr>
<td>Lesley Reynolds</td>
<td>Fullbright</td>
<td>(202) 662-0247</td>
<td>Fax: (202) 662-4643</td>
<td><a href="mailto:lesley.reynolds@nortonrosefulbright.com">lesley.reynolds@nortonrosefulbright.com</a></td>
</tr>
<tr>
<td>Julia Phillips</td>
<td>Aldridge Pite LLP</td>
<td>(206) 232-2655</td>
<td>Fax: (206) 232-2655</td>
<td><a href="mailto:jphillips@aldridgepite.com">jphillips@aldridgepite.com</a></td>
</tr>
<tr>
<td>Lisa Pittman</td>
<td>Louisianville</td>
<td>(713) 632-1772</td>
<td><a href="mailto:fpittman@gmail.com">fpittman@gmail.com</a></td>
<td></td>
</tr>
<tr>
<td>Eric Probst</td>
<td>Porzio Bromberg &amp; Newman PC</td>
<td>(973) 889-4320</td>
<td>Fax: (973) 538-5146</td>
<td><a href="mailto:eprobst@porzio.com">eprobst@porzio.com</a></td>
</tr>
<tr>
<td>James Proctor</td>
<td>McWane Inc</td>
<td>(205) 578-3800</td>
<td>Fax: (205) 414-3170</td>
<td><a href="mailto:jim.proctor@mcwane.com">jim.proctor@mcwane.com</a></td>
</tr>
<tr>
<td>Alexander Valdes</td>
<td>Winstead PC</td>
<td>(205) 502-0129</td>
<td>Fax: (205) 383-1925</td>
<td><a href="mailto:2avaldes@winstead.com">2avaldes@winstead.com</a></td>
</tr>
<tr>
<td>Latanishia Watters</td>
<td>Hand Arendall LLC</td>
<td>(205) 728-7250</td>
<td>Fax: (205) 728-7502</td>
<td><a href="mailto:lwatters@handarendall.com">lwatters@handarendall.com</a></td>
</tr>
<tr>
<td>Vanessa Williams</td>
<td>Ihs Markit Ltd.</td>
<td>(248) 728-4234</td>
<td>Fax: (248) 728-7502</td>
<td><a href="mailto:vanessa.williams@ihsmarkit.com">vanessa.williams@ihsmarkit.com</a></td>
</tr>
<tr>
<td>Lesley Reynolds</td>
<td>Fullbright</td>
<td>(202) 662-0247</td>
<td>Fax: (202) 662-4643</td>
<td><a href="mailto:lesley.reynolds@nortonrosefulbright.com">lesley.reynolds@nortonrosefulbright.com</a></td>
</tr>
<tr>
<td>April Savoy</td>
<td>Acceptance Insurance</td>
<td>(615) 844-1331</td>
<td>Fax: (615) 844-1331</td>
<td><a href="mailto:axsavor@acceptance.com">axsavor@acceptance.com</a></td>
</tr>
<tr>
<td>Sarah Sederstrom</td>
<td>Stillwater, MN</td>
<td>(651) 272-6235</td>
<td>Fax: (651) 272-6235</td>
<td><a href="mailto:ssederstrom@comcast.net">ssederstrom@comcast.net</a></td>
</tr>
<tr>
<td>Manpreet Singh</td>
<td>Farmers Insurance</td>
<td>(201) 708-5209</td>
<td>Fax: (201) 708-5209</td>
<td><a href="mailto:manpreet.singh@farmersinsurance.com">manpreet.singh@farmersinsurance.com</a></td>
</tr>
<tr>
<td>Anna Tejada</td>
<td>Kaufman Dolovich &amp; Voluck LLP</td>
<td>(201) 708-5209</td>
<td>Fax: (201) 708-5209</td>
<td><a href="mailto:atejada@kdview.com">atejada@kdview.com</a></td>
</tr>
<tr>
<td>Connect with Corporate Counsel</td>
<td>website</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Connect with Corporate Counsel

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.

americanbar.org/tips
SAVE THE DATE
Join us in celebrating TIPS 85th anniversary!

TIPS SECTION CONFERENCE
May 2-5, 2018 | Loews Hotel Hollywood
Los Angeles, CA

- **Learn:**
Absorb over 25 hours of CLE from distinguished panelist including prominent judges and leading in-house and corporate counsel.

- **Celebrate:**
Honor 85 years of excellence and professionalism in the industry at the highlighted social event - the TIPS Gala Night.

- **Network:**
Expand your circle at our complimentary nightly networking receptions.

- **Join:**
Become involved with our 31 practice-specific committees for professional development and leadership opportunities.

- **Enjoy:**
Explore Los Angeles and the sunshine state with colleagues, new and old.

americanbar.org/tips
Gathering Intelligence: Considering issues posed by Blockchain and Smart Contracts

With the 2017 run up in the price of bitcoin, public interest has increased in blockchain—the technology at the heart of bitcoin. Outside of the bitcoin space, this technology has the potential to make a significant impact on companies and their lawyers in the coming years. A blockchain is a distributed and digitized ledger for documenting transactions. The novelty of blockchain is that it allows for digitized transactions without the need for authentication, regulation, or oversight by a centralized third party. This technology has far reaching implications across several industries. With respect to the legal field, blockchain’s capabilities have given rise to the creation and availability of “smart contracts.” A smart contract is a software program that automatically performs contractual obligations, usually in an “if-then” format. Essentially, the software relies on blockchain to enforce pre-determined rules. For example, with respect to real property transactions, once the buyer’s payment is verified, the seller’s title to the property is automatically conveyed to the buyer and updated to reflect new ownership. The transaction is authenticated as a block in the centralized ledger that cannot be altered without consensus.

The advantages of blockchain and smart contracts are obvious: greater transparency, lower costs, and added efficiency—which makes smart contracts an increasingly popular option in areas of real estate, healthcare and securities. However, as with all new technology, smart contracts create their own share of problems. From an operational standpoint, coding errors may cause unexpected performance issues. There may be discrepancies between coding and natural language versions of a smart contract, or the contracts may perform on the basis of an inaccurate data feed. From a legal perspective, there are still fundamental issues to be resolved such as enforceability, choice of law, jurisdiction and forum selection, as well as dispute resolution. These challenges are certain to have an impact on the role of both inside and outside corporate counsel, particularly in those industries where blockchain could soon be making an impact.

Is a Smart Contract Legally Binding?

In many common law jurisdictions, a contract, to be valid, must be entered into by a natural person, or a legal person such as a corporation, with legal capacity to contract. There is also common law authority, English law, for example, that a contract cannot exist absent sufficient certainty as to the identities of the parties. Moreover, contracts are generally binding and enforceable when the parties take certain steps.
How To Manage And Prepare For Electronic Discovery In Litigation

A. Electronic Discovery Rules.

The Federal Rules of Civil Procedure have long recognized technology’s impact on discovery, and amendments to the Rules promulgated in 2015 updated how parties propound and respond to e-discovery requests. Further, ethical canons established in response to advances in technology and the prevalence of e-discovery in 21st Century litigation require lawyers to be fully familiar with a client’s computer and data systems and social media. This section will cover the amended Federal Rules and rules of professional conduct that pertain to the discovery of electronically-stored information (“ESI”).

Rule 26 outlines federal litigation discovery:

(3) Discovery Plan. A discovery plan must state the parties’ views and proposals on:

…

(C) any issues about disclosure, discovery, or preservation of electronically stored information, including the form or forms in which it should be produced;

…

(E) what changes should be made in the limitations on discovery imposed under these rules or by local rule, and what other limitations should be imposed[].


Federal Rule 34 long ago embraced the impact of changing technology on discovery. See Committee Note on Rule—1970 Amendment. In 2006, the Rule again recognized technology’s influence on litigation:

Electronically stored information may exist in dynamic databases and other forms far different from fixed expression on paper. Rule 34(a) is amended to confirm that discovery of electronically stored information stands on equal footing with discovery of paper documents…. The wide variety of computer systems currently in use, and the rapidity of technological change, counsel against a limiting or precise definition of electronically stored information. Rule 34(a)(1) is expansive and includes any type of information that is stored electronically. A common

Read more on page 17
Interview with Michael Sevi, Deputy Chief Compliance Officer at Marsh & McLennan Companies

Tell us about yourself.

Age: 37
From: Miami, FL
Undergraduate: Dartmouth College
Law School: Harvard Law School
Currently live: New York, NY

Describe for us your path to Marsh & McLennan?

After law school, I worked at Hogan Lovells in Washington DC, primarily conducting internal investigations and defending companies against alleged False Claims Act and Anti-Kickback Statute violations. After that, I joined DLA Piper where I was involved in similar work, conducting internal investigations and responding to government inquiries. In 2011, I was asked to join Florida Governor Rick Scott’s team as Assistant General Counsel. I moved to Tallahassee and oversaw the legal strategy of eight state agencies and defended the Governor’s initiatives against legal challenges. After a year-and-a-half in that role, I was asked to serve as the Governor’s Director of Cabinet Affairs overseeing 11 state agencies, including the Office of Insurance Regulation, Florida Hurricane Catastrophe Fund and Citizens Property Insurance. I returned to the private sector in 2014 when Marsh asked me to lead Compliance for their U.S. operations. I managed a team of regional compliance officers, led regulatory engagement, and handled responses to regulatory inquiries. Two years later, I was asked to join Marsh’s parent, Marsh & McLennan Companies, and assume a global role as the company’s Deputy Chief Compliance Officer. In this position, I manage the global compliance program, oversee internal investigations, and serve as the anti-corruption subject matter expert.

What was appealing to you about transitioning from private practice into the political realm, and then later moving from the public sector into an in-house counsel role?

I have always been motivated by making a difference, advancing a cause or purpose that I believe in. Governor Scott is an inspiring leader. His background and record Read more on page 28
Legal Considerations When Planning an Office Holiday Party

Every office holiday party requires planning ahead. Decorations? Check. Food? Check. Drinks? Check. Ensuring your Company’s anti-harassment and anti-discrimination policies are not forgotten prior to the annual gift exchange? Don't forget that important piece!

Of course, an office holiday party is supposed to be a fun time for employees to get together, unwind, and celebrate. The excitement leading up to the party can be crushed if everyone is forced to sign a dozen waivers, take a seminar on proper holiday party etiquette, and is limited to half a glass of wine. The focus of this article is to provide office holiday party planning tips to ensure your company does not kick off the New Year with a new lawsuit – without turning the occasion into a humdrum event.

Sexual Harassment

Preventing sexual harassment is an important consideration when planning party games, gift exchanges, music, and alcohol. Generally speaking, a company is responsible for preventing harassment and discrimination at corporate-sponsored holiday parties. The same remains true even if the party takes place after normal working hours at an off-site venue. Many lawsuits have involved incidents in which part of the misconduct at issue occurred at a holiday party.

Groping, touching, and making sexually suggestive remarks are not tolerated at any time by anyone, including the holiday party. That much is common sense. Allegations of misconduct should be investigated just as quickly and vigorously as if they occurred in the office. If an employee harasses someone during the office holiday party, chances are it's not the first time they did something inappropriate, and the misconduct may not end there unless it is addressed. What happens at the holiday party will most certainly not stay at the holiday party. More importantly, if you receive a complaint that an employee engaged in harassing or discriminatory conduct, chances are the same sort of behavior will continue until it is addressed.

Occasionally, sexual harassments lawsuits include incidents where an employee thought they were being funny, and another employee did not find the behavior to be humorous. A classic example comes up during an annual gift exchange. Employee A gifts Employee B a suggestive piece of clothing or toy. Employee A meant it as a joke. Employee B is highly embarrassed and reports the incident to human resources. Does this mean gift exchanges should be prohibited at holiday parties? Not at all, but you should be on the look-out for inappropriate conduct, and be ready to quickly take corrective action.
Tips for Preventing Sexual Harassment at the Holiday Party:

- Remind supervisors that the same workplace rules prohibiting harassment and discrimination are still in play at the holiday party, and to watch for inappropriate conduct.
- Consider allowing employees to bring their spouse/significant other to the holiday party.
- Send out a reminder in the weeks leading up to the holiday party regarding your employee handbook. Let employees know how they can get a copy of the handbook, and where to go if they have any questions or concerns.
- If there is a gift exchange, remind employees that gifts may not contain sexual or vulgar content.
- Skip the mistletoe!
- And as always, take complaints of harassment seriously and be proactive. Even if you do not hear the words “sexual harassment” and “complaint,” take steps to ensure behavior that may be considered harassment is prevented and corrected.

Alcohol

Relax, it’s okay to have alcohol at the office holiday party. Most companies do. Companies simply need to keep in mind that alcohol affects the way people act. In large quantities alcohol can really affect the way people act, and is usually a factor when an employee gets too friendly and says or does something inappropriate. A little extra planning up front and taking a few precautions will greatly reduce the chances the office holiday party gets out of hand and/or someone does something inappropriate.

Consider the following:

- Prior to the holiday party or as employees arrive, hand out two or three drink tickets to each person to prevent anyone from over indulging.
- Hire professional bartenders since they are trained to serve alcohol responsibly.
- Have food available to slow the rate at which alcohol is absorbed.
- Have non-alcoholic drinks available so employees do not feel compelled to have an alcoholic drink in their hand throughout the entire event.
• Have someone on the look-out for employees leaving the party that appear intoxicated and find out how they are getting home. By having alcohol at a company-sponsored event, the company might be liable for an accident involving an intoxicated employee leaving the party.

Other Important Topics and Considerations

In addition to preventing sexual harassment, there are several other important considerations to keep in mind when planning the office holiday party. For example, religious discrimination issues can arise if attendance at the company’s holiday party is mandatory and portions of the event involve religious readings or prayer. On a similar note, requiring employee attendance or strongly encouraging it may implicate wage and hour laws, requiring that employees be paid for their time.

When planning a holiday party, keep these suggestions in mind:

• Do not make attendance mandatory, or give employees the impression that attendance is mandatory i.e. strongly encouraged. It’s a party. People will show up.

• The way management acts at the party will set the bar for everyone else. If management is dancing on tables with a drink in each hand, chances are employees will follow suit.

• Let supervisors know the same workplace rules prohibiting harassment and discrimination are still in play at the holiday party, and to watch for inappropriate conduct.

• It is good practice for companies to review and revise their employee handbooks at least once a year. Reviewing and communicating the revised employee handbook each year prior to the holidays is a great way to: (1) ensure the handbook is effective and complies with changes in the law, and (2) reminds employees the handbook is available, which ideally instructs employees on how to report misconduct in the workplace. All too often, employees claim they did not know how to report inappropriate conduct.

A holiday party is a great way to bring employees together and celebrate. Simply remember that a company’s obligation to provide a safe work environment free from harassment and discrimination extends to a corporate-sponsored holiday party. And please, skip the mistletoe.
version released March 2, 2016, including the narrowed purpose of establishing “standards for data security and standards for the investigation of and notification to the Commissioner of a Cybersecurity Event applicable to Licensees…” The Model applies to all licensees, defined as individuals or non-governmental entities required to be authorized, registered, or licensed pursuant to a state’s insurance laws. Exceptions were made for a purchasing group or risk retention group chartered and licensed in another state, and for an assuming insurer domiciled in another state.

Information Security Program

The Model requires that all licensees develop, implement, and maintain a comprehensive written information security program (ISP). The ISP should be based on an individual risk assessment and be commensurate with the licensee’s size and complexity, the nature and scope of its activities, and the sensitivity of the nonpublic information used or in the licensee’s possession, custody, or control. The ISP must contain administrative, technical and physical safeguards for the protection of nonpublic information and the licensee’s information system.

Nonpublic information includes information that is not publicly available and covers material business information of the licensee as well as specified personal, financial, and health information concerning a consumer or a family member. The program should cover electronic and non-electronic nonpublic information.

The Model provides for three exceptions from the Section 4 ISP requirements: licensees with fewer than 10 employees (including independent contractors), licensees who certify in writing that they have established and maintain an ISP that meets HIPAA requirements, and a licensee who is an employee, agent, representative, or designee of another licensee, but is covered by that licensee’s ISP as long as that program complies with Section 4.

Board of Directors Oversight

The Model calls for oversight by the board of directors or an appropriate board committee, the designation of a responsible person for the ISP, and continuous cybersecurity awareness training of all personnel. Based on its risk assessment, each licensee must assess which security measures specified in the Model should be implemented. While the Model includes a comprehensive list of measures, examples include access controls, data management, encryption, secure development practices for applications, multi-factor authentication, regular monitoring and testing of systems, and audit trails to detect and respond to cybersecurity events and that are designed to reconstruct material financial transactions. Licensees must also
implement measures to protect against physical loss or damage of nonpublic information and follow secure disposal procedures for nonpublic information whether in paper or electronic format. A licensee must also monitor its program to adjust for changes in technology and must establish a written incident response plan.

**Third Party Service Providers**

Licensees are also required to exercise oversight of third party service providers. The oversight includes proper due diligence in selecting the providers and a provision that the licensee requires third party service providers to implement appropriate administrative, technical, and physical measures to protect and secure the information systems and nonpublic information accessible to, or held by, the third party service provider.

**Cybersecurity Event and Notice**

The Model includes specific requirements for investigation and notification to the applicable commissioner in the case of a cybersecurity event. A cybersecurity event is defined as an event resulting in unauthorized access to, disruption, or misuse of, an information system or information stored on such system. It does not include encrypted information where the key has not been acquired, released, or used, or events where the licensee has determined that the nonpublic information has not been used or released and has been returned or destroyed. Notification to the commissioner of the domicile or home state, and any other state where 250 or more impacted insureds reside, is required within 72 hours from determining a cybersecurity event has occurred. The Model requires that any notice to the commissioner contain 13 categories of specified detailed information concerning the cybersecurity event. Cybersecurity events at third party service providers are also subject to the notice provisions. Notification to affected consumers is governed by the state general data breach notification laws with copies of such notices provided to the commissioner.

**Annual Certification**

A licensee is required to certify to the commissioner annually (no later than February 15) that it is in compliance with the requirements of “Section 4 – Information Security Program,” as well as maintain the materials and documentation used to support the certification for five years.

**Confidentiality**

All documents and information obtained by a commissioner pursuant to the Model are recognized as confidential and privileged; not subject to any applicable state
open records, freedom of information or similar law; not subject to subpoena; and not discoverable or admissible in evidence in any private civil action. The commissioner does have the authority to use such documents and information in a regulatory proceeding or lawsuit brought by the commissioner. In addition, the commissioner may share such information with other state, federal and international regulators and the NAIC and state, federal, and international law enforcement so long as any recipient agrees in writing to maintain the confidentiality and privileged status of the information. The Model specifically states that “no waiver of any applicable privilege or claim of confidentiality in the documents, materials, or information shall occur as a result of disclosure to the Commissioner or the sharing of the information as permitted under the Act.”

After evolving through multiple versions and considering a multitude of comments from the insurance industry and interested parties, Version 6 of the Model significantly tracks New York’s Cybersecurity Regulation2 ("NY Regulation"). Importantly, the Model includes a drafting note indicating that the Cybersecurity WG intends compliance with NY Regulation to satisfy the Model’s requirements. The note states “The drafters of this Act intend that if a Licensee, as defined in Section 3, is in compliance with N.Y. Comp. Codes R. & Regs. tit.23, § 500, Cybersecurity Requirements for Financial Services Companies, effective March 1, 2017, such Licensee is also in compliance with this Act.”

While many industry participants view the inclusion of the NY Regulation concepts as a positive development, there is still industry concern regarding several aspects of the Model, including the complexity of the notice requirements and confidentiality. Many had argued that the confidentiality provisions contained in Section 8 of the NAIC’s Risk Management and Own Risk and Solvency Assessment Model Act3 (ORSA Model Act) should be the standard for confidentiality in the Model, but that approach was rejected.

Endnotes

1  Available at http://www.naic.org/documents/cmte_ex_171024_agenda_materials.pdf. The technical corrections are reflected in the Model redline contained in the Agenda and Materials document created for the October 24, 2017 Executive Committee and Plenary Meeting.
2  Available at: http://dfs.ny.gov/legal/regulations/adoptions/dfsrf500txt.pdf.
in formation of the agreement. One party makes an offer, the other party accepts, and there is consideration (or cause in Louisiana) underlying the transaction. However, in the context of smart contracts, the parties aren’t necessarily practicing offer and acceptance, for they are consenting to a computer platform that outlines the if-then conditions governing the transaction. In the eyes of a court, this by itself may not create a binding agreement, in which case it may be difficult to recover damages.

What Law Governs Smart Contracts?

Last March, Arizona lawmakers amended the Arizona Electronic Transactions Act, which sanctioned the enforceability of agreements with digital signatures to include digital signatures recorded on a blockchain. The law now clearly provides that a signature secured through blockchain is considered to be an electronic signature. Furthermore, a record or contract secured through blockchain is also considered to be in an electronic form and an electronic record. Consequently, parties can seek recourse in the state court system for the breach of a smart contract. While states such as Vermont and Nevada passed laws this year aimed to bring additional clarity to blockchain firms, Arizona remains the only state so far to have cemented the enforceability of smart contracts.

Jurisdiction: Is the Area of Jurisdiction Clearly Defined?

Another potential problem for smart contracts results from blockchain’s decentralized transaction system, for where the contract became final and binding can be difficult to determine. Theoretically, courts might find that parties can sue wherever validation of the transaction takes place; however, with millions validating transactions all over the country, parties could potentially be sued anywhere. This issue only emphasizes the need for a forum selection clause. A forum selection clause requires the parties agree to resolve any disputes in one particular jurisdiction. Although such clauses are usually a spot of contention as each party wants their own city as the jurisdiction selected, they decrease the risk of having to litigate in an unfamiliar or inconvenient jurisdiction. The existence of blockchain also heightens the importance of enforceability as having a court invalidate the clause potentially exposes a party to a lawsuit in the place of the opposing party’s choosing.

Do Smart Contracts Have a Clear Dispute Resolution Mechanism?

If the smart contract is silent, the parties will be required to resolve any issues in state or federal court, which is often an expensive and lengthy process. If the parties add a dispute resolution clause, they can instead resolve their disputes in front of an arbitrator. Thus, parties should be sure to establish consent to arbitration. This may
be an issue in circumstances where the smart contract is entered into by a computer, is in code and/or and does not create legally binding contractual obligations under the applicable law.

Similarly, the parties should ensure that the arbitrator has some knowledge and experience with blockchain technology. Many judges, attorneys and full time mediators and arbitrators today are not familiar with this technology, much less conversant in the ins-and-outs of program complexities. Including a dispute resolution clause requiring that the arbitrator have some blockchain experience may be a benefit to both sides. Also, parties should consider having a tribunal familiar with the technology against the importance of having the dispute decided by experienced contract lawyers. There is likely to be relatively little overlap between the two, so requiring both skill sets risks restricting the pool of potential arbitrators to such an extent that the arbitration agreement becomes unworkable.

Lastly, given the distributed nature of blockchain and the operation of smart contracts, it is important to avoid satellite disputes about the applicable forum and/or procedural law. Parties should check that the law of the chosen forum does not render a smart contract illegal or unenforceable, that the disputes likely to arise are arbitrable (in some jurisdictions for example, intellectual property disputes are not arbitrable), and that the codified arbitration agreement in question will be upheld and enforced by the courts.

Smart contracts may be the future of transactions. However, the technology is in its infancy and has not been thoroughly examined by state or federal courts. The challenges sure to be faced by corporate counsel whose employers and clients move quickly to adopt blockchain as their preferred method of doing business are not entirely novel. However, the nuances and new aspects of those challenges in a smart contract world are what seem to pose the biggest challenge. Sound, adaptive legal strategies for managing those nuances and challenges will hopefully help to make the impact of smart contracts and blockchain on the corporate counsel community a positive rather than a negative.
example often sought in discovery is electronic communications, such as e-mail. The rule covers—either as documents or as electronically stored information—information “stored in any medium,” to encompass future developments in computer technology.”

See Committee Note on Rule—2006 Amendment.

The 2015 amendments have again changed the Rule to address technology’s effect on discovery. Federal Rule of Civil Procedure 34 now reads:

(a) In General. A party may serve on any other party a request within the scope of Rule 26(b):

(1) to produce and permit the requesting party or its representative to inspect, copy, test, or sample the following items in the responding party’s possession, custody, or control:

(A) any designated documents or electronically stored information—including writings, drawings, graphs, charts, photographs, sound recordings, images, and other data or data compilations—stored in any medium from which information can be obtained either directly or, if necessary, after translation by the responding party into a reasonably usable form[.]

Fed. R. Civ. Proc. 34(a)(1)(A). Counsel propounding e-discovery requests “must describe with reasonable particularity each item or category of items to be inspected,” and “may specify the form or forms in which electronically stored information is to be produced.” Id. at 34(b)(1)(A)(C). The producing party should object to any e-discovery requests that fail to satisfy the “reasonable particularity standard” of paragraph (A). See id. at 34(b)(2)(C). The producing party can also object to the form in which ESI will be produced. Id. at 34(b)(2)(D). The Rule also addresses how ESI will be produced:

(E) Producing the Documents or Electronically Stored Information. Unless otherwise stipulated or ordered by the court, these procedures apply to producing documents or electronically stored information:

(i) A party must produce documents as they are kept in the usual course of business or must organize and label them to correspond to the categories in the request;

(ii) If a request does not specify a form for producing electronically stored information, a party must produce it in a form or forms in
which it is ordinarily maintained or in a reasonably usable form or
forms; and

(iii) A party need not produce the same electronically stored
information in more than one form.

_id. at 34(b)(2)(E).

The 2015 amendments attempt to remove discovery roadblocks objections to be
documents are being withheld based on the objection, _Fed. R. Civ. Proc. 34(b)(2)
(C)_. The amendments also advise counsel to identify the category of documents
being withheld from production based on an objection that the request is overbroad,
and compels them to produce documents in response to the part of the individual
document request that is not overbroad. See Committee Notes on Rule—2015
Amendment.

With the requirement that e-discovery requests be specifically tailored to the case,
_Rule 26(b)(1)_ imposes a proportionality requirement. _Fed. R. Civ. Proc. 26(B)(1)_.

(1) Scope in General. Unless otherwise limited by court order, the scope
of discovery is as follows: Parties may obtain discovery regarding any
non-privileged matter that is relevant to any party’s claim or defense
and proportional to the needs of the case, considering the importance
of the issues at stake in the action, the amount in controversy, the
parties’ relative access to relevant information, the parties’ resources,
the importance of the discovery in resolving the issues, and whether
the burden or expense of the proposed discovery outweighs its
likely benefit. Information within this scope of discovery need not be
admissible in evidence to be discoverable.

Proportionality levels the playing field in many cases and in others places the cost
of e-discovery more fairly on the party requesting the production of wide-ranging
categories of ESI.

The most significant amendment is 37(e)—Sanctions. The 2015 amendment
replaced section 37(e) in its entirety and applies exclusively to ESI. The 2006 version
of section 37(e) contained a “safe harbor” provision that protected a company from
sanctions if electronically-stored material was lost through “the routine, good-faith
now reads:
(e) Failure to Preserve Electronically Stored Information. If electronically stored information that should have been preserved in the anticipation or conduct of litigation is lost because a party failed to take reasonable steps to preserve it, and it cannot be restored or replaced through additional discovery, the court:

(1) upon finding prejudice to another party from loss of the information, may order measures no greater than necessary to cure the prejudice; or

(2) only upon finding that the party acted with the intent to deprive another party of the information's use in the litigation may:

(A) presume that the lost information was unfavorable to the party;

(B) instruct the jury that it may or must presume the information was unfavorable to the party; or

(C) dismiss the action or enter a default judgment.


Lawyers' e-discovery obligations go beyond familiarity with the federal and local rules of civil procedure. The 2012 Amendments to the ABA Model Rules of Professional Conduct reflect a lawyer's duty to embrace and understand evolving technology. Rule 1.1, Competence, provides that, “[a] lawyer shall provide competent representation to a client. Competent representation requires the legal knowledge, skill, thoroughness and preparation reasonably necessary for the representation.” ABA Model Rules of Professional Conduct, 1.1. Comment 8 to the 2012 Amendments—Maintaining Competence—highlights a lawyer's duty to understand technology: “To maintain the requisite knowledge and skill, a lawyer should keep abreast of changes in the law and its practice, including the benefits and risks associated with relevant technology, engage in continuing study and education and comply with all continuing legal education requirements to which the lawyer is subject.” Id. at comment 8 (emphasis supplied).

The impact of technology has reached the state level as state ethical guidelines impose similar obligations. See New York State Bar Association 2015 Guidelines (“A lawyer cannot be competent absent a working knowledge of the benefits and risks associated with the use of social media.”). Further, New York requires lawyers to “keep abreast of the benefits and risks associated with technology the lawyer uses to provide services to clients or to store or transmit confidential information.”
Comment [8] to New York Rule of Professional Conduct 1.1. New York has also written into the Rules these definitions:

“Computer-accessed communication” means any communication made by or on behalf of a lawyer or law firm that is disseminated through the use of a computer or related electronic device, including, but not limited to, web sites, weblogs, search engines, electronic mail, banner advertisements, pop-up and pop-under advertisements, chat rooms, list servers, instant messaging, or other internet presences, and any attachments or links related thereto.

New York Rules of Professional Conduct, Rule 1.0(c). 23 states have adopted ABA Comment 8 to Rule 1.1.¹

Ethical obligations have increased with the prevalence of data privacy issues. Rule 1.6, Confidentiality of Information, now requires a lawyer to “make reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client.” ABA Model Rules, 1.6(c). A lawyer’s ethical obligations to maintain the confidentiality of a client’s data is tied to Rule 1.1. Comment 16 to 2012 Amendments to ABA Model Rules of Professional Conduct (“A lawyer must act competently to safeguard information relating to the representation of a client against unauthorized access by third parties and against inadvertent or unauthorized disclosure by the lawyer or other persons who are participating in the representation of the client or who are subject to the lawyer’s supervision.”).

21st Century data privacy concerns are evident in the amendments to the Model Rules:

A client may require the lawyer to implement special security measures not required by this Rule or may give informed consent to forgo security measures that would otherwise be required by this Rule. Whether a lawyer may be required to take additional steps to safeguard a client's information in order to comply with other law, such as state and federal laws that govern data privacy or that impose notification requirements upon the loss of, or unauthorized access to, electronic information, is beyond the scope of these Rules.

Comment 16 to 2012 Amendments to ABA Model Rules of Professional Conduct.
B. Litigation Methods.

A critical component of a document retention policy is a “document hold” or “litigation hold” procedure. Once a company “reasonably anticipates” that a legal action or investigation is threatened, contemplated, or underway, the company must draft and disseminate a litigation hold letter to advise employees to preserve documents and suspend document destruction policies. When a legal action is “reasonably anticipated” is a difficult question for many companies. Does a trucking company have to issue a legal hold every time one of its drivers is involved in a fender bender? Probably not. If the motor vehicle collision results in serious injury or death, a legal hold letter should be disseminated. Does a company have to issue a legal hold every time it terminates an employee? Probably not. When the employee resigned and alleged mistreatment and discrimination, probably. A legal procedure or investigation can be reasonably anticipated when a corporation receives a notice of claim, an EEOC Notice of Charge of Discrimination, a complaint, a notice of the filing of an administrative proceeding, a demand letter from a lawyer or some other written or verbal communication that indicates that a suit will or has been filed. The nature of the proceeding will dictate the documents to be preserved, but the company should err on the inclusive side.

Several key elements apply to all litigation hold letters to ensure that employees preserve and do not destroy documents. The letter should be drafted and disseminated immediately after the corporation determines a triggering event has occurred. At the initial phase of the proceeding, the corporation should identify records custodians and advise them of the claim and the categories of documents that must be preserved. Immediacy is crucial because ESI, more so than paper documents, is often destroyed daily as part of automated document destruction policies and during the recycling of backup tapes. A company can face many sanctions—from an adverse inference to the striking of a pleading—if documents are destroyed, even inadvertently. Further, companies may compound the problem created when they fail to distribute a letter at the onset of the proceeding by failing to issue one later in the litigation; even a delinquent litigation hold letter will assist the company in meeting its document preservation and collection obligations.

The company need not send a global litigation hold letter. Instead, employees who possess potentially relevant information and documents must receive it. Records custodians in Human Resources, Research and Development, Operations, Marketing, and Information Technology, will also need to receive litigation hold letters to the extent appropriate.
The letter’s scope, tone, and author are important. The letter must explain that the duty to preserve records is important to the company’s litigation position. It should also identify the parties, the relevant dates, where the action is pending, and should convey the serious nature and facts – preferably without too much legalese. The import of the letter is bolstered if the General Counsel signs the letter and copies the Chief Executive Officer.

The letter should expansively define the term “document” and the duties to preserve and not destroy must be explained. The document custodian must be told not to destroy documents, either under the document retention policy or otherwise, even if they believe the documents may hurt the company and they should be reminded of that periodically until the matter is concluded. They should also be told that the company could be hurt just as much (if not more) by obstruction-of-justice and spoliation-of-evidence charges arising out of the destruction of documents than it might be by preserving documents that may hurt the company.

Finally, the letter should instruct that the duty to preserve and collect is ongoing and document destruction policies should be suspended until further notice. Attorney supervision of document collection, especially ESI collection, is imperative because employee-only searches more often destroy responsive documents than preserve them. Management, with the assistance of IT personnel, should periodically follow up with the letter’s recipients to ensure compliance with the employees’ preservation duties and to answer any questions that may arise.


A corporation’s information system policies and practices protect and secure a company’s data, instruct employees on the proper use of technology in the workplace, and provide a competitive advantage in the marketplace. Information technology (“IT”) departments develop the policies with the human resources, operations and legal departments. Like technology, information system policies are not static, and changes to technology require IT departments to review and revise the policies periodically to meet the business’s needs.

Companies typically tailor information policies to their business but the following general categories exist:

• Acceptable use policy
• Password policy
• Backup policy
• Confidential data policy
• E-mail use policy
• Document retention policy
• Mobile device/personal device/bring your own device to work policy
• Remote access policy

“Acceptable Use” policies, which establish the acceptable uses of company-owned technology, set the tone for employee computer use in the workplace. The policy should apply to all devices the employee uses to conduct company business including company computers, smartphones, cameras, networking equipment, and software, and to all uses of the technology, such as e-mail, texting, and instant messaging. Employees retain certain rights and freedoms when using company-owned technology—using e-mail to engage in labor practices protected by the National Labor Relations Act and other federal and state laws—and the policy must advise them that despite these rights company technology must be used for business purposes only. The acceptable use policy can contain password or e-mail policies, or they can be stand-alone policies.

Some businesses are required by law to implement policies and practice. For example, medical professionals must devise practices consistent with the Health Insurance Portability and Accountability Act and financial institutions must implement procedures to comply with Sarbanes Oxley and the Gramm-Leach-Bliley Acts.

Recent hurricanes underscore a need for business continuity and disaster recovery plans. What happens when the lights go out? Where is the back-up data stored? Is it secured? How quickly can employees gain access to data and get back on-line. Disaster recovery plans cover these situations.

Bring Your Own Device (“BYOD”) policies are critical to companies that allow employees to utilize their personal mobile devices for work purposes. The policy should identify the employees/positions allowed to use their own device at work, the need for IT approval of the device and the device’s compatibility with the company’s IT systems as a condition precedent to use of the device. The IT Department must install virus protection software on the device, and that the employee bears the risk for lost data. The employer also should be sensitive to wage and hour issues if the employee is an hourly employee. Last, the employee should acknowledge the conditions of use through a signed user agreement.

A document retention/destruction policy outlines how long documents—both paper and electronically stored—are kept before they can be destroyed. Federal and state law requirements and business and litigation needs dictate how long certain types of documents, such as tax, human resources, insurance and benefits information,
construction drawings, customer contracts, settlement agreements, and deposition transcripts must be kept. Historical corporate documents, such as by-laws, articles of incorporations, and asset purchase agreements should be kept indefinitely. Consistency is key—follow the policy’s destruction deadlines to avoid claims that documents were destroyed during pending litigation.

D. Preparing for the Rule 26(f) or Initial Scheduling Conference.

The Federal Rule 26(f) conference and initial scheduling conference are counsel’s first (and most important) opportunities to impress upon opposing counsel and the court the scope and magnitude of e-discovery issues in the case. These opportunities should not be wasted. The plaintiff should outline the affirmative e-discovery sought from the employer—personnel files, employment records, document retention policies, names of records custodians—while the employer should explain the company’s document retention and production capabilities, and cost issues. Preparation for the Rule 26(f) conference cannot wait, and should start when the client retains counsel to pursue or defend the claim.

Counsel should not delay discussing e-discovery capability issues with the client because the federal rules impose strict discovery deadlines on counsel. Rule 26(f) is very specific—“the parties must confer as soon as practicable—and in any event at least 21 days before a scheduling conference is to be held or a scheduling order is due under Rule 16(b).” Fed. R. Civ. Proc. 26(f)(1). An effective Rule 26(f) conference results from a counsel-client working relationship focused on understanding a client’s ESI capabilities, however limited they may be. A lawyer’s e-discovery pre-conference strategy should include the following:

1) Preparing for the initial conference means becoming educated on a client’s computer systems, document retrieval capabilities and retention policies. Counsel should meet or set aside time to discuss e-discovery issues with the client, even if lawyer and client initially do not think ESI will play a role in the case. Separate time must be set aside because the potential pitfalls of e-discovery, especially its costs, must be addressed before the issues arise. For plaintiffs’ counsel, the meeting may only concern the client’s personal computer, information stored on the work computer, and social media. However, the prevalence of smartphones, a plaintiff’s smartphone use, especially company-owned smartphones, should be discussed.

2) The defense lawyer will likely have a greater learning curve than plaintiff’s counsel to prepare for the conference given the size, nature and location of the employer’s ESI and records custodians; employer
defendants are naturally the logical target of electronic discovery requests. Typically, employers’ counsel must explain the employer’s electronic document capabilities at the initial scheduling conference, so the meeting should take place well before the conference and Rule 26(f) meet and confer.

3) In appropriate cases, lawyer and client should give immediate thought to assembling an e-discovery team. Often in-house counsel do not have the time or qualifications to be the front persons for outside counsel’s investigation of the client’s technology capabilities. Other company employees, such as the director of information technology or similar position, can facilitate the collection and production of ESI and explain the company’s document retention policy, preservation protocols, databases, servers, computers (desk and laptop), back-up tapes, disaster protocols, social media, and personal devices such as smartphones, cameras, laptops etc. The team also will identify records custodians and implement a legal hold (if not already distributed) to the custodians to preserve records. Third-party IT team members, including a representative from the lawyer’s firm’s IT department, may have to be recruited to facilitate the lawyer’s e-discovery learning curve and the ultimate production of documents; third-party IT consultants may take on a larger role for smaller clients that have no dedicated IT staff, or in cases involving large quantities of ESI.

4) The lawyer, whether plaintiff or defendant, must know the client. Not all cases and clients are created equal—not every employment lawsuit is against a Fortune 50 company. Not every defendant has sophisticated back-up systems, IT departments, databases, and document retention policies. The outside lawyer must be sensitive to these issues when working with the client. The lawyer should not discount a client’s technology capabilities if they appear “primitive” compared to recent advances in technology and computer systems. Rather, this issue should be front and center to all e-discovery discussions at the “meet and confer” and initial scheduling conference. Outside counsel should be candid with opposing counsel and the court about the client’s capability to respond to electronic discovery requests under Federal Rule of Civil Procedure 34. Finally, aggressive plaintiffs’ counsel will demand and pressure defendants at the conference on e-discovery
issues. Defense counsel must be prepared, and, if that means bringing an IT person to the conference or allowing a technology savvy associate to handle the e-discovery discussions then do so.

E. Preparing Requests and Responding to Discovery Requests Involving Electronic Data.

Depending on the case, e-discovery can be very expensive. Individual restrictive covenant and discrimination cases might be more paper intensive than a collective action under the FLSA, for example, which requires the production of electronically stored accounting and payroll records. No matter the case, certain factors govern how to prepare and respond to e-discovery requests.


With the amendment to Rule 26(b)(1), lawyers in federal court must draft discovery understanding that courts will balance the burden of e-discovery to make sure the requests are proportional to the case. In Noble Roman’s, Inc. v. Hattenhauer Distributing Company, 314 F.R.D. 304 (S.D. Ind. 2016), the court ruled that defendant’s “wide-ranging” discovery requests, including seeking documents about every aspect of the plaintiff’s business operations, was nothing more than a fishing expedition and “outside the proper bounds of discovery.” Id. at 311. The court noted that the proportionality requirement of Rule 26(b)(1) protects litigants from burdensome and far-reaching discovery, describing defendant’s discovery requests as “discovery run amok.” Id. at 311. The decision serves as a guide to drafting discovery requests:

Hattenhauer beats the drum of “relevancy.” It asserts that all of its deposition topics and document requests are “relevant.” That’s not good enough. Hattenhauer never attempts to demonstrate that the discovery is in any way proportional to the needs of this case, considering such things as the amount in controversy, the importance of the information in resolving contested issues, whether the burden of the discovery outweighs its likely benefits, whether the information can be obtained
from other and more convenient sources, or whether the information is cumulative to other discovery Hattenhauer has obtained.

Id. at 311. The discovery requests must be specifically tailored to the facts that are not only relevant to the dispute but proportionally relevant to the dispute. $100,000 in e-discovery productions expenses should not be spent on a $50,000 case. See id. Amended 26(b)(1) reinforces court management over discovery so counsel should follow the dictates of the amendment when drafting e-discovery requests. If counsel knows the case before drafting discovery, it will be easier to tailor specific requests that avoid costly fishing expeditions.

“Knowledge is power.” A lawyer must know where the documents are to draft concise and specific e-discovery requests. Relying on the client (both plaintiff and defendant) or former employees allows counsel to understand the computer systems used, storage locations, and destruction/retention policies. Further, with a working knowledge of the client’s computer systems, counsel can better manage any e-discovery issues that may arise with the court and opposing counsel.

Responding to e-discovery requests is no easy task and requires a team effort. Just like preparing for the initial conferences, counsel must communicate with client and client personnel to understand the systems, documents created and storage locations, how information is preserved, and the potential cost to produce it. Those factors all impact how counsel can respond to e-discovery requests.

When drafting responses remember that the Federal Rules demand specificity—so challenge those requests that are not and seek a protective order if necessary. Further, request follow-up conferences with the magistrate if e-discovery issues become unmanageable or unduly burdensome. E-discovery can overwhelm but it is manageable.

Endnotes
2 A portion of this section is an excerpt from FDLI Monograph Series, The New Reality of Sales Force Behavior and Management, Vol. 2, Number 6 (June 2011), and is used with permission.
4 Zubulake v. UBS Warburg LLC, 229 F.R.D. 422 (S.D.N.Y. 2004) (Zubulake V) (issuance of litigation hold letter is the beginning, not the end, of the company’s e-discovery duties).
5 See Pension Committee, 685 F. Supp. 2d at 471.
of accomplishment is remarkable. I knew I wanted to be a part of his effort to turn around Florida’s economy, and I am proud of what we achieved. The decision to leave government was hard, but coming in-house has allowed me to partner with the business and work to advance an important mission—the protection of our company—in a manner that replicates much of what I enjoyed about being in government.

**What was the biggest surprise or change in the way you did things when transitioning from government to in-house at Marsh, and then later at Marsh?**

When you are on the outside of a big company, you think that simply giving legal advice or writing a new policy is the solution. But when you come in-house, you realize that that’s not the answer—that’s the first step. The real work is turning legal advice into actionable guidelines and incorporating them into the company’s operations. Writing the policy may get points on the board, but it’s not a win.

**What are the challenges that you and your department face that are similar to those you faced in private practice?**

Keeping it simple. It takes tremendous discipline as lawyers because we are trained to care about the details. But in order to produce usable material, we must reduce complex content to short, readable guidance that doesn’t require a law degree to understand.

**What skills did you develop as a young lawyer in private service that have served you well in your current position at Marsh?**

Effective writing. When it comes to briefing executives, you have thirty seconds to grab their attention. Simple, clear writing is key.

**How have your experiences, from working in private practice, government, and now in-house, changed the way you view the practice of law?**

Too often, legal advice is not delivered with an eye towards operationalization. When we are seeking guidance on a regulation we have to comply with, we often get an almost academic response. It may be easier to give that type of advice because it doesn’t require understanding the intricacies of the client’s business. But effective legal advice is built upon a foundation of understanding our business and our risk profile.

**Through your experience in private practice and now at Marsh, what changes have you seen in the way outside and in-house counsel work together?**
The legal services space is getting more crowded. We work with companies that supply lawyers on a staff-augmentation basis. We get a lawyer dedicated to the company, who invests in learning the business. Another change is the emphasis we have placed on cybersecurity, whether that’s requiring our law firms to have multifactor authentication or to encrypt data-at-rest. We are adamant about the cybersecurity of the law firms we work with.

**What advice would you have for those who desire to obtain an in-house position with a Fortune 500 Company?**

Take an interest in a particular industry. Learn about the legal challenges facing that industry and make yourself an expert. Often, the best in-house positions are filled through referrals, so relationships are crucial.

---

**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!

- 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

[https://www.americanbar.org/diversity-portal/SpeakersDirectors.html](https://www.americanbar.org/diversity-portal/SpeakersDirectors.html)
<table>
<thead>
<tr>
<th>Date</th>
<th>Event</th>
<th>Contact Details</th>
<th>Location</th>
</tr>
</thead>
<tbody>
<tr>
<td>April 5-6, 2018</td>
<td>Motor Vehicle Products Liability Conference</td>
<td>Felisha A. Stewart – 312/988-5672</td>
<td>Arizona Biltmore Resort &amp; Spa Phoenix, AZ</td>
</tr>
<tr>
<td>April 6-7, 2018</td>
<td>Toxic Torts &amp; Environmental Law Conference</td>
<td>Felisha A. Stewart – 312/988-5672</td>
<td>Arizona Biltmore Resort &amp; Spa Phoenix, AZ</td>
</tr>
<tr>
<td>April 9, 2018</td>
<td>TIPS Free Member Monday CLE</td>
<td>Ninah Moore – 312/988-5498</td>
<td>Arizona Biltmore Resort &amp; Spa Phoenix, AZ</td>
</tr>
<tr>
<td>April 14-18, 2018</td>
<td>TIPS National Trial Academy</td>
<td>Donald Quarles – 312/988-5708</td>
<td>Peppermill Resort &amp; Spa Casino Reno, NV</td>
</tr>
<tr>
<td>April 14-18, 2018</td>
<td>TIPS Section Conference</td>
<td>Felisha A. Stewart – 312/988-5672</td>
<td>Loews Hotel Hollywood Los Angeles, CA</td>
</tr>
<tr>
<td>May 2-6, 2018</td>
<td>Fidelity &amp; Surety Law Spring Conference</td>
<td>Donald Quarles – 312/988-5708</td>
<td>La Fonda on the Plaza Santa Fe, NM</td>
</tr>
<tr>
<td>June 11, 2018</td>
<td>TIPS Free Member Monday CLE</td>
<td>Ninah Moore – 312/988-5498</td>
<td>Arizona Biltmore Resort &amp; Spa Phoenix, AZ</td>
</tr>
<tr>
<td>August 2-5, 2018</td>
<td>ABA Annual Meeting</td>
<td>Felisha A. Stewart – 312/988-5672</td>
<td>Swissotel Chicago Chicago, IL</td>
</tr>
<tr>
<td>October 10-14, 2018</td>
<td>TIPS Fall Leadership Meeting</td>
<td>Felisha A. Stewart – 312/988-5672</td>
<td>Ritz Carlton Amelia Island Amelia Island, FL</td>
</tr>
</tbody>
</table>

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.