Survey: Public Is Unprepared For Natural Disasters; & Unaware Or Unconcerned About Floods & Flood Insurance

The year 2017 was the worst in the number of natural disasters, and costliest, especially in the area of floods and flood insurance. And then came Hurricane Florence and Hurricane Michael in 2018, causing even more death, destruction, and insurance claims.

According to a recent survey conducted by Belfor Property Restoration in 2017, and released on September 10, 2008: in support of preparedness month recognized every September:

- Two thirds of American homeowners are unprepared in the event of a disaster
- 60% have not created a disaster preparedness plan.
Nearly 80% had no preparedness plan because they never thought about it, or people said they didn’t know how to do it, or not having enough time to do it.

40% did not know what items they should pack in the event of emergency; for those who did know, it was: food, water, & flashlight.

Most surprising was finding that only 8% were most concerned about flooding, and only 7% most concerned with hurricanes [according to Belfor, the 2017 hurricanes reached $283 billion in damages in the US.]

According to Belfor, the 2017 hurricanes reached to $283 billion in damages in the United States. Yet only 8% were concerned about flooding and only 7% most concerned with hurricanes.

Source: courtesy of New York Law Journal, and Belfor Property Restoration Newsletter September 10, 2018
Member Roster

**Chair**
Caroline Ruppert
Winestead PC
401 Congress Ave, Ste 2100
Austin, TX 78701-3798
(512) 370-2850
Fax: (512) 370-2850
cruppert@ifaw.org

**Chair-Elect**
Timothy Penn
Travelers
PO Box 213031
Hartford, CT 06123-1031
(860) 277-8345
Fax: (860) 277-8345
tpenn@travelers.com

**Representative**
Daina Bray
Winestead PC
401 Congress Ave, Ste 2100
Austin, TX 78701-3798
(512) 370-2850
dbray@ifaw.org

**Vice-Chairs**

**Scope Liaison**
Sandra Boyer
LEGUS Law Inc
151 N Franklin St, 11th Floor
Chicago, IL 60606
(312) 822-5267
maryjane.kowert@cna.com

**Young Lawyer Representative**
Mary Jane Kowert
CNA
151 N Franklin St, 11th Floor
Chicago, IL 60606
(312) 822-5267
maryjane.kowert@cna.com

**Immediate Past Chair**
Ronnie Johnson
McGlincey Stafford PLLC
301 Main St, 14th Fl
Baton Rouge, LA 70801-1411
(225) 382-3620
Fax: (225) 612-7065
rjohnson@mcglincey.com

**Diversity Vice-Chair, Membership Vice-Chair**
Kathleen Wharton
309 John Ave
McHenry, IL 60050-6913
(847) 407-3470
kathleenwharton@comcast.net

**Technology Vice-Chair**
Gregory Lestini
Bricker & Eckler LLP
100 S 3rd St
Columbus, OH 43215-4291
(614) 227-2390
Fax: (614) 227-2390

**Council Representative**
Daina Bray
Winestead PC
401 Congress Ave, Ste 2100
Austin, TX 78701-3798
(512) 370-2850
dbray@ifaw.org

Sue Carol Greene-Buckner
Prudential Financial Inc
80 Livingston Ave
Roseland, NJ 07068-1796
(973) 548-6215
suecarol.greenebuckner@prudential.com

Tracey Haley
Zurich North America
5932 Janet Court
Westlake, TX 76262-9603
(682) 237-2157
Fax: (800) 329-6105
tracey.haley@zurichna.com

Leo Jordan
1210 Midwest Ln
Wheaton, IL 60189-7382
(630) 480-2391
leojordan@dr.cc

Juanita Luis
175 County Road B2 E, Apt 201
Little Canada, MN 55117-1513
(651) 483-2583
Fax: (651) 979-7810
nluis@comcast.net

Anthony Macaulay
514 S Arroyo Blvd
Pasadena, CA 91105
(626) 840-3655
amacaulay@ttlaw.us

Helen Michael
Kalipatrick Townsend & Stockton LLP
607 14th St NW, Ste 900
Washington, DC 20005-2019
(202) 508-5866
Fax: (202) 585-0037
hmichael@kalipatricktownsend.com

Hilary Rowen
New York Dept of Financial Services
1 State St
New York, NY 10004-1561
(212) 480-2262
Fax: (212) 709-1655
alan.rachlin@dfs.ny.gov

Randolph Scott
57 Hayden Dr
Cincinnati, OH 45218
(832) 428-0699
rascott87@gmail.com

Francine Semaya
33 Dakaria Dr
Middletown, DE 19731
(302) 241-8090
Fax: (302) 708-5515
francesemaya@gmail.com

Jeffrey Thomas
Univ of Missouri KC School of Law
500 E 52nd St
Kansas City, MO 64110-2467
(816) 235-1644
Fax: (816) 235-5276
thomasj@umkc.edu

Mary Cannon Veed
Mary Cannon Veed & Associates
838 S Garfield St
Hinsdale, IL 60521
(630) 222-4030
Fax: (312) 876-6237
mccvi@veedlaw.com

Paige Waters
Locke Lord LLP
111 S Wacker Dr, Ste 4400
Chicago, IL 60606-4409
(312) 440-3815
Fax: (312) 443-1815
pwaters@lockelord.com

James Wynn
FTI Consulting
Three Times Square
New York, NY 10036
(212) 841-9366
Fax: (212) 841-9366
jim.wynn@fticonsulting.com

Z Jozefszniski
American Insurance Association
555 12th St NW, Ste 5
Washington, DC 20004-1211
(202) 828-7175
Fax: (202) 828-7175
szielesznski@aiadc.org
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
Chair Message

2018-2019 Exciting Programs And Events On Tap

Welcome to the 2018-2019 Bar Year! We have a lot of programs and events on tap and are looking forward to another exciting year for the ABA TIPS Insurance Regulation Committee (IRC).

Our committee consists of approximately 350 member attorneys from all across the country, with a long and distinguished history of leadership in insurance regulation. Our diverse and active membership has been active for decades in the all-important area of regulation of the insurance industry as it transitions into a new area of modernization.

The IRC’s goal is to stay on top of the many important changes in regulation of the insurance industry, at the state, federal, and international levels. The IRC also helps educate our colleagues about the impact insurance regulation has on their practice, and the impact insurance regulation has on business and the public in general. For instance, President Trump’s executive order and his administration’s subsequent rule, expanding the role of association health plans has sent ripples throughout the insurance industry. The rule is designed to make it easier for small businesses and the self-employed to band together based on a common industry or location to buy health insurance at a lower cost, but it also allows these groups to bypass many of the consumer protection regulations imposed by the Affordable Care Act. It will be interesting to see the true impact this order will have on the future of health care.

Our members are encouraged to follow issues such as this, and to write articles for ABA publications, including The Brief, TortSource, the Tort and Insurance Law Journal, and this, our updated Insurance Regulation Committee Newsletter. There are also many speaking opportunities, as our committee is often asked to participate in CLE programming sponsored by TIPS or other ABA groups. There are numerous other opportunities for members to get involved as well.

In January 2019, IRC will once again co-sponsor the Insurance & Employee Benefits Midwinter Symposium in Coral Gables, Florida, which will take place January 17-19, 2019. We will host a panel on Long-Term Care, present an update on the role technology has on the insurance industry in an InsureTech/Big Data panel, and participate in a discussion on what the regulatory and legislative landscape will look like after the November 2018 Midterms. And, back by popular demand, IRC will host a roundtable discussion with former Insurance

The IRC has approximately 350 members. The IRC’s goal is to stay on top of important changes in regulation of the insurance industry; and to educate colleagues, business and the public on the impact of insurance regulations
Commissioners, who will address hot topics and recent developments in insurance regulation. There will be an opportunity to earn a substantial amount of CLE credits at this Midwinter Symposium.

In addition to these exciting programs, IRC continues to hold monthly conference calls, both to discuss substantive regulatory updates and to conduct our business meetings. The IRC business meetings are held on the second Monday of each month at 4:00 Eastern/3:00 Central. IRC will also conduct four in-person business meetings. Our next in-person meeting is scheduled for Saturday, October 13, 2018 at 1:00 p.m. Eastern, in beautiful Amelia Island, Florida. Since many of our members are also involved with the National Association of Insurance Commissioners (NAIC) meeting, we will host a lunch before the Opening Session at the Fall National Meeting in San Francisco, CA. We will be back in Florida for our third in-person business meeting, which will be held in conjunction with the Midwinter Symposium in Coral Gables in January 2019. Then, from May 1-5, 2019, we will meet at the TIPS Section Conference in Times Square, NY. The 2018-2019 Bar Year will conclude with the 2019 Annual Meeting, which will be held August 8-11 in San Francisco, CA. While we work hard during our business meetings, we also make time to socialize and network with our IRC and ABA colleagues too. We hope you can join us at these fabulous venues.

Don’t Miss The Midwinter Symposium
January 17-19 2019
in Coral Gables, FL
Featuring CLE panels on: Long-Term Care, Technology Update; Future of Insurance Regulation After the Midterms; Former Commissioners’ Roundtable, and other panels of interest.

Also mark your calendar for the TIPS Section Conference in Times Square, New York City, from May 1-5, 2019.
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
After The 2018 Midterms, Here’s Why The Insurance Regulatory Pendulum Will Swing Back To The Center, In An Era Of Political Compromise & Exec Accountability

After the November 6, 2018 mid-term election results were announced, Democrats became the majority party of the U.S. House of Representatives in what many observers called a “blue wave”, effective on January 3, 2019. The Republicans retained control of the Senate. In post 2018, no matter who is in control politically, the future of insurance regulation needs to enter into a period of reconciliation between the left and the right, and a period of compromise between the financial industry and consumers. Most importantly, there needs to be a strong focus on enforcement of executive accountability in business, especially in the financial and insurance industry, something that has been missing for years.

The move to the regulatory center arises out of political and historical necessity. There is no better example of the regulatory compromise climate today, than the saga of Obamacare, and the shift to the middle. In 2017-2018, Republicans took control of the White House and the majority of both houses of Congress. They tried 70 times, unsuccessfully, to carry out President Donald Trump’s 2016 campaign promise to repeal the Patient Protection & Affordable Care Act of 2010 (a.k.a. PPACA, ACA, or Obamacare).

During the years that the ACA has been in effect, the public has grown to support Obamacare and to realize that the initial desire of Republicans to repeal Obamacare, if successful, would have removed, among other things, the insurer’s obligation to provide coverage for people with “pre-existing conditions”.

In the run-up to the midterm elections of 2018, the Democratic party had steadfastly believed that healthcare would be the most important issue for voters. They were right. Poll after poll confirmed that voters saw healthcare as the #1 issue, especially the requirement of insurers to cover pre-existing conditions. As a result, in 2018 Republican politicians who had previously marched in lockstep to President Trump, publicly reversed their position and supported the ACA.

Read more on page 15
Board Oversight and Cybersecurity: Leveraging Corporate Governance to Manage Cyber Threats

Editor’s Note: Reprinted with permission of the authors & from the July 21, 2018 edition of The Legal Intelligencer © 2018 ALM Media Properties, LLC.

Cybersecurity remains one of the biggest concerns facing the insurance industry. While all levels of operation within an organization are responsible for cybersecurity, recent litigation and regulatory action have demonstrated that the ultimate responsibility for enacting a company's cybersecurity rests with the board of directors. Many boards of directors have had to defend themselves against shareholders alleging that the board’s failure to take steps to prevent a data breach violated board members’ fiduciary duty of care. Regulators have also stepped up examinations of companies’ cybersecurity programs, sometimes reminding directors that cybersecurity is not merely a question for IT personnel, but rather a high-priority issue that must be addressed from the top-down. To avoid potential litigation or regulatory action, boards should be proactive and strive to create company-wide cybersecurity protocols and policies that regularly test cybersecurity systems, require training in cyber risk management, establish a data breach response plan, and implement appropriate oversight of third-party service providers.

As noted above, a board’s duty with respect to cybersecurity is generally to oversee the company’s cybersecurity policies, procedures, and strategies, and adequately assess cyber risk, in order to help ensure that appropriate mechanisms have been implemented by management. One oversight strategy is formation of a committee responsible for managing and overseeing the company’s cybersecurity systems and IT personnel. This could be the Committee responsible for overseeing the company’s risk management policies and procedures, such as a Risk Committee (“RC”). Larger companies may consider formation of an independent Cybersecurity Risk Committee (“CRC”) to focus exclusively on cybersecurity, data management, and IT. Whether to form an independent CRC or rely on an existing RC will depend on the size and complexity of the insurer and the sensitivity of the data that the company must safeguard.

The board, through an RC, CRC, or otherwise, should evaluate the company’s data management and IT systems to put in motion strategies to help identify vulnerabilities and weaknesses. This analysis will assist in
ACA Update: Many Groups Seek Repeal Of The 40% “Cadillac Tax” For High-End Employer-Sponsored Health Coverage – Stay Tuned

Editor’s Note: This article was written and submitted before the November 2018 midterm elections.

With H.R. 3798, the “Save American Workers Act of 2018”, The GOP-led House is seeking to impose another one-year delay in the Affordable Care Act’s 40% “Cadillac Tax” for high cost employer-sponsored health coverage until December 31, 2022. The Act also seeks to provide relief from the ACA’s employer mandate for tax years 2015 through 2018. The measure, sponsored by Devin Nunes (R-CA) and Mike Kelly (R-PA) was passed on a party-line vote. As to the ACA, the Act also modifies the ACA’s definition of “full-time employee” from one who is employed on average at least 30 hours of service a week to 40 hours of service per week.

Like the employer mandate and the individual mandate, Congress’ goal as to the Cadillac Tax, and that of many industry groups such as the American Benefits Council, has been its full repeal and they see this one-year delay as a move towards that goal. Unlike the other ACA C provisions, however, the repeal of the Cadillac Tax has garnered bipartisan support in the past. Nonetheless, the problem with this House bill proceeding is that Democrats do not support the other provisions in the bill pertaining to the employer mandate and full-time employee definition. Further, there is concern that the Senate will not take up the bill. Mid-term elections may also effect the measure.

On January 22, 2018, Congress passed and the President signed a two-year delay of the 40 percent excise tax on high-cost employer-sponsored health plans. This delay was part of a short-term federal spending bill and changed the effective date from 2020 to 2022. The tax was delayed once before through the Consolidated Appropriations Act of 2016. Now, Congress seeks to move the date back further. No regulations have ever been issued for the tax but in February and July 2015, the IRS issued notices covering a number of points and requested comments on the possible approaches that could ultimately be incorporated into proposed regulations. While the tax was originally non-tax deductible, the December 2015 changes make it tax deductible for employers who pay it.

The Cadillac Tax was made a part of the ACA so as to reduce tax preferred treatment of employer provided health care as well as reducing excess health care spending.

Read more on page 22
Corporate Governance in Insurance: The EU General Data Protection Regulation and Its Implications for United States Companies

Editor’s note: This article is a condensed version of article by the authors that article first appeared in the Summer 2018 issue of The Demotech Difference, a publication of Demotech, Inc., www.demotech.com. Reprinted with permission.

The protection of personal information remains one of the most significant concerns facing the insurance industry. New and evolving legal and regulatory requirements in the United States and abroad have shaped a new landscape that companies must learn to navigate. The ever-changing legal and regulatory requirements have made it more difficult than ever for companies to maintain a culture of compliance and avoid exposing themselves to regulatory and other legal risk.

Recently, the EU General Data Protection Regulation (GDPR) went into effect. With such a name, it would be easy to conclude that the law governs only the activities of businesses established in the European Union (EU) or European Economic Area (EEA), and that businesses operating or established elsewhere will not be impacted. This is not the case.

Under Article 3(2) of the GDPR, organizations that are not established within the EU or EEA are subject to GDPR when they process personal data of individuals who are in the EU or EEA if the processing activities are related to:

- The offering of goods or services to such individuals in the EU/EEA, even if payment is not required, or
- The monitoring of their behavior, to the extent that their behavior takes place within the EU/EEA. Profiling of individuals based on their use of the Internet is an example of such monitoring.

For U.S. insurers, this could be the case when an insurer is selling policies to cover assets located in the U.S. where the asset owner is established in the EU or EEA. There is no general rule; there have not yet been any case interpreting Article 3(2). Each situation must be evaluated in the full context of the actual activities of a specific business. The GDPR introduces new rules whose interpretation is uncertain at this moment. It is important for insurers to be aware of these new rules, and to evaluate the extent of their legal obligations under the GDPR, if any.
The GDPR imposes on entities that collect, use, store, share or process personal data of individuals in the EU or EEA significant obligations that go well beyond current common practices. For example, there are significant record keeping requirements as well as limitations to data retention.

The GDPR is a lengthy, complex document. Compliance efforts are expected to be commensurate with its complexity. For some businesses, evaluating their practices and conducting all activities that are required to achieve compliance can take several months, and in the case of the largest companies, has taken several years — and will continue over time.

The GDPR drafters have identified a long list of obligations. The document is comprised of 272 provisions that are divided into 173 recitals and 99 articles. Since the document is written in 23 different languages there are also inconsistencies in the interpretation made at the time of the translation. Increasing the confusion and the complexity, several member states have adopted laws or amendments that relate to the GDPR, as permitted by numerous provisions of the GDPR, and those provisions may create new obligations.

The basic Regulation is also supplemented by Guidelines and opinions issued by the EU institutions, or the Member States themselves — about 500 pages at this time. So far, the European Data Protection Board has endorsed 16 guidelines. The Article 29 Working Party ceased its existence at the same time as the GDPR took effect on May 25, 2018. The Supervisory Authorities of Member States have also published guidelines on other relevant GDPR topics.

Nevertheless, it is important to keep in mind that the GDPR is very recent and there is currently little official guidance, and numerous questions. No cases have yet been adjudicated under the GDPR. Until there is more clarity in the interpretation of the GDPR, a cautious approach is recommended. U.S. businesses should educate themselves on the key components of the GDPR and properly evaluate the extent to which the GDPR might apply to their activities.

The GDPR protects the personal data of individuals or natural persons. The term “personal data” is broadly defined as “any information relating to an identified or identifiable natural person (data subject).”

A person is deemed “identifiable” if the person can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number (e.g., a policy number), location data, online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that person. Examples of personal data include name, contact information,
addresses, person characteristics, and can include IP address, location data, or even device information, as well.

Insurers should also be aware that some categories of personal data receive additional protection, and their use is much more restricted than non-sensitive data. Some of these data might be routinely collected as part of some insurance applications, for example in connection with life insurance or health insurance. This data includes, among others: racial or ethnic origin, data concerning healthcare, data concerning a person’s sex life or sexual orientation, and in some cases, genetic and biometric data.

GDPR Art. 5 sets forth six principles governing the processing of personal data:

- Lawfulness, Fairness, Transparency;
- Purpose Limitation;
- Data Minimization;
- Accuracy;
- Storage Limitation; and
- Integrity and Confidentiality.

These six principles are the cornerstone of the GDPR. They must be addressed in any activity conducted, in the collection of personal data, in the design of a product, or in the preparation of a marketing campaign. And much more.

A seventh principle defines a separate requirement for accountability, which makes entities responsible for compliance with the six principles, and requires that they be able to demonstrate compliance with these principles. In addition, entities that collect or process personal information must maintain a record of processing activities under their responsibility, and the record must contain specified information.

It will be critical at all times for organizations to be able to prove, through written records and documented technical, physical and administrative measures that its management and staff understand the GDPR, and that its governance, its lead generation and marketing practices, and its products and services meet the six principles when processing personal data of individuals located in the EU/EEA.

In addition to the numerous disclosure, record keeping, and policy requirements, the GDPR grants data subject numerous rights. The exercise of these rights by any individual requires entities to respond within thirty days, which requires the affected entity to be prepared to act promptly and take the requested action, which may include for example, the correction of data and the provision of a complete file.

The EU GDPR is complex, still being defined. It protects the personal data of individuals and natural persons. U.S. businesses should educate themselves on key components.
Violation of the GDPR exposes an organization to administrative fines of up to EUR 20,000,000, or in the case of an undertaking, up to four percent of the total worldwide annual turnover of the preceding financial year, whichever is higher. In addition, individuals could initiate lawsuits and seek compensation if they have suffered damages because of an infringement of the GDPR.

U.S. businesses are well-advised to audit their processes for the collection and processing of personal data to determine their exposure and compliance needs under the GDPR. To do so, businesses must understand how the entity interacts with personal data of individuals located in the EU, then identify the changes to be made to comply with the GDPR when collecting and processing such personal data.

Organizations will have to adhere to the GDPR if they want to be able to continue doing business with individuals located in the EU/EEA. Individuals and businesses located in the EU/EEA may soon inquire whether your company can demonstrate that it meets the GDPR mandates when collecting, using, sharing or processing personal data of individuals located in the EU/EEA. If you have ignored the GDPR or have been casual in implementing it, and are unable to respond adequately to due diligence questions that will be sent to you, potential customers or investors may take their business to other companies who have made the effort to comply.

Francoise Gilbert, a partner at Greenberg Traurig, is the author of the two volume treatise “Global Privacy and Security Law” (Wolters Kluwer Publishing), covering 68 countries. Her practice has focused on information privacy and security for more than 25 years. Francoise deals regularly with compliance challenges raised by the EU General Data Protection Regulation (GDPR), connected objects, smart cities, big data, mobile applications, wearable devices, social media, data analytics, artificial intelligence, internet of things, autonomous vehicles and other cutting-edge developments. As a practicing attorney, she advises a wide range of entities on the entire spectrum of domestic and international privacy and cyber security issues legal issues.

Fred E. Karlinsky is Co-Chair of Greenberg Traurig’s Insurance Regulatory and Transactions Practice Group. Fred has nearly 25 years of experience representing the interests of insurers, reinsurers and a wide variety of other insurance-related entities on their regulatory, transactional, corporate and governmental affairs matters. Fred is a recognized authority on national insurance regulatory and compliance issues and has taken a leadership position in many insurance trade organizations, has led many industry-driven legislative and regulatory initiatives, and is a sought after thought leader who has spoken and presented to insurance executives and governmental officials, both nationally and internationally.

Christian Brito is a practice group attorney in Greenberg Traurig’s Insurance Regulatory and Transactions Practice Group in Fort Lauderdale. Christian focuses his practice on national insurance regulatory and compliance matters. Christian represents a wide variety of insurance entities, including insurance companies, reinsurers, managing general agencies, brokers, third-party administrators, claims companies, and other insurance-related entities in connection with regulatory, transactional, corporate, and governmental affairs matters. Christian advises clients on operational, regulatory, and compliance issues, including start-up initiatives, product filings, licensure and corporate governance assessments, business expansion initiatives, and financial and market conduct examinations.
Congress, for its part, is well aware of the political backdrop— that it has a 17% favorability rating from the public; that voters perceive Congress today as a “do nothing” body, adhering to almost “tribal” loyalty and heightened rhetoric. In order to stop the polarization in Congress, and the rising public anger about it, the solution needs to be to foster bipartisanship and compromise.

For many decades, insurance regulation has been like a pendulum, at times swinging toward deregulation with the government allowing the insurance industry to govern itself; at other times, the pendulum moving toward government-heavy oversight.

A trip through history will demonstrate that the regulatory climate reflects the mood of the country at the time. Today this climate will result in the regulatory pendulum swinging towards bipartisan compromise, and a healthy centrist position.

1900-1920s Antitrust & Prohibition – Pendulum On the Deregulatory Side, Leading to The Depression: In the beginning of the 20th century, in the early 1900s, the pendulum had moved to the deregulatory side. Big business had free reign, leading to monopoly and antitrust abuses, the Roaring 20s, bank failures, the stock market crash of ’29, and the Great Depression. President Teddy Roosevelt emerged to become the force for positive regulatory change, especially with his start of a third political party in 1912, The Progressive Party. By the 1930s and 1940s, most of the Progressive party had dissipated and was absorbed into the Democratic Party, led by Pres. Franklin D Roosevelt. During the period of its activity, the Progressive Party was a significant policy maker.

1930s Glass-Steagall Act – Which Moved The Pendulum to the Strict Regulatory Side. The Depression era of the ’30s caused the pendulum swing to strict government regulation with the passage of the Glass-Steagall Act of 1933 and The Banking Act of 1933. Both acts became known collectively as Glass-Steagall; The Banking Act created the Federal Deposit Insurance Corporation (FDIC) to protect consumers against failure of retail bank accounts; and Glass-Steagall which created legislative “walls” between banks, brokerage and insurance companies, especially the prohibition against the mingling of commercial and retail bank operations.

1944 – United States v South Eastern Underwriters Case – SCOTUS rules that Insurance Is Interstate Commerce; Therefore Federal Law (Sherman Act) & Regulations Apply. In 1944, the United States Supreme Court Case of U.S. v. South Eastern Underwriters Ass’n, 322 U.S. 533, ruled that insurance is to be considered interstate commerce, and therefore is subject to federal law (The Sherman Act). This opinion overturned a 70 year old SCOTUS ruling that held that states could enforce its own insurance laws. The 1944 South Eastern case caused the states...
to scurry to put pressure on Congress to enact a new law to clearly state that “the business of insurance” shall be governed by each state.

1945-McCarran-Ferguson Act – “Business of Insurance” Is To Be Governed By State Law The Supreme Court ruling in the Southeastern case was almost immediately legislatively overturned by Congress’ enactment of the McCarran-Ferguson Act of 1945. The act stated that the “business of insurance” is to be run by each state and not by the federal government, and also provided some antitrust exemptions. The National Association of Insurance Commissioners (NAIC) was set up to oversee the state insurance commissioners. And although NAIC has been effective and a well run nongovernmental association coordinating the states, it has no federal statutory authority and has no enforcement power. The issue of insurance being overseen by a trade association (NAIC), having to contend with the patchwork of 50 state laws, versus uniform regulation by the federal government is still an issue to be watched. As insurance becomes more national and they international in scope, it will require more uniformity of state law, and more oversight at the federal level.

1999-2000 Gramm Leach Bliley Act – A Mistake Which Moved The Pendulum To The Deregulatory Side: At the start of the 21st century, the pendulum swung back to a deregulatory period, with the passage of The Gramm-Leach-Bliley Act of 1999 (GLB), and subsequent acts (collectively referred to as GLB), which repealed the depression era Glass-Steagall act. The deregulatory GLB encouraged massive expansion of the subprime mortgage market. It allowed all financial institutions to intermingle, and it virtually deregulated the risky bank investment known as collateral debt obligations (derivatives). The deregulatory climate, including the government failure to properly oversee the use of derivatives, was said to have led to alleged criminal behavior of key executives of Wall Street financial institutions, said to have caused the Great Recession of 2008. Most surprising, was that not one key Wall Street financial executive was prosecuted and incarcerated during this period; unlike in the 1980s when hundreds of Savings & Loan bankers were prosecuted and jailed after being found guilty of fraud and other violations.

2009-2010 Federal Fraud Enforcement Recovery Act of 2009 & Dodd-Frank Act of 2010 – Congress Reacts to Alleged Criminal Behavior of Wall Street; Which Swings The Pendulum to the Government-Heavy Regulatory Side. Largely in reaction to the loose regulatory climate and alleged criminal behavior by key individual Wall Street executives leading to The Great Recession of 2008, the pendulum in 2009-2010 swung to the side of heavy government regulation. Democrats controlling both houses of Congress passed two new laws First, 2009, Congress passed the Fraud Enforcement & Recovery Act (FERA), which

In 1999, GLB created a deregulatory climate –, such that Not One key Wall Street executive alleged to have knowingly participated in multitrillion dollar criminal wrongdoing was ever prosecuted and incarcerated.
was intended to increase the funding for the Department of Justice, specifically to prosecute the alleged Wall Street executive misbehavior. However while the funds were approved, they were inadequately allocated, whether intentionally or otherwise, and therefore FERA was only partially effective.

Second, and most importantly, in 2010, Congress passed The Dodd-Frank Wall Street Reform and Consumer Protection Act of 2010 (Dodd-Frank), which established several watchdog federal agencies and federal policies, including The Federal Insurance Office (FIO), Financial Services Oversight Council (FSOC), Consumer Finance Protection Bureau (CFPB), and the Volcker rule (prohibiting proprietary accounts which conflict with client accounts). The financial lobby has attempted to impede the implementation and effectiveness of many parts of the act, by trying to slow or weaken completion of regulations for the various new agencies. Despite the lobby efforts to slow Dodd-Frank, and despite criticisms that the Act hurts small financial institutions, the Act has been considered to be the most important financial regulatory statute in the last several decades, and is praised by many to be an effective way to avoid a recurrence of the Great Recession of 2008.

2017-2018 Controversial Presidential Executive Order 2 for 1 Regulatory Rollback in 2017 – & new laws in 2018 to curb Dodd Frank – Pendulum Swings to the Deregulatory Area – With the election of Donald Trump in 2016, there has been a shift in emphasis on the regulation – an executive order signed January 30, 2017 by Pres. Donald Trump to eliminate regulations on a 2-for-1 basis. While this Executive Order by Pres. Trump has grabbed headlines, it is not clear that it has helped eliminate the regulatory hurdles facing many businesses. It is also not clear that this Presidential Executive Order to rollback regulations is allowed under the Constitution, since many legal scholars are of the opinion that the regulations and regulatory policies are the province of Congress, and not of the President. New laws passed in 2018 represent another attempt to curb the impact of Dodd Frank on smaller financial institutions.

2019 And Beyond – Regulatory Pendulum will swing to the center. Because of the various political pressures and polarization, many issues need to be regulated from centrist position. For 2019 and beyond, legislators, regulators and lawyers involved in insurance regulation will be busy, most likely fashioning regulations as a matter of bipartisan compromise in the central lane.
Insurance Regulatory Issues For 2019 and Beyond

- Patient Protection And Affordable Care Act (a.k.a. Obamacare)
- Expanding or Limiting Medicare
- Expanding or Limiting Medicaid
- Long-Term Care Benefits
- Mental Illness Treatment
- Disability Benefits
- Prescription Drugs
- Social Security
- Dodd Frank Financial Reform – Expansion Or Contraction
- Expansion of the Federal Enforcement & Recovery Act
- Expansion of The Flood Insurance Program To a Natural Disaster Program
- Cyber Security & Board of Director Liability
- Federal Versus State Control of the business of insurance – Power of NAIC
- International insurance representative – Covered Agreements
- Self Driving Automobiles; Uber; Lyft
- Insurance For Gun Liability
- Terrorism Risk Insurance Act
- Captive & Association insurance
- Other

In 2019 and beyond, to avoid the economic disasters of 2008, legislators, regulators, NAIC and insurance regulation attorneys will need to work in the center, in an era of bipartisan compromise.
the establishment of a written Cybersecurity Program ("Cyber Program") that, at a minimum, contains detailed data management and cybersecurity policies and procedures that should be followed by all employees throughout every level of the organization. The Cyber Program should be periodically reviewed by the board or a committee to evaluate its effectiveness and to determine whether improvements are needed. The board should also consider establishing the position of Chief Information Security Officer ("CISO") of the company, who will be responsible for the day-to-day operation of the Cyber Program. The CISO should regularly report to the board or its designated committee to enable the board to adequately oversee the implementation and effectiveness of the Cyber Program.

Adoption of safeguards, such as regular updating and patching of software and continuous monitoring of the company’s data network for unauthorized activity, are key functions of the Cyber Program. Additional safeguards should be implemented, as appropriate, to ensure that sensitive data is maintained within the company’s secure internal network and is never transferred to unsecured, external networks, such as the Internet, or unauthorized devices such as unencrypted USB drives or CDs unless the proper procedures are followed.

Retention and disposal of data is an often-overlooked component of a company’s cyber defenses. The Cyber Program should incorporate data retention policies that dictate the method and length of time data should be retained. Generally, sensitive data should be retained only as long as necessary for the company’s business purposes, or for so long as is legally necessary. Procedures must be adopted to ensure that such data is disposed of securely. However, some exceptions to the normal data disposal policies must be incorporated. For example, legal hold policies must be implemented to ensure retention of data that may be subject to pending or threatened legal or regulatory action. Failing to implement legal hold policies could lead to the imposition of civil and possibly criminal sanctions upon the company. Accordingly, it is critical that the designated board committee work with counsel to oversee the implementation of legal hold policies and adopt mechanisms to ensure that such policies are being strictly adhered to.

The Cyber Program should also establish cybersecurity training for employees. Many breaches have resulted from the mishandling of data or communications networks by negligent employees, or by accidentally clicking on a malicious link or attachment. While it is impossible to protect against every risk, the company should provide employees with practical guidance and training to help minimize a company’s exposure. It is especially important that training programs be updated regularly to

Fred E. Karlinsky is Co-Chair of Greenberg Traurig’s Insurance Regulatory and Transactions Practice Group. Fred has nearly 25 years of experience representing the interests of insurers, reinsurers and a wide variety of other insurance-related entities on their regulatory, transactional, corporate and governmental affairs matters. Fred is a recognized authority on national insurance regulatory and compliance issues and has taken a leadership position in many insurance trade organizations, has led many industry-driven legislative and regulatory initiatives, and is a sought after thought leader who has spoken and presented to insurance executives and governmental officials, both nationally and internationally.

Rich J. Fidei is a shareholder in Greenberg Traurig’s Insurance Regulatory and Transactions Practice Group and Government Law & Policy Group in Fort Lauderdale and Tallahassee. Rich focuses his practice on national insurance regulatory, transactional and compliance matters. He represents a wide variety of insurance entities, including insurers, health plans, reinsurers, and other related entities in connection with regulatory, corporate, compliance and transactional issues.

Jamey Zellner focuses his practice on government law and policy matters. He is experienced handling a wide range of insurance regulatory and corporate transactions, including company and agent/agency compliance, throughout the country.
address evolving cyber risks identified by the company. Controls, such as multi-factor authentication and limitations on who within the company may access certain data sets, should also be implemented to ensure that only authorized employees have access to secure networks.

The Cyber Program should also provide for requirements for contracting with third-party service providers to ensure that the company only does business with vendors who have adequate cyber safeguards in place. The company should also implement due diligence protocols to periodically assess the cybersecurity practices of contractors with which the company is doing business.

Incident response plans should also be prepared, implemented, and kept up to date to address new and emerging cyber threats. These response plans outline the procedures to be followed by the company following a data breach to help mitigate damage and make any required notices to consumers, law enforcement, and regulators. Directors should make sure that an emergency response team, sometimes composed of members of the designated board committee, legal counsel, IT personnel, compliance officers, and communications personnel, is in place to respond quickly to a breach. Each member of the response team should have clear roles and responsibilities, such as securing compromised IT assets to spear-heading necessary notices. These measures can help to mitigate any potential liability that results in the wake of a breach.

The board should further oversee the CISO in carrying out periodic testing of the Cyber Program to evaluate its effectiveness. A “penetration test,” designed to simulate a real-world cyber-attack, can be conducted by an in-house team or third-party professionals to identify vulnerabilities to be strengthened. Issued revealed by the test, as well as solutions that can be implemented, should be brought to the attention of the entire board and should be addressed as expeditiously as possible with follow-up monitoring to determine whether the issue has been adequately addressed.

Implementing important corporate governance mechanisms aimed at securing the company’s data management and IT systems helps develop a culture of compliance in light of new and evolving regulatory requirements. The New York Department of Financial Services (“NYDFS”) has taken the lead on establishing new cybersecurity standards with which insurance companies and financial institutions must comply. All insurance company boards should be aware of the requirements of the NYDFS regulation, regardless of whether they operate in New York, because those regulations have been highly influential on other regulators at both the state and
federal levels, who are now taking steps to impose their own new cybersecurity requirements on insurers and financial institutions. Also worth monitoring is the National Association of Insurance Commissioners’ recent adoption of the Insurance Data Security Model Law, which has already been adopted by South Carolina and is expected to be adopted by many other states.

Cybersecurity will continue to be a major issue affecting all companies, but especially for insurers that collect and store massive amounts of sensitive policyholder data. Insurance companies may be exposed to legal liability if they fail to implement and oversee cybersecurity protocols in their respective organizations, which could result in board member liability under certain circumstances. Regulators will continue to monitor companies and conduct IT-focused examinations, and may take action if a company has not adopted effective cybersecurity defenses. Effective cybersecurity corporate governance is key to ensuring compliance with regulatory standards, satisfying the board’s duty of care, and to avoiding the many negative consequences of a data breach. Boards are therefore well-advised to make cybersecurity concerns a top priority.
by employees and employers and, importantly, to help finance the expansion of health coverage under the ACA. When an employer provides or subsidizes health insurance, the worker does not pay taxes on the benefit. This practice encourages employers to offer more generous health insurance plans as opposed to paying higher wages. With the ACA, the Cadillac Tax took aim at limiting this tax break. It was also felt that the tax break encouraged overuse of the health-care system or favored inefficient providers. Unions, employers, insurance carriers and a host of others oppose the tax arguing that it will increase premium costs as the tax burden is passed along and that it will hamper efforts to obtain more generous employee benefits in lieu of higher wages.

Cost of coverage includes the total contributions paid by both the employer and employees, but not cost-sharing amounts such as deductibles, coinsurance and copays when care is received. The thresholds for high-cost plans are currently $10,200 for individual coverage, and $27,500 for down to deadlines paid family coverage but those amounts are due to be updated before the tax goes into effect. For pre-65 retirees and individuals in high-risk professions, the threshold amounts are currently $11,850 for individual coverage and $30,950 for family coverage. These amounts will also be indexed before the tax takes effect. As to who calculates, and who pays the tax, for insured plans, it is written such that employers calculate it, and insurers pay. For self-funded plans, employers may have to calculate the tax hit and the “person who administers the plan benefits” pays. The tax is based on the total cost of each employee’s coverage above the threshold amount and includes contributions toward the cost of coverage made by employers and employees.

The Cadillac Tax takes a backseat to overall efforts to repeal the ACA but its bipartisan unpopularity means that efforts to kick down the road its effective date have generally met with approval. It will be interesting to see if mid-term election results change this dynamic. 

Unless it is repealed or unless the start date is further extended, the Affordable Care Act’s “Cadillac Tax “ will start in 2022.

This Tax is part of the ACA’s effort to reduce the tax preferred treatment of employer-provided health care, to reduce excess healthcare spending by employees and employers, and to help finance the expansion of health coverage under the ACA.
Calendar

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: Danielle Daly – 312-988-5708  
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 NewYork Times Square  
New York, NY

May 8-10, 2019  
**Fidelity & Surety Law Spring Conference**  
Contact: Janet Hummons – 312-988-5656  
Contact: Danielle Daly – 312-988-5708  
JW Marriott Hotel Austin, TX