Locke Lord LLP

INSURANCE & REINSURANCE NEWSLETTER

JANUARY 2017

IN THIS ISSUE

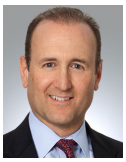
Locke Lord's Insurance Newsletter provides topical snapshots of recent developments in the fast-changing world of insurance. For further information on any of the subjects covered in the newsletter, please contact one of the members of our Insurance team.

OUR EDITORS:

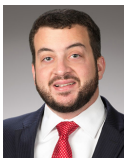
Alan J. Levin
Partner
Hartford | 860-541-7747
New York | 212-912-2777
alan.levin@lockelord.com

Thomas F. Bush
Partner
Chicago
312-201-2127
tom.bush@lockelord.com

OUR AUTHORS:



Theodore P. Augustinos
Partner
Hartford
860 541-7710
ted.augustinos@lockelord.com



Aaron Igdalsky
Associate
Hartford
860-541-7766
aaron.igdalsky@lockelord.com

Jonathan Bank
Of Counsel
Los Angeles
213-687-6700
jbank@lockelord.com

Molly McGinnis Stine
Partner
Chicago
312-443-0327
mmstine@lockelord.com

Al W. Bottalico
Insurance Specialist
Los Angeles
213-687-6781
al.bottalico@lockelord.com

New Corporate Governance Annual Disclosure Requirements for Connecticut Insurers to Take Effect in 2017

By Theodore P. Augustinos and Aaron J. Igdalsky

A recently enacted Connecticut statute intended to compel insurance companies to improve their corporate governance will impose significant new obligations on Connecticut domestic insurers, and their holding companies. Pursuant to Connecticut Public Act No. 16-206, by June 1, 2017, and annually thereafter, each domestic insurer or the insurance group of which that insurer is a member must submit to the Insurance Commissioner a confidential Corporate Governance Annual Disclosure (CGAD). If an insurer is a member of an insurance group, the insurer must submit the CGAD to the lead state commissioner, as determined by the procedures in the NAIC's applicable financial analysis handbook. Although the new statute is essentially a disclosure obligation, it will focus directors and senior management on analyzing and improving their corporate governance practices. Enactment of P.A. 16-206 follows the approval of the Corporate Governance Annual Disclosure Model Act and supporting Model Regulation by the NAIC. Similar CGAD statutes have already been enacted in several other states, including California, Florida, Vermont and Nebraska.

Under the new Act, the CGAD must contain the following information:

1. Description of Governance Framework: The CGAD must describe the insurer's or insurance group's corporate governance framework and structure, including consideration of the following:
   a) Board of Director Oversight: The Board of Directors (Board) and committees thereof ultimately responsible for overseeing the insurer or insurance group and the level or levels at which that oversight occurs. The insurer or insurance group must describe and discuss the rationale for the size and structure of the current board of directors.
   b) Board Duties: The duties of the Board and each of its significant committees and how they are governed, which may include bylaws, charters, or informal mandates as well as how the Board's leadership is structured and a discussion of the roles of the CEO and chairperson of the Board within the organization.
2. Description of Policies and Procedures: The insurer or insurance group must describe the policies and practices of the Board and significant committees thereof, including a discussion of:
   a) How each Board member's qualifications, expertise and experience meet the needs of the insurer or insurance group.
   b) How appropriate Board and significant committee independence is maintained.
   c) The number of Board and significant committee meetings over the past year (including information on director attendance).
   d) How the insurer or insurance group identifies, nominates and elects Board and committee members.
   e) The processes in place for the Board to evaluate its and its committees' performance, as well as any recent performance improvement measures (including any Board or committee training programs).
3. Senior Management Policies: The insurer or insurance group must describe the policies and practices for directing senior management, including a description of the following:
   a) Any processes or practices (such as suitability standards) to determine whether officers and key persons in control functions have the appropriate background, experience and integrity to fulfill their prospective roles.
   b) The insurer's code of business conduct and ethics.
   c) The plans for CEO and senior management succession.
   d) The insurer's or insurance group's processes for performance evaluation, compensation and corrective action to ensure effective senior management, including a description of the general objectives of significant compensation programs. The description must include sufficient detail regarding how the organization ensures that compensation programs do not encourage or reward excessive risk taking.
4. Oversight: The insurer or insurance group must describe the processes by which the Board, its committees and senior management ensure an appropriate amount of oversight to the critical risk areas impacting the insurer's or insurance group's business activities, including a discussion of:
   a) How oversight and management responsibilities are delegated among the Board, its committees and senior management.
   b) How the Board is kept informed of the insurer's or insurance group's strategic plans, the associated risks, and steps senior management is taking to manage those risks.
   c) How reporting responsibilities are organized for each critical risk area.
5. Reporting Level: For purposes of completing the CGAD, the insurer/holding company system may choose to provide information on governance activities that occur at the ultimate controlling parent level, an intermediate holding company level or the individual legal entity level, depending upon how the insurer or insurance group has structured its system of corporate governance. The CGAD may be completed at (i) the level at which the insurer's/holding company's risk appetite is determined, (ii) the level at which the earnings, capital, liquidity, operations, and reputation of the insurer are overseen collectively and at which the supervision of those factors are coordinated and exercised, or (iii) the level at which legal liability for failure of general corporate governance duties would be placed. If the insurer or insurance group determines the level of reporting based on these criteria, it must indicate which one of the three criteria was used to determine the level of reporting and explain any subsequent changes in the level of reporting.
6. Reference to ORSA, Form B, Form F, SEC Proxy: An insurer or insurance group may reference other existing documents including an own risk and solvency assessment ("ORSA") summary report, Form B, Form F, SEC proxy statements or foreign regulatory reporting requirements if those documents provide information that is comparable to the information required by Public Act 16-206. The insurer must attach such other documents to the CGAD if such documents are not already filed with or available to the commissioner, and clearly reference the applicable information within the CGAD.

Coverage for Voluntarily-Reached Settlements Addressed by Courts in 2016

By Molly McGinnis Stine

It's a common situation. A policyholder is sued and put its insurer on notice. The litigation proceeds and the opportunity to settle arises. The policyholder settles and turns to its insurer for coverage of the settlement amount.

Case law over the years has addressed policy language that concerns whether a policyholder is covered for voluntarily incurred amounts, including settlement amounts. Some policies also require a policyholder to secure the consent and sometimes the written consent of the insurer before reaching a settlement. Such wording can be in a policy's insuring agreement, an assistance and cooperation clause, an exclusion or elsewhere in a policy. In addition, courts often consider whether an insurer is obliged to show it is prejudiced by voluntary payments and if so, what constitutes sufficient prejudice.

These issues remained topical in 2016. The following are descriptions of just some of the recent decisions on these issues, which show that the outcomes can be affected by the facts, the policy language, and the jurisdiction at issue in a dispute.

A federal appellate court applying Michigan law upheld the plain language of a consent provision. In *Stryker Corp., et al. v. Nat'l Union Fire Ins. Co. of Pittsburgh, PA, et al.*, 842 F.3d 422 (6th Cir., Nov. 18, 2016)(Michigan law), a medical technologies firm sued its insurers for coverage relating to certain product liability claims. While the coverage action was pending, "Stryker unilaterally settled all of its individual product-liability claims for $7.6 million …." The insured sought this amount from TIG Insurance Company, its excess insurer, since the limits underlying the excess policy were exhausted by payment of a higher value judgment against Stryker for other claims. Both the settlement and the judgment had been reached while the underlying insurer still had available limits. That insurer opted to pay the judgment value and exhausted its limits. TIG denied coverage for the settlement amount because the insured failed to get TIG's written consent to the settlement. The trial court found for Stryker, holding that the consent provision was ambiguous. The appellate court disagreed and held that the plain language of the policy was clear. According to the court, the insured "was required to obtain consent for any settlements that were ultimately presented to TIG for payment," making irrelevant that the settlement was reached at a time that the underlying policy limits were still available.

A New York trial court relieved a policyholder from having to get their insurers' consent to settle because the insurers had denied coverage. In *J.P. Morgan Securities Inc., et al. v. Vigilant Ins. Co.,et al.*, 39 N.Y.S.3d 864 (Supr. Ct. N.Y., Jul. 7, 2016), an investment company policyholder (the former Bear Stearns) contended that its insurers were obligated to cover its securities-related settlement. Having previously denied coverage on various grounds for the claim, the insurers specifically denied coverage for the settlement, saying, in part, that the policyholder had failed to secure their consent to settle. While recognizing that the consent-to-settlement provision in the subject policies is a condition precedent to coverage, the court determined that the insurers' prior denial of coverage "excused" Bear Sterns from having to comply with the consent provision.

Two decisions analyzed whether an insurer must demonstrate it has been prejudiced by a policyholder's failure to obtain the insurer's consent to a settlement. A divided Supreme Court of Colorado held that no showing of prejudice was required. In *Travelers Prop. Cas. Co. of America v. Stresscom Corp.,* 370 P.3d 140 (Colo. Sup. Ct. 2016), a subcontracting concrete company, Stresscom, sought coverage from an insurer for amounts associated with a construction accident. Stresscom settled with the injured person. Travelers moved for summary judgment because that the settlement was a voluntary, and thus uncovered, payment. The trial court denied the motion, holding that Travelers could deny coverage for Stresscom's failure to comply with the consent provision only if Travelers suffered prejudice. The court likened a no-voluntary-payments provision to a notice provision in imposing a prejudice requirement on insurers. The intermediate appellate court agreed. However, the state supreme court, in a 4-3 decision, reversed, finding that the lower courts had improperly applied prior notice-related case law to the no-voluntary-payments provision in this case. The latter provision is, the court noted, "a fundamental term defining the limits or extent of coverage." As such, according to the court, the public policy justifying a prejudice requirement in the notice context does not apply to a no-voluntary-payments provision.

A California appellate court determined under Missouri law that the fact that a policyholder failed to follow a consent provision constituted proof of prejudice to an insurer. In *The Doe Run Resources Corp. v. The Fed. & Cas. Co. of NY,* 2016 WL 379839 (Cal. App. 4th., Feb. 1, 2016)(non-publishable)(Missouri law), the court found no coverage for a company's environmental cleanup settlement because the insured failed to get the consent of the excess insurer from which reimbursement was sought. The subject insurance policy's insuring clause required written consent from the insurer for any amounts paid by the policyholder. According to the court, the fact that the insured excluded the insurer entirely from the process of settling is "sufficient prejudice by itself."

Finally, in what may be a case to watch in 2017 on the issue of prejudice, the federal 9th Circuit Court of Appeals recently certified two questions to the California Supreme Court, one of which reads: "If the notice-prejudice rule is a fundamental public policy for the purpose of choice-of-law analysis, can a consent provision in a first-party claim insurance policy be interpreted as a notice provision such that the notice-prejudice rule applies?" It is not known whether the California Supreme Court will accept this question for review. Order Certifying Questions to the California Supreme Court, *Pitzer College v. Indian Harbor Ins.* Co., No. 14-56017 (9th Cir., Jan. 13, 2017).

New York's Cybersecurity Requirements for DFS Licensees: A New Item at the Top of the To Do List

By Theodore P. Augustinos

With a compliance date a few months away, licensees of the New York Department of Financial Services (DFS) must start taking action in response to coming cybersecurity requirements, which will be more onerous and difficult that any existing requirements in the United States. Even though the revised proposed regulation, published December 28, 2016 and available here, is open for comment until January 27, 2017, the DFS will focus

on new comments that were not raised in the original comment period. As the original comment drew 150 comments addressing nearly every aspect of the proposed regulation, it is unlikely that new comments will result in further substantive changes that would justify delaying a licensee's planning. This article identifies who will be subject to the new requirements, what is required and by when, and what steps should be taken to comply.

The new requirements deserve attention from persons and companies in the banking, insurance, securities, and other regulated financial industries, as it is likely that other states will look to the New York requirements as a model. The New York requirements also serve as a new and robust checklist for any business to consider for improving its cybersecurity risk profile.

I. WHO IS AFFECTED?

Nearly any DFS licensee: The proposed regulation applies to Covered Entities, defined to mean each individual or non-governmental entity that operates or is required to operate under a license, registration or other authorization under the New York banking, insurance, or financial services laws. There is a limited exemption from many (but not all) of the requirements for Covered Entities with fewer than 10 employees (including independent contractors), or less than $5 million in revenue in each of the past three years, or less than $10 million in assets (including affiliates). Exempt from nearly all of the requirements is any person or entity that does not directly or indirectly have any Information Systems or any Nonpublic Information. A Covered Entity that is an employee, agent, representative or designee of a Covered Entity and is covered by the cybersecurity program of the Covered Entity is exempt from the regulation. Covered Entities claiming an exemption must file a Notice of Exemption on a prescribed form.

II. WHAT SYSTEMS AND INFORMATION MUST BE PROTECTED?

Information System: Resources used to collect, process, and otherwise handle electronic information, and also any specialized systems such as for industrial/process controls, telephone switching, private branch exchange, and environmental control.
Nonpublic Information: Electronic information that is not publicly available, (i) the tampering with which, or unauthorized disclosure, access or use of which, would have a material adverse impact on the Covered Entity; (ii) personal information (as the term is commonly used in other privacy and security requirements); or (iii) health related information.

III. WHAT IS REQUIRED?

a) Administrative Safeguards

1. **Risk Assessment.** A risk assessment is required periodically, to include: (i) evaluating and categorizing cybersecurity risks and threats; (ii) assessing the confidentiality and security of Information Systems and Nonpublic Information; and (iii) mitigating identified risks. While not repeated throughout this summary, and not listed first in the regulation, nearly every other administrative and technical requirement of the regulation is tied to the risk assessment.
2. **Cybersecurity Program.** A cybersecurity program must be designed to protect the confidentiality, integrity, and availability of the Covered Entity's information systems, based on the required risk assessment, and to perform stated core cybersecurity functions.
3. **Cybersecurity Policy.** A cybersecurity policy approved by a senior officer or the governing board must provide for the protection of Information Systems and Nonpublic Information, based on the required risk assessment, and cover 14 specified areas including data governance and classification, systems and network security, data privacy and incident response.
4. **Vendor Management.** Policies and procedures must be adopted to protect the security of Information Systems and Nonpublic Information accessible to third party vendors.
5. **Personnel, Training, and Monitoring.** A qualified individual must be designated as the Chief Information Security Officer (CISO), responsible for the cybersecurity program and the cybersecurity policy. The CISO must report at least annually in writing to the Covered Entity's governing board concerning cybersecurity. Other cybersecurity personnel must be engaged, trained, and updated on cybersecurity risks, and all personnel must have regular cybersecurity awareness training. The Covered Entity must also implement safeguards to monitor the activity of Authorized Users and detect unauthorized access to, use of, or tampering with Nonpublic Information.
6. **Access Control.** User access to Information Systems must be limited, and periodically reviewed.
7. **Application Security.** All internally and externally developed applications must be secure, and procedures related to application security must be reviewed, assessed and updated periodically.
8. **Testing and Auditing.** Monitoring and testing of Information Systems for vulnerabilities must be conducted, including an annual penetration test, and bi-annual vulnerability assessments. Systems able to reconstruct material financial transactions must be maintained. Records of Cybersecurity Events (which include unsuccessful attempts) must be maintained for five years.
9. **Data Retention and Destruction.** Personal information and health information no longer needed to be retained must be securely destroyed.
10. **Incident Response Plan.** A written incident response plan must be established to guide the response to, and recovery from, Cybersecurity Events.

b) Technical Safeguards

1. **Encryption.** Generally, Nonpublic Information held or transmitted by the Covered Entity must be encrypted, both in transit and at rest. To the extent that encryption is determined to be infeasible, alternative compensating controls may be substituted, subject to review by the CISO at least annually.
2. **Multi-Factor Authentication.** To protect against unauthorized access to Nonpublic Information or Information Systems, each Covered Entity must use Multi-Factor Authentication or Risk-Based Authentication (as these terms are defined in the regulation). As an alternative, the CISO can approve other access controls that are at least as secure.

c) Notices

1. **Breach Notices.** Notice is required to the DFS superintendent as promptly as possible but no later than 72 hours from a determination that a Cybersecurity Event has occurred, where notice is required to any other governmental or supervisory body, or self-regulatory agency, or where the event has a reasonable likelihood of materially harming any material part of the Covered Entity's operations.
2. **Annual Compliance Certification.** An annual compliance certification on the prescribed form must be submitted to the DFS superintendent by February 15 of each year, starting 2018. Documentation supporting the certificate must be maintained for examination by the DFS for five years.
3. **Confidentiality.** All information provided by a Covered Entity pursuant to the regulation is exempt from disclosure under public records laws.

IV. WHEN ARE THE NEW REQUIREMENTS EFFECTIVE?

The regulation will be effective March 1, 2017, and Covered Entities will have until September 1 to comply. The following listing indicates the actual compliance date for the various requirements, given the separate deadline for the annual compliance certificate, and three different transition periods of the regulation.

Compliance Date	*Provision (with Regulation Section reference)*
September 1, 2017	Cybersecurity Program (§ 500.02) Cybersecurity Policy (§ 500.03) CISO (§ 500.04(a)) Access Privileges (§ 500.07) Cybersecurity Personnel (§ 500.10) Incident Response Plan (§ 500.16) Notice of Cybersecurity Event (§ 500.17(a)) Filing for Limited Exemption (§ 500.19(d))
February 1, 2018	Annual Compliance Certification (§ 500.17(b))
March 1, 2018	CISO's annual report to the governing board (§ 500.04(b)) Pen Testing and Vulnerability Assessments (§ 500.05) Risk Assessment (§ 500.09) Multifactor Authentication (§ 500.12) Cybersecurity Awareness Training for all Personnel (§ 500.14(a)(2))
January 1, 2019	Audit Trail (§ 500.06) Application Security (§ 500.08) Data Retention Limits (§ 500.13) Monitoring and Detection of activity of Authorized Users (§ 500.14(a)(1)) Encryption (§ 500.15)
March 1, 2019	Third Party Vendor Security (§ 500.11)

WHAT STEPS SHOULD BE TAKEN?

Each Covered Entity should start now to review existing programs, policies, and procedures to determine what is needed to satisfy the new requirements by the compliance dates mapped above. It is difficult to imagine any Covered Entity that would not have to take some action to comply with the new requirements. The following project steps are suggested for consideration by Covered Entities:

1. Determine whether or not the limited exemption for small businesses, or one of the other exemptions, would apply.
2. Identify and gather the project team, consisting of internal decision makers, IT personnel, and internal and experienced external legal and regulatory resources.
3. Identify outside resources that will be required for various functions, such as pen testing.
4. Catalogue all existing programs, policies, and procedures related to cybersecurity.
5. Assign team members responsible for reviewing and, as necessary, revising each existing program, policy, and procedure, and to draft any new documentation needed to comply with the new requirements.
6. Map the timeline of deliverables to achieve compliance by the effective date and the various transition dates.

Rhode Island Regulation 68, Voluntary Restructuring of Solvent Insurers Act

By Jonathan Bank and Al W. Bottalico

Recently Rhode Island revised its Voluntary Restructuring of Solvent Insurers Act as implemented by DBR Regulation 68. This was, in many respects, modeled after the UK's Part VII Transaction, which, subject to court approval, enables an insurance company to transfer/novate a book of business (and divest itself of all residual liability), to another unrelated insurer which assumes all liabilities associated with that business. Reg 68 is not as broad as the Part VII legislation, but nevertheless creates an option in the United States that had not heretofore been available. A number of Locke Lord US attorneys have been involved in Part VII Transfers, and thus are very familiar with the mechanism. Additionally, Al Bottalico joined the firm a year ago after 38 years with the California Department of Insurance. Al was Deputy Commissioner-Finance Surveillance, and has a good regulatory perspective and understanding of what the Rhode Island regulators will likely need in regards to such a transaction and has worked with the Rhode Island Department in the past. Al recently assisted in the preparation and review of one of the Reg 68. applications that was recently filed. Our Providence office gives us easy access to the Department.

The firm has been working with the Rhode Island Department for over 6 months to understand the nuances (pitfalls) of the Regulation, and have become very familiar with the required procedures. Thus far there have been no insurance companies formed or domiciled in Rhode Island for this purpose (two applications are pending), although we have had discussions with various parties interested in getting a company licensed in Rhode Island to transfer/novate business through Reg 68. In our various discussions, we have also become familiar with some of the potential issues that might arise if a company was formed and a transaction was entered into.

Once the transferor identifies the book (or books) of business to be transferred, the first step is obtaining the consent of the domiciliary regulator of the insurer seeking to transfer/novate business to a RI domestic. Without knowing which other state(s) may be involved, it is impossible to know the applicable regulator's predisposition to the transaction. Rhode Island has indicated that it is also possible that alien business could be transferred to the U.S. via a Rhode Island domestic company. Both Elizabeth Dwyer, Superintendent of Insurance and Jack Broccoli, Associate Director - Financial Regulation, will work with other regulators to address any regulatory concerns. Assuming no objections at this stage, the next step is to either setup a licensed Rhode Island domestic, or to identify one that is prepared to assume the business.

The Regulatory process to form and license a RI domestic to take advantage of Reg 68. is relatively simple, and requires a minimum capital of $3mm. An advantage of Reg 68. is that it permits one company to set up individual protected cells, thus allowing that company to assume disparate books of business. We can assist in most aspects of the licensing of a new Rhode Island domestic to whatever extent is desired. We may be most valuable coordinating the efforts of the team tasked with assembling the license application and appendices. Utilizing an existing Rhode Island domestic should be an easier process (the statute is limited to commercial property & casualty run-off liabilities so not all lines of business would qualify for a potential commutation plan, (for example workers' compensation would not qualify). Additionally, to qualify under Reg 68, the company must not have written new premium for 60 months.). Rhode Island has indicated there is nothing in Reg 68 that would preclude alien business from being transferred to Rhode Island under such a plan and there are various ways this could be accomplished. Many books of alien business have a substantial amount of U.S. policyholders and therefore regulators may view this favorably as policyholders would gain from the oversight provided by U.S. regulators.

There are a number of factors which should be kept in mind for utilizing a Rhode Island domestic for run off purposes such as:

- The new (or existing) Rhode Island insurer to which the book of business is transferred/novated may retrocede the business requiring review of the retrocessional agreement and collateral.
- The independent actuarial review (commissioned by the Rhode Island Department) must satisfy all interested parties and will be an important aspect to gaining approval from all the regulators involved.
- Communication with non-domestic regulators may be important in the process so they do not raise objections although their express approval may not be required. For example, review of the business transfer plan to fully understand what blocks of business and why these blocks are being transferred will be necessary in order to communicate with the regulators and gain their support. Although, as noted above, explicit approval may not be required from non-domiciliary states, it is likely Rhode Island will listen to concerns from other states and seek to gain their support.
- Credit for reinsurance of transferred book—business ceded or retroceded by the Rhode Island domestic to a non-admitted (including offshore) reinsurer may require collateral in the form of so-called Reg 114 trusts, letters of credit, other trusts or funds withheld.

As referenced above, these are some of the potential roadblocks/ pitfalls that may confront the transferor.

- Some states may be hostile and/or express concerns regarding a voluntary restructuring and transfers under the Rhode Island law. Early communication with other regulators is quite important.
- Some insurers, insureds, reinsurers and industry groups may oppose them.
- Whether the transfer and commutation plan are respected by other states has not been tested in court. There is a good argument to be made that states should give proper deference to the Rhode Island Reg 68.
- The Rhode Island insurer assuming business may be required to provide collateral such as Reg 114 trusts, letters of credit, etc. so that transferring insurer may claim full reserve credit for any transfer because:
- Assuming the Rhode Island company (particularly if a new domestic) cannot be widely licensed due to seasoning requirements, and may not have rating or significant assets or surplus.

In summary Locke Lord LLP can assist in the following areas based on our experience:

- Assist with the formation of a RI domestic company including assessing capital requirements or assist with the redomestication to RI of an existing company.
- Assist with the preparation and/or review of a business transfer plan from an insurer wanting to transfer business to a Rhode Island domestic for the purpose of running off the business for business purposes (solvent run-off).
- Assist with the preparation and/or review of all necessary agreements to effectuate a business transfer plan including quota share, loss portfolio transfer and assumption reinsurance agreements, retrocession agreements from the Rhode Island domestic to a retrocessionaire, trust agreements, letters of credit, and claims and other administrative services agreements.
- Communication with the Rhode Island Department of Insurance on any such plans.
- Communication with other regulators in other impacted states regarding such a plan.
- After Rhode Island has reviewed the plan, Rhode Island will then submit to its Court for review and approval of the plan, at which time policyholders, regulators, or other interested parties will be able to raise any objections they may have.

ACCOLADES:

- Locke Lord's Insurance Law Practice received National and Chicago Tier 1 ranking in the 2017 Best Law Firms survey by U.S. News/Best Lawyers®.

ARTICLES & QUOTES:

- Robert Romano, John Emmanuel and Stewart Keir (all from New York) co-authored a Locke Lord QuickStudy: US and EU Negotiate Covered Agreement on Insurance and Reinsurance Regulation, January 18, 2017.
- Jonathan Bank (Los Angeles) and Matthew Murphy (Providence) co-authored a Locke Lord QuickStudy: NY Bankruptcy Court Trumps Insurers Seeking to Compel Arbitration, January 18, 2017.
- Aubrey Blatchley (Hartford) authored a Locke Lord QuickStudy: District Court Compels Arbitration, December 27, 2016.
- Jonathan Bank (Los Angeles) and Aubrey Blatchley (Hartford) co-authored a Locke Lord QuickStudy: For Whom the Bell(efonte) Tolls, December 21, 2016.
- Mark Deptula (Chicago) authored a Locke Lord QuickStudy: Adding Fuel to the Bellefonte Fire? Second Circuit Asks New York's Highest Court For Guidance as to Reinsurer's Limit of Liability, December 14, 2016.
- Brian Casey (Atlanta) and Aaron Igdalsky (Hartford) co-authored CFPB's New Rules For Cellphone Carrier Third-Party Billers, Law360, November 30, 2016.
- Mark Deptula (Chicago) and Jonathan Bank (Los Angeles) co-authored a Locke Lord QuickStudy: No Thanksgiving Vacation for This Arbitration Award, November 16, 2016
- Jonathan Bank (Los Angeles) authored "Now You See It, Now You Don't: Tenn. Reinsurance Discovery, Law360, October 18, 2016.

EVENTS AND SPEAKING ENGAGEMENTS:

- Alan Levin (Hartford) will attend the IBA Challenges for the Insurance Industry Conference in London, UK on March 30-31, 2017.
- Elizabeth Tosaris (San Francisco) and Paige Waters (Chicago) will attend the IRES Foundation National School on Market Regulation in St. Petersburg, FL on March 12-14, 2017.
- Theodore Augustinos (Hartford) and Molly McGinnis Stine (Chicago) will attend the Advisen Cyber Risk Insights Conference in London, UK on March 7, 2017.
- Paige Waters (Chicago) will be a presenter at the IAIR Insurance Resolution Workshop in Austin, TX on February 1-3, 2017.
- Jon Gillum (Austin) will attend the Texas Association of Life and Health Insurers (TALHI) Legislative Forum & Lobby in Texas on January 30-31, 2017.
- Brian Casey (Atlanta) will attend the 7th Annual Life Settlement Institutional Investor Conference in New York, NY on January 30, 2017.
- Paige Waters (Chicago) attended the ABA 43rd Annual TIPS Mid-Winter Symposium in Insurance and Employee Benefits in Coral Gables, FL on January 12-14, 2017.
- Brian Casey (Atlanta) presented *"Insurance Regulatory Update"* at the RedChalk Group Blockchain Insurance Summit in Chicago, IL on November 8, 2016.

EVENTS:

- *Save the Date* - Locke Lord is co-hosting the Insurance M&A and Capital Raising Roundtable in New York, NY on February 23, 2017. More information to be posted on the Locke Lord Insurance Events page.
- Locke Lord will host its popular cocktail reception at the NAIC Fall National Meeting in Colorado on April 9, 2017 at the Hyatt Regency Denver at Colorado Convention Center's Peaks Lounge. Hope to see you there.

ANNOUNCEMENTS:

- Locke Lord has assembled a multi-disciplinary group of lawyers from our insurance, banking and technology practice teams focused on emerging issues relating to the use of Blockchain technology, which will build upon our electronic signatures and records practice. Brian Casey leads this group and is focused on Blockchain's application in the insurance and reinsurance industries.

insurereinsure.com

Locke Lord's Industry Blog dedicated to bringing you the latest news and important developments related to the insurance and reinsurance industry.

Subscribe to receive automatic emails on the latest information posted to insurereinsure.com

Locke Lord LLP

Practical Wisdom, Trusted Advice.

www.lockelord.com

Atlanta | Austin | Boston | Chicago | Cincinnati | Dallas | Hartford | Hong Kong | Houston | London | Los Angeles | Miami
Morristown | New Orleans | New York | Providence | Sacramento | San Francisco | Stamford | Washington DC | West Palm Beach