INSURANCE & REINSURANCE NEWSLETTER

SEPTEMBER 2018

In this Issue

2 Our Editor and Authors

3 Powerful But Not Responsible: Texas Department of Insurance Clarifies Licensed Officer Requirement for Insurance Agencies, *by Jon Gillum*

4 U.S. Insurer Group Capital Calculation Process Moves Ahead, *by Robert Kasinow*

4 Follow the Leader: NYDFS Cybersecurity Regulation Leads the Way for Other States and Industries, *by Theodore P. Augustinos and Molly McGinnis Stine*

6 Testing the Limits III – Cyber Coverage Litigation Focuses on Computer Fraud Losses, *by Molly McGinnis Stine and Matthew Murphy*

8 Accolades

8 Articles & Media Mentions

8 Recent Conferences, Presentations and Speaking Engagements

9 Events

9 Announcements

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 EDITOR:

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

OUR AUTHORS:

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

Matthew Murphy
Associate
Providence
401-276-6497
matthew.murphy@lockelord.com

Jon Gillum
Senior Counsel
Austin
512-305-4717
jgillum@lockelord.com

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

Robert B. Kasinow, CFE, ARe, MCM
Insurance Specialist
New York
212-912-2821
robert.kasinow@lockelord.com

Powerful But Not Responsible: Texas Department of Insurance Clarifies Licensed Officer Requirement for Insurance Agencies

by Jon Gillum

On May 31, the Texas Department of Insurance ("TDI") offered guidance on one of the most overlooked requirements for a Texas-licensed (both resident and non-resident) insurance agency: the requirement that an agency have an individually-licensed "officer" or "active partner" who holds an individual insurance agent license for the same line or lines of insurance as does the agency.

This requirement often surprises many applicants for a Texas insurance agency license—applicants who submit a TDI insurance agency license application (a TDI FIN507 Form) and overlook the instructions in Part II in the Form discussing the concept of an individually-licensed officer. And, this requirement is even easier to overlook when prospective buyers of an insurance agency consider officer changes while preparing a change of control filing (a TDI FIN531 Form) pursuant to Texas Insurance Code section 4001.253.

One reason that TDI's individually-licensed officer requirement is often overlooked is that TDI's conception of that requirement is not specified by statute. Indeed, the requirement is rooted in Texas Insurance Code section 4001.106(b)(2) which states only the following:

> [A]t least one officer of the corporation or one active partner of the partnership and all other persons performing any acts of an agent on behalf of the corporation or partnership in this state are individually licensed by the department separately from the corporation or partnership…

While this statute requires an individually licensed-officer or active partner, it does not mention that the license must be for the same line or lines that the entity is seeking to obtain. And, the statute does not elaborate on what it means to be an "officer" or "active partner."

Now, however, TDI has a new rule that explains the "same type" of license requirement for officers. Specifically, 28 Texas Administrative Code section 19.804 now contains examples of license types, and indicates that multiple individually-licensed officers can be used to fulfill the requirement for insurance agencies that are authorized for multiple lines of insurance. The full text of TDI's new rule can be found here.

Perhaps the most interesting part of TDI's recent rulemaking on this issue, however, is not found in the final rule at all. Instead, buried within TDI's comments to the new rule is the most extensive written guidance to date on the type of agency "officer" that meets TDI's requirement. While the statute and the new rule continue to speak only of an "officer or active partner," TDI offered the following commentary in response to submitted comments during the rulemaking process:

> TDI disagrees with the comment to the extent that a licensed officer or active partner required under Insurance Code §4001.106(b)(2) should not be in a position to have the power to direct or cause the direction of the management and policies of the license holder. *If the individual officer or active partner has no power to direct or cause the direction of the management and policies of the license holder, then the individual is little different than an employee or contractor, which renders the requirement in Insurance Code §4001.106(b)(2) that the person be an officer or active partner meaningless.* As previously stated, TDI does not consider that the control must be absolute or that it is limited to ownership. (emphasis added).

Given this commentary, it appears that TDI will insist that insurance agencies have an individually-licensed officer that has the power to influence the management and policies of the agency. In other words, while the title given to an officer may not matter, that officer will likely need to have a minimum level of authority to comply with TDI's requirement.

Finally, it is important to note that the final version of TDI's rules does not refer to the individually-licensed officer as a "responsible" person. As a result, neither TDI's statutes nor its rules have followed the path of some other states which expressly codify the concept of a "designated responsible licensed person". This distinction is important not only for insurance agencies seeking to obtain or maintain their licenses, but also for assessing potential enforcement liability for the individually-licensed officer that is necessary for the agency's Texas license.

TDI's recent commentary on this issue can be found here.

U.S. Insurer Group Capital Calculation Process Moves Ahead

by Robert Kasinow, Insurance Specialist

The NAIC is making significant progress on the development of a U.S. group capital calculation (GCC) for insurers. The objective is to provide a quantitative view of capital at the group level and identify contagion risk across the group. Most recently the Group Capital Calculation Working Group (GCCWG) met in August during the NAIC Summer National Meeting to primarily consider comments from interested parties on the scope of the group and treatment of non-insurance entities in the capital calculation.

As a result of discussions at the Summer Meeting, the GCCWG exposed a joint proposal from a group of property & casualty trade associations (the "Trades") for a forty-five day comment period ending September 21, 2018. The proposal focuses on the scope of the group and determining elements for non-insurance field testing. NAIC staff also integrated questions into the proposal on field testing approaches including related topics not specifically discussed at the meeting. The NAIC plans for field testing to be completed by the November Fall National Meeting. Following are key areas brought forth in the Trades proposal that insurers should follow closely to be proactive in determining how the resulting field testing and implementation of the GCC may affect their organization.

The Trades proposal considers certain exemptions and expedited approaches in reporting a GCC. A foreign based insurance group will be exempt from the GCC if the non-U.S. group recognizes the U.S. regulatory system and accepts a U.S. supervisor's capital requirement to satisfy its home jurisdiction group capital. The foreign based group is expected to file group capital at the same or substantially similar scope as determined by the lead state regulator. The lead state regulator must be able to obtain information from the foreign group supervisor to fully understand the group's financial condition. Also the Trades suggest that a U.S. based group be exempt from the GCC if they file an ORSA report with the lead state.

An expedited approach is proposed for U.S. groups that have a Federal Reserve group capital requirement to provide that calculation instead of completing the GCC. Also U.S. groups where the ultimate controlling party in an underwriting entity required to submit a Risk Based Capital (RBC) report may submit the RBC report.

Scope will be determined by the group based on an inventory of entities in their NAIC Annual Statement Schedule Y. Other Holding Company Filings for entities owned by the Ultimate Controlling Person should also be considered. Note that all financial entities and all entities owned directly or indirectly by an insurer will need to in the GCC.

Non-financial entities not owned directly or indirectly by an insurer that pose material risk to the group should be included in the scope. To make this determination, a formulaic approach may be field tested such as previously proposed by the NAIC where an entity with capital/stockholder's equity less than 5% of the group's capital at prior year-end is not a material source of capital, and an entity with net income in each of the most recent five years is not a material user of capital.

Aggregation of non-insurance, non-financial entities should be coordinated between the lead state regulator and the group. Combining entities with common characteristics may provide a clearer view of potential risks and greater informed insight on financial performance.

The lead state regulator will review a list of excluded entities to determine any that may create material risk. Examples of risks to be evaluated include a material dependency, providing intra-group financial support, structural or contractual relationships, or where the addition or subtraction of an entity's activities could have a material impact on the group. Regulatory discretion will allow entities to be added or subtracted to the group list depending on the likelihood of a capital loss. The final decision on scope is the responsibility of the lead state regulator.

An important objective of field testing is to determine appropriate capital charges. All insurance entities will be required to be listed in the calculation at their minimum regulatory required capital. Other financial entities will be individually listed in the calculation and tested as regulated or unregulated financial entities. Regulated financial entities such as banks and other depositories will be tested at a scaled and unscaled minimum required by their regulator to a Risk Based Capital (RBC) of 300%. Asset managers and registered investment advisers will be tested at Book Adjusted Carrying Value (BACV) and average revenue. Other financially regulated entities are to be tested at the minimum required by their regulator.

Field testing of unregulated financial entities will be differentiated based on those that provide financial activities to insurers and entities providing other than financial services. Unregulated financial entities providing financial services will receive a 22.5% BACV capital charge and entities providing other than financial services will be at the same BACV charge plus other factors based on input from testing participants.

Other non-financial entities will also be tested for capital charges. Industry participants are concerned that these entities do not transfer risk to the group to the same degree as regulated entities. Several testing methods have been proposed subject to agreement between the group and the regulator on how to best consider these entities including aggregation for a collective capital charge.

Continued input from insurers and interested parties will go a long way to inform development and implementation of the calculation. The GCC is intended to be an analytical tool, not a standard, while being consistent with existing state laws. Detailed and transparent field testing should accomplish that goal.

Follow the Leader: NYDFS Cybersecurity Regulation Leads the Way for Other States and Industries

by Theodore P. Augustinos and Molly McGinnis Stine

This article was originally published in CPO Magazine July 16, 2018. Used with permission.

The New York Department of Financial Services (NYDFS) blazed a cybersecurity trail with its 2017 regulation for the protection of information collected and processed in, and systems used in the operation of, the financial services and insurance industries. The Empire State's work has already formed the basis for the National Association of Insurance Commissioners' model cybersecurity law, several states' insurance laws, and similar laws for other industries in other states. With "imitation being

the sincerest form of flattery," other states and industries are expected to flatter the DFS by adopting similar requirements.

The NYDFS' work has been game-changing and will continue to be highly influential. As important as the NYDFS Cybersecurity Regulation is, however, it would be a disservice not to remember the earlier federal and state governmental laws, regulations and guidances that built a foundation on which the NYDFS has erected its New York cyber skyscraper. Taken together, the legal landscape has been dramatically altered in recent years and more changes are inevitable.

Also, as governmental edicts about cybersecurity proliferate, so too do related requirements about data breach notifications and privacy protections.

The NYDFS Cybersecurity Regulation

After drafts and revisions, and plenty of industry comment, effective March 1, 2017, the NYDFS promulgated its Cybersecurity Regulation (23 NY CRR 500) to address the cybersecurity threats facing "Covered Entities," defined to include all NYDFS licensees, including banks and other lenders, insurance carriers and producers, and others. Beyond other cybersecurity requirements found in existing U.S. laws and regulations, the NYDFS Cybersecurity Regulation expanded the scope of information to be protected by defining "Nonpublic Information" to include the traditional data sets that can expose individuals to identity theft and fraud, as well as information that, if compromised, could cause material harm to the Covered Entity. In addition, the NYDFS Cybersecurity Regulation also expanded the scope beyond information to include "Information Systems," including systems used to process Nonpublic Information, as well as operations systems (including HVAC and telephone systems) needed to operate the Covered Entity's business.

Also beyond other U.S. laws and regulations focused on cybersecurity, the NYDFS Regulation is highly prescriptive in identifying particular written policies and safeguards required to be adopted, particular requirements for general employee awareness and specific employee qualifications and training, and requirements for assessing and managing the cybersecurity risks presented by the Covered Entity's use of third party service providers with access to Nonpublic Information and Information Systems. Most of these requirements are based on a required periodic cybersecurity risk assessment.

In addition, the NYDFS introduced a requirement to notify NYDFS of certain types of cybersecurity events within 72 hours, much quicker than existing U.S. breach notification requirements, but consistent with the notice deadline of the new European Union General Data Protection Regulation (GDPR). The notification requirement is also broader, encompassing certain breaches covered by existing state breach notice requirements, and including certain breaches of systems that could threaten the Covered Entity without compromising the types of information that could expose individuals to identity theft and fraud.

The NAIC Insurance Data Security Model Law

Following the lead of the NYDFS, in October 2017 the NAIC adopted its Insurance Data Security Model Law (NAIC Model) to establish insurance industry standards for data security, and for the investigation and notification of certain cybersecurity events. The NAIC Model applies to any individual or nongovernmental entity licensed, authorized, or registered under the insurance laws, with certain exceptions. An NAIC taskforce had been working on cybersecurity standards for two years, but substantially revised its prior working drafts to follow the concepts and terminology used in the NYDFS Cybersecurity Regulation. The NAIC Model has the potential to affect the entire insurance industry, including InsurTech firms and other service providers with access to the data and systems of insureds and producers.

The NAIC Model, while based on the NYDFS Cybersecurity Regulation, differs from it in several important respects. To address concerns about inconsistency among the states, a drafters' note to the NAIC Model states that Licensees in compliance with the NYDFS Cybersecurity Regulation are deemed to be in compliance with the NAIC Model.

On May 3, 2018, the South Carolina Governor made South Carolina the first state in the nation to adopt a comprehensive cybersecurity statute for the insurance industry, by signing into law the South Carolina Insurance Data Security Act (H4655) based on the NAIC Model, which will become effective January 1, 2019.

Other states can be expected to propose similar legislation based on the NAIC Model. A bill following the NAIC Model was introduced in Rhode Island (Bill 2018 – H7789), although it has been recommended to be held for further study.

Activity by Other Jurisdictions

In 2017, Colorado (3 CCR 704-1 Rules 51-4.8 and 4.14) and Vermont (Vermont 4:4 Vt Code R. § 8:8-4) imposed cybersecurity requirements for the securities industry similar to the NYDFS requirements (which do not apply to securities firms).

In 2018, Colorado (House Bill 18-1128) went further, and adopted general cybersecurity requirements for all entities that maintain, own or license personal identifying information of a Colorado resident. While it does not mandate the same level of

specific activity as the NYDFS Cyber Regulation, it does require an entity to "implement and maintain reasonable security procedures and practices that are appropriate to the nature of the personal identifying information and the nature and size of the business and its operations." (Colo. Rev. Stat. § 6-1-713.5(1)). In this respect, the Colorado statute harkens to the first of the U.S. general cybersecurity requirements, the Massachusetts information security regulation (201 CMR 17), which has since 2009 required all businesses regardless of industry to protect personal information of Massachusetts residents, including by adopting a written information security program, encrypting certain information, managing risks presented by third party service providers, and taking other steps to protect the confidentiality and security of the information.

Colorado is an example of considerable legislative activity in 2018 that focuses chiefly on privacy and notification issues but includes cybersecurity requirements. Other states with new or amended data breach notification and privacy protection laws are Alabama, Arizona, Delaware, Louisiana, Massachusetts, Oregon and South Dakota.

Further, much has been written about the European Union's GDPR that took effect on May 25, 2018. This regulation, with its sweeping privacy considerations, general cybersecurity obligation, and strict notification requirements, should not be overlooked by U.S. enterprises. There are several ways U.S.-based operations can be subject to the GDPR and we encourage all entities to assess carefully its applicability and obligations.

California has taken notice of the GDPR and enacted the California Consumer Privacy Act of 2018 (A.B. 375) on June 28, 2018. [see "Dropping Another Stone in the Pond? California's New Consumer Privacy Act" in this issue.] It is viewed as a compromise to avoid a November statewide ballot on an initiative of the same name. While it does not take up the NYDFS Cybersecurity Regulation's prescriptive security requirements, this law, which takes effect in January 2020, closely tracks the various privacy concepts of the GDPR. Given the role California played in adopting the first breach notification statute in the U.S., which then rippled across the nation to be adopted in one form or another in every state, observers are closely following this new California legislation. Among the requirements of the California Consumer Privacy Act are a duty to maintain reasonable security; an obligation to disclose the types of data being collected about California consumers; the requirement to produce to a consumer the categories, as well as the specific pieces, of information collected; and a right to be forgotten.

What's Next?

Looking ahead, there will certainly be further governmental attention at all levels in response to ever-increasing awareness of cybersecurity risks, the consequences of incidents, privacy concerns, and more. This attention can manifest, for example, in new laws or regulations, changes to existing law, and heightened enforcement. Also, as industry sectors wrestle with their potential challenges and exposures, industry-specific standards will continue to emerge.

The goal of any business should be risk mitigation, not merely compliance with applicable requirements. Therefore, those charged with assessing and managing privacy and cybersecurity risks at their organizations must continually monitor the evolving landscape of standards and requirements. Currently, the NYDFS Cybersecurity Regulation provides a useful model for managing these risks, regardless of industry.

Testing the Limits III – Cyber Coverage Litigation Focuses on Computer Fraud Losses

by Molly McGinnis Stine and Matthew Murphy

Fraudsters deploy different computer-related techniques but toward the same end – "gaming the system" for their own financial gain. Some victims turn to insurance for recovery. Four recent federal appellate decisions reveal courts' continued analysis of whether policies with computer fraud, funds transfer fraud, crime or other coverages respond to such losses of funds. These recent opinions, which come from four different appellate circuits, stress the significance of specific policy language and the particular facts of the scams.

The federal Ninth Circuit kicked off the recent flurry of activity in April 2018. In *Aqua Star (USA) Corp. v. Travelers Cas. & Sur. Co. of America*, 719 F. App'x 701 (9th Cir. 2018), the insured received a fraudulent email from one of its vendors requesting that the insured change the vendor's bank account information. The insured manually changed the account information and future wire transfers were sent to the hacker's account. The insured sought coverage under the computer fraud provision of its crime policy. The trial court granted summary judgment to the insurer based on an exclusion that the policy "will not apply to loss or damages resulting directly or indirectly from the input of Electronic Data by a natural person having the authority to enter the Insured's Computer System …." *Id.* at 702. The appellate court affirmed that the exclusion barred coverage.

In May 2018, the federal Eleventh Circuit ruled for the insurer in *Interactive Communications Int'l, Inc. v. Great Am. Ins. Co.*, No. 17-11712, 2018 WL 2149769 (11th Cir. May 10, 2018). Fraudsters manipulated the insured's computerized interactive telephone system, allowing them to load value onto debit cards from a single redemption multiple times instead of just once. The debit cards were then used for various purchases, which were honored by the debit card bank based on the value in a debit card account. The insured sought coverage under its computer fraud policy (coverage for "loss of, and loss from damage to, money, securities and other property resulting directly from the use of any computer to fraudulently cause a transfer of that property from inside the premises or banking premises: (a) to a person (other than a messenger) outside those premises; or (b) to a place outside those premises."). *Id.* at *2. The trial court, applying Georgia law, found no coverage for losses incurred from unauthorized redemption, holding both that the redemptions were not made through computers and that the redemptions were not the direct cause of the insured's losses. The appellate court affirmed on the grounds that the loss of money did not result "directly" (that is, "straightaway, immediately, and without any intervention or interruption") from the use of a computer system and was also "temporally remote". *Id.* at *4. The reviewing court did, however, disagree with the trial court's finding that computers were not involved.

The busy season ramped up with two decisions in July. The federal Second Circuit in *Medidata Solutions, Inc. v. Federal Insurance Co.*, 729 F. App'x 117 (2d Cir. 2018), agreed with the lower court that the insured was entitled to coverage under New York law. The case concerned fraudulent funds transfers resulting from spoofed emails when the insured's employee believed the requests had come from the company's president. The appellate court agreed with the insured that the computer

fraud provision of the policy applied because "the fraudsters … crafted a computer-based attack that manipulated [its] email system" that resulted in "a fraudulent entry of data into the computer system [the spoofing code]" and which altered "the email system's appearance … to misleadingly indicate the sender." *Id.* at 118. The appellate court further concurred with the lower court that the insured's loss was the direct result of the computer fraud. Noting that under New York law a "direct loss is equivalent to proximate cause," the court concluded that:

> [T]he spoofing attack was the proximate cause of [the insured's] losses. The chain of events was initiated by the spoofed emails, and unfolded rapidly following their receipt. While it is true that the [insured's] employees themselves had to take action to effectuate the transfer, we do not see their actions as sufficient to sever the causal relationship between the spoofing attack and the losses incurred.

Id. at 119.

And still one more ruling in July. Unlike the other three decisions, all of which affirmed the lower courts, the federal Sixth Circuit reversed the trial court in *American Tooling Center, Inc. v. Travelers Cas. and Sur. Co. of Am.*, No. 17-2014, 2018 WL 3404708 (6th Cir. July 13, 2018). The insured was hoodwinked by emails purporting to be from one of its vendors into sending money to the impersonator's bank accounts. The lower court said that the insured's crime policy covered "direct loss" of funds "directly caused by computer fraud" which was defined as "the use of any computer to fraudulently cause a transfer of money." The lower court concluded, under Michigan law, that the loss was not direct because it was not immediate and due to the intervening steps taken by the insured between the time it received the fake emails and the time it effected the three wire transfers. The Sixth Circuit disagreed, citing Michigan law indicating that "direct" means "immediate or proximate" as opposed to "remote or incidental." *Id.* at *4. Also, although the insurer characterized the use of computers as not enough to render a fraud a "computer fraud," the appellate court noted that "here the impersonator sent [the insured] fraudulent emails using a computer and these emails fraudulently caused 'the insured' to transfer the money to the impersonator." *Id.* While the insurer, according to the court, seemed to want to limit "computer fraud" to "hacking and similar behaviors," the policy's definition did not reflect such a limitation. The court also summarily rejected application of three policy exclusions raised by the insurer.

Another decision awaits treatment by the federal Eleventh Circuit. Oral argument is currently scheduled for November 2018 in *Principle Solutions v. Ironshore Indemnity Co.,* No. 1:15-CV-4130-RWS, 2016 WL 4618761 (N.D. Ga. Aug. 30, 2016). There, the trial court determined that, under Georgia law, there was coverage under a crime policy for a funds transfer resulting from spoofed emails. The court said that the policy's computer and funds transfer fraud provision providing coverage for loss "resulting directly from a 'fraudulent instruction' directing a 'financial institution'" to debit the insured's account was ambiguous and that intervening steps between receipt of the fake email and the funds transfer did not bar coverage. *Id.* at *5. According to the lower court's opinion, "[i]f some employee interaction between the fraud and the loss was sufficient to allow [the insurer] to be relieved from paying under the provision at issue, the provision would be rendered 'almost pointless' and would result in illusory coverage." *Id.*

The judicial scrutiny is not over, as coverage actions remain pending throughout the country, seeking a determination under commercial crime/computer fraud policies. Also, new matters continue to be filed. See, e.g., *Quality Plus Services, Inc. v. Nat'l Un. Fire Ins. Co. of Pittsburgh, PA,* No. 3:18-cv-00454 (E.D. Va. filed Jul. 2, 2018).

Although the ways in which these computer-related schemes operate often reflect cutting-edge technologies or new techniques, courts wrestle with coverage issues that have long been at the heart of insurance disputes. What is the policy's language? What jurisdiction's law controls? What constitutes a direct loss or proximate cause? What are the public policy issues concerning the scope of policy provisions? These recent decisions illustrate that insureds and insurers face a wide array of arguments that will mark the legal landscape. Disputed claims will continue to shape the body of law that both insureds and insurers should consider in their insurance transactions going forward.

ACCOLADES

- Legal directory *Chambers USA* ranked 55 Locke Lord lawyers and 18 of its practice areas for excellence in its 2018 edition including in Illinois for Insurance: Dispute Resolution and Insurance: Transactional & Regulatory and in California "also noted" for Insurance: Insurer. In addition, individual lawyers **Jon Biasetti**, **Nick DiGiovanni** and **Paige Waters** were ranked in Illinois (**Nick DiGiovanni** was also ranked Nationwide); and **Jonathan Bank** and **Elizabeth Tosaris** were ranked in California.
- Locke Lord Attorneys **Jonathan Bank**, **Jon Biasetti**, **Nick DiGiovanni** and **Alan Levin** were named to The International Who's Who of Insurance & Reinsurance Lawyers 2018 List.
- Chicago Partner **Patrick Byrnes** was named to 2018 Who's Who Legal Aviation: Contentious.
- Locke Lord's Insurance Law group was recognized by U.S. News/Best Lawyers in the National Tier 1 ranking and the Metropolitan Tier 1 Ranking for Chicago.

ARTICLES & MEDIA MENTIONS

- **Jonathan Bank, Al Bottalico** and **Robert Romaro** authored a Locke Lord QuickStudy, "Mind the Queue: Oklahoma's New Insurance Business Transfer Act" on August 23, 2018.
- **Elizabeth Tosaris** and **Jamie Mei Cheng** co-authored "Mercury Casualty Company v. Jones" for *Federation of Regulatory Counsel (FORC) Journal*, Volume 29, Summer 2018 edition.
- **Alan Levin** authored "Connecticut Governor Malloy Enacted Senate Bill No. 198," for the Connecticut Category of the *Federation of Regulatory Counsel (FORC) Alert*, July 2018.
- **Brian Casey** authored "Georgia Case Summaries Part 1," for the Georgia Category of the *Federation of Regulatory Counsel (FORC) Alert*, July 2018.
- **Tom Jenkins**, **Ben Sykes** and **Molly McGinnis Stine** co-authored "Cybersecurity Threats: What Every Guaranty Fund Director Should Know About Board Responsibilities and Obligations," for *NCIGF Leadership Update*, July 20, 2018.
- **Ted Augustinos** and **Molly McGinnis Stine** co-authored "Follow the Leader: NYDFS Cybersecurity Regulation Leads the Way for Other States and Industries," *CPO Magazine*, July 16, 2018.
- **Brian Casey** and **Ben Sykes** co-authored "Association Health Plans: Opportunity, Risks and Upcoming Battles," for *AHLA Weekly*, July 13, 2018.
- **Jonathan Bank** and **Matt Murphy** co-authored "How to Lose the Right to Arbitrate in One Easy (Mis)Step" for *Mealey's Litigation Report: Reinsurance*, Volume 29, #5, July 7, 2018.
- **Brian Casey** was quoted in GWG Again Extends Closing of $800 Million Deal with Beneficient for *The Deal Pipeline*, June 29, 2018.
- **Brian Casey** wrote an article titled "E-Signature Laws Provide Legal Framework for Blockchain" for *Law360* which appeared June 13, 2018.
- **Jon Gillum** authored a Locke Lord QuickStudy, "Powerful But Not Responsible: Texas Department of Insurance Clarifies Licensed Officer Requirement for Insurance Agencies," June 7, 2018.
- **Brian Casey** authored "Georgia House Bill 754 Division of Insurers," for the *Federation of Regulatory Counsel (FORC) Alert*, May 31, 2018.
- **Jonathan Bank** and **Matt Murphy** co-authored a Locke Lord QuickStudy: "How To Lose the Right To Arbitrate In One Easy (Mis)Step," May 24, 2018.
- **Ted Augustinos** and **Chris Barth** co-authored "Blockchain Technology Presents Privacy Concerns for Insurers" for *Insurance Journal*, May 21, 2018.
- **Jack Dearie**, **John Emmanuel** and **Zach Lerner** co-authored the Surplus Lines Manual update: "Excess and Surplus Lines Laws in the United States," which was posted and distributed May 18, 2018.
- **Jon Gillum** and **Lauren Fincher** co-authored "Cross-Agency Regulation of Service Contract in Texas" for the *Texas Tech Administrative Law Journal*, Volume 19, Book 1.
- **Brian Casey**, **Thomas Sherman** and **Jaremi Chilton** co-authored Taxing Life Settlements Investment Funds Under the TCJA," for *Law360*, May 15, 2018.
- **Jonathan Bank** and **Patrick Byrnes** co-authored the Locke Lord QuickStudy "Back to the Future," May 14, 2018.
- **Ted Augustinos** authored "A Cresting Wave: State cybersecurity requirements for insurers and producers will follow the lead of the NAIC and the N.Y. Department of Financial Services" for *Best's Review*, May 14, 2018.
- **Chris Barth** was quoted in the Cook County Record on April 16, 2018 in an article entitled, "Lawyer: IL Appeals Ruling Gives Plaintiffs' Bar Another 'Arrow' to Wrest Deals From Dismissed Defendants."
- **Brian Casey**, **Thomas Sherman** and **Jaremi Chilton** co-authored "Structuring Life Settlements Investment Funds After TCJA" for *Law360* on May 3, 2018.

RECENT CONFERENCES, PRESENTATIONS AND SPEAKING ENGAGEMENTS

- Locke Lord was a sponsor of the Reinsurance Association of America (RAA) Re Underwriting Seminar in New York, NY on September 6-7, 2018. **Julie Young** (Chicago) will be a presenter.
- **Nick DiGiovanni** (Chicago) and **Nigel Montgomery** (London) attended the Rendez-Vous de Septembre in Monte-Carlo on September 8-13, 2018.
- **Paige Waters** (Chicago) served as a moderator at the CEFLI Annual Conference in Denver, CO September 10-12, 2018.
- **Brian Casey** and **Thomas Sherman** (both Atlanta) will present at The Life Settlements Conference 2018 (DealFlow Event) in New York, NY on September 13, 2018.
- Locke Lord will sponsor the Association of Insurance Compliance Professionals (AICP) Annual Meeting in Nashville, TN September 23-26, 2018. **Jon Gillum** (Austin), **Al Bottalico** (Los Angeles) and **Brian Casey** (Atlanta) will be speakers, and **Stephanie O'Neill Macro** (Chicago) and **Elizabeth Tosaris** (San Francisco) will attend.

- Locke Lord is a sponsor of Property Casualty Insures (PCI) Northeast General Counsel Seminar in Cambridge, MA on September 24-25, 2018. **John Emmanuel** (New York), **Rowe Snider** and **Michael Mannion** (both Chicago) will attend.
- Locke Lord is a sponsor of the 9th Annual Extended Warranty & Service Contract Innovations Conference in Nashville, TN on October 1-3, 2018. **Brian Casey** (Atlanta) will present.
- Locke Lord is a sponsor of InsureTech Connect in Las Vegas, NV on October 2-3, 2018. **Brian Casey** (Atlanta), **Alan Levin** (Hartford) and **Kathleen Swan** (Chicago) will attend.
- **Rowe Snider** (Chicago) will present at the National Conference of Insurance Guaranty Funds (NCIGF) Fall Workshop in Fort Lauderdale, FL on October 3, 2018.
- Locke Lord is a sponsor of the American Council of Life Insurers (ACLI) Annual Conference in Washington, DC on October 7-9, 2018. **Paige Waters** (Chicago) will attend.
- Locke Lord is a sponsor of AIRROC Annual NJ Commutations & Networking Forum in Jersey City, NJ on October 14-17, 2018. **Jonathan Bank**, **Al Bottalico** (both Los Angeles), **Robert Kasinow** (New York) and **Alan Levin** (Hartford) will attend.
- Locke Lord is a sponsor of the Life Insurance Settlement Association (LISA) 24th Annual Fall Life Settlement & Compliance Conference in Orlando, FL on October 21-23, 2018. **Brian Casey**, **Thomas Sherman** (both Atlanta) and **Matthew Furton** (Chicago) will attend.
- **Alan Levin** (Hartford), **Rowe Snider** and **Michael Mannion** (both Chicago) will attend the Property Casualty Insurers (PCI) Annual Meeting in Miami, FL on October 28-30, 2018.
- **Nick DiGiovanni**, **Matthew Furton** (both Chicago), **Jonathan Bank** (Los Angeles) and **Donald Frechette** (Hartford) will attend ARIAS Fall Conference in New York, NY on November 8-9, 2018.
- Locke Lord will sponsor the 22nd Annual Insurance Forum in Chicago, IL on December 12, 2018.

EVENTS

- Locke Lord co-hosted with AIRROC the Boston Regional Education Day and Reception in our Boston office on September 12. **Jonathan Bank**, **Al Bottalico** (both Los Angeles) **Robert Romano** (New York) and **John Whitlock** (Boston) were presenters.
- Locke Lord will host a complimentary 3-hour CLE on "Cybersecurity Risk in Vendor Management" in our Houston office on September 12 and in our Dallas office on September 13. To register, click here.
- Locke Lord will host its popular cocktail reception at the NAIC Fall National Meeting in San Francisco, CA November 15-18. Watch for details on NAIC.lockelord.com, dedicated to providing the latest information on NAIC national meetings.

ANNOUNCEMENTS

- Locke Lord is pleased to announce that **Keith Andruschak** has joined Locke Lord's New York office as a Partner in the Firm's Regulatory and Transactional Insurance Practice Group. Keith has vast experience advising clients on complex transactions involving the insurance industry, including mergers, acquisitions and dispositions of insurers and reinsurers, joint ventures, life insurance reserve financing transactions, and insurance and other risk-linked securities. He is a frequent author and speaker on the topic of state insurance laws and regulations.
- We also welcome **Eric Cunningham** who has joined the Firm as Of Counsel in the Aviation Group. Eric has extensive experience litigating aviation matters, from commercial disputes to multi-fatality crash cases. He has represented clients in a broad range of aviation matters, including product liability, aircraft/airline operations, piloting and pilot training, certification and maintenance, airports, aircraft valuation and insurance coverage, and FAA enforcement actions. He is a member of the Air and Space Law Forum, Aviation Insurance Association, Lawyer-Pilots Bar Association, Aircraft Owners and Pilots Association, and Experimental Aircraft Association.