2019 New York Conference
December 5, 2019
New York, NY

The Intersection of Claims-Side Compliance and Extra-Contractual Exposure: Building a Successful Foundation for Your Claims Department

I. Intersection between claims-side compliance and minimizing/mitigating extra-contractual ("EC") exposure

An effective claims-side compliance program is pivotal to minimizing extra-contractual exposure. First- and third-party claims, and the handling of those claims, make up a significant area of an insurer's financial loss risk profile, including potential for mistakes in claims handling/payment leading to increased claim payments over contracted benefits; bad faith awards; and fines to insurance regulators for violation of state laws and regulations addressing claims handling.

Leaving claims professionals to handle claims solely based on their own knowledge and experience, has proven difficult to defend in bad faith claim settings (especially when dealing with allegations of systemic bad faith in handling numerous claims of the same variety). A claims-side compliance program provides the insurer with the opportunity to educate and keep claims professionals apprised of developments in the law and best practices, while also being able to document employee participation in the same, as well as determining whether the program is being effective in accomplishing those goals.

II. Insurance company claims-side compliance "best practices"

A. Assessing claims "quality" and the use of claims manuals

The masterpiece of any insurer's compliance program is its written claim manual. Claim manuals instruct adjusters on day-to-day operations, serve as training guides for new staff, inspire consistent, best practice standards for customer relations, and help minimize risk of financial loss. Claim manuals also help ensure a company's compliance with applicable state laws and mitigate regulatory risk. *The Art of Drafting Claims Manuals, Wolters Kluwer Financial Services* (Denise Terrier).

However, drafting a useful and effective claims manual must take into consideration factors such as – (1) the specific and varying state laws for which compliance is sought; (2) does our company have the resources to actually comply with the standard or requirement articulated in the claims manual; and (3) can compliance with the claims manual be assessed and documented such that revisions or the need for additional training can be assessed. The fundamental notion when it comes to a claims manual is that if the insurer is going to articulate a requirement in writing – the executing employees need to be able to comply and document compliance. Habitual non-compliance can be the source concerns from a bad faith perspective, as well as from a regulatory and market conduct perspective. In other words, if your claims manual says to do it, claims professionals need to – (1) be made aware of that requirement through training; (2) and have a means to document compliance such that during a routine review or audit of a claims file such compliance can be confirmed.

B. Compliance audit program "best practices"

To have an effective compliance audit program, an insurer must first identify and clearly define its "best practices." This serves as the foundation for the compliance audit program and ensures consistency. The "best practices" should regularly be reviewed to ensure they continue the "best practices." The review should be periodical but should also respond to regulatory and compliance changes, and must adapt to the claims environment as a whole. Once the "best practices" are identified and defined, they must be implemented. There should be a regular review of a sample of claims to ensure the "best practices" are being followed. The results of the review should be shared with appropriate persons, which must include anyone who may be affected by or benefit from learning about results. Through this process, training for new and existing employees may be identified. A training program that address issues identified during the periodical reviews, and also addresses regulatory changes, is critical. A regular re-review of a sample of claims is useful to determine if the education and training were effective. Another critical aspect to having successful "best practices" is to obtain "buy-in" from leadership as to the process as a whole.

C. Disseminating documenting processes and legal/regulatory requirements

The dissemination of process and legal/regulatory requirements is another critical function to having a successful "best practices" program. There should be an effective way to disseminate changes to legal/regulatory requirements. The information should be disseminated to those who may be affected by any legal/regulatory requirements. An insurer should also maintain an internal repository or a website that contains information on the processes and legal/regulatory requirements so it is available at all times. Continual training

should also be utilized to ensure employees are knowledgeable of the applicable processes and legal/regulatory requirements.

D. Training program "best practices"

1. Must effectively communicate legal and regulatory changes
2. Must be kept up to date - avoid use of out-of -date information and forms.
3. Provide information in understandable and useable format
4. Provide written resource for future reference
5. Ideally, training is communicated in short increments or succinct information to allow retention, versus longer dumps of significant amounts of information
6. Provide opportunities for active involvement versus passive attendance
7. Ensure ability to track and documents 100% impacted employee participation.

E. Special Investigation Unit "best practices"

1. Having one point of contact with counsel throughout EUO process helps keep messaging clear.

2. Always documenting and memorializing each investigative step and the reason for same.

3. Always document the "set up conversation"

4. Always keep the ball in the insureds' court

5. To prevent against bad faith delay, make sure the claim file is well documented that it is the insured who is responsible for any delay.

6. Courts have held that a long claim investigation does not necessarily constitute bad faith delay is the insured was responsible for the delay. *See Tangle v. State Farm*, 444 Fed. Appx. 592, 593 (3d Cir. 2011) (no bad faith even though 17 month delay in paying homeowner's fire claim – red flags provided carrier with reasonable justification for carrier's arson investigation); *3039 B Street Associates, Inc. v. Lexington Ins. Co.*, 740 F.Supp.2d 671, 681-82 (E.D. Pa. 2010) (no bad faith delay where carrier: kept in frequent and regular communication with insured; conducted initial inspection only 5 days after loss; expert provided estimate 80 days after loss; carrier promptly responded to insured's request for an advance).

F. Practical tips for market conduct examinations

1. Prior to exam, conduct self-audits and testing of known areas as to which market conduct examinations are directed, and take corrective action as warranted and document same (especially as to areas where past criticism and issues have been identified).
2. Prior to exam, monitor complaints to identify any trends in complaints that may be area of focus in market conduct examinations (to identify and correct root causes if common).
3. Prior to the exam, understand areas of assessment under NAIC Market Analysis Review (system of collecting, organizing, and analyzing data and other information to enable regulators to identify general market disruptions and specific market conduct problems as soon as possible, while maintaining an efficient and effective regulatory framework). Takes into account publicized litigation or media coverage issues; agent complaint increases; confirmed complaint index trends; loss and expense ratios; and other factors.
4. When examination called, understand why the examination has been called (routine/periodic or in response to complaints, market analysis, regulator concern or other) and scope of the exam
5. Understand what is at risk – market conduct penalties range from thousand to millions, and insurers bear the cost of the examination.
6. Pay attention to details of what information is being requested by examiners, and provide consistent answers across the company (try to limit scope of persons providing official company responses)
7. Cooperate with examiners – almost no examination is perfect (avoid sugar coating when clear area of non-compliance detected). Instead offer proactive solutions as part of negotiation of final report.

III. Compliance "best practices" for managing third-party vendors and potential EC implications (30 minutes)

A. Managing general agents, third-party administrators and others with "authority"

1. **Key provisions for written agreements**

   (1) Scope of Work - Clear definitions of the services the vendor will provide along with both parties' responsibilities.

   (2) Confidentiality - Sufficient security and confidentiality provisions that cover non-public personal information as well as proprietary information.

(3) Subcontractors - Should identify any subcontractors and ensure that these relationships are in accordance with industry guidance. And if any are identified, it's important that they include other typical provisions: that the vendor remains responsible for all contractual obligations; that the vendor will monitor and provide oversight; and that subcontractors will be held to standards no less than those established between you and your vendor.

(4) Indemnification – Most vendor agreements will benefit from an indemnification clause. Indemnification, by definition, is an obligation by which one party engages to save another from a legal consequence of the conduct of one of the parties, or of some other person. In a vendor agreement, it's usually reasonably for a vendor to agree to indemnify for a breach of warranty under the agreement, willful or negligent acts, omissions and for infringement of a third party's rights.

(5) Limitation of Liability – This clause is very common in vendor agreements. Typically, you will see a clause excluding a special, indirect, incidental or consequential damages from a party's liability as well as some sort of overall monetary cap to a party's liability.

(6) Relationship – it is important in a vendor agreement to define the relationship of the parties. In circumstances where the vendor has "authority," this authority needs to be spelled out exactly.

2. **Practical issues in enforcing written agreements**. For vendors with authority, an essential issue is to ensure that the vendor does not surpass the provided authority.

B. Independent adjusters, experts and others lacking "authority"

1. **Historical relationships and determining whether to have a written agreement**. Generally, it is always important to have a written agreement. For those vendors lacking "authority," the agreement is essential in demonstrating that the vendors are to be legally considered independent adjusters. The agreement should clearly state that the vendor in no way has any right, power, or authority to act on behalf of the other party.

2. **EC implications of third-party "panels".** Discovery typically will be sought from the Company in EC actions regarding the extent of

relationships with third parties in an attempt to show that any level of economic reliance by the third party creates a bias toward the insurer and tendency to skew the third party's opinion in favor of the insurer – and against insureds/claimants.

C. Existing obligations, emerging law and the obligation of third-party oversight

1. **"Adjuster" licensing requirements**. Few states do not currently license their adjusters: Colorado, DC, Illinois, Iowa, Kansas, Maryland, Massachusetts, Missouri, Nebraska, New Jersey, North Dakota, Ohio, Pennsylvania, South Dakota, Tennessee, Virginia, and Wisconsin. The issue in these states are, however, that many employers will only deploy licensed adjusters. For each state that require a license and are being worked in by an adjuster, each license will need to be obtained. Texas is the hub for most if not all states, i.e. – if you have a Texas license, it will be reciprocated by other states. Some states license entities as well as individual adjusters.

2. **Changes to privacy law:**

   a) California Consumer Protection Act. The California Consumer Privacy Act of 2018 is a bill passed by the state of California legislature and signed by its governor on June 28, 2018. The measure is officially called AB-375. Beginning 1/1/20, the bill, in part, would grant a consumer the right to request a business to disclose the categories and specific pieces of personal information that it collects about the consumer, the categories of courses from which that information is collected, the business purposes for collecting or selling the information and the categories of third parties with which the information is shared. The bill would also require a business to make disclosures about the information and the purposes for which it is used. The Act applies to businesses that have annual gross revenues in excess of $25M. The takeaway? Prepare and prepare now if handling insurance claims in California or any states with emerging legislature with similar requirements. For insurance companies working with third-party vendors in California, processes will need to be in place for these requirements.

   b) NY Department of Financial Services Cybersecurity Regulation. This is a new set of regulations from the NY Department of Financial Services (NYDFS) that places

cybersecurity requirements on all covered financial institutions, including insurance companies. These new rules impose strict cybersecurity rules on the covered organizations, including the installment of a detailed cybersecurity plan, the designations of a Chief Information Security Officer (CISO), the enactment of a comprehensive cybersecurity policy, and the initiation and maintenance of an ongoing reporting system for cybersecurity events. A cybersecurity program that complies with the new NYDFS Cybersecurity Regulation will adhere to the following: identify all cybersecurity threats both internal and external; employ defense infrastructure to protect against those threats; use a system to detect cybersecurity events; respond to all detected cybersecurity events; work to recover from each cybersecurity event; and fulfill various requirements for regulatory reporting. As for third parties who are given permissions to access systems and files operated by insurance companies, the following will also be required: risk assessment of third-party service providers; the covered financial institution's security requirements of third-party service providers that must be met in order to conduct business with that entity; processes for evaluating the effectiveness of a third-party service provider's security practices; and periodic assessments of third-party policies and controls.

D. The lack of practical difference between those with/without "authority"

1. **EC/coverage litigation discovery practices**. Carriers will want to maintain control of discovery procedures, even in cases where a vendor is another named defendant**.** Unless the vendor clearly acted in the wrong, then the carrier and the vendor may enter into a joint defense agreement, so that privileges and defenses are not inadvertently waived. As for discovery, all materials should be provided to counsel for the carrier so that one production and privilege log can be produced.

2. **Trial strategies when a third-party is a litigation party**. The first consideration must be whether or not to enter a joint defense agreement. If the parties' interests are completely aligned, then the carrier and vendor may enter one. This should be done before the parties engage in pleadings. Thereafter, all litigation strategies and decisions will be aligned