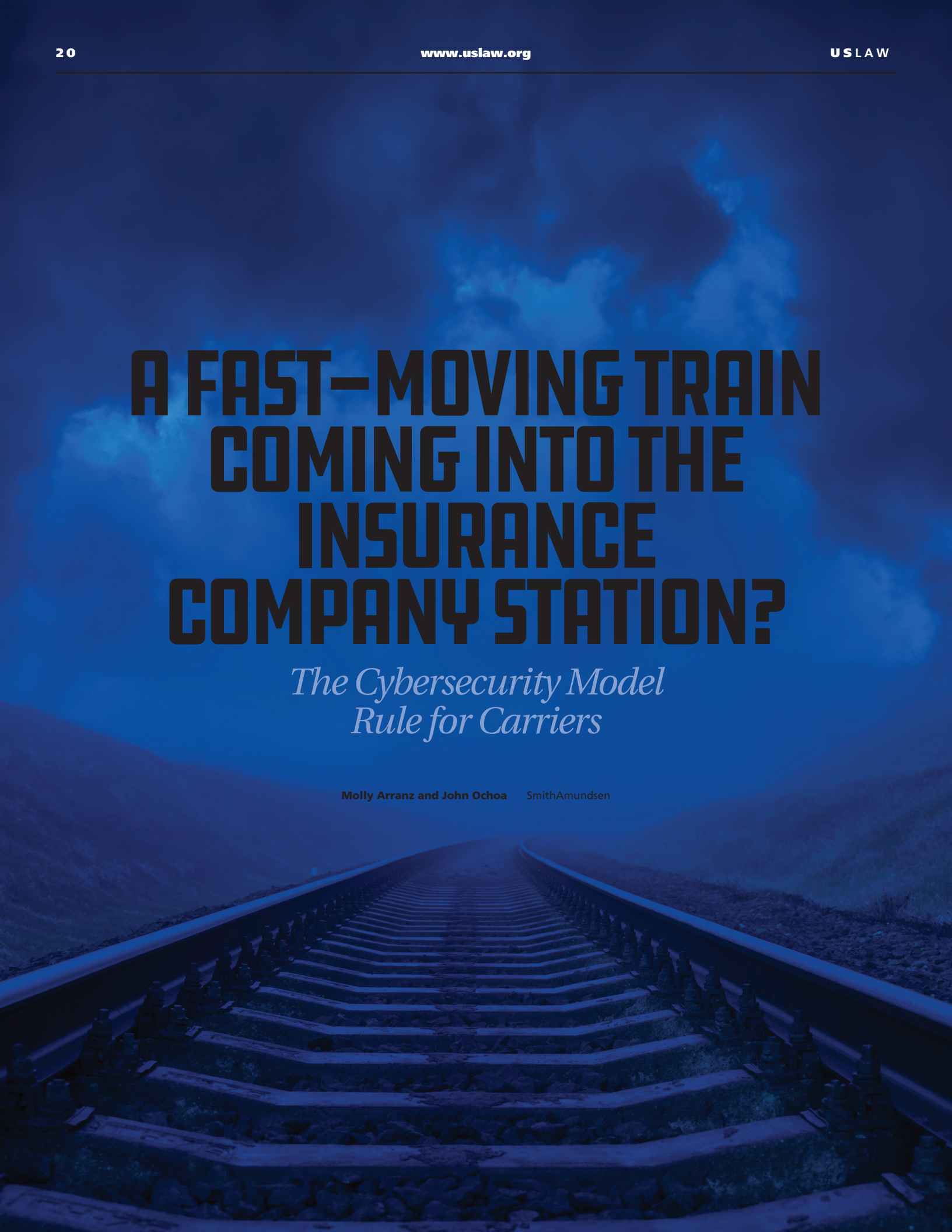

A FAST-MOVING TRAIN COMING INTO THE INSURANCE COMPANY STATION?

The Cybersecurity Model Rule for Carriers

Molly Arranz and John Ochoa SmithAmundsen

If you are an insurance provider, you already have pounding, regulatory headaches. Now, you may have one more.

Cybersecurity is perhaps one of the most important topics for any industry—and the insurance sector is chief among them. Insurers and insurance producers process and use highly sensitive information on a daily basis in the underwriting and claims processes. At the same time, there have been high-profile data breaches that have included two major hits in the insurance sector: Anthem and Premera Blue Cross.

These occurrences have heralded a swath of new state and federal legislation—and, the National Association of Insurance Commissioners (NAIC) has taken notice.

Last year, New York was the first state to enact regulations that require insurers to establish a comprehensive data privacy plan to protect their sensitive and confidential information from hackers and other unauthorized access. New York's cybersecurity regulations apply to any insurer licensed to sell insurance in the state of New York. That's (already) a broad group.

Other states have been getting in line. Specifically, the state legislatures in South Carolina, Michigan, Ohio, Mississippi and Alabama have all somewhat recently enacted cybersecurity legislation applicable to licensed insurance sellers in their states. And, within the next two years, insurance companies licensed in these states must be in compliance with state specific rules; they must file documentation certifying compliance—unless they qualify for an exemption. The consequences of non-compliance can range from revocation of licenses to fines.

Now that all 50 states have data breach notification laws, an unwary follower of cyber regulation may believe that those wide-ranging laws, in any given state, serve as the (sole) benchmark. Not so for insurance providers. In fact, South Carolina, Michigan, Ohio, Mississippi and Alabama all looked to and adopted, in substantial part, the NAIC's Data Security Model Rule, which came on the scene in the final quarter of 2017.

The NAIC's Model Rule is an acknowledgement that insurance companies often store and maintain large amounts of personal information about clients, and as a result, should proactively take steps to protect that information. The purpose and intent is: "to establish standards for data security and standards for the investigation of and notification to the Commissioner of a Cybersecurity Event applicable to Licensees."

The Model Rule contains several provisions with which insurers must comply, including, for example: a comprehensive data security program; designation of a chief information technology officer; regular training for employees on cyber risks; and, a data breach response plan. Notably, in light of the ever-developing ways in which cyberattacks occur—and are defined—a "cybersecurity event" means "unauthorized access to" "disruption [of]" or "misuse of" an information system or information.

It is expected that other states will soon follow these first five states. In fact, the NAIC drafted its Model Rule with the hope that all 50 states will have enacted this model rule in some form. Indeed, when a model rule is adopted, "it becomes a priority of the NAIC." The goal of such a Model Rule is to "encourage legislatures or regulatory bodies to adopt the model law, with as few changes as possible, in a majority of states within three years after its adoption by the NAIC members."

Now that all 50 states have data breach notification laws, an unwary follower of cyber regulation may believe that those wide-ranging laws, in any given state, serve as the (sole) benchmark.

Although the states that have looked to it have largely followed the NAIC's Model Rule, some variations exist, particularly with regard to the timeline for providing notice of a breach or incident to customers, as well as whether certain types of companies are exempted. Though the exemptions are generally based on both the total number of employees of a licensed insurer and the insurer's gross revenue, the critical mass for either benchmark can vary state-to-state.

In the end, this Model Rule may introduce additional or contrasting considerations and requirements for not only determining when a violation of a law or when a breach has occurred but also for reporting requirements. For example, a state may have a data breach notification law that defines a breach as "unauthorized acquisition" of sensitive data, while the Model Rule currently defines a reportable, cybersecurity event as, for example, a "disruption…of… an information system." If a state adopted the Model Rule wholesale, there would be competing deliberations for a triggering event that requires the carrier to notify. And, reporting to the state's attorney general may be the mandated requirement for a data breach, while notification to the Insurance Commissioner could be required for a "cybersecurity event." It appears there will continue to be a patchwork of laws, requirements and analysis.

With looming compliance requirements for adherence to the Model Rule, alone, insurance companies should take steps, today, toward the following:

- Review whether you do business in a state that has these cybersecurity regulations;
- Analyze whether your company qualifies for any exemptions from requirements in those state regulations;
- Partner with your cybersecurity advisors and attorneys to audit your current information systems to create a cybersecurity plan; and,
- Consider—and calendar—compliance and reporting deadlines in each particular state.

Finally, compliance with state cybersecurity laws is not only required—it could protect your company from litigation. In particular, Ohio's cybersecurity law contains a "safe harbor" provision, whereby a company that is in compliance with Ohio's cybersecurity law is entitled to an affirmative defense to any tort claim brought under Ohio law. This should provide added incentive for companies to ensure compliance with state cybersecurity laws.

Molly Arranz is the co-chair of SmithAmundsen's Data Privacy, Security and Litigation Practice Group and a partner in the firm's Class Action Practice Group. She is a CIPP-US, advising clients on how to protect against and respond to data and privacy incidents. She has defended more than eighty class actions involving a range of theories, including privacy violations, consumer fraud and breach of contract.

John Ochoa is a partner with SmithAmundsen's Class Action and Data, Security and Litigation Practice Groups. He has extensive experience litigating privacy and consumer protection claims. John advises companies on best practices for protecting their customers' and employees' personal information and in responding to suspected data breaches.