WHITE COLLAR

AGs: WATCHING OUT FOR CONSUMERS

State attorneys general have assumed a substantial enforcement role in recent years, and that trend continues. Companies need to be aware of the litigation risk this brings in several key areas—and to understand the potential opportunities that this trend creates, as well.

Today, state AGs are active on many fronts, from antitrust and environmental issues to the opioid epidemic. But they are especially focused on consumer protection—a natural fit for a group attuned to dealing with issues that resonate with the public. "The vast majority of AGs are elected," says Rebecca Monck Ricigliano, a partner in Crowell & Moring's White Collar and Regulatory Enforcement Group and former first assistant attorney general of New Jersey. "The few who aren't are appointed by the governor and confirmed by the state senate." As a result, they are sensitive to the attitudes of constituents—and "consumers" is a category that includes a wide swath of those constituents and cuts across social and political lines. "So consumer protection is a really good way for an AG to make a mark," she says.

Going forward, many AGs may be even more active on behalf of consumers as the Consumer Financial Protection Bureau and other federal consumer protection efforts are scaled back. Over the past year, groups of AGs have weighed in with the federal government on a variety of consumer-related issues, from net neutrality and the financial fiduciary rules to the Affordable Care Act, 3-D printing of guns, and cutbacks of federal regulations designed to protect nursing home patients.

TWO KEY AREAS OF FOCUS

Ricigliano says that in looking ahead to 2019, general counsel need to be aware of two areas of consumer protection that are on AGs' agendas:

- **Elder abuse and fraud.** AGs are pursuing more cases where senior citizens are victims. In 2018, the National Association of Attorneys General finished up an annual campaign targeting elder abuse, including financial exploitation, and many state AGs have established their own elder abuse units. In February of last year, a number of AGs participated in a coordinated multistate sweep of elder fraud cases that resulted in criminal charges for 200 people who were "engaged in financial schemes that targeted or largely affected seniors," according to a release from the Department of Justice, which helped coordinate the sweep. "In total, the charged elder fraud schemes caused losses of more than half a billion dollars," the DOJ noted. And in the health care arena, Ricigliano adds, "it's not just consumer fraud that companies need to think about if they're working with government. Many states have their own false claims acts, often with whistleblower provisions."

- **Technology.** With technology now an integral part of consumers' lives, AGs are looking at everything from cryptocurrency to mobile phone apps. In particular, they have made data privacy and cybersecurity a high priority, prompted in part by several well-publicized data breaches. For example, in May 2018, the New Jersey AG's office announced the creation of a Data Privacy and Cybersecurity unit that will work with other state agencies to investigate breaches and bring actions to protect residents' information. And in March 2018, the New York AG's office, which has participated in a number of data privacy-related investigations, joined with the Massachusetts AG to investigate Facebook's sharing of user data following the Cambridge Analytica scandal.

For most corporations, the chances of being involved in truly egregious fraudulent behavior are slight. The real risk lies in the less obvious problems, where seemingly innocent business practices can lead to unintentional violations of regulations. "In some states, there are requirements that prices need to be clearly displayed," says Ricigliano. "Or there may be rules about how a company does its billing or about making sure consumers are aware of fees that they are going to incur. Activities relating to the consumer's pocketbook usually get the attention of AGs and create risks for companies." Not surprisingly, many of the less obvious risks today are technology-related. "Is the corporation doing enough to advise people about the availability of parental controls? What are the opt-in and opt-out provisions for smart products' data use? Are customers being advised about how their information is being used?" she says.

WORKING WITH AGs

In assessing risk, companies should factor in the wide range of discretion and power that AGs have. They can enforce state laws and some federal laws, pursue civil suits on behalf of the state or citizens, issue opinions to state agencies, act as

"Unlike the DOJ, [AGs] have an extraordinary ability to identify an issue, enforce it through civil or criminal actions, and then look at holistic policy or legal changes."

—*Rebecca Monck Ricigliano*

public advocates in a number of areas, and propose litigation, among other things.

In addition, says Ricigliano, "a big difference between AGs and the federal government is that the federal government might have a few local districts in a state—New York has four federal districts, for example. But the AG covers the entire state. So they can take a really broad look at the issues and concerns of their constituents and figure out how to best tailor not only enforcement actions but programmatic policy changes. Unlike the DOJ, say, they have an extraordinary ability to identify an issue, enforce it through civil or criminal actions, and then look at holistic policy or legal changes."

What's more, Ricigliano continues, "AGs have the power to come together in concerted multistate actions, which can be a litigation morass for companies and result in very large fines." The best known of these actions is, of course, the 1998 $246 billion Tobacco Master Settlement Agreement. But AGs have continued to collaborate in areas such as loan and mortgage foreclosure fraud and, most recently, suing opioid manufacturers.

While weighing the growing risks of litigation at the state level, companies should also view this trend as an opportunity—and look for ways to leverage AGs' heightened interest in consumer protection. That could mean collaborating with the AG to attack fraud perpetrated on the company by scam artists or robo-callers identifying themselves as company agents, for example. In that type of case, says Ricigliano, "because the state AGs have that ability to look at an issue holistically, they can issue press releases warning of the scam and get the word out through the media to more quickly and efficiently educate the public and protect consumers."

Collaboration might also involve working with the AG's office to help identify consumer fraud in the company's industry, or participating in the AG's fraud-education programs for consumers. Or it could mean proactively approaching the AG's office when a company's internal investigation finds that it is inadvertently violating some consumer protection rule.

"Those kinds of actions may not make a problem go away," says Ricigliano. "But they will allow you to become a known quantity and be seen as a good corporate citizen. If you're self-reporting a problem, it's much easier to engage a state AG with a remedial plan of action if you have a relationship with that office—if you have come to them before as an aggrieved party or as a partner. It's a much easier conversation if there is already an existing relationship."

COOPERATION: STILL HARD TO PIN DOWN

Companies involved in government investigations usually face a difficult choice: disclose potentially privileged information to get credit for cooperation and risk waiving privilege or hold privileged information back and risk missing out on full credit. It's not always clear which route is best.

Case law has not provided clarity on what waives privilege in communications with the government or enforcement agencies. Erring on the side of caution, attorneys communicating with the government on behalf of their corporate clients will often share factual information obtained from privileged witness interviews by verbally providing hypothetical scenarios or blending information learned from multiple witnesses, rather than attributing information to specific witnesses.

In late 2017, a magistrate judge in the *SEC v. Herrera* case issued an opinion that served as a warning to attorneys who do not hew to the more cautious approach outlined above. In *Herrera*, attorneys for General Cable Corp. had conducted an internal investigation into accounting errors. When reporting their findings to the SEC, the firm's attorneys provided "oral downloads" of witnesses' individual interviews to the commission. When the SEC later sued several General Cable employees in the matter, the defendants asked for the written notes and memoranda for the interviews verbally recounted to the SEC. In late 2017, the court ruled in their favor, saying that the company had already disclosed the information to a potential adversary—the SEC—orally.

"The decision in *Herrera* shows the danger of providing verbatim information—even verbally—to the government, but it can be hard to know exactly how much information can be shared without waiving privilege," says Crowell & Moring's Rebecca Monck Ricigliano. "As a result," she adds, "it is critical to understand the judicial landscape where an investigation is taking place and adjust strategies for engaging on the facts with the government accordingly."