

ENFORCEMENT

DESPITE A SOFTENING IN REGULATIONS, ENFORCEMENT CONTINUES



The Trump administration's focus on reducing government regulation continues, but reduced regulation does not necessarily mean government enforcement will abate. In fact, steady enforcement continues, and agencies are focusing their resources on the administration's priorities.

"The regulatory landscape is fluid," says [Paul Rosen](#), a white collar, investigations, and cybersecurity partner at Crowell & Moring and a former federal prosecutor and chief of staff for the Department of Homeland Security. "It will evolve and change with significant events, and companies need to stay prepared and nimble."

Even with an overall softening in regulation, there are several key areas where the federal government will devote significant enforcement resources, such as drug trafficking, violent crimes, and immigration enforcement. And in the areas that the administration may not consider top priorities, such as consumer protection, in many cases, state attorneys general are likely to step up and fill the regulatory voids.

HEALTH CARE FRAUD AND OPIOIDS

Health care fraud clearly has the Trump administration's attention. Attorney General Jeff Sessions affirmed his support for prosecution of health care fraud, and civil and criminal enforcement across the health care industry continues unabated.

But that support comes with a caveat. "We will not likely see a significant number of new regulations, which means outdated and ambiguous regulations will continue to present a challenge for companies in the health care industry," says [Laura Cordova](#), a partner in Crowell & Moring's [White Collar & Regulatory Enforcement](#) and [Health Care](#) groups who served as assistant chief and head of the Corporate Health Care Fraud Strike Force in the Fraud Section of the Department of Justice Criminal Divi-

sion. "A lack of new regulations could actually have negative implications for companies that struggle to develop new and innovative business models that comply with ambiguous or outdated regulations," she adds.

In addition, some resources that were typically focused on traditional health care fraud are now being diverted to the opioid crisis, something the Trump administration has said is a top priority. "On the enforcement side," Cordova says, "when an investigator has a dozen cases sitting on her desk and one of those cases involves opioids, it will get the investigator's attention. Even though it might not be the biggest case with the highest dollar value, it will get attention because the administration has made clear that its strategy to address the opioid crisis includes prosecuting those engaged in illegal activity involving opioids."

FIGHTING FINANCIAL CRIME

Anti-corruption, foreign bribery, and securities fraud—offenses that occur across a broad range of industries and companies—are going to stay firmly in the government's crosshairs. "DOJ continues to focus on financial crimes, and that is likely to continue," Rosen says. These investigations include a more focused effort to work closely with foreign governments, to the point of embedding DOJ officials with law enforcement agencies overseas to increase cooperation in parallel cross-border investigations. Such cooperation will make it easier for federal investigators to get access to foreign evidence and witnesses that are otherwise potentially outside the reach of U.S. authorities.

Rosen notes that the Trump administration has clarified how it expects companies to stay in compliance with the Foreign Corrupt Practices Act. It recently unveiled a revised FCPA enforcement policy that essentially made permanent many provisions of a pilot program started under the Obama administration. However, the Trump policy comes with one key additional olive branch: a presumption of a criminal declina-



"The regulatory landscape is fluid. It will evolve and change with significant events, and companies need to stay prepared and nimble." —*Paul Rosen*



“We will not likely see a significant number of new regulations, which means outdated and ambiguous regulations will continue to present a challenge for companies in the health care industry.”

—Laura Cordova

tion (no criminal charges) if a company voluntarily self-discloses misconduct and cooperates early and fully.

“We’re continuing to see large FCPA and securities fraud cases,” says Cordova. “Enforcement continues at much the same pace, which is to be expected because prosecutors are making their cases. It’s not as if the whole workforce changed with the administration.”

BATTLING THE BREACHES

Over the past year, many have learned what experts and security insiders have long known: cybersecurity threats and attacks are here to stay. As digital attacks on companies such as Yahoo!, Equifax, and Uber—and even the SEC—have dominated headlines, the stunning speed with which the Petya/NotPetya ransomware viruses attacked thousands of companies around the world further underscores the seriousness, permanency, and global nature of the threat.

The government and the private sector are working hard to manage existing threats and prevent future attacks on their networks and systems. Meanwhile, courts are wrestling with damage claims by shareholders and consumers whose information may have been taken. As high-profile breaches continue, the government will keep evaluating and refining its asset protection and consumer protection regulatory role.

“Increasingly sophisticated cyberattack capabilities are a boon to criminals and state-sponsored actors seeking to get rich or wreak havoc from afar,” says Rosen. “No longer does somebody have to walk into a bank to rob it—they can simply conduct a ransomware attack from halfway around the world. And foreign adversaries that don’t have the skill or the will to innovate can just try to hack American companies that do. The stakes are high, and American businesses are on the front lines.”

The government is taking the cybersecurity challenge and threat seriously. It has the unique ability and set of tools to hold hackers accountable, and it will continue to do so.

KEEPING UP WITH INNOVATION

Technology has defined American innovation and advancement. But recently it has presented regulatory uncertainty because of the rapid advances in autonomous automobile and drone technology and the issues they raise regarding physical safety, cybersecurity, consumer protection, and insurance. In a sign of how the administration is approaching its regulatory treatment of these technologies, the Department of Transportation and

HOLDING INDIVIDUALS ACCOUNTABLE

As part of its new policy on the FCPA, the Department of Justice sent a message that it is continuing its focus on individuals by maintaining pressure on companies to turn over information on culpable individuals.

The FCPA policy announcement followed an October 2017 speech in which Deputy Attorney General Rod Rosenstein previewed that any changes to the policy detailed in the Yates Memo would reflect a continued resolve to hold individuals accountable for corporate crime.

The Yates Memo was the September 2015 pronouncement by then-Deputy Attorney General Sally Yates that called on DOJ prosecutors to focus their resources on investigating and charging individuals involved in criminal activity even when the crimes were committed on behalf of a corporation.

When it comes to individuals, Crowell & Moring’s Laura Cordova says there is likely to be little change to the policy and practice that individuals should be criminally charged where the evidence supports it. Indeed, we are likely to see a continued focus on prosecuting individuals. In the end, the government—and in particular DOJ—will continue to enforce laws by bringing civil enforcement actions and criminal charges against individuals and corporations across industries.

the National Highway Traffic Safety Administration issued new Automated Driving System guidance to encourage the development of self-driving cars while maintaining the safety of the roadways, with as little interference as possible from the federal government. In doing so, it relaxed the already flexible guidance issued at the end of the Obama administration.

The DOT and NHTSA guidance demonstrated that the Trump administration will, as expected, take a hands-off approach as companies roll out products based on the new technologies, Rosen says. “But the regulatory rope that these companies enjoy could quickly be curtailed if a significant cybersecurity or physical safety incident occurs, or if the power in Congress shifts—which is why businesses should tread carefully in this space,” he adds.