LAW360

Portfolio Media. Inc. | 111 West 19th Street, 5th Floor | New York, NY 10011 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

3 White Collar Trends To Watch In 2022

By **Jack Queen**

Law360 (January 3, 2022, 12:03 PM EST) -- After a slow start filling out its leadership ranks last year, the U.S. Department of Justice spent the second half of 2021 rolling out a parade of policy changes and enforcement initiatives aimed at tackling corporate malfeasance, corruption and cybercrime.

The flurry of policymaking contrasts with a lull in major enforcement activity. Blockbuster cases were sparse in 2021, and fresh industry sweeps didn't materialize. Prosecutors and the courts were still working through pandemic-induced backlogs, and lockdown measures undoubtedly slowed the pace of investigations.

But the feds are starting the new year with clear marching orders and a leadership vision crystallized through recent speeches and directives that could shape the white collar landscape for years to come. The biggest sea change was signaled by Deputy Attorney General Lisa Monaco, who unveiled a return to tougher Obama-era corporate enforcement standards that were shelved or softened under the Trump administration. The move indicates that a long-predicted surge in enforcement under President Joe Biden is approaching.

"The DOJ is sending a strong message that it wants to recommit to prosecuting corporate crime to the fullest extent of the law," Boies Schiller Flexner LLP partner and ex-prosecutor Lauren Bell told Law360.

Here's a look at three trends to watch.

A New Era in Corporate Enforcement

Monaco laid out her new enforcement blueprint in an October speech, detailing tougher standards for corporate cooperators, broader scrutiny of past misconduct and a renewed willingness to impose monitorships as conditions of settlements.

Attorneys are still parsing the implications, particularly around their clients' willingness to voluntarily report misconduct to the government. The new policies roll back some of the Trump administration's efforts to encourage self-reporting, placing greater emphasis on proactive policing.

To receive cooperation credit, companies will now be required to name every person potentially involved in misconduct, no longer just those who were "substantially" involved. Some attorneys are concerned that the change is a return to an onerous standard that bogs down investigations as companies search for people who aren't meaningfully connected to malfeasance.

"I hope it's not a significant shift, but I'm worried that it's going to be," Paul Hastings LLP partner and former federal prosecutor Nathaniel B. Edmonds told Law360. "If there's truly a request to find everyone who's potentially involved, that could grind investigations to a halt. ... Having been on both sides of the table, it can be very difficult to draw the line."

DOJ officials and recent alumni counter that having access to the lower ranks of an organization is crucial to investigations.

"The department doesn't want to limit itself," Morgan Lewis & Bockius LLP partner and former DOJ Fraud Section chief Sandra Moser told Law360. "Sometimes you get incredibly valuable information from lower-level people, not only about how a scheme might work but also who's giving the orders. If you start at 'substantially' involved, there might be a good chunk of people you miss."

In another change, Monaco said the department will now examine all past misconduct when evaluating possible nonprosecution or deferred prosecution agreements, citing estimates that 10% to 20% of corporate criminal resolutions involve repeat offenders. But the change has raised fears that minor slip-ups unrelated to the conduct in question could imperil a company's chances of getting a deal.

"How would a settlement with the SEC or an issue with the DOJ in a different area 15 years ago weigh in the department's thinking? There have been efforts to shed light on these issues, but ambiguity remains," Jessie K. Liu, a Skadden Arps Slate Meagher & Flom LLP partner and former D.C. U.S. attorney, told Law360.

Justice Department officials have sought to allay these concerns, saying prosecutors will have discretion to weigh the importance and relevance of past infractions. But the change could upset the balance the DOJ aims to strike between holding wrongdoers accountable and encouraging them to self-report.

"If I had to predict, I think these changes may make companies less likely to self-disclose," Liu said. "One thing the voluntary disclosure regime has struggled with is that it's not clear what benefits you get."

The DOJ has tried to clarify the benefits in public statements about settlements, detailing the penalty reductions they granted in exchange for specific elements of cooperation. But it's still not an exact science, according to Liu, who said Monaco's announcements could "muddy the waters."

Attorneys will have to wait for new cases to clarify how the department will apply the policies. But the department clearly feels that too many companies are repeatedly getting probation with nonprosecution and deferred prosecution agreements, meaning indictments could become more common.

"I think the only reasonable way to read that [Monaco] speech was: Once you get these diversions, like an NPA or a DPA, the next time you get in trouble, there will be nothing left to do but plead to something," Liu said.

Catching Up With Corruption

President Biden declared global corruption a national security risk in June and followed up in December with a governmentwide strategy to police graft around the world. The ambitious plan was widely hailed as a game-changer, even if some attorneys are skeptical the government will pony up the resources to

make it work.

Many aspects of the plan call for better communication between siloed agencies that don't always share information or use their unique enforcement tools in concert with one another. The unity of purpose could lead to more sophisticated, coordinated attacks on corrupt schemes, which will be key to achieving the administration's goal of cracking down on the lawyers, accountants, real estate brokers and other professionals who facilitate the flow of dirty money around the world.

"This is a high-level directive, so you're not going to have midlevel bureaucrats saying, 'No, this isn't what the government wants to do,'" Edmonds told Law360. "There's no ambiguity about what the larger mission is. ... It's going to encourage collaboration and innovation."

The plan is ambitious, with more than a dozen strategic objectives that will demand resources from scattered agencies with their own existing priorities. The scale of the problem itself is also daunting: The White House estimates that 3% to 5% of the global economy is linked to corruption, or roughly $250 million in illicit payments every hour.

Some attorneys caution that the plan will need additional investment to succeed.

"The deployment of resources to the relevant agencies, including DOJ — as opposed to the tradition of 'doing more with the same' — will be critical to seeing any one of these strategic objectives succeed," Moser said.

The Justice Department's Foreign Corrupt Practices Act unit, meanwhile, has been caught in a long period of pandemic-related travel restrictions that limited global corruption probes, which are uniquely reliant on in-person investigation. FCPA indictments last year largely stemmed from legacy investigations, including years-old probes into Brazil's Odebrecht SA and Venezuela's PDVSA.

"It feels like they have some catching up to do," Moser said. "We didn't see much action over the past year ... but these investigations do take a long time. There's always a lot in the hopper — nobody at the FCPA unit is looking around saying, 'Gee, we need something to investigate.'"

Plenty of work can still be done while office-bound, including the data analysis that has become increasingly important in the FCPA unit and beyond. Building custom algorithms to mine troves of data for leads and evidence is labor-intensive, but it's worth it, according to Bell, who said big data became a top priority in the years before she left the DOJ in 2020.

"Obtaining terabytes and terabytes of data from different agencies, working with experts to come up with an algorithm that can detect irregularities, and then applying that algorithm to these terabytes of data is expensive and time-consuming," Bell said. "But it pays off well, so I expect to see more of that."

Striking First on Cybercriminals

Monaco's tenure as deputy attorney general has been marked by a high-profile push to crack down on cybercrime and ransomware. The effort has yielded some early successes, but keeping the momentum going will require balancing cooperation with the private sector and accountability for those who neglect the security of their networks, experts say.

As cyberattacks continued to pile up in 2021, Justice Department officials implored companies to come

forward immediately after breaches to give investigators a jump on finding the culprits. Victims would be treated like victims, officials said, assuring companies they had no interest in penalizing them for holes in their defenses.

But Monaco sent a different message in October, when she unveiled a civil cyber-fraud initiative that will use the False Claims Act to penalize government contractors and grant recipients who knowingly provide deficient information security service, misrepresent their information security protocols or violate their duty to monitor and report breaches.

Monaco called out companies that "fail to follow required cybersecurity standards" and choose not to report incidents under the "mistaken belief that it is less risky to hide a breach." But the distinction may not be so clear for companies that suffer attacks, attorneys say.

"That got some criticism in white collar circles because there was a sense that if a company was a victim of a hack or ransomware attack, they might be blamed for not having enough cybersecurity," Liu said. "Some people wonder that with the announcement of that initiative, more companies might just quietly pay the ransom and hope it goes away."

The DOJ also unveiled its National Cryptocurrency Enforcement Team in October, which will focus on criminal activities by exchanges and so-called tumblers and mixers, or services that combine batches of cryptocurrency to obscure their sources.

The move builds on the government's efforts to better track and claw back cryptocurrency ransom payments. A notable success in 2021 included a seizure of $2.3 million worth of bitcoin paid by Colonial Pipeline to criminals who held its network hostage. In October, the department also announced a sweeping bust of 150 "dark net" drug suspects that yielded $32 million in cash and cryptocurrency.

Brandon Van Grack, a Morrison & Foerster LLP partner and former federal prosecutor, told Law360 that the feds appear to be increasingly going on the offensive against cybercriminals by shutting down servers and identifying threatening actors before they strike.

"They've done a lot of very proactive things on the ransomware and cyber front," Van Grack said. "I think they get top marks for marshaling resources and taking steps that the Justice Department and FBI typically didn't take before."

The government still has plenty of work ahead as it adapts regulations, enforcement mechanisms and divisions of labor between agencies to corral illicit flows of crypto and protect companies from digital raiders, according to Edmonds.

"Part of the struggle for our clients is, what do they do if the government isn't catching these people?" he said. "The regulations need to catch up with what's happening on the ground, otherwise companies get caught in the middle."

--Editing by Brian Baresch and Daniel King.

All Content © 2003-2022, Portfolio Media, Inc.