Davis Polk

Carlin speech signals DOJ white collar enforcement priorities

October 20, 2021 | Client Update

In a recent speech, PADAG John Carlin previewed DOJ's refocused corporate enforcement efforts and priorities. He addressed a variety of topics, including an upcoming review and revision of white collar enforcement policies; a "surge" in resources; greater international cooperation and use of data-driven enforcement techniques; increased enforcement related to sanctions, export controls, and cryptocurrency; and warnings regarding resolution and subpoena compliance.

Principal Associate Deputy Attorney General John Carlin previewed the Department of Justice's (DOJ) refocused corporate enforcement efforts during a speech on October 5, 2021 at GIR Connect: New York. Carlin's speech underscored the primary levers a new administration can pull to quickly and meaningfully impact the white collar enforcement space: messaging increased white collar enforcement to relevant stakeholders, instituting new and revising existing policies, creating dedicated taskforces, and increasing resources for white collar enforcement. Carlin addressed each of these categories by outlining key DOJ priorities, including increased enforcement related to sanctions, export controls, and cryptocurrency; continued expansion of international cooperation and coordination; a "surge" in resources, exemplified by a new dedicated FBI squad for Foreign Corrupt Practices Act (FCPA), market integrity, and health care fraud investigations; an upcoming review and revision of corporate enforcement policies; continued and increased use of data-driven enforcement techniques; enhanced and expanded international cooperation; and a warning regarding companies' compliance with subpoenas and the terms of resolution agreements.

1. Revision of white collar policies

While many anticipated a review and revision of DOJ's policies by the new administration, Carlin confirmed that DOJ plans to reassess and potentially update some of its most influential corporate enforcement policies in the near future. In particular, he previewed possible changes to policies regarding the role of individual accountability in white collar enforcement, the use and application of corporate resolutions, and the weight given to cooperation efforts. Carlin said that DOJ's evaluation of its corporate prosecution policies and guidance would be rooted in the administration's stated priorities of enhancing public trust not only in corporations but also in the capacity of regulators to provide impactful oversight.

One anticipated area of revision is the requirement that companies provide information related to individuals in order to receive cooperation credit from DOJ. The "Yates memo," which required companies to provide information related to all individuals involved in the alleged misconduct in order to receive any cooperation credit, was narrowed during the Trump Administration to require that companies need only provide information related to those individuals "substantially involved in or responsible for" the alleged misconduct. Commentators have speculated that the Biden Administration will revert back to the Yates formulation.

It is unlikely, however, that all policies across the board will be revised. For example, given that Carlin cited approvingly of the DOJ National Security Division's (NSD) voluntary disclosure policy—which incentivizes companies to identify and voluntarily self-disclose sanctions and export control violations—and that the FCPA Corporate Enforcement Policy was initially instituted as a pilot program during the Obama Administration, it is unlikely that these policies will see drastic pull-backs.

Insights

Carlin stated that more information about potential changes to the corporate enforcement policies is going to be announced in the coming weeks.

2. Surge in resources

Carlin emphasized DOJ's redoubled commitment and a forthcoming "surge" of resources for corporate enforcement to support investigation and prosecution efforts. As an example, he cited the creation of a new FBI squad dedicated to DOJ's Criminal Division, Fraud Section, which investigates and prosecutes all FCPA violations, as well as commodities and securities fraud, fraud involving cryptocurrency and financial institutions, and health care fraud. This dedicated squad will mean increased capacity to investigate these types of misconduct and, as Carlin explained, will enable greater focus on data-driven initiatives and cases, including programs focused on predicting corporate misconduct.

The Biden Administration's commitment to enhancing white collar enforcement through the use of specialized and inter-agency task forces is further underscored by the recent establishment of Joint Task Force Alpha, which will marshal the resources of DOJ and its partners (both domestic and foreign) to combat corruption in the Northern Triangle nations of Guatemala, El Salvador, and Honduras. President Biden's June 3 Executive Memorandum also initiated an interagency review process that includes DOJ and sets the goal of developing a strategy that will more appropriately resource and empower key agencies to promote good governance and combat corruption internationally.

In light of these initiatives and Carlin's announcement of a "surge" in resources, including citation to this FBI squad as but one example of such a surge, clients should expect yet additional resources to be allocated to white collar enforcement and a corresponding increase in investigations.

3. Increased use of data

As a corollary to the announcement of an FBI squad dedicated to data-driven initiatives, Carlin also previewed an increase in the use of data to investigate and prosecute white collar crimes more generally. While DOJ has long used data-driven techniques to investigate white collar crime, Carlin explained that such techniques now provide additional opportunities not only to hold criminals accountable, but also to predict and deter crime. Carlin cited as examples the Fraud Section's longstanding use of data analytics in the health care fraud and financial services fraud arena, and the U.S. Securities and Exchange Commission's (SEC) and SDNY's use of data analysis in connection with insider trading cases. He also noted that DOJ will continue to enhance its use of data-driven analytics across a variety of other white collar crimes, and that DOJ will expect corporations to embed and apply similar analytics in their compliance programs to identify and anticipate misconduct. The Criminal Division's Evaluation of Corporate Compliance Program, for example, was revised in 2020 to include additional questions and topics related to data analysis. Carlin noted that the best use of data will involve close working relationships with regulatory and other partners, adding that sharing the "same fruits of analytic labor" will be key.

4. Increased focus on sanctions and export control

A substantial portion of Carlin's speech focused on the recent trend of increased enforcement of sanctions and export controls, with open investigations now totaling 150. He noted that this enforcement activity is critical to protecting national security and U.S. technology, and that he expected this upward trend to continue. Carlin also conveyed an expectation that sanctions and export control enforcement would benefit from continued use of new tools and innovations. Among others, this includes a broader conception of what constitutes an export control violation. Carlin explained that now, the focus is not only on the transference of intellectual property, but also on "human knowledge," citing a recent deferred prosecution agreement (DPA) involving three U.S. citizens who agreed to pay over $1.6 million for serving as "hackers for hire" for another government.

Carlin encouraged companies to increase their familiarity with the DOJ NSD policy incentivizing companies to identify and voluntarily self-disclose sanctions and export control violations, close in kind to the FCPA Corporate Enforcement Policy. Deeming it a "proof of concept," he spotlighted the first non-prosecution agreement (NPA) reached as a result of the NSD policy in April 2021, in which SAP, a German software company, was required only to disgorge gains, without a fine or requiring a monitor, resulting from the company's voluntary disclosure, extensive cooperation, and strong remediation.

Carlin's remarks come at a time when the Treasury Department has expressed an intent to use economic and financial sanctions more strategically. There have been sixteen enforcement actions by the Treasury

Department's Office of Foreign Assets Control (OFAC) to date this year. Last month, for instance, OFAC settled with a Texas-based oil and gas supplier, Cameron International Corporation, for providing services to a sanctioned Russian energy firm. On Monday, however, Treasury Department officials said that while sanctions will remain a critical policy tool, they need to be better calibrated. Still, as the list of sanctioned countries and individuals continues to grow, clients will need to exercise additional due diligence to ensure compliance.

5. Increased enforcement of cryptocurrency crime

In addition to DOJ's focus on sanctions and export control enforcement, Carlin stressed that cryptocurrency was "ripe for vigorous enforcement." He cited its increasing prominence in a variety of criminal activities, including its use in drug transactions, child exploitation, ransomware attacks, and terrorism. Carlin teased "additional announcements about increasing [DOJ's] capacity and changing [its] structure as it comes to cryptocurrency enforcement." We now know that Carlin was referring to Deputy Attorney General Lisa Monaco's announcement the next day of a new National Cryptocurrency Enforcement Team—which will tackle complex criminal misuses of cryptocurrency, particularly by virtual currency exchanges, mixing and tumbling services, and money laundering infrastructure actors—and a new civil-cyber initiative that will use civil enforcement tools to try ensure compliance with recommended cybersecurity standards.

In his speech, Carlin referred to several tools DOJ intends to use to improve and increase its cryptocurrency crime enforcement capacity. The Bank Secrecy Act—including its requirement for financial institutions to maintain an adequate anti-money laundering compliance program and comply with record-keeping and reporting requirements—is one such tool. In addition, the recently-passed Anti-Money Laundering Act (AMLA) also has several provisions that DOJ is likely to use in enforcing cryptocurrency crimes. More generally, DOJ plans to better safeguard the financial system and the American public by increasing burdens on cryptocurrency exchange operators, holding conversion facilitators accountable, and continuing to study peer-to-peer and offshore exchanges.

DOJ's amplified focus is likely to lead to additional investigations of cryptocurrency-related money laundering, sanctions, and fraud, and comes at a time when the SEC, Commodity Futures Trading Commission (CFTC), and OFAC similarly have been messaging and exhibiting increased regulation and enforcement in this space. Carlin, in fact, highlighted a recent announcement by OFAC to designate a virtual currency exchange for allegedly facilitating financial transactions used in connection with ransomware attacks. Carlin announced that DOJ will be working in parallel with the SEC, CFTC, FinCEN, OFAC, and IRS to "maximize" enforcement impact in this space. As in other contexts, such parallel actions will pose challenges and risks to clients as they navigate investigations and demands by multiple authorities.

6. International cooperation

In describing tools needed to enhance DOJ's cryptocurrency crime enforcement, Carlin specified the need for input from international law enforcement partners. This is consistent with a broader recent trend in which DOJ has expanded the range of international authorities with which it cooperates, a trend we expect to continue under the current administration.

Recent notable enforcement actions reflect this critical focus on cooperation with international authorities, including the recent FCPA enforcement action involving Amec Foster Wheeler. There, DOJ, in coordination with British and Brazilian authorities, entered into a three-year DPA with the U.K.-based engineering company, requiring it to pay an $18 million penalty to resolve charges stemming from a bribery scheme in Brazil. International cooperation like this has become a common and important aspect of FCPA enforcement in recent years, and all signs point to it becoming even more so under the Biden Administration. On June 3, President Biden issued an Executive Memorandum directing his administration to formulate a strategy to "[w]ork with international partners to counteract strategic corruption" and "[e]nhance efforts to quickly and flexibly increase United States and partner resources of investigative, financial, technical, political, and other assistance to foreign countries that exhibit the desire to reduce corruption."

It appears that DOJ will attempt to replicate the international coordination and cooperation seen in the anti-corruption space, and more generally in the national security area, in other white collar crimes, including cryptocurrency and cyber/ransomware. This increased cooperation will likely lead to additional challenges to companies facing multi-jurisdictional investigations. Although DOJ's "Anti-Piling On" policy may mitigate the imposition of duplicative penalties for the same underlying conduct by multiple authorities where such authorities are intent on coordinating with one another, the policy does not remedy the broader problems that can arise during the pendency of an investigation or resolution, including unwillingness by certain

authorities to coordinate, competing legal regimes or practices, and conflicting demands by different authorities.

7. Scrutiny of resolution agreement obligations

Carlin also highlighted DOJ's commitment to stringently enforce violations of NPAs, DPAs, and plea agreements, warning that violations of such agreements may engender more painful results than originally posed by the underlying charges. Carlin's remarks were a reminder of then-Assistant Attorney General Leslie Caldwell's 2015 speech in which she cautioned that when a company under an existing agreement fails to cooperate or engages in new misconduct, the Criminal Division "will not hesitate to tear up a DPA or NPA and file criminal charges" where appropriate. Despite Carlin's warning, he made clear that DOJ is not rooting for companies under resolution agreements to fail, but rather is aligned with companies in their desire to succeed. Thus, although DOJ is not searching for opportunities to declare a breach, clients should expect DOJ to scrutinize companies' compliance with the obligations imposed by resolution agreements.

8. Subpoena compliance

Lastly, Carlin underscored the importance of timely and full compliance with subpoenas. His remarks particularly targeted companies accustomed to receiving such requests, citing banks, technology companies, and telecommunications providers as examples. He advised that prosecutors have been instructed to "explore all options" when companies "systemically fail" to adequately respond to subpoenas and other inquiries. This warning takes on additional importance given the AMLA's expansion of DOJ's ability to subpoena foreign banks for records where the foreign bank maintains a correspondence account in the United States.

Carlin's speech can be found **here**.

Davis Polk

If you have any questions regarding the matters covered in this publication, please contact any of the lawyers listed below or your usual Davis Polk contact.

Greg D. Andres	+1 212 450 4724	greg.andres@davispolk.com
Uzo Asonye	+1 202 962 7057	uzo.asonye@davispolk.com
Martine M. Beamon	+1 212 450 4262	martine.beamon@davispolk.com
Robert A. Cohen	+1 202 962 7047	robert.cohen@davispolk.com
Daniel S. Kahn	+1 202 962 7140	daniel.kahn@davispolk.com
Paul D. Marquardt	+1 202 962 7156	paul.marquardt@davispolk.com
Tatiana R. Martins	+1 212 450 4085	tatiana.martins@davispolk.com
Fiona R. Moran	+1 202 962 7137	fiona.moran@davispolk.com
Paul J. Nathanson	+1 202 962 7055	paul.nathanson@davispolk.com
Daniel P. Stipano	+1 202 962 7012	dan.stipano@davispolk.com

John Carlin on stepping up DOJ corporate enforcement

11 October 2021

Keynote by principal associate deputy attorney general John Carlin at GIR Connect: New York, co-chaired by F Joseph Warin of Gibson Dunn & Crutcher and Bruce Yannett of Debevoise & Plimpton, on 5 October 2021.

I think these events are an important opportunity for discussion of trends and really this area is one where your work, your advice to clients, changes the way that people behave. And it changes the way that people behave in a way that collectively helps to detect, deter and sanction corporate malfeasance. Ultimately, it benefits the rule of law and allows businesses to thrive. And that is in part through robust compliance and enforcement programmes.

[F Joseph Warin] referenced a little bit of returning to government on 20 January as a first official into the Justice Department, and it was a sobering reminder of how important it is that we maintain both the rule of law and respect for the Justice Department. That day, I had to have my marshall detail escort me. And the city was locked down. And the first floor of the Justice Department building was empty because of the pandemic. And on the first floor, the floor was covered with reserve soldiers who had been brought into the capital to help make sure we had a smooth and peaceful transfer of power. I appreciate their service but it was also something I do not want to see. And I'm sure you share that we do not want to see again.

Before I get started as well, it's been a sad week in the Justice Department. Yesterday we had a DEA agent killed in the line of duty, and other agents severely wounded; a task force police officer for Tucson who's supporting them was also wounded. Our thoughts go out to their families and our prayers for those that are wounded to safely recover. We also lost a US marshal to injuries sustained about a month earlier on the job.

Turning to corporate enforcement, the Justice Department has a long history of criminal actions against both corporations and their officers when they violate federal criminal law. And, in fact, the first ever indictment against a corporation in America happened right where some of you are assembled in Manhattan. I wish we could all be there in person. And that was about 115 years ago in 1906, when prosecutors from SDNY led by US Attorney Henry Stimson indicted the New York Central and Hudson Railroad Company and various individuals for a scheme to pay kickbacks designed to circumvent federal price controls on sugar. The New York Central indictment was a paradigm shift for criminal law. In the prior century corporations were thought to be immune from criminal prosecutions, since they had in the words of one congressman, “no bodies to be kicked and no souls to be damned”. And it took courage to break from outdated paradigms and recognise the shift in how we were doing business that then spawned a century of corporate criminal enforcement. In 1909, the Supreme Court unanimously held in *New York Central* that a corporation could be held criminally liable under US law. And in doing so the court noted that to give corporations immunity from all punishment – because of the old doctrine that a corporation cannot commit a crime – would virtually take away the only means of effectively controlling them and correcting the abuses in them.

In the century since *New York Central*, I think you've seen the department's efforts wax and wane at different times. And sometimes our enforcement has come too late. It's been successful, such as the 1000-plus convictions of banking officers during the savings and loans crisis and the aggressive prosecutions in the wake of Worldcom’s and Enron's respective collapses, the latter effort led in part of course by our current deputy attorney general.

But I think you'll see in the enforcement initiatives that we’re previewing really for the first time here today with this group of experts, many people we’ve worked with before... that there is a firm belief from the current leadership that prosecution is not success. That success is preventing the crime from occurring in the first place, from reducing the crime... Deterrence is certainly one method of reducing that crime, but we need to continue to look for ways on the front end to communicate clearly what the expectations are so there are effective compliance programmes in corporations and that the behaviour changes. And if that reduces the number of prosecutions, that's a good thing. Now in order to affect that mind shift, we also need to be clear that our prosecutors can't be afraid to bring difficult cases. They can't be afraid to try novel approaches to enforcement, just as those first prosecutors did in bringing a case against a

corporation. And they must be committed to holding those accountable for actions that threaten our collective economic, national and personal security.

In order to support that, I think you'll see in the days and months to come that we are building up to surge resources for corporate enforcement. That has begun and we have started to redouble the department's commitment to white-collar enforcement. First, in the dedicating of more resources, as just one example, the department recently is going to create a new squad of FBI agents to work full-time and be embedded with the department's criminal fraud section. We've seen that partnership bear fruit in the past. It'll give us more freedom and flexibility to pursue white-collar matters nationwide. Embedding agents and prosecutors together is a tried and trusted model and we've seen that it yields exponential results. It's been the go-to model for many of our most high-profile prosecutions, and I know it's one that both I and the current deputy attorney general have found to be successful in our own careers.

Second, we need to take advantage of the new tools that we can use to identify criminal conduct. In particular, the era of big data and data analysis. So for years we've used data to identify and prosecute new cases, whether that's healthcare fraud and commodities manipulation or insider trading. And for instance, the Healthcare Fraud Unit at Main Justice has had a data scientist on staff, dating back to its inception in 2007. And we've seen in US attorneys' offices, particularly in SDNY in prosecuting insider trading cases, that the SEC's critical data analytics programme Artemus, the advanced relational trading enforcement metric investigation system, is what drives and originates many cases. I think this era of big data and seeing it work in other areas offers new opportunities for prosecutors to detect wrongdoing. And it shouldn't just be, in particular importance to this group, the prosecutors that are using these new capabilities in order to detect misconduct; it's going to be the expectation here when evaluating compliance programmes that corporations are using the same type of analytics to look for and predict misconduct. You'll see it's an area where we're going to work closely with regulatory and other partners so that we're sharing the same fruits of analytic labour. Now look, it's never going to remove the need for search warrants wiretaps, other law enforcement tools in white-collar cases, but it does provide another tool for holding criminals accountable and also for predicting and preventing the crime from occurring in the first place.

We will continue to assess our practices and make some changes regarding the prosecution of corporate crime. Particular areas... that you should see change is going to be our use of corporate resolutions, our policies affirming the need to hold individuals accountable for white-collar crime, and the weight we give to companies' cooperation. But we're also interested in your feedback on other areas. Again that same mantra of how can we build on and improve what we have to address current threats or reduce crime. In the weeks ahead, you'll see more to come. We need to be

self-critical in order to serve as an adequate deterrent against white collar malfeasance, and to incentivise corporations to employ robust compliance programmes...

Likewise, we're going to carefully evaluate our existing policies and guidance regarding the prosecution of business organisations to ensure consistency with the administration's policy views and priorities. I think we're all seeing there's a crisis of confidence when it comes to the ability of the government to effectively monitor corporations and trust in corporations. That's bad for business and bad for government. And so we need to do what we can to build back that confidence.

Finally and most importantly, the department's leadership will make clear that prosecutors should never refrain from a white-collar prosecution out of fear of losing. They also need to be mindful of the Justice Manual and the principles of federal prosecution to do justice. So, "we might lose" is not an argument that will have much weight here, as long as the proposed action is supported by facts and the law, and it is more likely than not that a jury presented with those facts would convict. We need to encourage white-collar prosecutors also to be bold in the way that they investigate and have new thinking when it comes to new types of fraud manipulation, and other corporate malfeasance.

I'm going to talk a little bit about some of what those trends are. It is critical for this administration – and this is an area actually of continuity between Obama, Trump and Biden administrations that disagree on many other issues – that American, not just American foreign policy, but our like-minded and international partners around the world, that the use of sanctions and export control is critical to living in the world that we want to live in. And that means preventing things like the proliferation of weapons of mass destruction. It also means holding countries to account when they violate international norms on human rights or other areas.

So the first thing I'd like to discuss is our sanctions and export control enforcement. As many of you know it is overseen by the National Security Division in Main Justice and executed in partnership with US attorneys' offices. Currently, the department has about 150 open sanctions and export control investigations, and that's a significant increase over the last couple of years – expect that trend to continue. Around 70% of the cases relate to one of four countries: Iran, the People's Republic of China, Russia or North Korea. You will see those are the same four countries that have been called out year after year in the National Intelligence Estimate and the testimony of the Director of National Intelligence as countries that pose the greatest threat to our collective security.

In the past year, the number of North Korean cases has increased notably over historic levels because this is a key means of protecting security, and most notably the focus now on US technology and how it continues to be the most coveted, and we want other nations who compete to do so by investing in research and development, not by stealing what is developed

here or in like-minded countries. And we're also taking advantage in terms of foreign policy of where our strengths are. It's an old adage that you strike where you are strong and your enemy is weak. So it may be that there are actions such as when we've moved so quickly to a digital infrastructure, we're more vulnerable in the digital space than some of our adversaries. But the US dollar continues to be the currency of international trade, and so for foreign policy... sanctions will continue to be a vital instrument of American power. And in order to enforce those sanctions, that means vigorous enforcement including through the use of the federal justice system.

When I was last in the National Security Division, we recognised these trends, and we reorganised the sanctions and export control practice. And one of the things we look for – and this group will be quite familiar with – was to look over to what the Criminal Division had done when it came to enforcement. In the words of TS Eliot, "Good writers borrow. Great writers steal". And so we stole from the Criminal Division in terms of their approach on voluntary self disclosure. And so in 2016, the first voluntary self disclosure programme by the Justice Department was put in place to incentivise companies to come forward when they identify criminal violations of sanctions and export control laws so that the company and government can quickly remediate. That policy was further refined in the Trump administration in 2019 and in April of 2021 you saw the first ever NPA, non-prosecution agreement, of a company, SAP, based on its use of the voluntary self disclosure programme. As a result of the company's reporting, extensive cooperation and strong remediation, which they invested more than $27 million, the government sought no fine and no monitor and required the company only to disgorge the gain that was directly related to its conduct. With this proof of concept now established for the private sector, we anticipate and want to share the word with this group that the voluntary self-disclosure policy hopefully provides an incentive for companies to come forward after they identify sanctions and export violations. And for those of you practising in the space, I encourage you to familiarise yourself with that policy.

... For those in the export area, we're focused not just on transferring a particular formula or piece of IP but that which is in your mind to another person's mind – so human knowledge. We saw three US citizens who formerly served in the US intelligence community all enter deferred prosecution agreements with the government for work they have done as hackers for hire on behalf of the United Arab Emirates and a company there. As part of the DPA, the defendants collectively agreed to pay over $1.6 million, effectively a disgorgement of their salaries, cooperate with the department and accept a lifetime ban on US security clearances and employment.

I think you will also see us continue to use new tools and in export and sanctions cases including leveraging asset forfeiture in ways to have the maximum disruptive effect. For example, we saw the department last year seize over 1 million barrels of Iranian oil from tankers heading down for

Venezuela. This July, we seized a 2734 ton North Korean oil tanker based on its use to evade sanctions. The department also charged Kwek Kee Seng, a Singaporean captain of the ship, for sanctions violations. In sum, you should continue to see innovation and expansion of our enforcement of sanctions and export control cases in close partnership with the Treasury and Commerce Departments. We're really working together on this to use all tools to change conduct. And it will be a subject of the review that the deputy attorney general announces.

Another area ripe for innovation and vigorous enforcement involves the emerging area of cryptocurrency. We recognise and want to encourage the potentially useful and beneficial employment of cryptocurrency. I think it's going to be a competitive area with nation states who may not share the values not just of the United States but of like minded countries throughout the world. And today we're seeing cryptocurrency used prominently in a wide variety of criminal activity from ransomware and fraud with lucrative hacks of cryptocurrency exchanges. We're also troublingly seeing terrorist groups start to experiment with raising funds using cryptocurrency. And it's become the main way of transaction when it comes to drug transactions, child sexual exploitation material, firearms and other illicit materials. The sophistication of the criminal groups' use of cryptocurrencies does pose a challenge for law enforcement. Despite the challenge that it poses, the department has had some key successes recently. And we're going to continue to invest in new ways to enforce in this area.

Just last week, you saw SDNY and the National Security Division announce the guilty plea of a US citizen for conspiring to assist North Korea in evading sanctions using cryptocurrency and blockchain technology. Likewise in August, you saw the department announce the guilty plea of an operator of the Bitcoin mixer service Helix, which was responsible for over $300 million in funds. Key to this is going to be working with and trying to help develop, with the input of prosecutors and international law enforcement partners, new rules of the road with regulators. And we're meeting regularly in that space. The department's current cryptocurrency enforcement framework highlights many examples that demonstrate the success of working with those partners. And when you're thinking of practising in this space, you need to think about how you talk to FinCEN, OFAC, the SEC, CFTC, the IRS, along with the Justice Department. We're going to continue to try to coordinate parallel enforcement actions so we can maximise impact when it comes to investigating and dismantling and deterring criminal activity. We're going to continue to increase the burden on both those who operate those cryptocurrency exchanges, have the same type of KYC culture that you've had in banks, and also to focus – at the end of the day, from a cryptocurrency exchange you need to take that which is digital and convert it into currency – and we are going to focus on where that conversion occurs, and holding accountable and responsible those who facilitate those conversions so we can best safeguard the financial system and the

American public. We have a broad range of legal authorities and we're going to use an all-tools approach to dealing with cryptocurrency-related crime.

So, as I just touched on, KYC and the record keeping requirements under the Bank Secrecy Act are going to be one resource for law enforcement. Because cryptocurrency is using traditional banks as the exit and entry points for transactions, BSA compliance is going to be a key tool in the crypto space. Likewise, we're going to be looking at our anti-money laundering/ AML rules as another key tool for law enforcement. We're going to continue our study of peer-to-peer exchanges and offshore exchanges to try to avoid these regulatory obligations through what's known as jurisdictional arbitrage. And I would encourage you, if you have not focused on it, to focus on last week's action by the Treasury Department as it announced its first ever sanctions against a virtual currency exchange based on this laundering of a cyber ransom... And it's also sort of part of our ransomware task force initiative.

We've also, as I think you've seen, tried to use the blockchain to our advantage and seized the proceeds in cryptocurrency, when we identify them as the proceeds of crime. Most notably in June of 2021, the department announced the seizure of $2.3 million cryptocurrency that was paid as the ransom in the Colonial Pipeline attack. Even as this area remains unsettled, in terms of the regulatory terrain on cryptocurrency, we're going to look to enforce the criminal law.

And so you should expect in the days ahead that we'll have additional announcements about increasing our capacity and changing our structure as it comes to cryptocurrency enforcement. Now of course the crimes we see in that space are often the same old crimes that we've seen in the physical world and they similarly can be enforced using the same criminal statutes, whether it's wire fraud or sanctions violations to prosecute those matters.

Let me offer some final observations that everyone knows here today, but might be worth reiterating. First, we're going to continue to use NPAs, DPAs and guilty pleas. But that is not the end of an obligation for a company, and to the contrary it's just to start. And particularly now with scrutiny on the use of those agreements, we'll need to make sure that those who get the benefit of such an arrangement comply with their responsibility. And if not, you should expect to see serious repercussions. Just like if you did a guilty plea, if you violate the terms of an NPA or DPA or plea agreement, we are going to enforce. Violating those conditions may result in punishment greater than the original sentence. And similarly, companies need to understand that violating NPAs and DPAs may be worse than the original punishment. To be absolutely clear with this group, we are not rooting for companies to fail; we're rooting for them to succeed when we use those agreements or work closely with you and help you work closely with them to ensure that they do. But to make sure that we are fair and just and

equitable – and for those companies who are investing the resources – we are going to be firm with those who do not comply with the terms and the agreements that they have signed up to.

Second, this is a more of a narrow area, but for those of you with clients who receive a significant amount of legal process – banks, technology companies, telecommunications providers – we are focusing on ensuring that there is timely production and that it is complete... We've made clear here to our prosecutors that they should explore all options for companies who systematically fail to respond appropriately to legal process.

I hope this is helpful to this group in terms of giving a sense of where we're going to come in the days and weeks. Again, this preview is new. I look forward to feedback, and I think you should expect to hear more formal announcements in the days and weeks to come from the deputy attorney general. And this ends where I began, which is I do think we're in a crisis moment for our country, a combination of the pandemic and also changes and challenges to the American and democratic world order where we've seen sustained peace and growth over near 50 years; and simultaneously, here at home, a lack of trust in government institutions, including corporations. And I view this challenge and the work that you are doing in terms of corporate enforcement compliance to be critical, not just to dollars and cents, or to a particular company, but really to the health and safety of our nation. And together we need to succeed to make a world where companies are trusted to follow the rules, and, because of that trust, thrive. Thank you.

The transcript was lightly edited for brevity and clarity.

Davis Polk

Deputy Attorney General Lisa Monaco announces significant DOJ corporate enforcement policy changes

October 29, 2021 | Client Update

On Thursday, October 28, 2021, Deputy Attorney General Lisa Monaco announced significant changes to the DOJ's corporate enforcement program during her speech at the ABA's National Institute on White Collar Crime. The changes address: (1) corporate cooperation requirements; (2) the treatment of a corporation's history of prior resolutions with the Department; and (3) the imposition of corporate compliance monitors.

Together these new or revised policies will likely have a significant impact on DOJ's corporate enforcement program, and they signal harsher treatment of corporate actors who are confronted with a DOJ investigation and resolution. DAG Monaco also announced a new Corporate Crime Advisory Group to evaluate DOJ's corporate policies and said that more changes are coming. Notably, the DAG also forecasted heightened scrutiny of companies' compliance with the requirements of their prior criminal resolutions with the Department, which follows the disclosures made by two companies that the DOJ has declared them in breach of existing resolution agreements, one a Non-Prosecution Agreement (NPA) and one a Deferred Prosecution Agreement (DPA). Taken together, along with the DAG's commitment to "surge resources" to white collar enforcement, the DOJ is following through on recent messaging that it will ratchet up white collar enforcement and will treat companies more harshly than in prior administrations.

1. Changes to cooperation requirements

First, the DAG announced that the DOJ would revert to an earlier formulation in its memorandum on "Individual Accountability for Corporate Wrongdoing" (the so-called Yates Memo), which required that, in order to receive cooperation credit, companies under investigation would need to provide information related to *all* individuals involved in the alleged misconduct. In 2018, the Trump Administration narrowed the Yates Memo's effect by requiring companies only to provide information related to individuals "substantially involved in or responsible for" the alleged misconduct.

According to the DAG, the "substantially involved in or responsible for" limitation is "confusing in practice and afford[s] companies too much discretion in deciding who should and should not be disclosed to the government," and also "ignores the fact that individuals with a peripheral involvement in misconduct may nonetheless have important information to provide to agents and prosecutors." Whether this change will allow the government to charge more corporate officers and employees engaged in misconduct is unclear, but the change will require companies to meet a heightened standard to receive cooperation credit.

2. Treatment of prior misconduct

Second, the DAG announced that in reaching a resolution, prosecutors should consider "all prior misconduct . . . when it comes to decisions about the proper resolution with a company, whether or not that misconduct is similar to the conduct at issue in a particular investigation." Thus, "[a] prosecutor in the FCPA unit needs to" determine whether the company has "run afoul of the Tax Division, the Environment and Natural Resources Division, the money laundering sections, the U.S. Attorney's Offices, and so on," as well as "whether this company was prosecuted by another country or state, or whether this company has a history of running afoul of regulators."

Insights

This change will significantly broaden the scope of misconduct that prosecutors consider when determining whether and how to resolve a corporate criminal investigation. Many companies – particularly large corporations – routinely face regulatory scrutiny by different authorities, both domestic and foreign. Such actions – even those involving the lowest level employees and totally unrelated conduct – are now fair game for DOJ to consider as part of any resolution. And while the DAG conceded that "[s]ome prior instances of misconduct may ultimately prove to have less significance," the consideration of prior misconduct and resolutions will almost certainly lead to harsher treatment of corporations.

In addressing what changes are yet to come, the DAG stated that the DOJ will be reviewing "whether and how to differently account for companies that become the focus of repeated DOJ investigations" and whether NPAs and DPAs are appropriate for such companies. If a decision is made that companies with prior DOJ resolutions will automatically be forced to resolve matters by pleading guilty, this may decrease the incentives these companies have to self-disclose misconduct to the government and cooperate with the government's investigation.

3. Resurgence of monitorships

Third, the DAG stated that, to the extent that prior DOJ guidance suggested that monitors were "the exception and not the rule" or that "monitorships [were] disfavored," she is "rescinding that guidance." The DAG's remarks signal a meaningful increase in the appointment of monitors.

Clients should expect heightened scrutiny of their compliance programs and a frequency of monitors more akin to 2016 when, for example, eight FCPA monitors were imposed in that year alone, as compared to the six FCPA monitorships that were imposed in the last five years combined. It will become increasingly important that clients continue to review and enhance their compliance programs and, with the help of defense counsel, appropriately communicate to DOJ the effectiveness of these programs early and often throughout the investigation and resolution process.

4. More to come

In addition to the changes announced Thursday, the DAG also revealed the creation of a Corporate Crime Advisory Group composed of representatives from across the DOJ with corporate enforcement experience, to review and evaluate existing corporate enforcement policies and to determine what additional changes should be made. The group will "consider some of the issues [the DAG] previewed," including "monitorship selection, recidivism and NPA/DPA non-compliance — as well as other issues, like what benchmarks we should use to measure a successful company's cooperation." The DAG also announced that this group will "consult broadly," which suggests that it may engage in outreach to the business community and defense bar for feedback on potential changes.

One of the issues on the Corporate Crime Advisory Group's agenda will be a consideration of how to treat companies that violate the terms of existing resolution agreements. According to the DAG, DOJ will have "no tolerance for companies that take advantage of [DPAs and NPAs] by going on to continue to commit crimes, particularly if they then compound their wrongdoing by knowingly hiding it from the government," and noted that "[i]t is hard for me to think of more outrageous behavior by a company that has entered into a DPA or NPA in the first place." This comes on the heels of disclosures by two multinational companies that each had received a breach notification from the DOJ, declaring them in breach of existing resolution agreements.

The DAG also reiterated what PADAG Carlin had previously noted – that the DOJ would "surge resources" to white collar enforcement, providing as an example "a new squad of FBI agents [that] will be embedded in the Department's Criminal Fraud Section," responsible for FCPA cases, financial fraud, and healthcare fraud. She further indicated that "[t]his team model has a proven track record and is one we've used in numerous high-profile cases."

5. Takeaways

Overall, DAG Monaco underscored the DOJ's commitment to increased—and harsher—enforcement of companies that engage in corporate crimes. The speech presents a compelling reason for companies to ensure that both company and counsel understand the DOJ's expectations and communicate effectively with the Department. Companies should also continue to prioritize the implementation of effective compliance programs. These factors will allow clients to distinguish themselves from companies that may face the

imposition of a monitor and overall harsher resolutions. But more importantly, implementing these mechanisms increases a company's ability to avoid a DOJ investigation altogether.

DAG Monaco's speech can be found here.

Davis Polk

If you have any questions regarding the matters covered in this publication, please contact any of the lawyers listed below or your usual Davis Polk contact.

Greg D. Andres	+1 212 450 4724	greg.andres@davispolk.com
Uzo Asonye	+1 202 962 7057	uzo.asonye@davispolk.com
Martine M. Beamon	+1 212 450 4262	martine.beamon@davispolk.com
Angela T. Burgess	+1 212 450 4885	angela.burgess@davispolk.com
Robert A. Cohen	+1 202 962 7047	robert.cohen@davispolk.com
Daniel S. Kahn	+1 202 962 7140	daniel.kahn@davispolk.com
Tatiana R. Martins	+1 212 450 4085	tatiana.martins@davispolk.com
Fiona R. Moran	+1 202 962 7137	fiona.moran@davispolk.com
Paul J. Nathanson	+1 202 962 7055	paul.nathanson@davispolk.com
Kenneth L. Wainstein	+1 202 962 7141	ken.wainstein@davispolk.com

THE UNITED STATES DEPARTMENT of JUSTICE
STICE NEWS

Deputy Attorney General Lisa O. Monaco Gives Keynote Address at ABA's 36th National Institute on White Collar Crime

Washington, DC ~ Thursday, October 28, 2021

Remarks as Prepared for Delivery

Thank you, Ray, for that introduction, and thank you all for having me today. I'm sorry that I am not able to be there in person but appreciate the ability to join you virtually.

I have three priorities for my time with you. First, I want to describe three new actions that the department is taking today to strengthen the way we respond to corporate crime. Second, I want to look forward and tell you about some areas we will be studying over the next months, with an eye to making additional changes to help further invigorate the department's efforts to combat corporate crime. But before both of those, I want to set the scene by discussing trends, as well as the Attorney General's and my enforcement priorities, when it comes to corporate crime.

We can all agree the department's enforcement activities in the white-collar space ebb and flow due to a variety of factors — some internal to the department and some external. When I started as a newly minted AUSA, it was an active time for enforcement against corporate crime — one that witnessed the prosecutions of executives at WorldCom, Qwest Communications, Adelphia, Tyco and Enron. I've experienced how — when given the right resources and support including dedicated agents — prosecutors can uncover and prosecute the most sophisticated corporate criminals. As Deputy Attorney General, my goal is to set our investigators and attorneys up for continued success, so that they can enforce the criminal law fairly and vigorously, as the facts and law dictate.

At the same time, I am focused on ensuring the department is clear with those of you who are counselors and voices in the C-Suite and Boardroom — so that you can provide well-informed advice to your clients. Having served as a board member when I was out of government, I can appreciate the difficult conversations that arise surrounding compliance and measures designed to proactively stop misconduct, and the tradeoffs that may need to be considered when making investment decisions. Clear department guidance strengthens the case for these measures because it makes clear why taking steps to root out misconduct, and avoid the "edge case," often can be the most valuable guidance a general counsel or trusted legal advisor can provide.

Since returning to the Justice Department this year, I've spent time considering the current enforcement landscape. That landscape has evolved in some noticeable ways from my last tour. Corporate crime has an increasing national security dimension — from the new role of sanctions and export control cases to cyber vulnerabilities that open companies up to foreign attacks. Second, data analytics plays a larger and larger role in corporate criminal investigations, whether that be in healthcare fraud or insider trading or market manipulation. Third, criminals are taking advantage of emerging technological and financial industries to develop new schemes that exploit the investing public.

At the same time, these developments are changes of degree and not of kind. We have long had corporate criminal cases with national security implications. We have been using data to assist investigations for well over a decade. And prosecutors have always had to grapple with evolutions in corporate fraud —whether that be the junk bond firms of the 1980s, the various fraud schemes created by the so-called "smartest guys in the room" at Enron, or the prolific mortgage fraud of the 2000s, or cryptocurrency schemes today.

But throughout, our mission must remain the same — enforce the criminal laws that govern corporations, executives, officers and others, in order to protect jobs, guard savings and maintain our collective faith in the economic engine that

fuels this country. We will hold those that break the law accountable and promote respect for the laws designed to protect investors, consumers and employees.

Accountability starts with the individuals responsible for criminal conduct. Attorney General Garland has made clear it is unambiguously this department's first priority in corporate criminal matters to prosecute the individuals who commit and profit from corporate malfeasance.

I recognize that cases against corporate executives are among some of the most difficult that the department brings, and that means the government may lose some of those cases. But I have and will continue to make clear to our prosecutors that, as long as we act consistent with the Principles of Federal Prosecution, the fear of losing should not deter them. As set forth in the Justice Manual, a prosecutor should commence a case if he or she believes that a putative defendant's conduct constitutes a federal offense, and that the admissible evidence will probably be sufficient to obtain and sustain a conviction. So long as those principles are followed, we will urge prosecutors to be bold in holding accountable those who commit criminal conduct.

We are also going to find ways to surge resources to the department's prosecutors. As one example, a new squad of FBI agents will be embedded in the Department's Criminal Fraud Section. This team model has a proven track record and is one we've used in numerous high-profile cases. As I've seen personally, putting agents and prosecutors in the same foxhole can make all the difference, particularly in complex cases.

While the priority remains individual accountability, where appropriate, we will not hesitate to hold companies accountable.

Now, I recognize the resources and the effort it takes to manage a large organization and to put in place the right culture. The Department of Justice has over 115,000 employees across dozens of countries and an operating budget equivalent to that of a Fortune 100 company. So, I know what it means to manage and be accountable for what happens in a complex organization. But corporate culture matters. A corporate culture that fails to hold individuals accountable, or fails to invest in compliance — or worse, that thumbs its nose at compliance — leads to bad results.

Let me also be clear: a company can fulfill its fiduciary duty to shareholders and maintain a commitment to compliance and lawfulness. In fact, companies serve their shareholders when they proactively put in place compliance functions and spend resources anticipating problems. They do so both by avoiding regulatory actions in the first place and receiving credit from the government. Conversely, we will ensure the absence of such programs inevitably proves a costly omission for companies who end up the focus of department investigations.

Although we understand the costs that enforcement actions can place on shareholders and others, our responsibility is to incentivize responsible corporate citizenship, a culture of compliance and a sense of accountability. So, the department will not hesitate to take action when necessary to combat corporate wrongdoing.

With those priorities in mind, let me talk about three actions I am taking today with respect to department policies on corporate criminal enforcement. I anticipate that these changes are just a first step and will be followed by others as we study certain issues more closely. In the meantime, each of these will enable our prosecutors to continue to hold individuals and corporations accountable for their misconduct.

The first announcement augments our efforts to ensure individual accountability. To hold individuals accountable, prosecutors first need to know the cast of characters involved in any misconduct. To that end, today I am directing the department to restore prior guidance making clear that to be eligible for any cooperation credit, companies must provide the department with all non-privileged information about individuals involved in or responsible for the misconduct at issue. To be clear, a company must identify all individuals involved in the misconduct, regardless of their position, status or seniority.

It will no longer be sufficient for companies to limit disclosures to those they assess to be "substantially involved" in the misconduct. Such distinctions are confusing in practice and afford companies too much discretion in deciding who should and should not be disclosed to the government. Such a limitation also ignores the fact that individuals with a peripheral involvement in misconduct may nonetheless have important information to provide to agents and prosecutors. The department's investigative team is often better situated than company counsel to determine the relevance and culpability of individuals involved in misconduct, even for individuals who may be deemed by a

corporation to be less than substantially involved in misconduct. To aid this assessment, cooperating companies will now be required to provide the government with all non-privileged information about individual wrongdoing.

I anticipate some may say this means the government is going to unfairly prosecute minimal participants. Asking for this information does not alter the principles that govern fair and just charging decisions. Like every case, prosecutors will make decisions about individuals implicated in corporate criminal matters based on the facts, the law and the Principles of Federal Prosecution.

The second change I am announcing today deals with the issue of a company's prior misconduct and how that affects our decisions about the appropriate corporate resolution.

Today, the department is making clear that all prior misconduct needs to be evaluated when it comes to decisions about the proper resolution with a company, whether or not that misconduct is similar to the conduct at issue in a particular investigation. That record of misconduct speaks directly to a company's overall commitment to compliance programs and the appropriate culture to disincentivize criminal activity.

To that end, today I am issuing new guidance to prosecutors regarding what historical misconduct needs to be evaluated when considering corporate resolutions. This will include an amendment to the Department's "Principles of Federal Prosecution of Business Organizations." Going forward, prosecutors will be directed to consider the full criminal, civil and regulatory record of any company when deciding what resolution is appropriate for a company that is the subject or target of a criminal investigation.

Going forward, prosecutors can and should consider the full range of prior misconduct, not just a narrower subset of similar misconduct — for instance, only the past FCPA investigations in an FCPA case, or only the tax offenses in a Tax Division matter. A prosecutor in the FCPA unit needs to take a department-wide view of misconduct: Has this company run afoul of the Tax Division, the Environment and Natural Resources Division, the money laundering sections, the U.S. Attorney's Offices, and so on? He or she also needs to weigh what has happened outside the department — whether this company was prosecuted by another country or state, or whether this company has a history of running afoul of regulators. Some prior instances of misconduct may ultimately prove to have less significance, but prosecutors need to start by assuming all prior misconduct is potentially relevant.

Taking the broader view of companies' historical misconduct will harmonize the way we treat corporate and individual criminal histories, as well as ensure that we do not unnecessarily look past important history in evaluating the proper form of resolution.

The final change I am announcing today deals with the use of corporate monitors. Stepping back, any resolution with a company involves a significant amount of trust on the part of the government. Trust that a corporation will commit itself to improvement, change its corporate culture, and self-police its activities. But where the basis for that trust is limited or called into question, we have other options. Independent monitors have long been a tool to encourage and verify compliance.

In recent years, some have suggested that monitors would be the exception and not the rule. To the extent that prior Justice Department guidance suggested that monitorships are disfavored or are the exception, I am rescinding that guidance. Instead, I am making clear that the department is free to require the imposition of independent monitors whenever it is appropriate to do so in order to satisfy our prosecutors that a company is living up to its compliance and disclosure obligations under the DPA or NPA.

Of course, the decision to use monitors must also include consideration of how the monitorship is administered and the standards by which monitors are expected to do their work. And the selection of monitors will continue to be accomplished in a fashion that eliminates even the perception of favoritism. The department will study how we select corporate monitors, including whether to standardize our selection process across the divisions and offices.

The changes I am announcing today are only the first steps to reinforce our commitment to combatting corporate crime. In addition to the issue of monitorship selection, we have other issues to explore. Let me now preview some of the other issues we will review and tell you how we'll go about conducting that review.

The first area will examine is how to account for companies who have a documented history of repeated corporate wrongdoing. In certain cases, the department sees the same company become the subject of multiple investigations — not just in the same office or section, but in multiple sections and divisions across the department. For example, a company might have an antitrust investigation one year, a tax investigation the next, and a sanctions investigation two years after that.

Because I'm concerned about this kind of repeat offender, I asked my office to start looking at the data on corporate resolutions. What we saw is that recently somewhere between 10% and 20% of all significant corporate criminal resolutions involve companies who have previously entered into a resolution with the department. So, we need to consider whether and how to differently account for companies that become the focus of repeated DOJ investigations.

One immediate area for consideration is whether pretrial diversion — NPAs and DPAs — is appropriate for certain recidivist companies. Corporate recidivism undermines the purpose of pretrial diversion, which is after all to give a break to corporations in exchange for their promise to fix what ails them, as well as to recognize a company's cooperation. Some have questioned whether pretrial diversion is appropriate for any company who has benefited previously from such an arrangement. Does the opportunity to receive multiple NPAs and DPAs instill a sense among corporations that these resolutions and the attendant fines are just the cost of doing business? Are there other approaches that can promote cultural and institutional changes that will have a greater impact on deterring misconduct? These are some of the questions we will be studying in the coming months.

Another issue we will be studying is whether companies under the terms of an NPA or DPA take those obligations seriously enough. I want to be very clear — we have no tolerance for companies that take advantage of pre-trial diversion by going on to continue to commit crimes, particularly if they then compound their wrongdoing by knowingly hiding it from the government. It is hard for me to think of more outrageous behavior by a company that has entered into a DPA or NPA in the first place.

We will hold accountable any company that breaches the terms of its DPA or NPA. DPAs and NPAs are not a free pass, and there will be serious consequences for violating their terms. Recently, two different multinational corporations separately announced that each had received a breach notification from the Justice Department. This is obviously not a step we take lightly, but we will do so where necessary and appropriate.

These issues implicate the work of many different parts of the department, and so this review will need to consult a range of stakeholders. We also want to get your views given the implications any changes may have for your clients.

To that end, today I am announcing the formation of the Corporate Crime Advisory Group, which will be made up of representatives from every part of the department involved in corporate criminal enforcement. This group will have a broad mandate and will consult broadly. It will consider some of the issues I previewed today — like monitorship selection, recidivism and NPA/DPA non-compliance — as well as other issues, like what benchmarks we should use to measure a successful company's cooperation. It will also make recommendations on what resources can assist more rigorous enforcement, and how we ensure that individual accountability is prioritized. The advisory group will then develop recommendations and propose revisions to the department's policies on corporate criminal enforcement.

I'm sure many of you in the audience are going to get calls from clients over the next few days with questions about what this all means. So, let me conclude by giving you the answers — with these five points:

- Companies need to actively review their compliance programs to ensure they adequately monitor for and remediate misconduct — or else it's going to cost them down the line.
- For clients facing investigations, as of today, the department will review their whole criminal, civil and regulatory record — not just a sliver of that record.
- For clients cooperating with the government, they need to identify all individuals involved in the misconduct — not just those substantially involved — and produce all non-privileged information about those individuals' involvement.
- For clients negotiating resolutions, there is no default presumption against corporate monitors. That decision about a monitor will be made by the facts and circumstances of each case.
- Looking to the future, this is a start — and not the end — of this administration's actions to better combat corporate crime.

As we review and reassess our approach to corporate criminal enforcement, let me assure you that we will be in dialogue with those in this audience. We value your input and views on what are a complex set of issues.

Thank you again to the ABA for having me, and I look forward to speaking with you all soon.

Speaker:
Lisa O. Monaco, Deputy Attorney General

Topic(s):
Financial Fraud
Securities, Commodities, & Investment Fraud

Component(s):
Office of the Deputy Attorney General

Updated October 28, 2021