GIR Global Investigations Review

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

GIR Global Investigations Review

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.

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...

consistently 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,

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

GIR Global Investigations Review

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.

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.

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.