JUSTICE NEWS

Principal Deputy Assistant Attorney General John P. Cronan Delivers Remarks at Practising Law Institute Event

Washington, DC ~ Wednesday, November 28, 2018

Remarks as prepared for delivery

Thank you, Brackett, for the generous introduction, and thanks to the Practicing Law Institute for inviting me to speak this afternoon. It is an honor to be here representing the Department of Justice.

I have had the privilege of serving in the Department for almost my entire professional career. After spending most of that time as a federal prosecutor here in Manhattan, I now serve as the Principal Deputy Assistant Attorney General of the Department's Criminal Division. The Criminal Division includes over 600 attorneys spread across 17 sections and offices, and stationed throughout the United States and indeed around the globe. Our attorneys investigate and prosecute a wide array of crimes – including, as most pertinent to my remarks today, sophisticated economic fraud, money laundering, global financial corruption, and cybercrime.

I want to talk today about the importance of law enforcement and private industry working together in pursuit of common, shared objectives. There can be a perception – and I would say, often a misperception – of the Department of Justice and private industry as adversaries. While that certainly is sometimes the case, viewing law enforcement and the private sector in such stark black and white terms all too often is an oversimplification and simply inaccurate. That misperception not only can pose an obstacle to effective law enforcement, but it can also work against the interests of corporations that are victimized by crime or whose employees engage in misconduct.

In reality, prosecutors and companies frequently are very much aligned in their shared desire to prevent and detect criminal conduct. Both the Department of Justice and private industry have an overwhelming interest in combatting cyber intrusions and attacks on U.S. companies, as well as protecting our businesses from the theft of their trade secrets. It similarly behooves us to recognize that a culture of compliance with the rule of law inures to our mutual benefit – just as corruption and crime work to the detriment of both the private sector and the public trust. Prosecutors and companies alike play a critical role in fostering that corporate culture.

At the Department of Justice, we have been, and we will continue to be, steadfast in our commitment to robust white-collar criminal enforcement and the promotion of law-abiding business practices. For instance, in the past fiscal year, the Criminal Division's Foreign Corrupt Practices Act Unit brought public charges against over 30 individuals, and secured 19 convictions – which is on par with the prior year. We also reached eight corporate FCPA resolutions, with about $925 million in total corporate U.S. criminal fines, penalties, and forfeiture – figures that also are consistent with the prior fiscal year.

In-house counsel are also on the front lines of efforts to promote lawful business practices. Those of us in law enforcement well recognize that in-house counsel – together with boards of directors and senior management – are leading the charge from within companies to detect, deter, and rectify corporate misconduct and misbehaviors. It is often you who will confront difficult decisions about how to respond to bad actors; what compliance, audit, and ethics programs will look like; what resources will be devoted to those programs; and the level of access that compliance personnel will have to management and the board. It therefore is you to whom we in government want to make our message clear about the incentives for companies to prevent and redress corporate misconduct.

To that end, the Department is striving to bring greater clarity to the "rules of the road" by which prosecutors exercise their discretion in enforcing our laws. We have sought to establish and articulate more predictable and settled guideposts by which companies and business leaders can gauge expectations and conform their conduct. We want

companies to comprehend what actions on their part will be favorably credited and what will be penalized, as well as the standards and factors that will guide our decisions at the Department to pursue or not pursue charges.

The Department, of course, has instituted a framework for incentivizing industry with respect to our enforcement of the Foreign Corrupt Practices Act through the Corporate Enforcement Policy. The Policy, in clear terms, sets out how prosecutors should evaluate a company's violation of the FCPA, based on our assessment of actions taken by that company in the face of the misconduct and the credit we afford those actions.

The key takeaway from the FCPA Corporate Enforcement Policy is as follows: If a company voluntarily self-discloses the misconduct in a timely manner, fully cooperates with the Department, and engages in timely and appropriate remediation, including by paying all disgorgement, forfeiture, and restitution for the misconduct, there will be a presumption of a declination. The Policy also enumerates a non-exhaustive list of aggravating circumstances that can overcome that presumption.

If aggravating circumstances call for a criminal resolution, notwithstanding a company's voluntary self-disclosure, full cooperation, and timely and appropriate remediation, the Policy instructs that prosecutors shall seek up to a 50 percent reduction off the bottom of the applicable fine range pursuant to the U.S. Sentencing Guidelines, unless the company was a criminal recidivist, and further provides that prosecutors normally will not require the appointment of a monitor assuming an effective compliance program has been implemented. Meanwhile, the Policy provides that if a company fails to voluntarily self-disclose, but then turns the corner and engages in full cooperation and timely and appropriate remediation, the government will recommend up to a 25 percent reduction off the bottom of the Sentencing Guidelines range.

The Policy also contains detailed, multi-factor definitions of "voluntary self-disclosure," "full cooperation," and "timely and appropriate remediation." Again, we have articulated those definitions because we understand the benefits of transparency and predictability in this space. We want to make sure companies and their counsel understand what these terms mean, so they can conduct themselves accordingly.

The principles of the FCPA Corporate Enforcement Policy make sense and are rooted in sound policy. For that reason, in March, we explained that the Criminal Division will consider the Policy's criteria as "nonbinding guidance" in corporate criminal cases outside the FCPA context. In July, we clarified that the Corporate Enforcement Policy also applies to mergers and acquisitions that uncover potential FCPA violations. And in September, we announced that Criminal Division prosecutors also will look at these same principles in the context of mergers and acquisitions that uncover other types of criminal wrongdoing, not just FCPA violations. By formalizing the principles of the FCPA Corporate Enforcement Policy and making clear their broad applicability in Criminal Division prosecutions, our goal is to create a climate in which companies of all stripes can expect to be treated fairly when they timely and voluntarily report misconduct, cooperate, and remediate.

Transparency in this space can induce results that benefit law enforcement and the private sector alike. We realize that companies regularly face difficult decisions with respect to law enforcement – perhaps most notably, for purposes of today's attendees, how to respond after uncovering misconduct. If a company knows what factors we will consider in making prosecutorial decisions, and what outcome the company can reasonably expect based on the actions it takes, that company is better positioned to make an informed, rational decision as to what course of action is in its interests. To state that more directly, we believe that if we articulate guiding prosecutorial principles that are set with an eye on both incentivizing good corporate behavior and pursuing fair and appropriate corporate resolutions, companies are more likely to in fact engage in that good corporate behavior by implementing robust internal controls and effective compliance programs, and if they uncover misconduct, by voluntarily disclosing to law enforcement, cooperating, and remediating.

We are trying to foster similar collaboration between government and industry in the cyber arena. The unfortunate reality of operating a company in 2018 is that many of you have fallen or will fall victim to criminal cyber intrusions, data breaches, or trade secret theft.

Combatting intellectual property theft and economic espionage is a high priority of this Department of Justice. U.S. companies have long been global leaders in their advancements in science and technology. And because of that, rivals – whether state actors or competing companies – often try to steal our innovations to their benefit. Brilliant discoveries

that were the product of years of research and development, costing millions of dollars in investment, can be swiftly pilfered by a skilled hacker, a computer intrusion, a treasonous employee who has been co-opted, or a combination of these unscrupulous tactics.

Earlier this month, the Department of Justice announced an initiative to counter Chinese economic aggression. We have repeatedly seen Chinese actors engage in efforts to steal American trade secrets to strengthen their economic position at the expense of U.S. businesses. The Department's prosecutions have exposed Chinese actors for stealing intellectual property in sectors ranging from wind turbine technology to agricultural research to cancer drug research to software code. In fact, the Department is currently prosecuting multiple cases involving the alleged theft or attempted theft of trade secrets to the benefit of the Chinese government.

Many companies unfortunately, though understandably, fear that reporting cyber incidents to law enforcement will unduly disrupt their businesses or even potentially risk lawsuits or sanctions. We understand those fears, and the Criminal Division is committed to working collaboratively with companies after cyber incidents. The reason for that is simple: Self-reporting when one has been victimized by a cyber incident is critical to our ability to disrupt, identify, and apprehend the criminal perpetrators. Time is of the essence once an intrusion is identified, and the ephemeral data needed to investigate any cyber incident must be secured as quickly as possible. At the same time, we are committed to conducting our investigations with discretion to prevent the unwarranted release of information about the incident, to avoid vitiating claims of privilege, to protect trade secrets from disclosure, and to minimize disruption to businesses. Reporting cyber incidents also often is in the best interest of private industry because, not only could there be legal obligations to disclose certain types of cyber incidents, but regulators like the Federal Trade Commission (FTC) and Securities and Exchange Commission (SEC) very well may look more favorably upon a company that has self-disclosed and cooperated with the investigation than one that has not.

In the interest of promoting that collaboration, the Criminal Division's Computer Crime and Intellectual Property Section, known as CCIPS, has set forth guidance on what the private sector can do before, during, and after a cyber attack or intrusion, spelling out how companies can better prepare for cyber incidents and productively work with law enforcement in their aftermath. These "best practices" are set forth in a 25-page document available for download on the CCIPS website. The document lays out concrete steps that companies can take in advance of an incident, such as identifying mission-critical data and assets; assessing threats stemming from the use of contractors, service providers, and other outside agents; designing and testing incident response plans; and instituting basic cybersecurity protocols. The guidance also distills lessons learned by federal investigators, prosecutors, and private sector companies, including direction to victim organizations on what not to do following an attack. The FTC and SEC, meanwhile, have published guidance of their own, including lessons from prior enforcement actions, to help businesses manage cyber risk and minimize the prospect of regulatory action in the event of a cyber incident.

As in the FCPA context, we appreciate the value of providing guidance in the context of cyber attacks or intrusions in helping companies make informed and rational decisions. Similarly, we depend on and invite the input and participation of the private sector to most effectively combat cybercrimes. Indeed, in recent years, the Department has conducted several successful disruption operations in collaboration with our industry partners. With private sector cooperation, we were able to dismantle the Coreflood, GameOver Zeus, Avalanche, and Kelihos botnets and disrupt online criminal activity that had been used to steal data and conduct large-scale fraud.

The bottom line is this: Whether prosecutors or companies, whether compliance officers or in-house counsel or boards, whether in the white-collar arena or the cyber arena, we all have critical roles to play in compliance. And we all stand to benefit from companies that build effective compliance programs and internal controls that not only prevent and deter criminal incidents from occurring in the first instance, but also pave the way for more open channels of communication between government and industry.

To be sure, when we at the Department talk about compliance, we are referring to effective compliance. The Principles of Federal Prosecution of Business Organizations make that clear. Under those Principles, in determining whether to charge a corporation, prosecutors must consider, among other factors, the existence and effectiveness of the corporation's preexisting compliance program, as well as the corporation's subsequent remedial actions including efforts to implement an effective compliance program or improve an existing one. In assessing a compliance program, the Principles specifically direct prosecutors to consider "whether a corporation's compliance program is merely a

'paper program' or whether it was designed, implemented, reviewed, and revised, as appropriate, in an effective manner."

We have seen time and time again examples of what happens when compliance recommendations are papered over or inadequately resourced or tested. A few weeks ago, MoneyGram International, a global money services business headquartered in Texas, agreed to extend its deferred prosecution agreement and forfeit $125 million due to serious flaws in its anti-fraud and anti-money laundering programs. Those failures to maintain effective compliance programs resulted in MoneyGram's breach of its 2012 deferred prosecution agreement (DPA).

MoneyGram's 2012 DPA arose from fraudulent schemes by which corrupt MoneyGram agents and others had enabled fraudsters to induce elderly victims to send funds through MoneyGram's money transfer system. The fraudsters posed as relatives in dire need of money, promised large cash prizes, or promised deeply discounted items for sale over the Internet. The Department uncovered violations of the Bank Secrecy Act and determined that MoneyGram was aiding and abetting the fraud. As part of the DPA, MoneyGram agreed to enhanced compliance obligations and structural changes to prevent a repeat of the charged conduct.

But during the course of the DPA, MoneyGram experienced significant weaknesses in its anti-money laundering and anti-fraud programs. It then inadequately disclosed those weaknesses to the government, and instead told the Department that a rise in the number of consumer fraud transactions it was processing was substantially related to external circumstances. MoneyGram also failed to complete the enhanced compliance undertakings required by its 2012 DPA. As a result of these compliance failures, MoneyGram processed at least $125 million in additional fraudulent consumer transactions between April 2015 and October 2016, and found itself facing a 30-month extension of its DPA, as well as forfeiture in the amount of $125 million.

Another example of ineffective compliance was seen with respect to Western Union. In January 2017, Western Union entered into a DPA for aiding and abetting wire fraud and willfully failing to maintain an effective anti-money laundering program in violation of the Bank Secrecy Act. For years, Western Union had identified numerous agents who were involved in, or facilitated, fraud-related transactions, but the company failed to take corrective action. In 2004, Western Union's Corporate Security Department proposed global guidelines for discipline and suspension of Western Union agents that processed a materially elevated number of fraud transactions, and recommended automatically suspending any agent that facilitated transactions resulting in 15 consumer fraud reports within 120 days. But Western Union nonetheless continued to engage in business with these agents. Had Western Union taken the recommended corrective actions, significant fraud losses could have been averted – losses that are estimated to have victimized more than 500,000 people.

Western Union's Bank Secrecy Act failures also included acquiring a significant agent that Western Union knew had an ineffective anti-money laundering program and had contracted with other agents that were facilitating substantial consumer fraud. Western Union also failed to discipline agents who allowed customers to structure transactions to avoid Bank Secrecy Act recording and reporting requirements.

As a result of this conduct, which spanned a period of eight years, Western Union entered into a DPA in which it agreed to forfeit $586 million and also settled a related action with the FTC. Western Union is now subject to three years of oversight by an independent compliance auditor imposed by the FTC and obligation to share information learned from the auditor with the Department of Justice.

Again, as with MoneyGram, the conduct flowed directly from facts on the ground, which were known by the company and which exposed gaping holes in its compliance program as implemented – holes that an effective compliance program would have identified.

On the flip side, the Department has sought to reward companies that have taken meaningful, effective compliance seriously. That entails, upon uncovering misconduct, prosecutors looking at a business's compliance both retrospectively and prospectively. Of course, companies that lack adequate compliance measures are less likely to deter and prevent misconduct, and also are less likely to uncover a problem at an early stage. But at the same time, we appreciate that, even if a company has implemented a strong and effective compliance program, that program still may not prevent one or a few bad actors from engaging in misconduct. What matters to us in the Criminal Division – as embodied in the FCPA Corporate Enforcement Policy and the application of its principles outside the FCPA – is both

the effectiveness of the program in place at the time of the misconduct, as well as how the company responds upon discovering the misconduct in terms of disclosing to law enforcement, cooperating with the government, and taking meaningful remedial measures.

Our discretionary prosecutorial decisions have made plain the benefits for a company that does the right thing upon uncovering misconduct. Thus far in 2018, we have issued multiple corporate declinations under the FCPA Corporate Enforcement Policy. In August, for instance, we declined to prosecute the Insurance Corporation of Barbados Limited (ICBL) for bribery of a Barbadian government official in exchange for insurance contracts. Our declination letter cited, among other relevant factors, the company's voluntary disclosure, significant remediation efforts, and cooperation with the Department's investigation, including with respect to culpable individuals. We emphasized that ICBL conducted a comprehensive investigation and undertook remedial actions that included terminating all employees involved in the misconduct and implementing an enhanced compliance program and internal accounting controls.

Just three days before the ICBL declination, we issued a declination letter for Guralp Systems Limited for bribery of an earthquake research center in Korea. We similarly declined in that case because of, among other things, the company's voluntary self-disclosure, substantial cooperation, and significant remedial efforts.

These two declinations are particularly notable because the conduct at issue in both cases entailed the involvement of senior executives in the companies. While the involvement of senior management is an aggravating factor that can weigh against a declination, it did not preclude declinations in these cases in light of the companies' overall efforts to do the right thing. And that included cooperation with law enforcement that enabled the Department to bring charges against culpable individuals in both of these cases.

I also note that the Department of Justice has made public the ICBL and Guralp declination letters, as well as eight other declinations that preceded them under the Corporate Enforcement Policy and the predecessor Pilot Program. Publishing these declination letters further promotes transparency and reflects our broader interest in conveying to the private sector the measures taken by companies that prosecutors have credited in issuing declinations, so other companies in the future can guide their conduct accordingly.

Before I conclude, I want to say a few words about compliance in the context of mergers and acquisitions. When we talk of top-to-bottom cultures of compliance, the Department fully recognizes that there are unique challenges that arise during mergers and acquisitions.

Let me start with stating the obvious. We recognize that considerable benefits flow from law-abiding companies with robust and effective compliance programs acquiring or merging with companies with inferior compliance programs. The acquiring or merging company can help uncover compliance shortcomings or employee misconduct, and then right the ship going forward after acquisition or merger. This, of course, is a good thing, and something we want to encourage. We also do not want concerns about future exposure to deter good actors from acquiring or merging with troubled companies, and as a result giving way to acquisition or merger by companies with weaker compliance.

That is why, as I mentioned before, we have announced that the FCPA Corporate Enforcement Policy applies to mergers and acquisitions, and that the Criminal Division would apply the principles of the Corporate Enforcement Policy to mergers and acquisitions outside the FCPA context.

We recognize that it would be a rare situation for an acquiring or merging company to conduct a full, worldwide pre-acquisition deep dive on the acquisition or merger target, but it makes sense to get an understanding of the target company's risk profile and control systems. This permits the acquiring or merging company to identify what areas it needs to take a close look at, as well as any subsidiaries or divisions it wants to focus on reviewing.

It stands in a company's interest to take a close look at those soft spots and, if misconduct is uncovered, to attempt to address the issue prior to merger or acquisition. This could entail disclosure of the issues, if appropriate given the posture of the merger or acquisition, or it could entail taking advantage of the Fraud Section's FCPA Opinion Procedure. For those unfamiliar with the FCPA Opinion Procedure, issuers and domestic concerns can obtain an opinion from the Department of Justice as to whether certain specified, prospective conduct conforms with the Department's present enforcement policy under the FCPA.

Why does that make sense? By taking such pre-merger or acquisition action – whether through self-disclosure or an FCPA Opinion – the companies entering into the merger or acquisition are able to receive more certainty going into the transaction and more accurately build that certainty into the transaction. The government may respond after a merger or acquisition in a manner that the companies did not anticipate and, as a result, the companies failed to appropriately price the transaction. Similarly, self-disclosure prior to an acquisition, or at the earlier possible point, permits companies to take full advantage of the significant benefits that are available to voluntarily disclosing companies. Furthermore, when two companies are involved in a transaction, the chance that a whistleblower will learn of the misconduct and report it only increases.

But we also realize that, in some circumstances, even the best pre-acquisition due diligence may not uncover problems until after a deal closes. And even an acquiring company with a strong culture of compliance may struggle to impose and imprint that culture on a newly-acquired business. But again, the Department endeavors to be clear-eyed about the importance of self-reporting and proactively addressing problems as they arise, whenever they come to light, even if it is after-the-fact. Our interest will be to zero in on the culpable individuals, and to focus on giving due credit to efforts to cooperate and remediate, not to punish a company for punishment's sake.

Compliance is a fast-moving and fluid field. Companies and business leaders – as well as prosecutors – must navigate issues of compliance in the face of emerging technologies, such as ephemeral and encrypted messaging services, which pose a challenge to traditional investigative methodologies. Companies will have to navigate implementation challenges to compliance programs in foreign jurisdictions where certain laws might impede procedures or programs that have proven effective in the United States. Companies will also have their pick of an increasing array of data analytics and other tools that purport to facilitate compliance.

At bottom, government and industry should be grappling with these ever-evolving issues and challenges together. Our interests in rooting out corporate crime are invariably aligned, and our collective efforts are necessary to achieve that end.

Thank you very much, and enjoy the rest of the conference.

Topic(s):
Cyber Crime
Financial Fraud
Foreign Corruption

Component(s):
Criminal Division
Criminal - Criminal Fraud Section

Updated November 28, 2018