NOW & NEXT

Government Investigations & White Collar Alert

MARCH 6, 2023

New DOJ corporate enforcement measures cover messaging applications, executive compensation, national security

By Christopher D. Grigg, Timothy D. Sini, and Michal E. Cantor

The new measures offer further incentives to invest in compliance but may also present difficult decisions.

What's the Impact?

- New DOJ policies will require businesses to consider risk in three new areas: workforce messaging platforms; executive compensation structures; and the increasing impact of national-security-driven sanctions and export enforcement issues in established and emerging industries alike.
- DOJ and other federal agencies are realigning resources and taking action; businesses should, too.
- Enforcement is on the rise and is changing risk profiles; the time is right for businesses to invest in an ounce of prevention.

Speaking at the American Bar Association's annual white-collar crime conference in Miami this past Thursday and Friday, U.S. Department of Justice officials announced new measures sharpening aspects of recent policy updates. Deputy Attorney General Lisa O. Monaco again emphasized DOJ's interest in incentivizing voluntary disclosure of corporate wrong-doing and in

pursuing individual accountability. She also previewed new announcements delivered by Assistant Attorneys General Matthew G. Olsen, who leads DOJ's National Security Division, and Kenneth A. Polite, Jr., who leads DOJ's Criminal Division. Monaco, Olsen, and Polite highlighted the increasing overlap of corporate enforcement and national security concerns and rolled out new policies in two important areas: the use of messaging applications by corporate workforces and executive compensation.

In January, DOJ updated its Corporate Enforcement Policy (CEP) for the first time in five years. In late February, it extended that policy to its ninety-four U.S. Attorney's Offices to ensure that businesses choosing to disclose misconduct are treated consistently and predictably across the country.[1]

Scrutinizing messaging applications and executive compensation

DOJ has increasingly emphasized the importance of compliance as a key element of good corporate citizenship and a key factor for companies facing criminal enforcement actions. DOJ's Evaluating Corporate Compliance Program (ECCP) details the factors that federal prosecutors weigh when assessing whether companies meet, exceed, or fall short of expectations. Speaking Friday, AAG Polite announced significant changes to the ECCP in two key areas that companies should now consider.

Use of personal devices and communications platforms, including those offering ephemeral messaging

While recognizing that messaging applications have become "ubiquitous . . . and offer important platforms for companies to achieve growth and facilitate communication," DOJ has voiced concerns over its inability to obtain evidence of suspected wrongdoing when companies fail to capture or preserve communications on third-party devices and platforms. Under the newly revised ECCP, when evaluating an enforcement target's policies and mechanisms for addressing suspected wrongdoing, prosecutors will now expressly "consider a corporation's policies and procedures governing the use of personal devices, communications platforms, and messaging applications, including ephemeral messaging applications." In DOJ's view, those policies should be tailored to a company's risk profile to "ensure that, as appropriate and to the maximum extent possible, business-related electronic data and communications are accessible and amenable to preservation by the company."

Mr. Polite said prosecutors "will ask about the electronic communications channels used by the business and their preservation and deletion settings," as well as about "any 'bring-your-own device,' or BYOD program, and associated preservation policies." Prosecutors will also expect companies to produce third-party records during investigations. Failure to do so without—or even possibly despite—a reasonable explanation could face potential adverse consequences. "A company's answers—or lack of answers," Mr. Polite said, "may very well affect the offer [a

---

[1] For more information on the CEP update and the policy directive to the U.S. Attorney's Offices, please see our prior alerts: "DOJ Corporate Enforcement Policy sees "first significant" revisions since 2017," and "DOJ announces new policy to incentivize voluntary self-disclosure of corporate misconduct."

company] receives to resolve criminal liability. So when a crisis hits, let this be top of mind." Prudent companies, of course, would do well to address this issue, and document their efforts to do so, long before a crisis hits.

By tying potential benefits or punishments to messaging and BYOD policies and practices, DOJ is plainly trying to incentivize preserving evidence that it can use against companies and individuals suspected of wrongdoing. But even if preservation will actually help companies, by enabling them either to demonstrate a lack of wrongdoing or to obtain a reduced penalty, implementation can be costly and raises a host of difficulties for companies focused on efficient business operations, employee morale and stability, employee and customer privacy, state and federal privacy laws and regulations, logistical issues like data storage capacity and retention, and more. The stakes can be high, especially for companies in heavily regulated industries like healthcare, finance, and certain advanced technology fields, as well as businesses in emerging sectors like cryptocurrency and digital assets where enforcers are highly active despite a fragmented regulatory landscape.

The revised ECCP recites a litany of questions prosecutors will now ask, but it offers no answers. As a consequence, businesses bear a hindsight risk, namely that the policies and practices they implement today may be viewed as deficient when prosecutors investigate and assess their operations after discovering misconduct months or years down the road. This hindsight risk is not new of course and is readily mitigated by periodic reviews and updates to policies and procedures. Success here requires diligence. Companies that have not conducted a tailored risk assessment recently and have not formulated or implemented policies for preserving communications on third-party platforms and devices would do well to consult experienced counsel. An investment in that effort now can be time and money well spent and, if done right, will help avoid or mitigate a "crisis" later.

Compliance, compensation, and claw backs

In DOJ's view, compensation structures that "impose financial penalties for misconduct can deter risky behavior and foster a culture of compliance," and rewards and incentives for good conduct can "drive compliance." By extension, a lack of those structures and incentives arguably increases misconduct risk. Thus, under the revised ECCP, prosecutors will now scrutinize compensation systems and "consequence management" to assess how compensation systems contribute "to the presence—or lack—of an effective compliance program." DOJ's claimed goal here is to shift the burden of corporate misconduct from uninvolved shareholders to culpable individuals.

Although the revised ECCP now expressly describes the scrutiny prosecutors will apply, the link between compensation and effective compliance is not new (for example, the United States Sentencing Guidelines already call upon courts to weigh incentives to comport with compliance and ethics programs). But what is new is the compensation incentives and claw back pilot program that DOJ unfurled last week. Under this new program, which will run for an initial three-year period, in all criminal resolutions DOJ will now:

- Require companies to implement compliance-related criteria into their compensation and bonus systems and report to the Department about that implementation.
- Offer incentives for companies that claw back or attempt to claw back payments to law-breaking executives and employees during the term of the resolution period.

In formulating requisite compliance criteria, prosecutors will exercise discretion based on the applicable facts and law. Appropriate criteria could include: a prohibition on bonuses for failure to meet compliance performance measures; disciplinary measures for wrongdoers and responsible supervisors who either knew about or were wilfully blind to misconduct; and incentives for employees who demonstrate full commitment to compliance measures.

The new claw back incentives are limited to potential reductions in criminal fines; they will not affect any applicable disgorgement or restitution obligations. And, in parallel criminal and civil investigations, they likely will have no effect on any civil or administrative penalties unless the government agrees to an offset.

In practice, a company seeking a claw-back reduction will initially pay the full amount of the applicable fine, less 100% of the amount it will attempt to claw back. At the end of the resolution term, the company will pay the difference, if any, between the full amount it sought to claw back and any amount it successfully recouped. If, despite good faith efforts, a company is unable to claw back any compensation, prosecutors may, but are not required to, accord a 25% reduction of the full amount the company sought to claw back. In other words, the company will be required to pay no less than 75% of the attempted claw-back amount.

Because compensation structures are creatures of contract, any effort to claw back bonuses or other remuneration will likely entail costly litigation that, except perhaps in cases involving highly lucrative compensation packages, will quickly eclipse the value of any possible fine reduction. That is true even if an employer can craft readily enforceable claw-back provisions. But it is especially true if the individual target of the claw-back effort has not been criminally convicted or civilly held liable for any misconduct during the company's DOJ resolution term. Even though targeting executive compensation will not garner instant support among business leaders, with this latest policy change, DOJ is making it part of the conversation going forward.

A "top" risk priority: sanctions and export enforcement

While the new ECCP provisions and claw-back program apply broadly to the full sweep of corporate criminal enforcement, DOJ officials addressing the ABA conference also highlighted a new substantive area of focus. Speaking shortly after the one-year anniversary of Russia's most recent invasion of Ukraine, DAG Monaco noted that the global response to Russia's actions has "elevated the importance of sanctions and export control enforcement" and that "[w]hat was once a technical area of concern for select businesses should now be at the top of every company's risk compliance chart."

DOJ is backing its new national security focus with action. It is hiring an additional 25 new federal prosecutors for its Counterintelligence and Export Control Section (CES), which partners with

U.S. Attorney's Offices to investigate and prosecute sanctions and export control offenses and related economic crimes across the country and around the world. Moreover, those "new hires will include the National Security Division's first-ever Chief Counsel for Corporate Enforcement."

Given the "very uncertain" geopolitical environment, DAG Monaco said, "corporate crime and national security are overlapping to a degree never seen before, and the Department is retooling to meet that challenge." That retooling includes:

- Partnering with the Commerce and Treasury Departments to issue joint advisories informing the private sector about enforcement trends and the departments' expectations pertaining to national security-related compliance
- Working closely with the Russia-focused KleptoCapture Task Force and the recently announced Disruptive Technology Strike Force (for more information on the strike force, see our alert here) to disrupt and hold wrongdoers accountable
- Investing additional resources in the Money Laundering and Asset Recovery Section's Bank Integrity Unit to prosecute global financial institutions for sanctions violations

Signaling the government's multi-agency approach to sanctions and export enforcement, AAG Olsen delivered his remarks as part of a panel discussion with Matthew S. Axelrod, Director of the Commerce Department's Office of Export Enforcement (the law enforcement arm of Commerce's Bureau of Industry and Security (BIS)); Andrea M. Gacki, Director of the Treasury Department's Office of Export Enforcement (OFAC); and Steve K. Francis, Director of Homeland Security Investigations (HSI, a law enforcement agency within the Department of Homeland Security). Their collective message was clear: enforcement is ramping up. Some clients are already seeing an impact in the form of queries and compulsory document requests from investigators.

Companies familiar with US export controls and sanctions regimes likely have invested in learning the often complex, technical, and rapidly evolving regulations, record-keeping requirements, and compliance expectations that affect nearly every aspect of their business. Many are also familiar with regulators at agencies like BIS, OFAC, and the State Department's Directorate of Defense Trade Controls. DOJ's enhanced partnerships with these agencies and their collective focus on the corporate enforcement and national security "overlap" mean that more businesses—including many previously unaware that national security concerns might affect them—will need to educate themselves quickly, conduct risks assessments for their specific business models, and update their policies and practices where appropriate.

Looking ahead

Some may construe DOJ's new voluntary disclosure and compliance incentives merely as an effort to help it bring more cases by coercing businesses to serve as its investigative proxies. DOJ certainly disagrees and maintains that its goal is to incentivize good corporate citizenship to prevent crime before it happens.

But even if some criticism is warranted, companies should consider the broader perspective: DOJ is not waiting around for companies to deliver new cases. Instead, it and every other federal agency wielding enforcement and forfeiture authorities are increasingly combining efforts, committing resources, and acting on their authorities. DOJ has promised to "zealously pursue corporate crime in any industry." And, like other enforcement agencies, it has again signaled that, in appropriate cases, it will seek to make examples of errant companies to maximize deterrence.

In their remarks last week, DAG Monaco, AAG Polite, AAG Olsen, and Director Axelrod each highlighted recent charges, arrests, forfeitures, and resolutions as examples of their agencies' commitment to pursue enforcement actions in all areas of the law. They also signaled that announcements of more cases are coming. Many state attorneys general and regulatory agencies are also increasingly active.

In short, government is prioritizing enforcement in old and new areas of the law and is realigning resources accordingly. Businesses should consider retooling, too, especially if their enforcement risk profile is changing. Companies should partner with experienced counsel to conduct tailored risk analyses, implement or refine compliance strategies, and make other course corrections where needed. The environment is right to invest in an ounce of prevention.

For more information on the content of this alert, please contact your Nixon Peabody attorney or:

Christopher D. Grigg
213.629.6134
cgrigg@nixonpeabody.com

Timothy D. Sini
516.832.7655
tsini@nixonpeabody.com

Michal E. Cantor
516.832.7634
mcantor@nixonpeabody.com