5 Resolutions That Could Help Cos. Pass A DOJ Checkup

By **Holly Drumheller Butler, Thomas Zeno and Rebecca Fallk** (January 11, 2023)

Holly Drumheller Butler

Thomas Zeno

Rebecca Fallk

Certain New Year's resolutions are worth keeping. As we enter 2023, we can expect the U.S. Department of Justice to make good on its announced intention to increase white collar enforcement efforts. The five resolutions below will help your company receive a clean bill of health in the event of an examination by the DOJ.

1. Update your document preservation practices to address third-party messaging platforms.

In 2022, the DOJ released two separate forms of guidance related to the use of personal messaging devices. First, DOJ Deputy Attorney General Lisa Monaco released a memorandum on Sept. 15 instructing prosecutors to consider whether a company "has implemented effective policies and procedures governing the use of personal devices and third-party messaging platforms."[1]

This includes a corporation's ability to preserve, collect and provide to the government all nonprivileged, responsive documentation relevant to the investigation, including that which is stored on personal devices such as an employee's cell phone, tablet or computer.

Subsequently, on Dec. 1, the DOJ's Criminal Division doubled down on the Monaco memo. The division discussed how the use of third-party and secret messaging apps can hinder government investigations and can compromise an otherwise well-functioning compliance program.

Companies should consider data mapping their work-related communications, evaluating permissible apps and determining mechanisms to capture data.

2. Evaluate your need to conduct due diligence before and after acquisitions.

In that same Sept. 15 memorandum, Monaco provided two enforcement policies that may have practical implications for how companies conduct acquisition due diligence.[2]

First, the DOJ advised that it will evaluate the prior compliance record of acquired companies. Second, the DOJ directed prosecutors to assess a company's compliance program both at the time of offense and at the time of the charging decision.

This suggests that the DOJ may consider that post-acquisition conduct could mitigate or exacerbate preacquisition conduct, and an acquirer may want to consider extending its preclosing compliance review and risk assessments to the post-closing integration of the target company.

3. Check your hotlines.

Of course, it is preferable for a company to hear about possible concerns from employees directly, rather than learning about them through a government investigation of a whistleblower tip.

Many companies maintain hotlines that allow employees to anonymously report potential ethics and compliance issues. Below are questions to consider when evaluating the effectiveness of your hotline:

- Does your hotline work? When is the last time it was tested?

- Is your hotline anonymous? If not, consider the hesitation of employees to report when their name is tied to the complaint.

- Is your hotline actually used? A lack of complaints does not mean an absence of problems.

- When is the last time that employees were reminded of the hotline resource? Is it time for a refresher?

4. Conduct a tabletop exercise to confirm your cyber readiness.

If your systems are hacked tomorrow, would you be prepared? Fortunately, the adverse impacts of hacks can be mitigated by thoughtful preparation and readiness. Three primary elements to effective cyber readiness are: protection, response and continuous training.

Protection

Companies should identify their company's most critical cyber assets and risks and evaluate how to protect them.

Companies should implement training and auditing protocols, as well as an incident response plan and written information security program that defines security practices and exposures.

Response

Companies should be prepared in the event of a hack. They should follow protocol as laid out in the aforementioned incident response plan.

Continuous Training

All employees should receive continuous training as to the type of cyber risks that exist and the need to report any suspicious communications.

In addition to implementing this training, companies should consider the use of reporting initiatives and consequences for failure to report.

5. Assess your compliance programs.

When is the last time you checked your compliance program? A culture of compliance is the best way to avoid the DOJ. However, in a situation when a company finds itself under government investigation, a vigorous compliance program is of the utmost importance.

While this may seem like rudimentary advice, almost 90% of organizational offenders since fiscal year 1992 did not have a compliance or ethics program.[3]

The robust nature of a compliance program will affect the direction of a government investigation, including any penalty imposed. More specifically, the government considers, among other factors, whether or not the compliance program is tailored to the risks the company actually faces.[4]

Regular risk assessments are needed in order to reevaluate risks and understand where the company's time and money is best spent.

Additionally, periodic assessments of the company's entire compliance program are necessary to effectively compare the company to its benchmarks, identify program strengths and program enhancement opportunities, and assess the overall current state of the compliance program. This preemptive and continual assessment can be important to success in the case of an unexpected government investigation.

Remember: Corporate fitness does not end in January. Repeat these exercises throughout the year.

Holly Drumheller Butler is a principal and co-leader of the white collar, fraud and government investigations practice at Miles & Stockbridge PC.

Thomas Zeno is counsel and co-leader of the white collar, fraud and government investigations practice at the firm. He formerly served as an assistant U.S. attorney at the U.S. Attorney's Office for the District of Columbia.

Rebecca Fallk is an associate at Miles & Stockbridge.

[1] https://www.justice.gov/opa/speech/file/1535301/download.

[2] https://www.justice.gov/opa/speech/file/1535301/download.

[3] https://www.ussc.gov/sites/default/files/pdf/research-and-publications/research-publications/2022/20220829_Organizational-Guidelines.pdf.

[4] https://www.justice.gov/criminal-fraud/page/file/937501/download.