CEP Magazine - January 2021
Balancing effective compliance policies against the ubiquity of ephemeral messaging

By Daniel J. Polatsek

Daniel J. Polatsek (daniel.polatsek@icemiller.com) is a Chicago-based partner in Ice Miller's White Collar Defense and Investigations Groups, where he oversees internal investigations and handles sensitive corporate governance and litigation matters for both public and private companies.

As we enter into the first quarter of 2021, the available evidence indicates that remote work is going to remain part of the work-life balance for much of this year. The US workforce continues to face unexpected pay cuts, furloughs, and layoffs, while senior executive teams and upper management face pressures to meet revenue expectations and budgeted projections for both shareholders and Wall Street.

For many companies, these economic pressures require reductions in force, consolidating greater authority within a smaller workforce and executives who have less time to supervise and approve operational decisions. The dilemma now is how the private sector responds to the challenge of having to do more with less but just as fast.

The answer, in part, is better, faster, and more secure communication platforms, but the technologies that make speed and efficiency possible, such as ephemeral messaging (i.e., mobile-to-mobile transmissions that are designed to self-delete from the recipient's screen after the message has been viewed) and employee use of personal devices for business, raise complicated issues for compliance departments seeking to manage risk without overmanaging business solutions that allow companies to stay productive.

Compliance programs in the pandemic

Over the past year, the Department of Justice has made clear that the pandemic will not excuse a substandard compliance infrastructure.[1] Companies are still required to tailor compliance programs designed to prevent, detect, and remediate unlawful conduct. This was most recently discussed in the virtual town hall held by representatives of the Department of Justice, the Securities and Exchange Commission, and the Federal Bureau of Investigation on May 20, 2020. These agencies made clear that while the pandemic is a challenging environment for compliance programs, the pandemic is not a defense to inadequate compliance protocols resulting in unlawful conduct.[2] Following the virtual town hall this past May, the Department of Justice also issued its updated *Evaluation of Corporate Compliance Programs* guidance in June 2020.[3] The guidance touched upon several different factors necessary for an effective compliance program. One key takeaway was that an organization's compliance program must be rationally tailored to the risks inherent to that organization's business operations. Put another way, *how and why* a company designed its compliance program can be an important factor in whether the company is afforded leniency later by a regulator if one or more of its employees is involved in unlawful conduct.

The necessity of internal investigations

If the past is prologue, companies will continue to have to investigate civil and criminal conduct such as conflict

of interest schemes, trade secret misappropriation, public corruption, price fixing, embezzlement, and insider trading, to name a few. Each scheme dictates its own appropriate investigatory methodology and constituent audiences, but the objectives remain the same: stop potential unlawful conduct, understand the nature and extent of the unlawful conduct, lawfully mitigate the legal and business risks arising from the unlawful conduct, and prevent the same or similar unlawful conduct from reoccurring. Meeting the foregoing objectives during an internal investigation is accomplished through an examination of the available evidence that generally hails from two sources: (1) witness interviews and (2) documentary evidence (i.e., electronic and hard-copy documents and communications). When witnesses cannot or will not fill in the details of a fraud scheme or other unlawful conduct, transactional records, hard-copy documents, and electronic communications are critical to filling in the information gaps.

Those overseeing an internal investigation, such as in-house counsel, audit committees, boards of directors, and other authorized stakeholders, must frequently assess whether the current circumstances warrant voluntary disclosure of the conduct being investigated to a regulator. Among other important considerations is whether a company's voluntary disclosure would allow it to seek leniency; cooperation credit; or, in a best case scenario, avoid any adverse consequence all together. The extent to which a company may be extended leniency within the context of a voluntary disclosure can be linked, in part, to its own root cause analysis of the underlying unlawful conduct. In other words, the degree to which leniency is extended to a company may be contingent on the company's efforts to understand the who, what, where, when, and how behind the unlawful conduct being investigated. Stated differently, corporate leniency extended by a regulator may be measured, in part, by how much a company can inform the government about what happened.

Once a voluntary disclosure is made and leniency is sought through cooperation credit or another avenue, it should be anticipated that a company's compliance program will be evaluated with respect to its capabilities to prevent and detect unlawful conduct through its preexisting compliance policies. Because ephemeral messaging is quickly becoming an integral part of how employees in corporate America communicate, companies can expect regulators to inquire about ephemeral messaging, the compliance policies underlying its use, and the policies underlying its preservation and collection during an investigation.