THE REVIEW OF
SECURITIES & COMMODITIES REGULATION
AN ANALYSIS OF CURRENT LAWS AND REGULATIONS AFFECTING THE SECURITIES AND FUTURES INDUSTRIES

Vol. 56 No. 13 July 19, 2023

DEALING WITH (AND HOW NOT TO DEAL WITH) WHISTLEBLOWERS

Recent enforcement actions demonstrate an increasing reliance on whistleblowers by federal regulators and law enforcement. Therefore, it is more likely than ever that a company will have to face whistleblower complaints, and more critical than ever that companies do so effectively. This article outlines best practices for dealing with whistleblowers and encouraging internal reporting, as well as how to steer clear of the common mistakes companies make when a whistleblower complaint arises.

By Terri L. Chase, David Peavler, and Alexander J. Wilson *

Whistleblowers today play a prominent role in the enforcement efforts of the principal financial market regulators, the Securities and Exchange Commission, and the Commodity Futures Trading Commission. The SEC explicitly acknowledges this in public statements, characterizing its whistleblower program as "critical" to its enforcement success[1] and "instrumental in helping the SEC detect and prosecute wrongdoing . . . "[2]

The trend in whistleblower awards bears this out. The SEC, for instance, reported its two largest aggregate awards payouts, both in number of recipients and amount awarded, in the last two fiscal years, and just announced the largest single whistleblower award ever granted by SEC or CFTC of $279 million on May 5, 2023.[3] The SEC also reported receiving a record number of whistleblower tips in fiscal year 2022 — more than 12,300 — narrowly breaking the record set a year earlier.[4] The CFTC likewise announced record-breaking whistleblower numbers in 2022, including what

[1] SEC Press Release, *SEC Announces Enforcement Results for FY 2021*, November 18, 2021, *available at* https://www.sec.gov/news/press-release/2021-238.

[2] SEC Press Release, *SEC Issues $28 Million Award to Joint Whistleblowers*, January 24, 2023, *available at* https://www.sec.gov/news/press-release/2023-16.

[3] SEC FY 2021 Results, *supra* note 1; SEC Press Release, *SEC Announces Enforcement Results for FY 2022*, November 15, 2022, *available at* https://www.sec.gov/news/press-release/2022-206.

[4] SEC Whistleblower Program 2021 Annual Report to Congress, *available at* https://www.sec.gov/files/owb-2021-annual-report.pdf; SEC FY 2022 Results, *supra* note 3.

* *TERRI L. CHASE is a partner in the Miami office of Jones Day. DAVID PEAVLER is a partner in the firm's Dallas office. ALEXANDER J. WILSON is a partner in the firm's New York City office. Their e-mail addresses are tlchase@jonesday.com, dpeavler@jonesday.com, and alexanderwilson@jonesday.com. The views and opinions set forth herein are the personal views or opinions of the authors; they do not necessarily reflect views or opinions of the law firm with which they are associated.*

RSCR Publications LLC Published 22 times a year by RSCR Publications LLC. Executive and Editorial Offices, 2628 Broadway, Suite 29A, New York, NY 10025-5055. Subscription rates: $1,197 per year in U.S., Canada, and Mexico; $1,262 elsewhere (air mail delivered). A 15% discount is available for qualified academic libraries and full-time teachers. For subscription information and customer service call 609-683-4450; fax 609-683-7291; write Subscriber Services, RSCR Publications, PO Box 585, Kingston NJ 08528; e-mail cri.customer.service@comcast.net; or visit our website at www.rscrpubs.com. General Editor: Michael O. Finkelstein; tel. 212-876-1715; e-mail mofinkelstein@gmail.com. Associate Editor: Sarah Strauss Himmelfarb; tel. 301-294-6233; e-mail sarah.s.himmelfarb@gmail.com. To submit a manuscript for publication contact Ms. Himmelfarb. ISSN: 0884-2426.

was then the largest ever single award of $200 million.[5] Since making their first whistleblower awards in 2012 and 2014, respectively, the SEC and CFTC together have awarded approximately $2 billion to more than 350 claimants. More than two-thirds of this amount has been awarded since 2020.[6]

As a result of recent congressional action to expand the use of whistleblowers for federal enforcement, the Treasury Department's Financial Crimes Enforcement Network (or "FinCEN") has now joined the ranks of federal regulators with robust whistleblower programs.[7] Like the SEC and CFTC, FinCEN incentivizes whistleblowing by offering sizable cash awards based on the monetary sanctions it collects as a result of a whistleblower's information regarding violations of (1) the Bank Secrecy Act and associated anti-money laundering regulations and (2) violations of U.S. economic sanctions.[8] FinCEN extends cash-award eligibility and anti-retaliation protection to corporate compliance professionals and internal-only whistleblowers, which generally is not the case under the SEC and CFTC programs.[9]

Against this backdrop, it is more likely than ever that a company will have to address a whistleblower complaint, whether from an employee reporting through internal channels or externally through a government investigation, and more critical than ever that companies do so effectively. Accordingly, it is important to follow best practices when dealing with whistleblowers and, in particular, to avoid actions that could be perceived as retaliatory or inhibitive, which the government has frequently punished as fervently as the underlying misconduct itself. Importantly, companies should focus on maintaining policies and practices that encourage internal whistleblowing. Federal prosecutors and regulators are increasingly insistent that companies self-report potential wrongdoing swiftly and comprehensively to qualify for cooperation credit. This places a premium on early detection of alleged misconduct, coupled with timely investigation and assessment of its seriousness, scope, and impact. Companies whose employees first report alleged misconduct to the government may lose the self-reporting advantage, so persuading employees to report complaints to the company first — *i.e.*, to be internal rather than external whistleblowers — can be critical to minimizing the risks of government enforcement action and the potential penalties where wrongdoing is discovered.

This article outlines best practices for dealing with whistleblowers and encouraging internal reporting, as well as how to steer clear of the common mistakes companies make when a whistleblower complaint arises.

BEST PRACTICES

A corporate whistleblower program's primary objective should be to encourage employees to raise complaints internally with the company in the first instance and to ensure that the company gives those complaints the attention they deserve. An effective corporate whistleblower program will take advantage of the role that such complaints often play in improving corporate compliance and operations, while mitigating the legal and other risks that may arise from external whistleblowing to regulatory authorities, the media, and other third parties.

[5] CFTC Press Release No. 8613-22, *CFTC Release Annual Enforcement* Results, October 20, 2022, *available at* https://www.cftc.gov/PressRoom/PressReleases/8613-22.

[6] SEC Whistleblower Program 2021 Report, *supra* note 4; SEC Press Release, SEC Whistleblower Office Announces Results for FY 2022, https://www.sec.gov/files/2022_ow_ar.pdf; CTCF Whistleblower Program Reports to Congress for 2020-2022, *available at* https://www.whistleblower.gov/reports#: ~:text=The%20CFTC%20submits%20an%20annual,awards%20and%20customer%20education%20initiatives.

[7] Anti-Money Laundering Act, Public Law 116-283 (January 1, 2021), Section 6314 and Anti-Money Laundering Whistleblower Improvement Act, Public Law 117-328 (December 12, 2022), Section 401, both codified at 31 U.S.C § 5323.

[8] *Id.*

[9] Public Law 116-283 (1/1/2021), Section 6314, codified at 31 U.S.C § 5323.

Creating an Environment that Encourages Internal Reporting

Encouraging potential whistleblowers to first report concerns in-house brings numerous advantages. Chiefly, it helps companies identify risks at an earlier stage when they can be dealt with more effectively and before they threaten more serious harm to the organization. In addition, academic research suggests that internal whistleblowing strengthens a company's culture of compliance and leads to fewer material lawsuits.[10] Establishing an effective internal whistleblower program also promotes employee trust and reduces the likelihood of open-ended regulatory inquiries that can consume time and resources.

Early internal reporting also allows the company to investigate and self-report potential wrongdoing to law enforcement and regulators, a key requisite for receiving cooperation credit in the event of an enforcement action. For instance, the Department of Justice recently announced new policies for both its Criminal Division and the 93 U.S. Attorney's Offices nationwide that emphasize "voluntary self-disclosure [] made immediately upon the company becoming aware of the allegation of misconduct" as a key factor in potential declination of charges and up to 75% reductions in penalty amounts.[11] To be considered a voluntary self-disclosure, the updated policies require that it be made prior to an imminent threat of disclosure or government investigation, or before being publicly disclosed elsewhere or otherwise known to the government, and not required by another legal obligation. The self-disclosure must be made within a reasonable time of discovery, with the company obliged to demonstrate timeliness. The disclosure also must be comprehensive, based on the facts the company knew at the time. The SEC and CFTC policies on cooperation similarly prioritize voluntary self-disclosure as a key mitigating factor in enforcement actions, though without the same clarity on the precise benefits of self-disclosure.[12]

Because voluntary self-disclosure credit is unavailable when the information is already known to the government, companies that fail to encourage internal whistleblowing as the first step for concerned employees will generally be unable to receive such credit and its attendant benefits. If the government has already received a whistleblower report, disclosure by the company will not qualify even if the information was disclosed immediately upon the company's receipt of the same report.

To encourage potential whistleblowers to report internally first, companies should ensure that they have established clear channels by which employees can report complaints easily, confidentially, and without fear of retaliation. Companies must also clearly communicate to their employees that they are encouraged to report complaints internally through those channels and how they can do so. Ethics hotlines and e-mail boxes, web-based reporting, and similar systems are ubiquitous in corporate America, but their effectiveness must be tested and assessed regularly to ensure they are functioning as designed and that employees are aware of and using them; companies should not assume that a low incidence of complaints through these systems indicates an absence of potential concerns. Also, importantly, companies should foster other communication channels, such as through supervisors and human resources, and internal compliance or audit departments. These groups should receive periodic training for appropriately engaging with and responding to potential whistleblowers and how to escalate complaints to legal or compliance departments. Further, written policies should be established, and trained on, that clearly prohibit direct or indirect retaliation against those who submit complaints.[13] Any internal structure should provide for prompt

[10] *See, e.g.*, Stubben, Stephen and Welch, Kyle T., Evidence of Internal Whistleblowing Systems (October 26, 2018), *available at*: https://papers.ssrn.com/sol3/papers.cfm?abstract_id =3273589.

[11] Remarks of Kenneth Polite, January 17, 2023, *available at* https://www.justice.gov/opa/speech/assistant-attorney-general-kenneth-polite-jr-delivers-remarks-georgetown-university-law; Department of Justice Criminal Division Corporate Enforcement and Voluntary Self-Disclosure Policy, *available at* https://www.justice.gov/criminal-fraud/file/1562831/download; United States Attorneys' Offices Voluntary Self-Disclosure Policy, *available at* https://www.justice.gov/d9/press-releases/attachments/2023/02/22/usao_voluntary_self-disclosure_policy_0.pdf. (USAOs will not seek a guilty plea against a company that (1) voluntarily self-discloses, (2) fully cooperates, and (3) timely and appropriately remediated.)

[12] SEC Enforcement Manual, November 28, 2017, pg. 98, *available at* https://www.sec.gov/divisions/enforce/enforcementmanual.pdf; CFTC Enforcement Advisory, Updated Advisory on Self Reporting and Full Cooperation, September 25, 2017, *available at* https://www.cftc.gov/sites/default/files/idc/groups/public/@lrenforcementactions/documents/legalpleading/enfadvisoryselfreporting0917.pdf.

[13] *See, e.g.*, Best Practices for Protecting Whistleblowers and Preventing and Addressing Retaliation, April 21, 2015, *available at* www.whistleblowers.gov/sites/default/files/2016-11/WPAC_BPR_42115.pdf.

acknowledgment of a whistleblower's complaints, followed by an independent review, escalation, and resolution.

Investigating Whistleblower Complaints When They are Made

When a company learns of a potential whistleblower, how it responds can be critical to the outcome. The recent case of Danske Bank provides an apt example of the dangers of inadequately addressing whistleblower complaints. In December 2022, Danske Bank pled guilty to U.S. bank fraud charges and agreed to pay total penalties of over $2 billion to DOJ, the SEC, and Danish authorities.[14] The underlying conduct, which involved massive AML failures and suspected money laundering at Danske Bank's Estonian branch, had been the subject of an internal whistleblower report. Despite being aware of the whistleblower report, Danske Bank's management allowed the underlying conduct to continue for years, during which the bank made critical misrepresentations to U.S. financial institutions to induce them to process U.S. dollar payments for Danske Estonia that were the basis for much of the U.S. criminal liability. In short, the failure to effectively investigate and evaluate the whistleblower report and to remediate the underlying conduct both exposed Danske Bank to additional criminal liability and was considered a critical aggravating factor by U.S. authorities in reaching an unusually severe corporate resolution and penalty.

While there is no one-size-fits-all approach to handling whistleblower complaints, there are certain common steps that companies can take to ensure that they are handling complaints effectively.

First, for an internal whistleblower, it is important to acknowledge receipt of their complaint and assure them that it will be taken seriously. The firm should consider whether, when, and how to interact with the internal whistleblower. In some cases, it is advisable to interact early to gather all their complaints and to fully understand their complaints, while in others, some initial fact-gathering might be beneficial prior to engaging with the whistleblower. In all cases, it is important for the company to avoid conveying any impression to the whistleblower that his or her internal reporting was futile or that external reporting is the only viable means of redress.

Next, a company should evaluate whether the complaint implicates issues that should be escalated to the board of directors (or comparable body, if any) or senior management. The appearance of independence is important to both the whistleblower and to regulators, and law enforcement who may review the firm's response in hindsight. Therefore, where the complaint implicates senior leadership, the company should ensure that independent decision-makers of sufficient seniority oversee any evaluation of the complaint.

A closely related assessment is whether to investigate the complaint with internal resources or to employ outside counsel. This determination includes consideration of a number of factors, including the seriousness of the complaint's allegations and its significance to the company or its customers; the firm's internal resources and expertise; the independence of those internal resources; and the likelihood of regulatory or law enforcement scrutiny and/or private litigation. While using internal resources may sometimes be more expedient or economical in the short term, engaging outside counsel can signal greater independence of the investigation, which may prove beneficial to the company in the long term.

Upon learning of a whistleblower complaint, companies should develop an investigative plan that appropriately scopes the investigation, taking into account such factors as civil, regulatory, or criminal exposure; the seriousness and nature of the allegations; the company personnel implicated in the allegations; and whether the alleged conduct is ongoing. An investigative plan should include an estimated timetable for completion, taking into account internal and external factors (such as pending litigation or impending disclosure requirements) that may require faster resolution.

Starting from receipt of a complaint, the company should promptly preserve potentially relevant evidence and document that through a written preservation and retention policy tailored to the complaint and communicated to relevant employees. The firm's IT department should be involved in suspending any regular document deletion programs and creating backups of relevant systems and, where appropriate, individual devices. The company should carefully consider when and how to obtain forensic images of employees' company-issued devices, which may potentially contain critical information, but whose collection will usually reveal the existence of the

[14] DOJ Press Release, Danske Bank Pleads Guilty to Fraud on U.S. Banks in Multi-Billion Dollar Scheme to Access the U.S. Financial System, December 13, 2022, *available at* https://www.justice.gov/opa/pr/danske-bank-pleads-guilty-fraud-us-banks-multi-billion-dollar-scheme-access-us-financial.

investigation and allow potential wrongdoers to destroy evidence or otherwise frustrate an investigation.[15] An investigative plan should include a process for reviewing the data collected and other data relevant to the matter, such as personnel files of those involved with the allegation and potential witnesses. This often entails a "rolling" or segmented review that allows interviews to start before all data has been reviewed.

After reviewing data collected during the initial phases of the investigation, the company should plan and conduct witness interviews with relevant individuals — giving thought to sequencing them in a manner most likely to deliver the most useful information. It is also imperative that any interviews by or at the direction of the firm's counsel are accompanied by *Upjohn* warnings, alerting the witness of the interview's purpose, that the interviewer represents the company or the board in the interview, and that any privileges belong to the company or the board, which may choose to waive the privilege and provide the interview contents to others.[16] Interviews should be conducted by one or more questioners and a separate notetaker. Interview notes ideally should be reduced to a privileged summary shortly after the interview is complete.

The last step in the investigative process is to report and close the investigation. Depending on the circumstances, a report can be a formal written document, a summary, a slide deck, or an oral presentation. Regardless of format, the report typically should address all the issues and allegations involved, the investigative process, key findings, any limitations on the investigation (e.g., witness resistance or unavailability), and remedial actions recommended. It is critical to assess the likely use of the report and potential for waiver of privileges over the report before deciding the scope of the content and level of detail for the report. Upon review of the report, the company should adopt appropriate remedial action and ensure that such remediation is documented and overseen to conclusion by someone of appropriate seniority and authority. The company should also evaluate whether to update the whistleblower on findings and remediation and, if so, when to make those updates. Depending on the magnitude of the issue, closing the loop with the whistleblower can reinforce that the company took the matter seriously and forestall external reporting. Finally, the company should consider whether it has legal obligations to report conclusions to regulators, investors, customers, or others.

The general investigative steps are the same when the potential whistleblower reports externally, but in those circumstances, time is typically of the essence because the regulator or law enforcement agency acting on the complaint is often pursuing its own investigation. Independence is also critical to avoid the appearance that the internal investigation is biased or that it simply constitutes advocacy. In either situation, a timely, properly conducted, scoped, and appropriately independent internal investigation may be a decisive factor for the government to take no or diminished action with respect to the firm.[17]

PITFALLS TO AVOID

A critical component of any effective compliance program is a clear prohibition on retaliation against whistleblowers. Yet in addressing a whistleblower complaint, companies must not only be concerned about more obvious forms of retaliation, which are clearly prohibited, but also less obvious forms of retribution that the SEC has dubbed "pretaliation."

[15] More broadly, companies should carefully consider their policies and practices for employee communication methods and preservation of communications in light of recent SEC and CFTC enforcement actions and DOJ announcements that it will consider such policies when assessing corporate cooperation and remediation. SEC Press Release, SEC Charges 16 Wall Street Firms with Widespread Recordkeeping Failures, September 27, 2022, *available at* https://www.sec.gov/news/press-release/2022-174; CFTC Press Release, CFTC Orders 11 Financial Institutions to Pay Over $710 Million for Recordkeeping and Supervision Failures for Widespread Use of Unapproved Communication Methods, September 27, 2022, *available at* https://www.cftc.gov/PressRoom/PressReleases/8599-22; September 15, 2022 Memorandum of Lisa Monaco, p. 11, *available at* https://www.justice.gov/opa/speech/file/1535301/download; DOJ Criminal Division Evaluation of Corporate Compliance Programs, at 17-18, *available at* https://www.justice.gov/criminal-fraud/page/file/937501/download.

[16] *Upjohn Company v. United States*, 449 U.S. 383 (1981).

[17] Remarks of Kenneth Polite, *supra* note 20; DOJ Corporate Enforcement Policy, *supra* note 20; Report of Investigation Pursuant to Section 21(a) of the Securities Exchange Act of 1934 and Commission Statement on the Relationship of Cooperation to Agency Enforcement Decisions, Exchange Act Rel. No. 44969 (October 23, 2001) (SEC statement regarding corporate cooperation).

Retaliation

Terminating, demoting, or publicly shaming a known or suspected whistleblower obviously invites potential liability under whistleblower retaliation provisions. The SEC has brought numerous enforcement actions premised on this type of conduct.[18] These adverse actions may also provide grounds for a private cause of action by the affected employee, as permitted by the SEC and CFTC whistleblower statutes.[19]

But potential retaliation may come in more subtle forms as well. Each agency's whistleblower rules include anti-retaliation provisions whose language is subject to broad reading. The SEC's anti-retaliation statute, for instance, provides that "[n]o employer may discharge, demote, suspend, threaten, harass, *directly or indirectly*, or *in any other manner discriminate against*, a whistleblower in the terms and conditions of employment" for any act lawfully taken as a whistleblower.[20] The CFTC and FinCEN anti-retaliation rules contain virtually identical language.[21] Accordingly, these agencies may interpret "retaliation" to include such conduct as an employer's active efforts to discover a whistleblower's identity, alter their access to information necessary to do their jobs, redirect their duties,[22] or gather facts to undermine their credibility.

What if the whistleblower is an employee otherwise in line for termination or other discipline for performance or other non-whistleblower-related reasons, such as a planned reduction in force? In these circumstances, contemporaneous documentation of the company's reasons for taking action is critical to show that the proffered reasons were not merely pretextual to punishing a whistleblower. Companies are not required to refrain from disciplining poor employees simply because they are whistleblowers. But this can be a challenging line to walk. The SEC, for instance, sued an energy company that had terminated a whistleblowing employee as part of a broader reduction in force.[23] Company documents showed that the employee had earlier been offered a promotion (which he declined) and was otherwise well-regarded. But after he raised complaints about the company's public reporting, company officials expressed among themselves that the employee's concerns were "disruptive" and that he could be replaced with someone "who could do the work without creating all of the internal strife." They also searched his e-mails for evidence that he had reported to the SEC before deciding to include him in the reduction in force. Based on these facts, the SEC concluded that the company's reasons for terminating the employee were pretextual and thus levied a $1.4 million fine.

It is important to note that merely consulting with employment counsel before terminating a whistleblower is not a shield against an SEC action for retaliation, where the overall circumstances appear to the SEC to be retaliatory. In the *Paradigm Capital Management* case, an investment adviser's head trader made a whistleblower report to the SEC that his company had engaged in inadequately disclosed or authorized principal trades with an affiliate. A few months later, the head trader alerted his supervisors that he was concerned about these trades and had made a report to the SEC. Although the company maintained his pay and benefits at existing levels, it relied on advice of counsel to immediately remove him from his former duties, cut off his work e-mail, strip him of supervisory duties, require him to work from home, and assign him menial duties. The company also accused him of removing confidential company information from its systems, in violation of his terms of employment. Ultimately, the employee resigned. The SEC charged the company and its president with principal trading violations and whistleblower retaliation and fined them $300,000, covering both violations.[24]

In addition to federal anti-retaliation provisions, state law may impose additional risks for companies addressing whistleblowers and potential whistleblowers. For example, a number of states have statutes that prohibit retaliation against employees who raise allegations that the company has engaged in conduct that violates a statute, regulation, or ordinance.[25] Companies

[18] *See, e.g.*, In the Matter of SandRidge Energy, Inc., Exchange Act Rel. No. 79607 (December 20, 2016) (termination of a whistleblower who had previously been in line for promotion); In the Matter of Paradigm Capital Management, Inc., et al., Exchange Act Rel. No. 72393 (June 16, 2014) (relief of duties and then termination of the whistleblower).

[19] 15 USC §78u-6(h)(1)(B) (SEC); 7 USC §26(h)(1)(B) (CFTC).

[20] Securities Exchange Act of 1934, Section 21F(h)(1)(A), codified at 15 U.S.C. §78u-6(h)(1)(A) (emphasis added).

[21] 17 CFR §165.20(a) (CFTC); 31 USC §5323(g) (FinCEN).

[22] In the Matter of International Game Technology, Exchange Act Rel. No. 78991 (September 29, 2016).

[23] In the Matter of SandRidge Energy, Inc., Exchange Act Rel. No. 79607 (December 20, 2016).

[24] In the Matter of Paradigm Capital Management, Inc., Exchange Act Rel. No. 72393 (June 16, 2014).

[25] *See, e.g.*, NY Lab L § 215 (2023) (New York Labor Law prohibiting workplace retaliation); N.J.S.A. § 34:20-9 (2023)

should therefore carefully assess the applicable retaliation law in the states in which they operate, and consult with outside counsel as necessary, to ensure their whistleblower practices are compliant.

"Pretaliation"

Companies must also beware of so-called "pretaliation," which is a term the SEC uses to describe efforts to inhibit potential whistleblowers from reporting information to the government. SEC regulations expressly prohibit anyone from taking "any action to impede an individual from communicating directly with Commission staff about a possible securities law violation," including by enforcing or threatening to enforce a confidentiality agreement with respect to such communications.[26] The SEC has interpreted this prohibition broadly to include agreements or policies that require someone to get approval from the employer before speaking with the SEC,[27] to alert their employer that they are speaking with the SEC,[28] or to forego or waive claims for whistleblower awards.[29]

Actions a company or its executives take with respect to potential whistleblowers can also be considered inhibitive of whistleblowers, as illustrated by the SEC's April 2022 enforcement action against a software company executive. After the executive learned of a subordinate's concerns about the company's public disclosures, he took a number of actions to cut the subordinate off from critical information systems and to learn whether the employee had reported to the SEC. For example, the executive (1) removed the employee's access to the company's IT systems so that he could not obtain additional information about his complaints; (2) remotely accessed the employee's company-issued laptop to view what the employee was working on in real-time; and (3) remotely accessed the password keeper on the employee's laptop to obtain passwords, which were then used to access the employee's social media accounts. While none of these actions actually prevented the subordinate from reporting his concerns to the SEC (which he ultimately did), the SEC found that the executive's actions discouraged such reporting and fined him nearly $100,000.[30]

Similarly, as part of its revised policies regarding its assessment of corporate cooperation, DOJ is also taking into account the extent to which a corporation uses or has used non-disclosure or non-disparagement provisions in compensation, severance, or other agreements so as to inhibit the public disclosure of criminal misconduct by the corporation or its employees.[31]

To avoid these problems, companies should be sure to review employment and confidentiality policies, employment agreements, severance agreements, and non-disclosure agreements to ensure that they have no conditions, limitations, or prerequisites for employees to communicate with the government. The SEC has tended to treat any such limitations as violations. Ideally, these materials should expressly provide that employees are free to communicate with the SEC and other government agencies concerning any potential violations of the law the employee believes may have occurred. Companies should also train managers and supervisors not to interrogate employees or otherwise seek to discover whether anyone is acting as a whistleblower. Such actions may constitute both "inhibiting communications" and "retaliation," depending on what the supervisor does. ■

---

footnote continued from previous page…

(New Jersey's statute prohibiting discrimination and adverse action against any person in retaliation when asserting the following workplace rights); Cal. Code Regs. tit. 2 § 1102.5 (California's protection against retaliation against an employee who believes that he or she is disclosing a violation of state or federal statute, or a violation or non-compliance with a local, state, or federal rule or regulation); 940 Mass. Reg. 33.08 (Prohibition in Massachusetts on retaliation and interference by employer when its employee opposes practices which the employee reasonably believes to be in violation of state law); IHRA, 740 ILCS 174 (Providing a series of acts or omissions an employee may take while being protected against retaliation by his or her employer in Illinois).

[26] Rule 21F-17.

[27] In the Matter of KBR, Inc., Exchange Act Rel. No. 74619 (April 1, 2015).

[28] In the Matter of Activision Blizzard, Inc., Exchange Act Rel. No. 96796 (February 3, 2023).

[29] In the Matter of Blue Linx Holdings Inc., Exchange Act Rel. No. 78528 (August 10, 2016).

[30] In the Matter of David Hansen, Exchange Act Rel. No. 94703 (April 12, 2022).

[31] Monaco Memorandum, *supra* note 23, p. 10.