Articles + Publications | July 13, 2021

Companies Should Exercise Caution When Addressing Anonymous Whistleblower Complaints

WRITTEN BY

Jay A. Dubow | Ghillaine A. Reid | Meredith Sherman

Public companies should proceed with caution when receiving and investigating anonymous whistleblower complaints. Several public companies recently received whistleblower complaints from an anonymous source – each with identical or similar wording – purporting to concern alleged insider trading by employees at the recipient company. These complaints, which have been submitted to the third-party ethics or whistleblower e-mail hotlines at a number of public companies, allege that unidentified company employees made statements suggesting that the employees traded in the company's stock based on non-public information.

Similarly, certain companies have received purported whistleblower claims from an anonymous employee relating to alleged bribery of clients. One recent complaint claimed a co-worker provided preferential pricing in exchange for anticipated return favors from a large customer's wife, a government official who could provide potential employment opportunities or school admissions. A separate anonymous complaint circulating contains claims about employees approving invoices for excess amounts who have a friend or relative at a vendor company.

Because the complaints contain similar language and content, they are believed to be a hoax. Companies should collaborate with their cybersecurity and internal audit teams to evaluate whether the complaints relate to ransomware or a cybersecurity attack.

Whistleblower Claims Generally

Whistleblower laws have been enacted at the state and federal level to protect employees who report, in good faith, conduct that the employee believes to be unlawful or unethical. Under these laws, employees may refuse to follow instructions from an employer if the employee believes the actions are unlawful. Whistleblower laws typically include anti-retaliation provisions that prohibit employers from taking adverse employment action against a reporting employee, including termination or demotion.

Typically, when a company receives a credible whistleblower complaint, the proper course of action is to promptly and thoroughly commence an internal investigation to assess the merits of the allegations. The internal investigation should be conducted by and at the direction of in-house and/or outside counsel in order to preserve the integrity and privileged nature of the review, and ensure that proper legal guidance is rendered regarding applicable laws, rules and regulations. The engagement of a third-party investigator may be appropriate in certain circumstances.

The company should thoroughly document all steps undertaken in its investigation of the complaint, whether or not

the allegations ultimately are substantiated. Finally, the company should address any necessary or appropriate corrective measures in consultation with in-house or outside counsel.

However, in cases where companies receive an anonymous and unspecific whistleblower complaint with language that is identical to that of these hoaxes, such companies should discuss with their counsel whether or not an investigation needs to be done, and if so, if it could be on a more limited basis, due to the likelihood of it being a hoax.

Recent Anonymous Whistleblower Claims

Over the course of the last month, numerous public companies have received similarly worded anonymous whistleblower complaints concerning alleged insider trading by unspecified company employees. In other instances, companies have received purported whistleblower claims from anonymous employees alleging that an unidentified employee provided favorable pricing to a client in exchange for potential *quid pro quo* from the client's wife, who was allegedly a government official. A third alleged whistleblower complaint contains claims about employees approving invoices for excess amounts who have a friend or relative at the vendor company.

Although the motives of the complainants in these cases are unclear, it appears that these complaints may relate to attempted cybersecurity scams. These potential "hoax" insider trading, bribery, or accounting fraud claims may present initial challenges for companies in evaluating whether the whistleblower complaints are legitimate grievances, or attempts to circumvent company cybersecurity controls. Accordingly, companies should take special care in investigating purported insider trading or other whistleblower claims where the source of the complaint and/or the employee involved in the alleged misconduct is/are anonymous. Specifically, company counsel (both internal and outside counsel) should collaborate with the company's compliance and ethics, internal audit, cybersecurity and information technology personnel to evaluate the legitimacy of the complaint and determine whether any response to the complaint is warranted. If a company is unsure whether a recent whistleblower complaint alleging insider trading or other alleged misconduct is a hoax, we recommend that the company err on the side of caution and include IT when responding to the complaint to avoid downloading any links or other information that may be contained in the complaint.

As with any whistleblower claim, the company should promptly document all steps taken in investigation of the complaint, whether or not the allegations are ultimately substantiated. This memorialization of the company's internal review should be retained in the event of a later inquiry by any government agency, shareholder, or other third-party.

In the event that the anonymous whistleblower ultimately discloses his or her identity, or the identities of the individuals allegedly involved in the insider trading, the company should promptly investigate the allegations based on this additional information.

Upon the conclusion of a comprehensive internal investigation, the company should – in consultation with counsel and its human resources division – make any necessary employment decisions. Finally, in the event of a cybersecurity breach, the company should seek legal guidance regarding whether self-reporting to the Securities and Exchange Commission (SEC) or other government entities is warranted. Concerns regarding cybersecurity breaches are a high priority for the SEC's enforcement staff, which recently launched an investigative sweep

involving voluntary information requests to several companies inquiring about the impact of the widely-publicized *SolarWinds* cybersecurity attack in December 2020.

Please do not hesitate to contact our Securities Investigations and Enforcement team with any questions regarding how to handle an anonymous whistleblower complaint, or other related issues.

RELATED INDUSTRIES + PRACTICES

- Securities Investigations + Enforcement
- White Collar Litigation + Investigations