Debevoise & Plimpton

Debevoise Update D&P

Cybersecurity and AI Whistleblowers: Unique Challenges and Strategies for Reducing Risk

November 2, 2021

Several recent developments have caused companies to review their whistleblower policies and procedures, especially in the areas of cybersecurity and artificial intelligence (“AI”).

First, on October 28, 2021, New York State amended its Labor Law to dramatically increase whistleblower protections. This brings New York in line with a small but growing number of states, including New Jersey, with very broad protections for whistleblowers.

Second, the Securities and Exchange Commission (the "SEC") recently announced that it has surpassed $1 billion in awards to whistleblowers, including a recent payment of $110 million. Whistleblowers become potentially eligible for an award when they voluntarily provide the SEC with original, timely and credible information that leads to a successful enforcement action. When sanctions exceed $1 million, these awards can range from 10–30% of the money collected. As the SEC continues to escalate its cyber and data management enforcement, and regulators increase their scrutiny over AI, we can expect whistleblower actions in these areas to become more common as well.

Third, on October 6, 2021, the U.S. Department of Justice launched its Civil Cyber-Fraud Initiative, which aims to use the False Claims Act (the “FCA”) to bring actions against companies that offer services to the U.S. federal government who knowingly (1) provide deficient cybersecurity products; (2) misrepresent their cybersecurity practices or protocols; or (3) violate obligations to monitor and report cybersecurity incidents and breaches. This initiative will likely accelerate the number of *qui tam* actions that are filed by current or former employees of government contractors who blow the whistle on their company's deficient cybersecurity standards and practices. Under the FCA, these whistleblowers can receive a percentage of the money recovered by the government as well as protection from retaliation.

Fourth, many companies are rapidly adopting AI programs and using algorithms to assist in important decisions that affect their employees and customers, like hiring, lending, insurance underwriting, marketing and content promotion. Without clear guidance from regulators, internal disputes are likely to arise regarding the appropriate levels of governance and compliance for these AI programs, including with respect to transparency, bias testing, explainability, privacy protections and human oversight. Similarly, with increasing regulatory scrutiny of companies' cybersecurity, there are likely to be internal disagreements over which measures are necessary to protect the company and meet regulatory obligations, and which are not worth the cost or the friction they would create for business operations.

Taken together, these factors: (1) the rise of internal company disputes over cybersecurity and AI, (2) expanding whistleblower protections, (3) the prospect of significant awards and (4) the media's interest in these kinds of disputes due to the public's suspicion that companies are not doing enough in cybersecurity and AI to protect consumers point to a likely significant increase in the number of data-related whistleblowers in the coming years.

Practical Tips for Addressing Whistleblower Complaints. To better prepare and respond to cyber and AI whistleblower complaints, companies should consider adopting the following measures:

- Training: Provide training to management in cyber and AI operations, who may not be very familiar with whistleblowers, on how to identify complaints that may qualify for protection and how to minimize retaliation risks.

- Policies: Review whistleblower policies and procedures to see whether they adequately address issues that arise from cyber- and AI-related complaints. And when investigating a complaint, make sure to follow the established policies.

- Addressing Complaints Promptly: Because cyber- or AI-related concerns are often technical in nature and may require expertise to properly evaluate, they sometimes languish. Delays in responding to whistleblowers increase the likelihood that they will become frustrated and escalate their complaints to the board, regulators or the media.

- Taking Concerns Seriously: Whistleblower complaints are often vague and inflammatory. They should nevertheless be taken seriously. Even when most elements of a complaint are baseless, if one legitimate concern is not properly investigated, a company can face serious consequences.

- Consulting Counsel: Consider involving counsel when faced with complaints regarding alleged violations of law in connection with cybersecurity or AI, especially if any adverse action is being considered against the employee or independent contractor who has raised the concern. Bringing in outside counsel may also help strengthen privilege claims over the investigation and provide a level of independence.

- The Investigation Team: Given the technical nature of many cyber and AI whistleblower claims, it is important that the investigation team has the necessary expertise to evaluate the allegations or has access to consultants who can assist in that evaluation. When consulting in-house experts, be careful not to involve anyone who is implicated by the allegations.

- Avoiding Retaliation: Even the appearance of retaliation can create problems for the company. If the whistleblower is anonymous, it is advisable not to conduct an investigation to figure out their identity. If the identity of the whistleblower is known to investigators, it is best not to share this identity with others, unless it is strictly necessary for the investigation, in order to limit the risk of retaliation.

- Providing Context for Allegations: Whistleblowers sometimes have an incomplete view of their companies' risks. They may have valid concerns but lack a broader context for the priorities of their organization and the competing considerations that ultimately caused their preferred approach not to be adopted by the company. For cybersecurity, there is always more that a company can do, so it is important to assess the costs and business impact of the employee's proposed measures, and whether not addressing their concerns in the way they had wanted resulted in any actual harm such as unauthorized access to sensitive materials.

To subscribe to the Data Blog, please click here.

The authors would like to thank Debevoise law clerk Andreas Pavlou for his contribution to this article.

* * *

Please do not hesitate to contact us with any questions.

NEW YORK

Avi Gesser
agesser@debevoise.com

Corey Jeremy Goldstein
cjgoldstein@debevoise.com

Anna R. Gressel
argressel@debevoise.com

Michael Pizzi
mpizzi@debevoise.com