Cyber Whistleblower Leads to DOJ Civil Settlement

November 5, 2024

On October 22, 2024, the U.S. Department of Justice ("DOJ") announced that The Pennsylvania State University ("Penn State"), a public university in University Park, Pennsylvania, agreed to pay $1.25 million to resolve allegations that it violated the False Claims Act (the "FCA"). Specifically, Penn State allegedly failed to meet cybersecurity requirements in federal government contracts, misrepresented compliance timelines and plans, and failed to use a qualified external cloud service provider.

This is the latest settlement of cybersecurity-related FCA claims since DOJ announced its Civil Cyber-Fraud Initiative in October 2021. The case stems from a complaint filed in the Eastern District of Pennsylvania by Penn State's Chief Information Officer ("CIO"). The complaint was brought under the FCA's qui tam provisions, whereby a private citizen can bring a lawsuit on behalf of the government. The underlying failures alleged in the settlement occurred between 2018 and 2023.

The action against Penn State highlights the importance of tracking compliance with the myriad cybersecurity regulations. As governance over cybersecurity comes sharper into focus, the compliance department's potential role likewise continues to evolve. The settlement also underscores the need to provide a channel for personnel to escalate perceived compliance failures.

THE *PENN STATE* SETTLEMENT

The *Penn State* settlement resolved claims first filed in 2023 by whistleblower Matthew Decker, the former CIO for Penn State's Applied Research Laboratory and Vice Provost, Information Technology for Penn State itself. Decker was responsible for ensuring Penn State's Applied Research Laboratory and Penn State adhered to the U.S. Department of Defense cybersecurity regulations following a significant cyber breach at Penn State.

Decker alleged that, throughout his tenure at Penn State from 2015 to 2022, the university neglected to meet federal regulatory requirements to safeguard confidential

information and violated federal agency contractual regulations. Decker further alleged that Penn State had provided false self-attestations of compliance to federal agencies from at least 2017 to 2022. Finally, he claimed that Penn State neglected to provide accurate dates and timelines for achieving compliance, as required by federal regulation.

Decker filed the action after allegedly repeated attempts to raise internally the issue of compliance proved unsuccessful between 2018 and 2022. For example, Decker alleged that in 2018 he highlighted the compliance gaps to management and was told that Penn State was sufficiently compliant. He also alleged that he offered to create working groups to address compliance gaps, but Penn State had no interest in such working groups in early 2021. Ultimately, Decker alleged that he was allowed to put together a review team in April 2022, and the team's review ultimately demonstrated that many records were falsified.

The DOJ formally intervened in the case on October 23, 2024 and notified the court that it settled with Penn State. Penn State and DOJ reached a $1.25 million settlement to resolve all claims, and Decker received $250,000 from the settlement amount.

The DOJ's Civil Cyber-Fraud Initiative

The *Penn State* settlement comes as the Biden administration increasingly has emphasized the need to combat emerging cyber threats. In announcing the settlement, Special Agent in Charge Greg Gross, Naval Criminal Investigative Service Economic Crimes Field Office, stated: "As our cyber adversaries become increasingly sophisticated, the importance of cybersecurity in safeguarding Department of Defense research, development and acquisitions information cannot be overstated." Additionally, U.S. Attorney Jacqueline C. Romero stated: "Federal contractors who store or access covered defense information must take required steps to protect that sensitive information from bad actors. When they fail to meet their cybersecurity obligations, we and our law enforcement partners will use every available tool to remedy the situation."

As Debevoise previously discussed (and here), the Civil Cyber-Fraud Initiative enforces regulations covering cybersecurity requirements against a much broader group than just those contracting with the DoD or NASA. Previous settlements have included hospitals, software companies, and other defense contractors.

Although the Civil Cyber-Fraud Initiative is aimed at federal contractors, internal whistleblowers may identify other potential liability from false information security attestations. While not all would give rise to claims under the FCA, attestations of compliance could give rise to other forms of civil, or even criminal, penalties.

More broadly, as Debevoise recently noted, DOJ implemented a pilot program in August offering financial awards to whistleblowers who provide information regarding certain corporate crimes. In parallel, DOJ continues seeking to incentivize companies to develop their internal compliance programs.

Key Takeaways

To mitigate the risk of liability under the FCA and better prepare for and respond to cybersecurity-related whistleblower complaints in general, companies should consider the following:

- **Compliance Department Seat at the Cyber Table**: As cybersecurity governance has matured, many companies have increased the size of cyber legal teams and even information security risk teams. Companies also should consider adding subject matter experts to their compliance teams. Compliance personnel have deep experience in monitoring regulations and tracking actual compliance and attestations with such regulations. These teams should consider creating and updating compliance schedules documenting which units are attesting to the firm's compliance with each element.

- **Internal Responsiveness to Cybersecurity Complaints**: All cybersecurity (and other) whistleblower reports merit objective assessment, even when vague or inflammatory, and careful consideration of appropriate next steps. It is important to share such complaints internally with subject matter experts to help determine, at least initially, the appropriate scope of any internal investigation and who is best situated to investigate, including potentially external counsel. Such investigations should proceed expeditiously. In addition, it is important to communicate with whistleblowers in a manner that demonstrates seriousness of purpose and to take steps internally that protect whistleblowers from any retaliation.

- **Technical Expertise of 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 seek to determine their identity. If the identity of the whistleblower is known to investigators, it is best not to share this identity with others, unless strictly necessary for the investigation or otherwise, in order to limit the risk of retaliation.

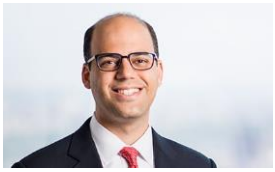
- **Consider Periodic Internal Audits or Similar Reviews of the Whistleblower Process:** As with other important processes, companies should consider how best to monitor that their whistleblower processes are working as designed. This includes, among other things, verifying that complaints are properly received, recorded, escalated, investigated, and resolved, including any appropriate remediation. An internal audit function can play a vital role in such validation, helping (for example) to identify repeat allegations that received insufficient internal attention and therefore present continuing concerns.

* * *

Please do not hesitate to contact us with any questions.

Luke Dembosky
Partner, Washington, D.C.
+1 202 383 8020
ldembosky@debevoise.com

Avi Gesser
Partner, New York
+1 212 909 6577
agesser@debevoise.com



Andrew M. Levine
Partner, New York
+1 212 909 6069
amlevine@debevoise.com

Erez Liebermann
Partner, New York
+1 212 909 6224
eliebermann@debevoise.com

Jim Pastore
Partner, New York
+1 212 909 6793
jjpastore@debevoise.com

Stephanie Cipolla
Associate, New York
+1 212 909 7473
smcipolla@debevoise.com

Michelle Shen
Law Clerk, New York
+1 212 909 6600
mcshen@debevoise.com