Cybersecurity Issues Continue to Require Great Care, Despite Recent Whistleblower Case Dismissal

Publications you may also be interested in:

Federal Agency Announces Million Dollar Award to Culpable Whistleblower

Identify Issues Early: Foster a "Speak Up/Listen Up" Culture

Ensure That Issues Surface: Implement an Independent Retaliation Prevention and Response System

Eliminate Confusion: Train Workers and Managers in Whistleblower Rights and Anti-retaliation

Identify Conflicting Incentives: Measure Results and Mitigate Conflicting Messages

Monitor Effectiveness: Conduct Independent Audits of the Program

Build Credibility: Demonstrate Leadership Commitment and Accountability

What the case means for employers:

On July 16, 2020, the Third Circuit decided *Reilly v. GlaxoSmithKline, LLC* and affirmed the dismissal of a lawsuit brought by a former GlaxoSmithKline ("GSK") employee. The Plaintiff alleged that GSK wrongfully discharged him in retaliation for reporting cybersecurity concerns in the company's manufacturing and financial servers. The Court held that the former employee did not have an objectively reasonable belief that such complaints violated any of the six forms of fraud enumerated in the Sarbanes-Oxley Act ("SOX").

The decision is a useful win for employers in the area of whistleblowing over cybersecurity issues, but employers should nevertheless be cautious. The law continues to evolve in the face of a growing wave of such complaints – with courts rendering divergent rulings depending on the jurisdiction and the facts of each case.

What happened:

Thomas Reilly ("Reilly" or the "Plaintiff") worked for sixteen years in GSK's IT department. His responsibilities included remediating performance and security issues related to AS/400, a computer operating system that hosts manufacturing and financial applications for portions of GSK's business. Between 2011 and 2013, Reilly complained to his direct management of alleged security exposures, performance problems and access privilege issues in the AS/400 system. Reilly's supervisor addressed both issues but, apparently dissatisfied with the responses, Reilly escalated his complaints to GSK's Global Compliance Office in 2014. A year later, Reilly further escalated his complaints to GSK's CEO. Along with detailing alleged cybersecurity issues, Reilly noted that the risks he complained of should have been, but were not, disclosed in GSK's 2013 annual SEC disclosure reports. GSK conducted two investigations into Reilly's complaints and found his complaints unsubstantiated and unfounded.

Meanwhile, in 2013 GSK started a program to reorganize Reilly's department and outsource the AS/400 system to a third-party vendor. In 2014, Reilly learned that every position in the AS/400 team was being eliminated except for Reilly's supervisor and one Analyst position. Reilly did not apply for the Analyst position. GSK eliminated Reilly's position and notified Reilly of his separation from the company in April 2015.

Reilly subsequently filed a whistleblower complaint with the Occupational Safety and Health Administration ("OSHA") that OSHA ultimately dismissed. Reilly appealed to the Administrative Review Board and, while that appeal was pending, filed a complaint in federal court claiming that he had been terminated in retaliation for engaging in SOX-protected activity. The district court granted summary judgment for GSK, finding that Reilly failed to establish facts showing that his complaints about computer security "were even remotely related to fraud of any kind, either at the time of his complaints or in the future."

The Third Circuit affirmed, noting that Reilly's complaints "were nothing more than workplace disagreements about routine IT issues—ones that do not relate to illegal conduct or fraud." The Court emphasized that "although Reilly is not required to show a reasonable belief that each element of a listed anti-fraud law is satisfied, he must still have an objectively reasonable belief of a violation of *one of the listed federal laws*." The Third Circuit ultimately held that no reasonable person in Reilly's place, with his training and experience, could have possibly believed that GSK's conduct violated SOX.

What you need to do:

Reilly is a useful win for employers but cybersecurity remains a major area of focus as IT professionals continue to file aggressive complaints against their former employers in federal courts across the country. By way of example, a complaint filed just last week in the Southern District of New York alleged that a company terminated its former employee as retaliation for reporting "massive holes in its cybersecurity systems" that left the company vulnerable to "potentially seismic" impact. *See Moniodes v. Autonomy Capital (Jersey) LP.* In such cases, courts are rendering divergent rulings depending on the jurisdiction and facts of each case. Therefore every complaint relating to IT and cybersecurity should be carefully investigated and employers should consult with counsel before taking any adverse action against an employee who has raised IT or cybersecurity issues.

For additional guidance on the recent rise in whistleblower claims and what employers can do now to mitigate this threat, please view our recent eBook on the topic by clicking here.

About the authors: Greg Keating is the chair of Choate's Labor, Employment & Benefits and Whistleblower Defense Groups and Anna Roy is an associate in Choate's Litigation Department.

LABOR, EMPLOYMENT & BENEFITS TEAM

Greg Keating
Practice Group Leader – Labor, Employment & Benefits
617-248-5065 | gkeating@choate.com

Alison Reif
Partner
617-248-5157 | areif@choate.com

Lyndsey Kruzer
Principal
617-248-4790 | lkruzer@choate.com

Wells Miller
Principal
617-248-4838 | wmiller@choate.com