

NOT PRECEDENTIAL

UNITED STATES COURT OF APPEALS
FOR THE THIRD CIRCUIT

No. 19-2897

THOMAS REILLY,
Appellant

v.

GLAXOSMITHKLINE, LLC

On Appeal from the United States District Court
for the Eastern District of Pennsylvania
(D.C. Civil No. 2:17-cv-02045)
District Judge: Honorable J. Curtis Joyner

Submitted Pursuant to Third Circuit L.A.R. 34.1(a)
April 14, 2020

Before: CHAGARES, SCIRICA, and ROTH, Circuit Judges

(Filed: July 16, 2020)

OPINION*

* This disposition is not an opinion of the full Court and, pursuant to I.O.P. 5.7, does not constitute binding precedent.

CHAGARES, Circuit Judge.

Appellant Thomas Reilly claims he was wrongfully discharged by his former employer GlaxoSmithKline (“GSK”) in retaliation for reporting his concerns regarding computer stability and security in GSK’s global manufacturing and financial servers. The District Court granted summary judgment to GSK for Reilly’s claim under section 806 of the Sarbanes-Oxley Act of 2002 (“SOX”), 18 U.S.C. § 1514A(a). We will affirm.

I.

We write only for the parties, so our summary of the facts is brief.

A.

GSK is a publicly traded global pharmaceutical company. Reilly worked for GSK for sixteen years in its Information Technology (“IT”) Department, first as an Analyst and then as a Senior Consultant on the AS/400 service team (“AS/400 Team”). The AS/400 is a computer operating system manufactured by IBM that hosts manufacturing and financial applications for portions of GSK’s business. Reilly’s job responsibilities included designing, engineering, and delivering AS/400 servers, and remediating performance and security issues relating to them. He did not set internal security controls.

Beginning in 2011, Reilly complained about “[s]erious security exposures [and] serious performance problems” with the AS/400. Joint Appendix (“JA”) 84. His concerns included the decision to uncapping the AS/400 processors and resulting performance issues. Uncapping processors allows one server to use capacity from another server if capacity is available. Reilly believed that uncapping the processors resulted in the

AS/400 servers becoming “destabilized” — in effect, causing “bad performance” and “corrupted data.” JA 94. First, he complained to his supervisor Jo Taylor, who noted that “it was IBM’s recommendation to turn on Shared Processors,” JA 220, and then he emailed Taylor’s supervisor to report the same concerns regarding server stability and uncapped processors. An IBM representative told Reilly that “[r]egarding uncapped versus capped [processors,] there is no right or wrong answer” because “[i]t depends on the workload and what other resources are assigned.” JA 246. Taylor decided to cap the processors, putting Reilly in charge of the recapping. Ultimately, performance issues persisted even after the processors were capped.

In 2013, Reilly reported an additional concern about computer security: that some AS/400 “users . . . are identified as having more authority than the standard or [GSK’s] system access management plan would” allow. JA 164. Reilly was placed in charge of remediating these access privilege issues, but eventually, Taylor took over and addressed the security risk.

Dissatisfied with GSK’s response to his previous complaints, on January 2, 2014, Reilly escalated his complaints to GSK’s Global Compliance Office. He detailed his concerns with AS/400 server performance issues and his disagreement about enabling uncapped processors. A year later, on January 15, 2015, Reilly further escalated his complaints to GSK’s CEO. In his email, Reilly noted that the problems, which included the “stability, quality control and compliance of the AS[/]400 computer systems . . . could eventually lead to drug manufacturing quality problems, financial data irregularities and even more FDA penalties against GSK.” JA 323. He also noted that the risks he

complained of should have been, but were not, disclosed in GSK's 2013 annual report to the U.S. Securities and Exchange Commission ("SEC").

In response to Reilly's complaints, GSK conducted two investigations. The first, completed in 2014, found Reilly's complaints unsubstantiated. The second, following Reilly's email to the CEO, determined that Reilly's complaints "regard[ing] . . . the stability of the AS[/]400 system" were "unfounded." JA 339.

Form 20-F — part of GSK's annual report to the SEC — provides certifications as to "internal control over financial reporting." JA 356, 370. GSK's 2013 and 2014 20-F Forms identified numerous risk impacts including the "[f]ailure to adequately protect critical and sensitive systems and information [which] may result in [GSK's] . . . business disruption including litigation or regulatory sanction and fines." JA 355, 369. The Forms also noted that GSK "rel[ies] on critical and sensitive systems and data" and "[t]here is the potential that malicious or careless actions expose [GSK's] computer systems or information to misuse or unauthori[z]ed disclosure." JA 355, 369. GSK also disclosed the "[r]isk to the Group's business activity if critical or sensitive computer systems . . . are not available when needed, are accessed by those not authori[z]ed, or are deliberately changed or corrupted." JA 355, 368.

B.

In 2013, GSK started a program to reorganize Reilly's department; as part of this reorganization, GSK decided to outsource the AS/400 system to a third-party vendor. GSK announced the outsourcing in March 2014, when Reilly learned that every position in the AS/400 Team was being eliminated except the Manager position, then occupied by

Taylor, and one Analyst position. On May 6, 2014, the AS/400 Team was informed that all people who were not selected for the Analyst position would be terminated effective September 28, 2014.

Nevertheless, Reilly decided not to apply for the Analyst position. Reilly testified that he believed he would be “protected” because “[he] was escalating to Global Compliance, and they were trying to save [his] job.” JA 110–11. After Reilly declined to apply for the Analyst position, the date on which his termination would become effective changed more than once. Before any effective termination dates arrived, however, Reilly took a short-term disability leave in July 2014, during which his “official notification of separation” was “postponed.” JA 273.

Reilly returned to work in January 2015, and he was informed that he would receive his notice of separation on January 23, 2015. However, because there was a pending internal investigation of Reilly’s complaints made to the CEO, Reilly’s notification of separation was postponed once again. Once the investigation was complete, Reilly was notified in April 2015 that, based on the prior outsourcing of the AS/400 Team, his “official notification of separation from GSK is 8th April 201[5].” JA 377. His last day of employment was June 30, 2015.

Reilly filed a whistleblower complaint with the Occupational Safety and Health Administration in July 2015, which was eventually dismissed. He then filed a petition for review with the Administrative Review Board. While that petition was pending, Reilly 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 has not established 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.” JA 36. The District Court concluded, therefore, that “[n]o factfinder could find [Reilly’s] belief that GSK violated SOX by not naming precise server issues to be objectively reasonable.” JA 36.

This timely appeal followed.

II.

The District Court had jurisdiction under 28 U.S.C. § 1331 and 18 U.S.C. § 1514A(b) and we have jurisdiction under 28 U.S.C. § 1291. “We review a district court’s grant of summary judgment de novo, applying the same standard the district court applied.” Edmonson v. Lincoln Nat’l Life Ins. Co., 725 F.3d 406, 420 n.12 (3d Cir. 2013) (quotation marks omitted). “Summary judgment is appropriate when there is no genuine dispute of material fact and the movant is entitled to judgment as a matter of law.” Id.

III.

Reilly argues that issues of material fact exist regarding whether he made SOX-protected complaints; specifically, that his “complaints about GSK’s computer instability and security and breakdown of internal controls are SOX-protected.” Reilly Br. 20. We disagree.

Congress introduced SOX “to prevent and punish corporate and criminal fraud, protect the victims of such fraud, preserve evidence of such fraud, and hold wrongdoers accountable for their actions.” Lawson v. FMR LLC, 571 U.S. 429, 434 (2014)

(quotation marks omitted). Section 806 of SOX “protects whistleblowing employees from retaliation” by their employers, Wiest v. Tyco Elecs. Corp. (Wiest II), 812 F.3d 319, 328 (3d Cir. 2016), for “provid[ing] information [to their supervisors] . . . regarding any conduct which the employee reasonably believes constitutes a violation of section 1341 [mail fraud], 1343 [wire fraud], 1344 [bank fraud], or 1348 [securities fraud], any rule or regulation of the Securities and Exchange Commission, or any provision of Federal law relating to fraud against shareholders,” 18 U.S.C. § 1514A(a)(1).

For his anti-retaliation claim to survive summary judgment, Reilly “must identify evidence in the record from which a jury could deduce . . . [he] ‘engaged in a protected activity’” under section 806. Wiest II, 812 F.3d at 329 (quoting 29 C.F.R. § 1980.104(e)(2)(i)). An employee’s activity is “protected” if he had “both a subjective and an objective[ly reasonable] belief that the conduct that is the subject of [his] communication relates to an existing or prospective violation of one of the federal laws referenced in § 806.” Wiest v. Lynch (Wiest I), 710 F.3d 121, 134 (3d Cir. 2013). “A belief is objectively reasonable when a reasonable person with the same training and experience as the employee would believe that the conduct implicated in [his] communication could rise to the level of a violation of one of the enumerated provisions in [s]ection 806.” Id. at 132.

Reilly does not meet this standard. He fails to show that his “belief” that GSK was committing one of section 806’s enumerated forms of fraud was objectively reasonable. Reilly argues that “[d]isclosures can be protected even if they do not mention fraud, illegal activity, or anything that could reasonably be perceived to be a violation of

the six enumerated categories in SOX.” Reilly Br. 20. This is true, but immaterial in this case. 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.” Wiest I, 710 F.3d at 132 (emphasis added).

Reilly’s complaints about uncapped processors were nothing more than workplace disagreements about routine IT issues — ones that do not relate to illegal conduct or fraud. Indeed, in response to Reilly’s complaints about uncapping the processors, Taylor worked with Reilly to get IBM’s input and then made the decision to have all processors capped again. Taylor even assigned Reilly to the task of implementing the capping. The same scenario occurred regarding purported inappropriate access privileges: Taylor assigned Reilly to remediate and fix the issue. It is not objectively reasonable in these circumstances to believe that Taylor would assign Reilly to remediate those issues and, at the same time, was perpetuating a cover-up or fraud.

Reilly believed that GSK had an obligation to disclose to the SEC “a recurring incident that is caused by a deficiency in internal controls”; for example, “[i]f [a computer] goes down for an hour and comes back up once a week for a year.” JA 125. In Reilly’s view, GSK failed to disclose “all significant deficiencies and material weaknesses” by omitting the intricacies of computer performance issues from its annual SEC reports. JA 125. Even assuming this is true, however, Reilly fails to explain how this is fraud. His assertions that “GSK’s computer instability and security and breakdown of internal controls . . . [and] [d]isclosures about deficient information security controls are protected under SOX” — without more — do not make it so. Reilly Br. 20. They fall

short of showing that his complaints about internal controls “relate in an understandable way” to any of section 806’s enumerated forms of fraud. Weist I, 710 F.3d at 134.

Reilly, therefore, fails to identify a prohibition within the scope of SOX.

And, in any event, GSK did disclose the “[r]isk to the Group’s business activity if critical or sensitive computer systems or information are not available when needed, are accessed by those not authori[z]ed, or are deliberately changed or corrupted.” JA 355, 368. GSK also reported the risk to its business posed by “[f]ailure to adequately protect critical and sensitive systems and information . . . which could materially and adversely affect [GSK’s] financial results” and “the potential that malicious or careless actions [could] expose [GSK’s] computer systems or information to misuse or unauthori[z]ed disclosure.” JA 355, 369.

Based on these facts, no reasonable person in Reilly’s place, with his training and experience, could have believed that GSK’s conduct violated SOX.¹

IV.

For these reasons, we will affirm the judgment of the District Court.

¹ Reilly also claims that issues of material fact exist regarding whether his SOX-protected activity contributed to GSK terminating his employment. Because we will affirm the District Court on the grounds discussed above — that Reilly did not engage in SOX-protected activity — we need not reach this argument.