IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF ILLINOIS
EASTERN DIVISION

UNITED STATES ex rel. MARK PANNEK, Plaintiff, v. ARCHER DANIELS MIDLAND COMPANY, Defendant.	Case No. 23 CV 15145 Honorable Sunil R. Harjani

MEMORANDUM OPINION AND ORDER

According to Mark Pannek, his former employer, Archer Daniels Midland, made false representations about its cybersecurity and data protection practices to receive funds for various government contracts and grants. So, Pannek sued ADM for violations of the False Claims Act, 31 U.S.C. §§ 3729 *et seq*.

ADM moves to dismiss under Rule 12(b)(6) and Rule 9(b), arguing that Pannek fails to plead any element of the alleged fraud with sufficient particularity. It further contends that it is not bound by many of the cybersecurity regulations and standards that Pannek cites.

The Court finds that Pannek has not demonstrated that any statements related to the company's cybersecurity practices were material to the government, and some of the alleged misstatements are not pled with sufficient particularity. Accordingly, the Court dismisses the Complaint without prejudice.

Background

ADM receives grants and contracts from the federal government related to food commodities and biofuel processing.[1] [27] ¶¶ 17, 94, 98, 100. According to the Complaint, certain federal grants and contracts include representations about ADM's

[1] When evaluating a motion to dismiss, the Court accepts as true all factual allegations in the Complaint. *Heredia v. Cap. Mgmt. Servs., L.P.*, 942 F.3d 811, 814 (7th Cir. 2019). The Court notes that the Complaint is sprawling, and so full of jargon and acronyms that it is difficult for the Court to identify the pertinent facts.

compliance with federal laws and regulations, including regulations concerning cybersecurity and data protection. *Id.* ¶ 86. Specifically, Pannek alleges that:

- ADM must register with the federal government's System for Award Management to receive any contracts and grants, which involves certifying that the company does not use banned telecommunications equipment, *id.* ¶¶87–88;
- The company received a Climate-Smart Commodities grant, which required it to comply with federal laws and regulations, and to take reasonable measures to safeguard sensitive information, *id.* ¶ 94;
- The government awarded multiple grants for ADM's Advanced Biofuel Program and for COVID relief, which the company may only receive if it adheres to applicable federal laws and regulations, *id.* at ¶¶ 98–100;
- The company accepted two grants from the Department of Energy which required it to maintain internal controls and a data management plan to protect sensitive information, *id.* ¶ 114; and
- ADM entered into over 250 contracts which included express and implied terms that instruct the company to protect sensitive information. *Id.* ¶¶ 102–105.

As Pannek contends, while receiving government funds from these grants and contracts, ADM had cybersecurity deficiencies that violated federal regulations. According to Pannek, ADM maintains vast amounts of sensitive information on a centralized data repository with no encryption. *Id.* ¶¶ 43–46. It also fails to limit who can access this protected data and to maintain access logs. ¶¶ 48, 55–62. Other defects in ADM's data management practices include sending unencrypted sensitive information to external systems, inadequately screening third-party service providers, and using banned telecommunications equipment. *Id.* ¶¶71–74, 79–81, 83. According to Pannek, the company learned of these data protection issues from 2019 audits and a 2022 investigation report. *Id.* ¶¶ 119–120, 123. Results from those reviews were shared with various ADM executives. *Id.*

These flawed cybersecurity practices supposedly violate federal regulations and standards, including regulations related to Controlled Unauthorized Information, 32 C.F.R. § 2002 *et seq.*, guidelines from the National Institute of Standards and Technology, Federal Acquisition Regulations, and other data safeguarding requirements. *Id.* ¶¶ 47, 56, 68–72, 76, 83–84. Since ADM's data security fell short of various federal regulations, Pannek contends that any statement that the company complied with all federal regulations or otherwise protected sensitive data was false. *Id.* ¶ 117.

Legal Standard

ADM moves to dismiss the Complaint under Rule 12(b)(6). In considering a Rule 12(b)(6) motion, the Court construes the Complaint in the light most favorable

to plaintiff, accepts well-pleaded facts as true, and draws all inferences in plaintiff's favor. *Bell v. City of Chicago*, 835 F.3d 736, 738 (7th Cir. 2016). To survive a motion to dismiss, plaintiff must set forth "sufficient factual matter, accepted as true, to 'state a claim to relief that is plausible on its face.'" *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009) (*quoting Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 570 (2007)). "A claim has facial plausibility when the plaintiff pleads factual content that allows the court to draw the reasonable inference that the defendant is liable for the misconduct alleged." *Adams v. City of Indianapolis*, 742 F.3d 720, 728 (7th Cir. 2014).

Because Pannek alleges a violation of the False Claims Act, the Complaint is also subject to the heightened pleading requirements of Rule 9(b). *Lanahan v. County of Cook*, 41 F.4th 854, 861 (7th Cir. 2022). Rule 9(b), in turn, requires plaintiffs to "state with particularity the circumstances constituting fraud or mistake." Fed. R. Civ. P. 9(b). To survive a motion to dismiss, the complaint must set forth the "who, what, when, where, and how" of the fraud. *United States v. Molina Healthcare of Illinois, Inc.*, 17 F.4th 732, 739 (7th Cir. 2021).

Discussion

Pannek only brings one claim under the False Claims Act based on multiple alleged false statements related to ADM's contracts and grants. Section 3729(a)(1)(B) of the False Claims Act prohibits "knowingly mak[ing], us[ing], or caus[ing] to be made or used, a false record or statement material to a false or fraudulent claim." [2] To state his claim, then, Pannek must allege with particularity that (1) ADM made a statement in order to receive money from the government; (2) the statement was false; and (3) ADM knew the statement was false. *United States ex rel. Enloe v. Heritage Operations Grp., LLC*, 2026 WL 2389722, at *3 (7th Cir. Aug. 17, 2026). In addition, Pannek must demonstrate the statement was material to the government's funding decision. *Lanahan*, 41 F.4th at 862. According to ADM, Pannek fails to plead any of the required elements.

I. Materiality

ADM contends that none of the alleged cybersecurity deficiencies or purported regulatory violations are material to the grants and contracts it receives from the government. The False Claims Act has a "strict materiality requirement." *Molina Healthcare*, 17 F.4th at 740. A false statement is material if it has "a natural tendency to influence, or be capable of influencing, the payment or receipt of money." 31 U.S.C. § 3729(b)(4). To establish materiality, Pannek's allegations must indicate "that the government actually attaches weight" to the cybersecurity requirements and that it

[2] Pannek does not specify which particular subsection of the False Claims Act forms the basis of his Complaint. The parties proceed as if Pannek is alleging a violation under 31 U.S.C. § 3729(a)(1)(B).

"relies on compliance" with those regulations. *Molina Healthcare*, 17 F.4th at 740. It is not enough to contend that the government could have declined to pay had it known about the defendant's noncompliance. *United States v. Sanford-Brown, Ltd.*, 840 F.3d 445, 447 (7th Cir. 2016). Rather, the Complaint must include facts to demonstrate that noncompliance would have "significantly affected the government's actions." *Molina Healthcare*, 17 F.4th at 743.

Pannek makes only broad allegations about the importance of cybersecurity to the agencies that administer ADM's contracts and grants. He generally points to internal policies and obligations at the U.S. Department of Agriculture and Department of Energy for protecting sensitive data. He also suggests that other False Claims Act settlements concerning cybersecurity shortcomings establish that such regulations are of material concern to the government. But none of these allegations relate to the government's specific decisions to fund ADM's contracts and grants. The government may care about cybersecurity generally, but Pannek has not plausibly alleged that the government attaches weight to ADM's data security practices. Pannek includes no facts to suggest that the government's payment decisions would have been significantly affected had it known about the company's purported cybersecurity deficiencies.

At best, Pannek alleges that adhering to certain cybersecurity regulations is a condition of payment for ADM's contracts and grants, and that constitutes grounds for the government to deny funding. But the Supreme Court specifically rejected that theory. "A misrepresentation cannot be deemed material merely because the Government designates compliance with a particular statutory, regulatory, or contractual requirement as a condition of payment." *Universal Health Servs., Inc. v. United States*, 579 U.S. 176, 194 (2016). Further, Pannek cannot establish materiality by merely pleading that the government could decline to fund ADM's contracts and grants. *Sanford-Brown, Ltd.*, 840 F.3d at 447. Instead, Pannek must include allegations that the government relied on the company's cybersecurity practices in some way in making its payment decisions.

Pannek has failed to do so here. He rests on unspecific statements about data security practices generally and makes a conclusory claim that the government would have changed its funding decision had it known about the company's cybersecurity deficiencies. That is insufficient to support his False Claims Act claim under the heightened pleading requirements of Rule 9(b). *See United States v. Joel Kennedy Constructing Corp.*, 584 F. Supp. 3d 595, 618–20 (N.D. Ill. 2022) (finding materiality allegations insufficient where plaintiffs only alleged the city could exact penalties for non-compliance with its residency and local business preference ordinances and that those ordinances generally served important goals for the city); *United States ex rel. Nedza v. Am. Imaging Mgmt., Inc.*, 2019 WL 1426013, at *7–8 (N.D. Ill. Mar. 29, 2019) (merely asserting that defendants must comply with all requirements and conditions of the Medicare Advantage program is inadequate to allege that a

noncompliant review process is material to the government's Medicare payments). Accordingly, the Court grants ADM's motion to dismiss.

II. Alleged Statements

Although the Complaint can be dismissed on materiality alone, the Court addresses ADM's remaining arguments in the event that Pannek repleads the allegations in an amended complaint.

ADM maintains that Pannek fails to plead any false statement with sufficient particularity. Recall that actions under the False Claims Act must comply with the heightened pleading requirements of Rule 9(b) and identify details of the fraud with particularity. *Lanahan*, 41 F.4th at 861–62. The Seventh Circuit has cautioned that courts "should not take an overly rigid view of the formulation." *Molina Healthcare*, 17 F.4th at 739. However, Pannek's allegations must be precise and substantiated. *Id.* For a violation of the False Claims Act, it is essential to plead a false statement, though such a statement may be inferred through enough particularized allegations. *United States ex rel. Mamalakis v. Anesthetix Mgmt. LLC*, 20 F.4th 295, 301 (7th Cir. 2021).

To support his False Claims Act allegation, Pannek asserts multiple supposedly false statements related to ADM's contracts and grants. The allegations about three of these statements portray the purported fraud in sufficient detail. For example, regarding the Climate Smart Commodities grant, Pannek pleads who signed the grant, when it was signed, and the amount awarded. He also alleges that the grant terms included conditions that required ADM to take various cybersecurity precautions. By applying for and accepting the grant, ADM affirmed its compliance with those requirements. Pannek similarly provides details about ADM's registration through the System for Award Management, alleging that the company stated it did not use banned telecommunications devices. And the company's Department of Energy grants allegedly required ADM to agree to take certain cybersecurity measures and submit a data management plan for sensitive information. By accepting these grants, ADM made false representations about its cybersecurity compliance. For these statements, Pannek provides sufficient details about the false statements ADM supposedly made to receive the grant awards.

By contrast, Pannek's other statements lack this requisite particularity. Pannek makes conclusory allegations that the Advanced Biofuel and COVID grants somehow equate to ADM's representation that it complied with all applicable federal laws and regulations. Pannek provides details about these grants, including the dates of awards and, for some, the amounts. But that is not enough to surmise that ADM made an affirmative false statement connected to the grants.

Pannek's allegations about ADM's contracts also suffer from pleading deficiencies. Pannek includes a long list of ADM's government contracts as an exhibit

to the Complaint, which lists the dates, amounts, and identification numbers for each contract. According to the Complaint, contracts after February 13, 2025, expressly incorporated certain cybersecurity requirements. For these contracts, the Court can plausibly infer that the terms themselves formed ADM's allegedly false statements. But Pannek fails to allege a similarly definite statement for the contracts that precede February 2025. Instead, Pannek supposes that these contracts include implied terms, and that ADM's failure to comply with these implied terms constitutes a misstatement. But again, these allegations are insufficient to demonstrate what statement ADM allegedly made.

To the extent Pannek contends the company implicitly certified its regulatory compliance, rather than making an express false statement in these contracts and grants, his allegations still fall short. Under an implicit certification theory, a defendant's representations about its goods or services may amount to a misleading half-truth if it omits other, material information about its noncompliance with regulatory requirements. *Universal Health Servs.*, 579 U.S. at 190. The omission renders the affirmative representation misleading and thus constitutes a false statement. *Id.* at 181. But to leverage this theory, Pannek must still plead that ADM made some specific representation to the government about the goods provided. *Id.* at 190. He must identify what affirmative statement the company made, and again allege the materiality of any omission about its cybersecurity deficiencies. For the Advanced Biofuel and COVID grants, and the majority of the contracts, Pannek has failed to do so.

Pannek's vague allegations resemble the claim in *United States ex rel. Berkowitz v. Automation Aids, Inc.*, 896 F.3d 834 (7th Cir. 2018). In that case, the relator alleged the defendant supply companies sold products to the government that failed to comply with specific regulations as required by their contracts. *Id.* at 838. To support his claim, relator submitted lists of defendants' non-compliant product sales. *Id.* at 839. But the Seventh Circuit found that relator could not establish a False Claims Act violation by merely alleging that these sales took place and that defendants failed to comply with a specific regulation. *Id.* at 841–42. Among other things, the relator failed to plead what information was on the sales orders submitted to the government, meaning he failed to identify a supposedly false statement. *Id.* at 841. Relator only alleged that defendants sold non-compliant products in violation of the regulations, which did not amount to a knowing false statement under the False Claims Act. *Id.* at 841–42.

Pannek's Complaint suffers from defects similar to those identified in *Berkowitz* because he has not tied the alleged regulatory violations to a false statement from the company. Like that relator, Pannek pleads that ADM failed to comply with certain regulations while it received government funds. But the Complaint lacks facts demonstrating that the company made a knowing false statement in connection with these grants and contracts. Violating a federal regulation does not, by itself, equate to making a false statement. *United States ex*

rel. Grenadyor v. Ukrainian Vill. Pharmacy, Inc., 772 F.3d 1102, 1107 (7th Cir. 2014). Without more particularized allegations, these allegations are insufficient to state a claim under the False Claims Act.

III. Falsity and Scienter

ADM further argues that Pannek's Complaint fails on falsity and scienter. As discussed above, to state a claim under the False Claims Act, Pannek must allege that the purported statements were false, and that the company knew they were false. *Mamalakis*, 20 F.4th at 300. These two elements are interrelated, but Pannek must still plead both elements. *United States ex. rel. Streck v. Eli Lilly & Co.*, 152 F.4th 816, 839 (7th Cir. 2025).

A statement about defendant's regulatory compliance is false if it is not in accordance with the truth. *Id*. at 840. As discussed above, Pannek fails to articulate exactly what statements ADM made to support some of his allegations. However, if ADM did allegedly make statements about its compliance with cybersecurity regulations, Pannek pleads a variety of deficiencies at the company that would render such statements false. For example, Pannek alleges that hundreds of individuals have access to sensitive information in ADM's data storage system, in violation of National Institute of Standards and Technology requirements. He further pleads that the company violates these standards because it fails to maintain adequate records of access to that sensitive information. Though ADM contends that its cybersecurity practices are reasonable and that it adequately protected sensitive information, meaning it did not violate any regulations, its argument is premature. Whether any alleged statements were actually false or fraudulent can only be determined with the benefit of discovery. *See United States ex rel. Roberts v. Lutheran Hosp.*, 1998 WL 1753335, at *12 (N.D. Ind. Apr. 17, 1998).

Turning to scienter, a defendant "knowingly" makes a false statement in violation of the False Claims Act if it acts with actual knowledge, deliberate ignorance, or reckless disregard for the truth or falsity of the statement. *Streck*, 152 F.4th at 842. Reckless disregard is the broadest of these mental states. *United States v. King-Vassel*, 728 F.3d 707, 712 (7th Cir. 2013). A defendant acts with reckless disregard if it "had reason to know of facts that would lead a reasonable person to realize that it was causing the submission of a false claim, or failed to make a reasonable and prudent inquiry into that possibility." *Streck*, 152 F.4th at 842. (citation omitted). But a defendant's innocent mistakes or negligence do not give rise to a violation of the False Claims Act. *King-Vassel*, 728 F.3d at 712.

In the Complaint, Pannek alleges that ADM broadly knew about the purported cybersecurity deficiencies because internal investigations revealed data protection issues. He points to a 2019 formal cybersecurity audit and 2022 report that identified concerns with the company's data storage and controls. Pannek contends that these findings were shared with executive leadership, making the problems well known.

The timing of these reports undermines scienter for some of Pannek's claims because he alleges false statements that predate the investigations. It is implausible that ADM made a knowing false statement about its cybersecurity practices before the reviews exposed any problems. But for later purported statements, Pannek has sufficiently alleged that the company knew its data protection practices were defective. The Court can reasonably infer that ADM had this information while making alleged statements about its compliance with cybersecurity regulations. Thus, it is at least plausible that the company acted with the requisite scienter.

IV. Cybersecurity Regulations

Finally, ADM contends that some of the cybersecurity regulations raised are irrelevant to the company's grants and contracts. Specifically, ADM argues that Controlled Unclassified Information regulations, 32 C.F.R. § 2002 *et seq.*, National Institute of Standards and Technology guideline SP 800-171, and Federal Acquisition Regulation § 52.204-21 cannot form the basis of any alleged false statement because they do not apply to the company at all. It submits that because these specific regulations are irrelevant, Pannek's theories related to these regulations should be dismissed with prejudice. There is no doubt that at the motion to dismiss stage, the Court must accept well-pled facts as true. *Carlson v. CSX Transp., Inc.*, 758 F.3d 819, 826 (7th Cir. 2014). Thus, Pannek need only plead that these regulations plausibly apply to the company's contracts and grants at this early stage of the litigation.

Pannek alleges ADM maintains Controlled Unclassified Information on its systems for the government. Controlled Unclassified Information is "information the Government creates or possesses, or that an entity creates or possesses for or on behalf of the Government[.]" 32 C.F.R. § 2002.4(h). The regulations apply indirectly to non-executive branch entities through incorporation into contracts, grants, and other agreements that set out specific requirements for handling Controlled Unclassified Information. 32 C.F.R. §§ 2002.1(f), 2002.4(c). According to the Complaint, the government requires that ADM maintain complete records about anyone who produces the food commodities in its grants and contracts. These records include sensitive information about the producers such as names, Social Security numbers, addresses, and pricing information. Pannek contends that the company must make this information available to the government, including by submitting reports. Further, Pannek alleges that National Institute of Standards and Technology guideline SP 800-171 is a mandatory requirement for handling Controlled Unclassified Information.

As for Federal Acquisition Regulation § 52.204-21, this provision applies to "federal contract information," which is information "generated for the Government under a contract to develop or deliver a product or service to the Government." 48 C.F.R. § 52.204-21(a). Pannek alleges that the same information that constitutes Controlled Unclassified Information is also federal contract information because ADM must maintain specific records related to its contracts and make them available

to the government. Further, Pannek alleges that this regulation is a term in the company's contracts after 2025.

At this early phase of the case, the specific contract and grant terms are not before the Court. But, accepting these allegations as true, the Court can plausibly infer that the Controlled Unclassified Information requirements are incorporated into ADM's agreements with the government. Pannek has alleged that the company maintains such data, leading to the inference that the Controlled Unclassified Information regulations apply. And Pannek has alleged that the Federal Acquisition Regulation requirements are express terms of some of the company's contracts. Though the company disputes that it maintains any Controlled Unclassified Information or federal contract information on its systems, Pannek has plausibly alleged that it does. Taking these allegations as true, the regulations related to Controlled Unclassified Information, 32 C.F.R. § 2002 *et seq*., National Institute of Standards and Technology requirement SP 800-171, and Federal Acquisition Regulation § 52.204-21 plausibly apply to the company's contracts and grants. Because ADM's agreements may be subject to these cybersecurity requirements, an alleged False Claims Act violation based on such regulations would not be futile.

Conclusion

For the reasons stated above, ADM's motion to dismiss [44] is granted. Pannek fails to allege that the purported cybersecurity regulation violations were material to the government's decision to fund ADM's grants or contracts, so the Court dismisses the Complaint. Further, many of Pannek's alleged misstatements are not pled with sufficient particularity to survive scrutiny under Rule 9(b). However, Pannek plausibly alleges that the cybersecurity regulations at issue apply to ADM. Therefore, the dismissal is without prejudice. Pannek may refile an amended complaint if he can cure the deficiencies and such an amendment is consistent with his obligations under Federal Rule of Civil Procedure 11. *Runnion ex rel. Runnion v. Girl Scouts of Greater Chicago & Nw. Indiana*, 786 F.3d 510, 519–20 (7th Cir. 2015) ("Unless it is certain from the face of the complaint that any amendment would be futile or otherwise unwarranted, the district court should grant leave to amend after granting a motion to dismiss."). If Pannek does not file an amended complaint by September 23, 2026, then the dismissal will automatically convert to a dismissal with prejudice.

SO ORDERED.

Dated: September 2, 2026

Sunil R. Harjani
United States District Judge