The Department of Justice's Civil Cyber-Fraud Initiative and Its Impact on the False Claims Act

---

By: Kim Bessiere Martin and Peter J. Pizzi

Kim Martin is a partner in the Huntsville, Alabama office of Bradley Arant Boult Cummings LLP. She focuses her practice on general litigation with significant experience in investigating and defending False Claims Act litigation, as well as defense of pharmaceutical manufacturers in personal injury claims. She has tried cases in state and federal court including trials alleging violations of the False Claims Act. Nationally ranked in Chambers USA *for Product Liability and Mass Torts, Kim is listed as one of the "Top 250 Women in Litigation" by* Benchmark Litigation *and as a "Life Sciences Star" by* LMG Life Sciences*.*

Peter J. Pizzi is a partner at Walsh Pizzi O'Reilly Falanga LLP, a majority women-owned firm with offices in Newark, Philadelphia, and Manhattan. A business litigator with over 40 years of experience in commercial litigation, class action defense, internal investigations, technology litigation and employee mobility law, Peter holds the CIPP/US certification and is a Certified Civil Trial Attorney, a designation of the Supreme Court of New Jersey. Peter represents corporate clients in a broad array of industries, including healthcare, food distribution, pharma, financial services, and information technology. Peter received the IADC's Yancey Award in 2022 and is past Chair of the IADC Cyber Security, Data Privacy and Technology Committee. Currently, Peter serves as a Vice Chair of IADC Corporate Compliance and Government Investigations Committee and its Amicus Committee. He is also Co-Chair of the NYSBA's Privacy, Data Security, and Information Technology Litigation Committee of the NYSBA Commercial & Federal Litigation Section.

On October 6, 2021, The Department of Justice ("DOJ") announced the launch of the Civil Cyber-Fraud Initiative (the "CCFI"), which is designed to combat emerging cyber threats to the security of sensitive information through the use of civil fraud enforcement tools. This initiative proposes to use civil enforcement tools to pursue government contractors who receive federal funds in the event that those contractors fail to meet required cybersecurity standards. The DOJ developed the CCFI as a result of its review of cyber threats with a focus on developing recommendations to combat those threats. At the time of its announcement, Deputy Attorney General Lisa O. Monaco stated that the use of civil enforcement tools was intended to "ensure that taxpayer dollars are used appropriately," as well as to combat the "mistaken belief that it is less risky to hide a breach than to bring it forward and to report it. . . ."[1]

The Initiative relies on the False Claims Act ("FCA")[2] to pursue cybersecurity-related fraud by government contractors, grant recipients, and other entities which rely upon federal funding. The FCA, addressed in more detail below, is the main vehicle by which the government addresses false claims for federal funds. In its launch of the CCFI, the DOJ highlighted the FCA's whistleblower provisions, which allow for a private party who successfully brings forward instances of fraudulent conduct to share in any recovery by the government. The DOJ anticipates that the Initiative will "hold accountable entities or individuals that put U.S. information or systems at risk by knowingly providing deficient cybersecurity products or services, knowingly mis-representing their cybersecurity practices or protocols, or knowingly violating obligations to monitor and report cybersecurity incidents and breaches." The DOJ's use of the FCA as a part of its initiative to combat cyber-threats adds another layer of complexity to an already challenging landscape for companies navigating cybersecurity issues. This article provides an overview of the FCA

[1] Press Release, Department of Justice, Deputy Attorney General Lisa O. Monaco Announces New Civil Cyber-Fraud Initiative, (October 6, 2021), https://www.justice.gov/opa/pr/deputy-attorney-general-lisa-o-monaco-announces-new-civil-cyber-fraud-initiative.

[2] 31 U.S.C. § 3729 *et seq*.

and discusses recent use in the context of cybersecurity issues.

I. The False Claims Act

The FCA imposes treble damages and a civil penalty from $12,537 to $25,076 per claim[3] on anyone who *knowingly* submits or causes the submission of a false or fraudulent claim payable by the United States government or related entities.[4] In particular, the government has a civil cause of action against any person or entity who:

> knowingly presents, or causes to be presented, a false or fraudulent claim for payment or approval;[5]
>
> knowingly makes, uses, or causes to be made or used, a false record or statement material to a false or fraudulent claim;[6]
>
> has possession, custody, or control of property or money used, or to be used, by the Government and knowingly delivers, or causes to be delivered, less than all of that money or property;[7]
>
> knowingly makes, uses, or causes to be made or used, a false record or statement material to an obligation to pay or transmit money or property to the Government, or knowingly conceals or knowingly and improperly avoids or decreases an obligation to pay or transmit money or property to the Government[;][8] or
>
> conspires to commit [one of these violations].[9]

Claims for violation of the FCA can be brought by the government or as *qui tam* actions on the government's behalf by a private individual, known as a relator.[10] Suits brought by relators are often called "whistleblower" suits, and provisions applying to whistleblowers will be discussed in more detail below.

A. Elements

To state a claim under the FCA, the government generally must make at least four showings by a

[3] The amount of civil monetary penalties is adjusted annually for inflation and was last adjusted on May 9, 2022.
[4] 31 U.S.C. § 3729(a)(1).
[5] *Id*. at § 3729(a)(1)(A).
[6] *Id*. at § 3729(a)(1)(B).
[7] *Id*. at § 3729(a)(1)(D).
[8] *Id*. at § 3729(a)(1)(G).
[9] *Id*. at § 3729(a)(1)(C).
[10] 31 U.S.C. § 3730(b).

preponderance of the evidence.[11] First, the government must establish the existence of a claim actionable under the FCA. Second, the government must establish that the claim was false, either factually or legally. Third, the government must demonstrate that the falsity was material to the payment of the claim. Finally, the government must establish that the defendant acted with knowledge of the falsity. The following sections provide a brief overview of each requirement for FCA liability.

i. Claim

The submission of a claim is "the *sine qua non* of a False Claims Act violation."[12] The FCA broadly defines "claim" as "any request or demand . . . for money or property whether or not the United States has title to the money or property" either (a) "presented to an officer, employee or agent of the United States" or (b) "made to a contractor, grantee or other recipient, if the money or property is to be spent or used on the Government's behalf or to advance a Government program or interest" and the government has provided or will reimburse for any portion of the money or property requested.[13] Entities that routinely receive payment through government programs or contracts—namely government contractors, health care suppliers and providers and financial services companies—are the most likely to find themselves targets of an FCA claim or investigation.

ii. Falsity

To establish a violation of the FCA, the government must show the existence of a "false or fraudulent claim."[14] A claim may be considered false under the FCA if it is factually or legally false.[15] The **factually false claim** is one "in which a contractor or other claimant submits information that is untrue on its face."[16] A factually false claim generally involves "an incorrect description of goods or services provided or a request for

[11] 31 U.S.C. § 3731(d).
[12] United States *ex rel*. Clausen v. Lab. Corp. of Am., 290 F.3d 1301, 1311 (11th Cir. 2002).
[13] 31 U.S.C. § 3729(b)(2).
[14] 31 U.S.C. § 3729(a)(1).
[15] *See* United States *ex rel.* Wilkins v. United Health Group, Inc., 659 F.3d 295, 305 (3d Cir. 2011) *overruled on other grounds* as recognized by United States *ex rel.* Freedom Unlimited, Inc. v. City of Pittsburgh, 728 F. App'x 101 (3d Cir. 2018).
[16] United States v. Kellogg Brown & Root Servs., Inc., 800 F. Supp.2d 143, 154 (D. D.C. 2011) (citing United States v. Sci. Applications Int'l Corp., 626 F.3d 1257, 1266 (D.C. Cir. 2010)).

reimbursement for goods or services never provided."[17]

In contrast, a **legally false claim** or certification is one that is "predicated upon a false representation of compliance with a federal statute or regulation or a prescribed contractual term."[18] Courts further divide legally false claims into those claims made legally false by an "express certification" and those claims made legally false by an "implied certification."[19] In an *express* false certification claim, the claim "falsely certifies compliance with a particular statute, regulation or contractual term, where compliance is a prerequisite to payment."[20] False certification claims based on broad and vague certifications of compliance with law may be found insufficient to give rise to FCA liability.[21]

An *implied* false certification claim "is based on the notion that the act of submitting a claim for reimbursement itself implies compliance with governing federal rules that are a precondition to payment."[22] The United States Supreme Court clarified this theory of FCA liability in 2016 in *Universal Health Services v. United States ex rel. Escobar*.[23] In *Escobar*, the Court held that the "implied certification theory can, at least in some circumstances, provide a basis for liability . . ." and did not require that the government "expressly designated" compliance as a condition for payment.[24] The circumstances under which this theory may apply, however, were limited by the Court to circumstances where two conditions are satisfied.[25] First, a claim must make specific representations about a good or service (as opposed to merely requesting payment). Second, the defendant's failure to disclose noncompliance with the material statutory, regulatory or contractual requirements makes those specific representations "misleading half-truths."[26]

---

[17] *Sci. Applications Int'l Corp.*, 626 F.3d at 1266 (quoting Mikes v. Straus, 274 F.3d 687, 697 (2d Cir. 2001)).
[18] *Mikes*, 274 F.3d at 696-697.
[19] *Id.* at 697-700.
[20] *Id.* at 698.
[21] *See, e.g.*, United States *ex rel.* Conner v. Salina Reg'l Health Ctr., 543 F.3d 1211, 1218–1223 (10th Cir. 2008) (holding that annual certification of compliance with "laws and regulations regarding the provision of health care services" was too general to impose liability); *but see* United States *ex rel.* Phalp v. Lincare Holdings, Inc., 857 F.3d 1148 (11th Cir. 2017) (holding that "[s]cienter is not determined by the ambiguity of a regulation, and can exist even if a defendant's interpretation is reasonable.").
[22] *Mikes*, 274 F.3d at 699.
[23] Universal Health Services, Inc. v. United States ex rel. Escobar, 579 U.S. __, 136 S. Ct. 1989 (2016).
[24] *Id.* at 2001.
[25] *Id.*
[26] *Id.*

iii. Materiality

The FCA also requires that false statements be "material" to a false claim. Since the 2009 amendments, materiality has been defined as "having a natural tendency to influence, or be capable of influencing, the payment or receipt of money or property."[27] The Supreme Court also addressed the materiality requirement of the FCA in *Escobar* by defining it as "demanding."[28] The Court stated that the materiality standard turns on the "likely or actual behavior of the recipient of the alleged misrepresentation."[29] It is not enough for the government or relators to show that "[g]overnment would be entitled to refuse payment were it aware of the violation."[30] The Court did not find that an express designation as a condition of payment was required to state a claim but found this to be relevant to the materiality inquiry.[31] The government's past practices in paying such claims are relevant to the determination.[32]

While the government and relators may argue that the "materiality" analysis was unaffected by the *Escobar* decision, many post-*Escobar* decisions have applied a heightened materiality standard. This heightened scrutiny is resulting in courts requiring more facts supporting materiality to be pled and a closer examination of the government's actions.[33]

---

[27] 31 U.S.C. § 3729(b)(4). Prior to the Fraud Enforcement Recovery Act of 2009, sometimes referred to as the "FERA amendments," the statute did not include a materiality requirement at all, but every circuit court to decide the issue had determined materiality to be an element of the FCA. *See* Harrison v. Westinghouse Savannah River Co., 176 F.3d 776, 785, 788 (4th Cir. 1999); United States *ex rel.* Marcy v. Rowan Co., 520 F.3d 384, 389 (5th Cir. 2008); United States *ex rel.* A+ Homecare, Inc. v. Medshares Mgmt. Grp., Inc., 400 F.3d 428, 442 (6th Cir. 2005); Luckey v. Baxter Healthcare Corp., 183 F.3d 730, 732 (7th Cir. 1999); United States *ex rel.* Costner v. URS Consultants, Inc., 317 F.3d 883, 886-887 (8th Cir. 2003); United States *ex rel.* Hendow v. Univ. of Phx., 461 F.3d 1166, 1172-1173 (9th Cir. 2006); *Conner,* 543 F.3d at 1219 n.6 (10th Cir. 2008); United States v. TDC Mgmt. Corp., 24 F.3d 292, 298 (D.C. Cir. 1994). *Cf. Mikes,* 274 F.3d at 697 (2d Cir. 2001) (declining to address whether the FCA contains a materiality requirement).

[28] *Escobar*, 136 S.Ct. at 2003.

[29] *Id.* at 2002.

[30] *Id.*

[31] *Id.*

[32] *Id.*

[33] *See, e.g.,* Abbott v. BP Exploration & Production, Inc., 851 F.3d 384 (5th Cir. 2017) (finding that the Interior Department's decision to allow Atlantis to continue drilling after its substantial investigation into relator's allegations was strong evidence that engineer approval at various stages of construction was not material); United States *ex rel.* McBride v. Halliburton Co., 848 F.3d 1027 (D.C. Cir. 2017) (finding DCAA's award of a fee for exceptional performance to KBR after investigating relator's allegations was "very strong evidence" that allegedly inflated headcounts were not material); United States *ex rel.* Kolchinsky v. Moody's Corp., 238 F. Supp.3d 550 (S.D.N.Y. 2017)

Since this decision, appeals of adverse verdicts based on *Escobar* materiality grounds have had success. For example, the Fifth Circuit reversed a $663 million jury verdict in a suit alleging that the defendant had submitted false claims to the government by not disclosing changes to highway guardrails.[34] In reaching this result, the court concluded that "continued payment by the federal government after it learn[ed] of the alleged fraud substantially increase[ed] the burden on the relator in establishing materiality."[35] The *Escobar* materiality requirement is also being raised at the pleading stage under Rule 9(b), with some courts requiring additional facts to be pled on the materiality element or dismissing complaints.[36]

(dismissing allegations of false claims based on inaccurate credit ratings where, despite awareness of the alleged fraud, government continued to pay Moody's for its credit-ratings products each year).

[34] United States*. ex rel.* Harman v. Trinity Indus. Inc., 872 F.3d 645, 663 (5th Cir. 2017).

[35] *Id.*

[36] *Escobar,* 136 S. Ct. 1989, 2004 n.6 (2016). *See, e.g.,* Carlson v. DynCorp Int'l, LLC, 657 F. App'x 168 (4th Cir. 2016) (relator could not show alleged violations of accounting regulations or best practices was material); United States *ex rel.* Scharff v. Camelot Counseling, No. 13-CV-3791, 2016 WL 5416494 at *8 (S.D.N.Y. Sept. 28, 2016) (finding that the plaintiff had failed to allege facts sufficient to meet the demanding materiality requirement where the complaint did not "explain why the purportedly fraudulent conduct was material to the payment of reimbursements."); United States *ex rel.* Schimelpfenig v. Dr. Reddy's Labs. Ltd., No. CV 11-4607, 2017 WL 1133956, at *7 (E.D. Pa. Mar. 27, 2017) (dismissing FCA complaint for failure to allege materiality); United States *ex rel.* SE Carpenters Reg. Council v. Fulton County, Ga., No. 1:14-CV-4071-WSD, 2016 WL 4158392, at *8 (N.D. Ga. Aug. 5, 2016) (dismissing false certification claims for failing to "show[] that Defendants misrepresented matters 'so central' . . . that the government 'would not have paid [Defendants'] claims had it known of these violations.'"); United States *ex. rel.* Dresser v. Qualium Corp., No. 5:12-CV-01745-BLF, 2016 WL 3880763, at *6 (N.D. Cal. July 18, 2016) (dismissing false certification claim because the complaint "d[id] not explain why" false certifications were material, and granting leave to amend

iv. Knowledge

To establish a FCA violation, the government must show that the defendant acted "knowingly." To act "knowingly," the individual may, but need not, have actual knowledge of the claim's falsity or have a specific intent to defraud the government.[37] Rather, the individual need only "act[] in deliberate ignorance"[38] or "in reckless disregard of the truth or falsity of the information."[39] The statute expressly provides that the government is not required to prove that a defendant specifically intended to defraud.[40] While Federal Rule of Civil Procedure 9(b) allows knowledge to be alleged "generally," relators must still plead facts under Rule 8 to support a plausible inference that the Defendants knowingly submitted a false claim.[41] General and conclusory allegations that a defendant "knowingly" submitted false claims, without supporting facts, do not suffice under Rule 8.[42]

Reckless disregard under the FCA is "an extension of gross negligence or an extreme version of ordinary negligence."[43] As the Supreme Court explained in an analogous context, to show recklessness the government must show that the party's conduct entailed "an unjustifiably high risk of harm that [was] either known or so obvious that it should [have] be[en] known."[44] The Supreme Court has before it in the 2022-2023 Term a case which involves the application of the reckless disregard standard, which lower courts have said could suffice for FCA liability.[45] The law on this precise point could change in the coming months.

Determining whether conduct raises an "unjustifiably high risk" of violating the law depends on a variety of factors. Relevant factors cited by various courts include:

- the personal knowledge of the defendants and their familiarity with

because the complaint was filed pre-*Escobar*).

[37] 31 U.S.C. § 3729(b)(1)(B).

[38] 31 U.S.C. § 3729(b)(1)(A)(ii).

[39] 31 U.S.C. § 3729(b)(1)(A)(iii).

[40] 31 U.S.C. § 3729(b)(1)(B).

[41] *See* United States *ex rel.* Barrett v. Beauty Basics, Inc., No. 2:13-1989, 2015 WL 3650960, at *5 (N.D. Ala. Jun. 11, 2015).

[42] *See* Estate of Helmly v. Bethany Hospice and Palliative Care of Coastal Georgia, LLC, 853 Fed. App'x. 496 (11th Cir. 2021), cert. denied, 143 S.Ct. 351 (2022); United States *ex rel.* Complin v. N.C. Baptist Hosp., 818 Fed. App'x 179, 183 (4th Cir. 2020).

[43] Urquilla-Diaz v. Kaplan University, 780 F.3d 1039, 1058 (11th Cir. 2015).

[44] Safeco Ins. Co. of Am. v. Burr, 551 U.S. 47, 68 (2007) (citing Farmer v. Brennan, 511 U.S. 825, 836 (1994)).

[45] United States *ex rel.* Schutte v. Supervalu Inc., 9 F.4th 455 (7th Cir. 2021), *cert. granted*, 2023 WL 178398 (Jan. 13, 2023).

governing legal rules and obligations;[46]

- the clarity of existing statutory, regulatory, and contractual guidance addressing the conduct at issue;[47]
- the defendant's justifiable reliance on experts, attorneys, or other entities in making the challenged statements;[48]
- the defendant's compliance with industry practice in taking the challenged actions;[49] and
- the government's knowledge of or acquiescence towards the challenged conduct.[50]

b. Whistleblower Provisions

A private individual, known as a relator, may bring a *qui tam* action and enforce the FCA on the government's behalf.[51] The relator may be anyone with knowledge of the allegations—such as a current or former employee, a competitor, a customer, or a consultant. When

[46] United States *ex rel.* Yannacopoulos v. Gen. Dynamics, 652 F.3d 818, 833–834 (7th Cir. 2011); United States *ex rel*. Burlbaw v. Orenduff, 548 F.3d 931, 950–951 (10th Cir. 2008); United States *ex rel.* Augustine v. Century Health Servs., Inc., 289 F.3d 409, 416 (6th Cir. 2002).

[47] *Safeco*, 551 U.S. at 69; *Burlbaw*, 548 F.3d at 957–958; United States *ex rel.* K & R Ltd. P'ship v. Mass. Housing, 530 F.3d 980, 983 (D. D.C. 2008).

[48] United States *ex rel.* Folliard v. Govplace, 930 F. Supp.2d 123, 130-137 (D. D.C. 2013).

[49] United States *ex rel.* Williams v. Renal Care Group, 696 F.3d 518, 531 (6th Cir. 2012).

[50] United States *ex rel.* Durcholz v. FKW Inc., 189 F.3d 542, 544–555 (7th Cir. 1999).

[51] 31 U.S.C. § 3730(b).

brought by a relator, a complaint is filed under seal and remains unserved on the defendant until the presiding federal court orders otherwise.[52] While the complaint is under seal, the government may investigate the relator's claims and decide whether it will elect to intervene and take responsibility for prosecuting the action or decline to intervene, leaving the relator to litigate his or her complaint.[53] The FCA incentivizes private relators to bring claims by providing them with a share of any proceeds of the action or settlement—15% to 25% if the government intervenes and 25% to 30% if the government does not intervene.[54]

The government may settle an action brought by a relator, notwithstanding any objection by the relator, "if the court determines, after a hearing, that the proposed settlement is fair, adequate, and reasonable under all the circumstances."[55] The Supreme Court has before it in the 2022-2023 Term the issue whether the government can move to dismiss a FCA action in which it has not intervened and the procedural steps in order for the government to do so.[56] The law on this precise point also could change in the coming months.

II. Application of the FCA to Cybersecurity Issues

Since the start of the CCFI, there have been two reported FCA cyber-fraud settlements. The first occurred in March 2022 and involved the resolution of two whistleblower actions pending in the Eastern District of New York against Comprehensive Health Services LLC ("CHS").[57] CHS is contracted to provide medical support services at government-run facilities in Iraq and Afghanistan. The government asserted that, under one of the contracts, CHS submitted claims to the State Department for the cost of a secure electronic medical record (EMR) system to store all patients' medical records. The DOJ alleged that, between 2012 and 2019, CHS billed the State Department $485,866 for storing medical records in a secure system, even though some of the medical records were saved on an internal network drive that was accessible to non-clinical staff. This was asserted to be a direct violation of government contractual requirements. The DOJ

[52] 31 U.S.C. § 3730(b)(2).
[53] 31 U.S.C. § 3730(b)(4).
[54] 31 U.S.C. § 3730(d).
[55] 31 U.S.C. § 3730(c)(2)(B).
[56] Polansky v. Executive Health Resources Inc, 17 F.4th 376 (3rd Cir. 2021), *cert. granted* 142 S.Ct. 2834 (2022).
[57] United States *ex rel.* Lawler v. CHS Middle East, LLC, No. 20-CV-698, Eastern District of New York, Settlement Agreement, Doc. 26-1.

alleged that CHS did not take adequate steps to store information exclusively on the EMR system, even after concerns were raised about the privacy of protected information. CHS resolved claims relating to these allegations, and allegations that it falsely represented certain medical supplies as being approved by the FDA or EMA, for $930,000.[58]

On July 8, 2022, the DOJ reported another settlement involving alleged cybersecurity violations by defense contractor Aerojet Rocketdyne Holdings and Aerojet Rocketdyne Inc. (collectively "Aerojet"), who allegedly failed to comply with requirements in certain federal government contracts.[59] The case was watched closely by practitioners in this area. The claim was originally filed by former Aerojet employee Brian Markus – the former senior director of Cybersecurity, Compliance & Controls. Markus alleged that Aerojet knew its cybersecurity programs fell short of Department of Defense and NASA acquisition regulations, which were part of contracts between Aerojet and the agencies.

Despite declining to intervene in the Aerojet case in June 2018, the government filed a statement of interest two weeks after it announced the Civil Cyber-Fraud Initiative, assailing Aerojet's arguments that it was entitled to summary judgement.[60] Notably, the government argued that Aerojet's contractual deficiencies were a source of damages even if Aerojet otherwise complied with the contracts because "the government did not just contract for rocket engines, but also contracted with [Aerojet] to store the government's technical data on a computer system that met certain cybersecurity requirements." The government also argued that assertions that the entire defense industry is not compliant with cybersecurity requirements has no bearing on whether such compliance is material to the

---

[58] Press Release, Department of Justice, Medical Services Contractor Pays $930,000 to Settle False Claims Act Allegations Relating to Medical Services Contracts at State Department and Air Force Facilities in Iraq and Afghanistan, (March 8, 2022), https://www.justice.gov/opa/pr/medical-services-contractor-pays-930000-settle-false-claims-act-allegations-relating-medical.

[59] Press Release, Department of Justice, Aerojet Rocketdyne Agrees to Pay $9 Million to Resolve False Claims Act Allegations of Cybersecurity Violations in Federal Government Contracts, (July 8, 2022), https://www.justice.gov/opa/pr/aerojet-rocketdyne-agrees-pay-9-million-resolve-false-claims-act-allegations-cybersecurity#:~:text=Aerojet%20Rocketdyne%20Inc.%2C%20headquartered%20in,the%20Justice%20Department%20announced%20today.

[60] United States *ex rel.* Markus v. Aerojet Rocketdyne Holdings, Inc., 15-CV-02245, Doc. 135.

government's payment decision in any particular case.

On February 1, 2022, the United States District Court for the Eastern District of California ruled that the case against Aerojet could proceed on triable issues of fact as to whether noncompliance with government cybersecurity requirements are material to the government's decisions to approve contracts. The federal court denied Aerojet's motion for summary judgment and issued the first major ruling in an FCA case testing the Department of Justice's new CCFI.

The court commented that the relevant regulations required government contractors to implement specific safeguards to protect unclassified technical information from cybersecurity threats. A key component of Aerojet's argument was that it had disclosed to the government areas in which it did not meet the cybersecurity requirements of the contract. While the court acknowledged that Aerojet may have disclosed its cybersecurity shortcomings to the government, the court questioned whether Aerojet failed to disclose key events and the results of audits showing gaps in Aerojet's cybersecurity. The court also expressed concern as to whether Aerojet knowingly misrepresented their intention to comply with the cybersecurity provisions of their contracts in the first place. These issues presented a question of fact for trial.

Following the ruling of the district court, the case proceeded to trial, which commenced on April 26, 2022. On the second day of trial, the parties reported that the matter had been settled. On July 8, 2022, the DOJ issued a press release detailing the terms of the settlement.[61]

III. Conclusion

The DOJ's CCFI highlights for companies the need to understand and comply with the cybersecurity requirements contained in federal contracts. The initiative is well-staffed and encourages whistleblowers to bring forward instances of violations. Companies should expect increased action by the DOJ with regard to alleged violations.

Federal contractors should implement processes for identifying the cybersecurity requirements in their contracts and assessing compliance with them. These processes should include collaboration and coordination between the IT, legal, and compliance functions. In some instances, third-party vendors maintain information that may be implicated by a company's cybersecurity obligations. The FCA exposure applies particularly in the healthcare field, where third-party

[61] *See* Press Release, *supra* note 59.

vendors often maintain protected healthcare information. A vendor management review conducted on a regular basis – at least annually – is an important tool to ensure that vendors are meeting cybersecurity obligations. To the extent that such a review identifies deficiencies either internally or with vendors, companies should develop a process for escalating and responding to these deficiencies. This process may include disclosure to the government.