AN A.S. PRATT PUBLICATION
SEPTEMBER 2022
VOL. 8 NO. 7

PRATT'S PRIVACY & CYBERSECURITY LAW REPORT

LexisNexis

Pratt's Privacy & Cybersecurity Law Report

VOLUME 8 **NUMBER 7** **September 2022**

LexisNexis®

QUESTIONS ABOUT THIS PUBLICATION?

For questions about the **Editorial Content** appearing in these volumes or reprint permission, please contact:
Alexandra Jefferies at ..... (937) 560-3067
Email: ..... alexandra.jefferies@lexisnexis.com
For assistance with replacement pages, shipments, billing or other customer service matters, please call:

Customer Services Department at ..... (800) 833-9844
Outside the United States and Canada, please call ..... (518) 487-3385
Fax Number ..... (800) 828-8341
Customer Service Web site ..... http://www.lexisnexis.com/custserv/
For information on other Matthew Bender publications, please call

Your account manager or ..... (800) 223-1940
Outside the United States and Canada, please call ..... (937) 247-0293

ISBN: 978-1-6328-3362-4 (print)
ISBN: 978-1-6328-3363-1 (eBook)

ISSN: 2380-4785 (Print)
ISSN: 2380-4823 (Online)

Cite this publication as:
[author name], [*article title*], [vol. no.] PRATT'S PRIVACY &CYBERSECURITY LAW REPORT [page number] (LexisNexis A.S. Pratt);
Laura Clark Fey and Jeff Johnson, *Shielding Personal Information in eDiscovery*, [1] PRATT'S PRIVACY & CYBERSECURITY LAW REPORT [82] (LexisNexis A.S. Pratt)

An A.S. Pratt Publication
Editorial

Editorial Offices
630 Central Ave., New Providence, NJ 07974 (908) 464-6800
201 Mission St., San Francisco, CA 94105-1831 (415) 908-3200
www.lexisnexis.com

MATTHEW BENDER

(2022–Pub. 4939)

Editor-in-Chief, Editor & Board of Editors

Pratt's Privacy & Cybersecurity Law Report is published nine times a year by Matthew Bender & Company, Inc. Periodicals Postage Paid at Washington, D.C., and at additional mailing offices. For customer support, please contact LexisNexis Matthew Bender, 1275 Broadway, Albany, NY 12204 or e-mail Customer.Support@lexisnexis.com. Direct any editorial inquires and send any material for publication to Steven A. Meyerowitz, Editor-in-Chief, Meyerowitz Communications Inc., 26910 Grand Central Parkway Suite 18R, Floral Park, New York 11005, smeyerowitz@meyerowitzcommunications.com, 631.291.5541. Material for publication is welcomed—articles, decisions, or other items of interest to lawyers and law firms, in-house counsel, government lawyers, senior business executives, and anyone interested in privacy and cybersecurity related issues and legal developments. This publication is designed to be accurate and authoritative, but neither the publisher nor the authors are rendering legal, accounting, or other professional services in this publication. If legal or other expert advice is desired, retain the services of an appropriate professional. The articles and columns reflect only the present considerations and views of the authors and do not necessarily reflect those of the firms or organizations with which they are affiliated, any of the former or present clients of the authors or their firms or organizations, or the editors or publisher.

POSTMASTER: Send address changes to *Pratt's Privacy & Cybersecurity Law Report*, LexisNexis Matthew Bender, 630 Central Ave., New Providence, NJ 07974.

Justice Department Lays Foundation for More Vigorous Enforcement of Contractor Cybersecurity Requirements Under the False Claims Act

By Alicia N. Washington, Taylor Sutton and Bryce Friedman*

In this article, the authors explain that, to minimize risk of liability under the False Claims Act, directors, management, and information technology personnel should monitor and ensure compliance with the cybersecurity obligations specified in the company's government contracts.

On October 6, 2021, Deputy Attorney General Lisa O. Monaco of the U.S. Department of Justice ("DOJ") announced the Civil Cyber-Fraud Initiative, a program aimed at redressing cybersecurity-related fraud by government contractors through increased enforcement under the False Claims Act ("FCA").[1] Light on details, the initiative promised a range of benefits, from ensuring a level playing field for contractors that comply with their cybersecurity obligations to improving overall cybersecurity practices.[2]

A mere 14 days later, the government, after it had previously declined to intervene, filed a statement of interest in *United States ex rel. Markus v. Aerojet Rocketdyne Holdings, Inc*,[3] a rare cybersecurity-related FCA case.

Coming on the heels of Monaco's announcement, the government's statement of interest shed light on the new initiative's likely priorities, cautioning against any assumption that the government will turn a blind eye to a contractor's noncompliance with its cybersecurity requirements simply because the government previously declined to enforce such requirements. Going forward, government contractors must strictly comply with the cybersecurity provisions of their contracts and ensure that directors, management, and appropriate information technology personnel monitor cybersecurity practices.

---

* Alicia N. Washington, Litigation counsel at Simpson Thacher & Bartlett LLP and a former Assistant U.S. Attorney for the U.S. Attorney's Office for the Eastern District of New York, represents companies, boards and executives in government and internal investigations and high-profile disputes. Taylor Sutton is an associate in the firm's Litigation Department. Bryce Friedman, co-head of the firm's Business Litigation Practice, represents clients in complex disputes, trials and arbitrations. Resident in the firm's office in New York, the authors may be contacted at alicia.washington@stblaw.com, taylor.sutton@stblaw.com and bfriedman@stblaw.com, respectively.

[1] 31 U.S.C. § 3729 et seq.

[2] Lisa O. Monaco, Deputy Att'y Gen., U.S. Dep't of Just., Deputy Attorney General Lisa O. Monaco Announces New Civil Cyber-Fraud Initiative (Oct. 6, 2021).

[3] No. 15-CV-02245 (E.D. Cal. Oct. 20, 2021).

CYBERSECURITY AND THE FCA

The FCA permits the government, or individuals acting on the government's behalf (known as relators), to recover damages for false claims submitted to the government. A person or entity may be liable under the FCA for procuring a contract by fraud – in which case all claims submitted under the contract are false[4] – or submitting a false claim.[5] Under either theory, the fraud or falsehood must be material.[6]

For government contractors subject to cybersecurity requirements, failure to comply with these requirements, if not adequately disclosed to the government, may make a claim for payment false.

In announcing the Civil Cyber-Fraud Initiative, Monaco declared that the government would enforce the FCA more vigorously against contractors who fail to comply with their cybersecurity requirements. Monaco explained that the government's enforcement priorities included government contractors and grant recipients that endanger U.S. information or systems by knowingly supplying inadequate cybersecurity products or services, misrepresenting their cybersecurity practices or policies, or failing to report cybersecurity incidents as required.

THE *AEROJET* CASE

The *Aerojet* dispute arose from cybersecurity requirements that the Department of Defense ("DOD") and NASA imposed on Aerojet Rocketdyne ("Aerojet") in more than a dozen contracts. The relator, a former senior cybersecurity official for Aerojet, alleged that his erstwhile employer procured the contracts by fraud and falsely certified claims for payment under the contracts, knowingly misleading the government about the extent of its cybersecurity compliance before and after entering into the contracts. The relator alleged, for example, that Aerojet failed to disclose a 2013 breach of its systems when negotiating the DOD and NASA contracts.

According to the relator, Aerojet's alleged failures once under contract – and while negotiating additional contracts – were numerous. Aerojet allegedly complied with, at most, only 25 percent of the cybersecurity controls required under the contracts. The relator asserted that Aerojet did not patch publicly-known system vulnerabilities, failed to screen emails delivered to certain external recipients, and lacked control over the use of external devices on company systems. The relator further asserted that external auditors compromised Aerojet systems within four hours, accessing usernames, passwords, legal documents, sensitive personal information, and even security cameras. Compounding these alleged deficiencies, Aerojet allegedly misrepresented to the government its

---

[4] *United States ex rel. Hendow v. Univ. of Phoenix*, 461 F.3d 1166, 1173 (9th Cir. 2006).

[5] *Universal Health Servs. v. United States ex rel. Escobar*, 579 U.S. 176, 186-87 (2016).

[6] *Hendow*, 461 F.3d at 1174.

compliance with mandated cybersecurity controls, claiming compliance with controls even when compliance had ceased, was grossly incomplete, or had not been attempted.

In June 2018, before Aerojet filed a motion to dismiss, the government declined to intervene.

In May 2019, the court denied Aerojet's motion to dismiss.

The parties filed cross-motions for summary judgment in September 2021. Notably, Aerojet argued that the government's failure to enforce cybersecurity requirements against Aerojet, and other contractors, in the past demonstrated that the requirements were immaterial. Aerojet also argued that its noncompliance was immaterial because the government continued its contracts with Aerojet even after Aerojet had partially disclosed that noncompliance to the government. Aerojet further argued that the government suffered no damages from Aerojet's alleged noncompliance because Aerojet did not suffer a data breach during the contract period.

The relator disagreed, arguing that a reasonable person would assign importance to cybersecurity for sensitive national security data. The relator also alleged that the DOD, in connection with a missiles contract, informed Aerojet that strict cybersecurity compliance was necessary.

THE GOVERNMENT'S STATEMENT OF INTEREST

On October 20, 2021, the government filed a statement of interest in support of the relator, an unusual move that suggests that *Aerojet* may be a test-case for the DOJ's Civil Cyber-Fraud Initiative. In its statement of interest, the government rejected Aerojet's arguments and asserted that the relator's FCA lawsuit should not be barred merely because the government had declined to strictly enforce contractual cybersecurity obligations.

First, the government argued that a federal agency does not need to rescind an agreement with a contractor, after learning of a relator's allegations, in order for a court to find that a contract was procured by fraud. In support of this argument, the government explained that an agency may not know the full extent of a contractor's breach under its contracts.

Similarly, the government argued that a contractor's breach of cybersecurity requirements may be material even if the government knew of earlier breaches by a contractor, or by other contractors within the same industry, because the precise nature and extent of any breach, as well as the period during which a contractor is in breach, all contribute to what constitutes the government's knowledge of noncompliance. The government also argued that an agency may tolerate breaches, even where a contractor is in serious breach of its cybersecurity requirements, because a disruption of the contractual relationship would cause greater harm to its mission. In the government's

view, an agency's tolerance of breaches to provide essential social services should not foreclose a finding of materiality.

Finally, the government insisted that damages under the FCA are available for breach of cybersecurity obligations even if there has been no cybersecurity breach or loss of data. The government argued that cybersecurity compliance is part of the full value of its bargain with a contractor.

On February 1, 2022, the court largely denied each party's motion for summary judgment, holding that there were disputed facts regarding the extent to which Aerojet disclosed its cybersecurity noncompliance to the government. In denying summary judgment, the court declined to address the government's arguments, relying primarily on a disputed issue of fact regarding the government's knowledge of Aerojet's cybersecurity noncompliance and finding whether the government suffered damages was for the jury to decide. The court further held that there was insufficient evidence that the government failed to enforce competing contractors' cybersecurity obligations, and that any such evidence must relate to non-enforcement of particular types of claims that are similar to those submitted by Aerojet.

The parties subsequently reached a settlement.

IMPLICATIONS

While the court did not address the government's arguments in *Aerojet*, the government's position as set forth in its statement of interest has several implications.

Historically, FCA suits targeting cybersecurity violations have been few. However, the government's position in its statement of interest suggests that the lack of past enforcement efforts will not be a significant obstacle to more vigorous prosecution in the future and that the government will advocate for courts to focus on the alleged falsehoods underlying the dispute.

Moreover, the government's proposed damages approach would permit recovery predicated on cybersecurity fraud even in the absence of cybersecurity breaches or data loss. Such an approach would allow proactive enforcement of contractors' cybersecurity obligations, deterring risky cybersecurity practices even before they ripen into a security breach.

Finally, the arguments in the government's statement of interest support its goals of improving cybersecurity broadly and eliminating any competitive disadvantage for contractors who comply with cybersecurity requirements. If defendants can shield themselves from FCA liability by showing that the government failed to enforce cybersecurity requirements against competitors, then no contractor has an incentive to

comply with cybersecurity requirements because there is little risk of future enforcement against noncompliance. However, if the argument advanced by the government prevails, it will be difficult for contractors to avoid liability simply by demonstrating the government previously declined to enforce cybersecurity requirements, including against competitors.

Thus, companies with government contracts that impose cybersecurity obligations should heed the government's increased interest in enforcement and not assume that their own past cybersecurity practices or their industry's usual cybersecurity practices are adequate simply because the government has previously tolerated them. Companies subject to cybersecurity requirements should treat all required controls seriously. Defense contractors for whom a control is inapplicable should, where permitted, observe the formal process for establishing inapplicability.[7] To minimize risk of liability under the FCA, directors, management, and information technology personnel should monitor and ensure compliance with the cybersecurity obligations specified in the company's government contracts.

[7] 48 C.F.R. § 252.204-7012(b)(2)(ii)(B).