

AN A.S. PRATT PUBLICATION

JANUARY 2018

VOL. 4 • NO. 1



PRATT'S
**GOVERNMENT
CONTRACTING
LAW**
REPORT



EDITOR'S NOTE: DISASTER RELIEF

Victoria Prussen Spears

**AVOIDING FCA LIABILITY IN THE
AFTERMATH OF DISASTER RELIEF**

P. Randy Seybold

**GOOD NEWS FOR FCA DEFENDANTS:
SEVENTH CIRCUIT ABANDONS
LONGSTANDING PRECEDENT IN
RESPONSE TO *ESCOBAR***

Courtney Gilligan Saleski and
Andrew J. Hoffman

***McDOWELL v. CGI FEDERAL INC.*: A
STARK REMINDER TO GOVERNMENT
CONTRACTORS OF THEIR
CYBERSECURITY OBLIGATIONS**

Michael F. Mason, Thomas A. Pettit,
Michael J. Scheimer, and Stacy Hadeka

**FALSE CLAIMS ACT WATCH: CALIFORNIA
FEDERAL JUDGE DISMISSES DOJ
COMPLAINT ALLEGING MEDICARE
ADVANTAGE FRAUD**

Jaimie Nawaday and
Alexandra Barbee-Garrett

**ARMED SERVICES BOARD OF CONTRACT
APPEALS BACKLOG SHRINKS, BUT
CHALLENGES REMAIN**

Glenn Sweatt and Michael R. Rizzo

IN THE COURTS

Steven A. Meyerowitz

PRATT'S GOVERNMENT CONTRACTING LAW REPORT

VOLUME 4

NUMBER 1

JANUARY 2018

Editor's Note: Disaster Relief

Victoria Prussen Spears

1

Avoiding FCA Liability in the Aftermath of Disaster Relief

P. Randy Seybold

3

**Good News for FCA Defendants: Seventh Circuit Abandons
Longstanding Precedent in Response to *Escobar***

Courtney Gilligan Saleski and Andrew J. Hoffman

8

***McDowell v. CGI Federal Inc.*: A Stark Reminder to Government
Contractors of Their Cybersecurity Obligations**

Michael F. Mason, Thomas A. Pettit, Michael J. Scheimer, and
Stacy Hadeka

12

**False Claims Act Watch: California Federal Judge Dismisses
DOJ Complaint Alleging Medicare Advantage Fraud**

Jaimie Nawaday and Alexandra Barbee-Garrett

15

**Armed Services Board of Contract Appeals Backlog Shrinks,
But Challenges Remain**

Glenn Sweatt and Michael R. Rizzo

18

In the Courts

Steven A. Meyerowitz

21

QUESTIONS ABOUT THIS PUBLICATION?

For questions about the **Editorial Content** appearing in these volumes or reprint permission, please call:

Heidi A. Litman at 516-771-2169
Email: heidi.a.litman@lexisnexis.com
Outside the United States and Canada, please call (973) 820-2000

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 Website <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

Library of Congress Card Number:

ISBN: 978-1-6328-2705-0 (print)

Cite this publication as:

[author name], [article title], [vol. no.] PRATT’S GOVERNMENT CONTRACTING LAW REPORT [page number] (LexisNexis A.S. Pratt);

Michelle E. Litteken, GAO Holds NASA Exceeded Its Discretion in Protest of FSS Task Order, 1 PRATT’S GOVERNMENT CONTRACTING LAW REPORT 30 (LexisNexis A.S. Pratt)

Because the section you are citing may be revised in a later release, you may wish to photocopy or print out the section for convenient future reference.

This publication is sold with the understanding that the publisher is not engaged in rendering legal, accounting, or other professional services. If legal advice or other expert assistance is required, the services of a competent professional should be sought.

LexisNexis and the Knowledge Burst logo are registered trademarks of Reed Elsevier Properties Inc., used under license. A.S. Pratt is a registered trademark of Reed Elsevier Properties SA, used under license.

Copyright © 2018 Reed Elsevier Properties SA, used under license by Matthew Bender & Company, Inc. All Rights Reserved.

No copyright is claimed by LexisNexis, Matthew Bender & Company, Inc., or Reed Elsevier Properties SA, in the text of statutes, regulations, and excerpts from court opinions quoted within this work. Permission to copy material may be licensed for a fee from the Copyright Clearance Center, 222 Rosewood Drive, Danvers, Mass. 01923, telephone (978) 750-8400.

An A.S. Pratt® Publication

Editorial Office
230 Park Ave., 7th Floor, New York, NY 10169 (800) 543-6862
www.lexisnexis.com

MATTHEW  BENDER

Editor-in-Chief, Editor & Board of Editors

EDITOR-IN-CHIEF

STEVEN A. MEYEROWITZ

President, Meyerowitz Communications Inc.

EDITOR

VICTORIA PRUSSEN SPEARS

Senior Vice President, Meyerowitz Communications Inc.

BOARD OF EDITORS

MARY BETH BOSCO

Partner, Holland & Knight LLP

DARWIN A. HINDMAN III

Shareholder, Baker, Donelson, Bearman, Caldwell & Berkowitz, PC

J. ANDREW HOWARD

Partner, Alston & Bird LLP

KYLE R. JEFCOAT

Counsel, Latham & Watkins LLP

JOHN E. JENSEN

Partner, Pillsbury Winthrop Shaw Pittman LLP

DISMAS LOCARIA

Partner, Venable LLP

MARCIA G. MADSEN

Partner, Mayer Brown LLP

KEVIN P. MULLEN

Partner, Morrison & Foerster LLP

VINCENT J. NAPOLEON

Partner, Nixon Peabody LLP

STUART W. TURNER

Counsel, Arnold & Porter LLP

WALTER A.I. WILSON

Senior Partner, Polsinelli PC

PRATT'S GOVERNMENT CONTRACTING LAW REPORT is published twelve times a year by Matthew Bender & Company, Inc. Copyright 2018 Reed Elsevier Properties SA., used under license by Matthew Bender & Company, Inc. All rights reserved. No part of this journal may be reproduced in any form—by microfilm, xerography, or otherwise—or incorporated into any information retrieval system without the written permission of the copyright owner. For permission to photocopy or use material electronically from *Pratt's Government Contracting Law Report*, please access www.copyright.com or contact the Copyright Clearance Center, Inc. (CCC), 222 Rosewood Drive, Danvers, MA 01923, 978-750-8400. CCC is a not-for-profit organization that provides licenses and registration for a variety of users. For subscription information and customer service, call 1-800-833-9844. 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, 718.224.2258. Material for publication is welcomed—articles, decisions, or other items of interest to government contractors, attorneys and law firms, in-house counsel, government lawyers, and senior business executives. 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 Government Contracting Law Report*, LexisNexis Matthew Bender, 630 Central Avenue, New Providence, NJ 07974.

McDowell v. CGI Federal Inc.: A Stark Reminder to Government Contractors of Their Cybersecurity Obligations

*By Michael F. Mason, Thomas A. Pettit, Michael J. Scheimer, and Stacy Hadeka**

The authors of this article discuss a U.S. District Court for the District of Columbia decision in a class action lawsuit, which could have significant repercussions for government contractors operating information systems that house government information.

The U.S. District Court for the District of Columbia has issued a decision in a class action lawsuit, *McDowell v. CGI Federal Inc.*,¹ which could have significant repercussions for government contractors operating information systems that house government information. The case arose after employees of CGI Federal Inc. (“CGI”) allegedly stole personally identifiable information (“PII”) CGI obtained pursuant to a contract with the U.S. Department of State.

THE CONTRACT

Under this contract, CGI processed passport applications, which contained a significant amount of PII. The plaintiffs alleged that, as part of its activities under the contract, CGI processed information on CGI-owned systems and assisted with maintaining Department of State systems. According to the filings, the contract provided that all information submitted through passport applications was U.S. government property and required CGI to safeguard all such information.

THE COMPLAINT

In the complaint, the plaintiffs alleged:

* Michael F. Mason (mike.mason@hoganlovells.com) is a partner at Hogan Lovells representing clients in bid protest litigation before the Government Accountability Office and U.S. Court of Federal Claims. Thomas A. Pettit (thomas.pettit@hoganlovells.com) is an associate at the firm representing clients across industry sectors facing a range of government contracting challenges. Michael J. Scheimer (michael.scheimer@hoganlovells.com), a senior associate at the firm, advises clients on government contracts with a particular focus on national security, cybersecurity, and IT contracting. Stacy Hadeka (stacy.hadeka@hoganlovells.com) is a senior associate at the firm practicing all areas of government contracting.

¹ Civ. Action No. 15-1157 (GK) (D.D.C. 2017) (The parties settled the case, and the plaintiffs stipulated to dismissal of all claims on September 20, 2017. The terms of the settlement are presumably confidential and thus unknown).

- (1) violations of the District of Columbia Consumer Protection Procedures Act;
- (2) negligence;
- (3) breach of contract, including a third-party beneficiary claim;
- (4) breach of bailment; and
- (5) unjust enrichment.

CGI filed a motion to dismiss each of the claims. The court granted CGI's motion to dismiss each ground except the third-party beneficiary breach of contract theory. The plaintiffs claimed that because the information was PII, CGI was charged with securing it for their benefit. Although decided on a motion to dismiss rather than on the merits, this decision should serve as a reminder to all government contractors of their cybersecurity obligations.

THE LAW

The Federal Information Security Management Act ("FISMA") of 2002,² as amended by FISMA 2014, and OMB Circular A-130³ require agencies to create and implement agency-wide information security programs and have served as the statutory authority and catalyst for many information security requirements facing government contractors. Although FISMA technically applies only where a contractor operates a system on behalf of an agency, internal contractor systems that process government data in performance of a contract can still be subject to various requirements as implemented by the Federal Acquisition Regulation ("FAR") and applicable FAR supplements, such as the Defense FAR Supplement ("DFARS").

For example, FAR 52.204-21 establishes a baseline of information security requirements that contractors must follow when operating contractor information systems that process, store, or transmit non-public information that the U.S. government provides to a contractor pursuant to a contract. DFARS 252.204-7012 applies to contracts with the Department of Defense ("DOD") and requires contractors to protect "covered defense information" and establishes cyber incident reporting requirements. DFARS 252.239-7010 imposes various information security requirements on cloud service providers. Some of these clauses require contractors to comply with Federal Information Processing Standards and National Institute of Standards and Technology ("NIST") special

² 44 U.S.C. § 3541 *et seq.*

³ <https://obamawhitehouse.archives.gov/sites/default/files/omb/assets/OMB/circulars/a130/a130revised.pdf>.

publications (“SPs”), including NIST SP 800-171, *Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations*.

A NEW FAR CASE

A new FAR case, Case No. 2017-013,⁴ is particularly relevant to government contractors, such as CGI, that process PII. The FAR Council is considering issuing a proposed rule to implement OMB Memorandum M-17-12,⁵ which establishes federal policies for responding to breaches that compromise PII. The goal of this FAR case is to create contract clauses that will apply where “a contractor has access to, creates, collects, or maintains [PII] on behalf of the agency or operates an information system on behalf of the agency that may have [PII] residing in or transiting through the information system.” A Notice of Proposed Rulemaking was expected in December 2017.

CONCLUSION

While *McDowell* is a significant case, contractors should not interpret this decision as establishing a rule that contractors are liable to the public for failing to comply with information security requirements.

First, it is important to remember that this decision was issued on a motion to dismiss and is not a decision on the merits. Consequently, it has no precedential effect.

Second, as the court correctly noted, members of the public are generally considered to be only “incidental beneficiaries” who “have no right to sue for breach of contract.”⁶ However, this decision may, at a minimum, embolden prospective plaintiffs to litigate these issues.

As a result, it is important that contractors ensure they are complying with their cybersecurity obligations.

⁴ <https://www.reginfo.gov/public/do/eAgendaViewRule?pubId=201704&RIN=9000-AN44>.

⁵ https://obamawhitehouse.archives.gov/sites/default/files/omb/memoranda/2017/m-17-12_0.pdf.

⁶ *McDowell* at 13; see also *Orff v. United States*, 358 F.3d 1137, 1145 (9th Cir. 2004) (“Parties that benefit from a government contract are generally assumed to be incidental beneficiaries” and thus “may not enforce the contract *absent a clear intent to the contrary*.”) (emphasis added).