ALSTON & BIRD

WWW.ALSTON.COM

Privacy, Cyber & Data Strategy / White Collar, Government & Internal Investigations ADVISORY ■

OCTOBER 20, 2021

New Civil Cyber-Fraud Initiative Signals Increased Litigation Risk Arising from Cybersecurity Practices

by *Kim Peretti*, *Edward Kang*, *Jody Hunt*, *Kellen Dwyer*, *Jon Knight*, and *Ryan Martin-Patterson*

On October 6, 2021, Deputy Attorney General Lisa O. Monaco announced the Department of Justice's (DOJ) "Civil Cyber-Fraud Initiative." This new enforcement project led by the DOJ's Civil Fraud Section will seek civil penalties under the False Claims Act (FCA) against government contractors and grant recipients that put U.S. information or systems at risk, for example by providing deficient cybersecurity products, misrepresenting cybersecurity capabilities, or knowingly violating obligations to monitor and report data breaches. The initiative is the latest in a line of Biden Administration actions that aim to combat the growth in cyber-attacks with aggressive use of criminal enforcement against the attackers and new requirements for industry.

The Initiative Signals Increased Risk of FCA Litigation with the DOJ or Private Plaintiffs

The DOJ used the FCA to recover $2.2 billion in settlements and judgments in 2020 and anticipates using the FCA's "very hefty" monetary penalties to change contractors' cybersecurity behavior. FCA liability involves claims that are factually false, which may include "false certifications" if contractors expressly or implicitly certify compliance with a particular statute, regulation, or contractual term when compliance is a prerequisite to payment. Under this new initiative, it appears the DOJ intends to use a similar theory to enforce compliance with cybersecurity and breach-reporting provisions contained in federal contracts. To the extent compliance with these provisions is not already a contractual prerequisite for payment, contractors should expect that to change. Indeed, federal departments and agencies are already in the process of implementing the President's May 2021 Executive Order that, among other things, required a broad review of federal contracting rules on cybersecurity and breach reporting.

There are few known FCA cases involving cybersecurity claims, though given the sensitive nature of the subject matter, more may be filed under seal. Relators have had mixed results attempting to bring such FCA cases, with one case against an aerospace contractor moving past a motion to dismiss, while another case against a computer manufacturer was dismissed. The initiative likely signals an aggressive civil enforcement approach, with the DOJ bringing more FCA cases on its own volition, intervening more frequently in relator cases raising colorable claims and encouraging whistleblowers to more willingly come forward.

Contractors should use this announcement as a call to revisit their cybersecurity controls and certifications, confirm that their processes satisfy all contractual requirements, and investigate whether corrections need to be made to prior statements or representations to the government regarding the security of their systems or their products. The following are questions companies can ask internally as they evaluate these risks.

Do you have a process to investigate and remediate cybersecurity-related complaints?

FCA litigation often arises from whistleblowers either contacting the government or independently bringing suit under the FCA's qui tam provisions. This initiative will be no different – the DOJ's announcement specifically mentions relying on whistleblowers to assist the government in bringing these actions. One practical way companies can reduce the likelihood of triggering these suits is to ensure there is a robust internal investigations process for receiving and resolving employee concerns about cybersecurity or product vulnerabilities. Counsel can assist in building a process for triaging, investigating, responding, and remediating these complaints that is protected by privilege, run independently, and provides ammunition for defeating a subsequent claim that the company ignored or inadequately addressed concerns.

Do you know if your cybersecurity controls and processes satisfy current standards required by contract and/or a minimum baseline of reasonable security?

Currently, there is not a unified cybersecurity standard for government contractors. While FAR 52.204-21 lays out "basic safeguarding of covered contractor information systems," additional requirements will be contract-specific and can change depending on the procuring agency, data at issue, and type of service or product being offered. For civilian agencies in particular, more detailed cybersecurity requirements were often included in a scope of work, which could result in vague, confusing, and conflicting requirements. But going forward, contractors should expect a stricter level of standardization in contractually required cybersecurity controls and certifications. At the Department of Defense, the Cybersecurity Maturity Model Certification program is getting off the ground with its five levels of security assessments and certifications. Similarly, the National Institute of Standards and Technology is currently developing additional guidelines for contractors based on the May 2021 Executive Order. While final guidelines may not yet have been completed, we can expect more contractual requirements that reflect the "reasonable security" standard as a baseline. Consider conducting an internal assessment of your controls and processes to confirm you could satisfy either any existing contractual requirements or this baseline of reasonable security. Alston & Bird has published a separate guide, the "12 Elements for Effective Cybersecurity: What Does 'Reasonable Security' Look Like Organizationally?," that can be a starting point for your internal discussions.

Do you know what you are telling (or have told) the government about your cybersecurity controls and capabilities?

The announced initiative specifically highlights misrepresentations made to the government about cybersecurity. Once contractors have determined their cybersecurity controls baseline, they may want to consider conducting an internal investigation with counsel comparing the statements they have made (or are making) to the government on the cybersecurity front with their cybersecurity controls baseline. This effort will help paint a picture of any existing FCA cyber-risk and provide an opportunity to address any discrepancies with the government outside the litigation/whistleblower context.

Are you monitoring the changing landscape for reporting cyber incidents to the federal government?

While you may (or may not) have contractual obligations to report certain types of cybersecurity incidents to your contracting officer or the procuring agency, it appears that the government may soon require expanded reporting of security incidents from contractors. The May 2021 Executive Order already signaled new cybersecurity reporting regulations for contractors, and additional legislation is moving through Congress on this issue. Monitoring and testing your existing incident notification procedures and preparing for changes to this landscape will be important.

As you ask these questions internally, our cross-functional Alston & Bird team has the experience in internal investigations, government procurement, cybersecurity, False Claims Act enforcement, and litigation to not only help you build out these processes and conduct internal investigations and assessments but also to defend you against any government action or whistleblower claims. Please reach out to any of our team members to address how these questions can be addressed by your organization.

You can subscribe to future *Privacy, Cyber & Data Strategy* and *White Collar, Government & Internal Investigations* advisories and other Alston & Bird publications by completing our **publications subscription form**.

If you have any questions or would like additional information please contact your Alston & Bird attorney or any of the following:

Kimberly Kiefer Peretti
202.239.3720
kimberly.peretti@alston.com

Edward T. Kang
202.239.3728
edward.kang@alston.com

Joseph H. Hunt
202.239.3278
404.881.7811
jody.hunt@alston.com

Kellen Dwyer
202.239.3240
212.905.9340
kellen.dwyer@alston.com

Jon Knight
202.239.3270
jon.knight@alston.com

Ryan Martin-Patterson
202.239.3038
ryan.martin-patterson@alston.com

ALSTON & BIRD

WWW.ALSTON.COM

ATLANTA: One Atlantic Center ■ 1201 West Peachtree Street ■ Atlanta, Georgia, USA, 30309-3424 ■ 404.881.7000 ■ Fax: 404.881.7777
BEIJING: Hanwei Plaza West Wing ■ Suite 21B2 ■ No. 7 Guanghua Road ■ Chaoyang District ■ Beijing, 100004 CN ■ +86.10.85927500
BRUSSELS: Rue Guimard 9 et Rue du Commerce 87 ■ 3rd Floor ■ 1000 Brussels ■ Brussels, 1000, BE ■ +32.2.550.3700 ■ Fax: +32.2.550.3719
CHARLOTTE: One South at The Plaza ■ 101 South Tryon Street ■ Suite 4000 ■ Charlotte, North Carolina, USA, 28280-4000 ■ 704.444.1000 ■ Fax: 704.444.1111
DALLAS: Chase Tower ■ 2200 Ross Avenue ■ Suite 2300 ■ Dallas, Texas, USA, 75201 ■ 214.922.3400 ■ Fax: 214.922.3899
FORT WORTH: 3700 Hulen Street ■ Building 3 ■ Suite 150 ■ Fort Worth, Texas, USA, 76107 ■ 214.922.3400 ■ Fax: 214.922.3899
LONDON: 5th Floor ■ Octagon Point, St. Paul's ■ 5 Cheapside ■ London, EC2V 6AA, UK ■ +44.0.20.3823.2225
LOS ANGELES: 333 South Hope Street ■ 16th Floor ■ Los Angeles, California, USA, 90071-3004 ■ 213.576.1000 ■ Fax: 213.576.1100
NEW YORK: 90 Park Avenue ■ 15th Floor ■ New York, New York, USA, 10016-1387 ■ 212.210.9400 ■ Fax: 212.210.9444
RALEIGH: 555 Fayetteville Street ■ Suite 600 ■ Raleigh, North Carolina, USA, 27601-3034 ■ 919.862.2200 ■ Fax: 919.862.2260
SAN FRANCISCO: 560 Mission Street ■ Suite 2100 ■ San Francisco, California, USA, 94105-0912 ■ 415.243.1000 ■ Fax: 415.243.1001
SILICON VALLEY: 1950 University Avenue ■ Suite 430 ■ East Palo Alto, California, USA 94303 ■ 650.838.2000 ■ Fax: 650.838.2001
WASHINGTON, DC: The Atlantic Building ■ 950 F Street, NW ■ Washington, DC, USA, 20004-1404 ■ 202.239.3300 ■ Fax: 202.239.3333