King & Spalding
Client Alert

OCTOBER 18, 2021

DOJ Announces Civil Cyber-Fraud Initiative to Use False Claims Act to Enforce Cybersecurity Standards in Government Contracts

For more information, contact:

Paul B. Murphy
+1 404 572 4730
pbmurphy@kslaw.com

David Balser
+1 404 572 2782
dbalser@kslaw.com

Steve Cave
+1 202 626 9628
scave@kslaw.com

Sumon Dantiki
+1 202 626 5591
sdantiki@kslaw.com

Chris Burris
+1 404 572 4708
cburris@kslaw.com

King & Spalding

Atlanta
1180 Peachtree Street, NE
Atlanta, Georgia 30309-3521
Tel: +1 404 572 4600

Washington, D.C.
1700 Pennsylvania Avenue, NW
Washington, D.C. 20006-4707
Tel: +1 202 737 0500

FCA ENFORCEMENT SHIFT

On October 6, the Deputy Attorney General ("DAG") announced a new Department of Justice ("DOJ") Civil Cyber-Fraud Initiative – an effort that pulls together attorneys and experts across DOJ focused on fraud enforcement, government procurement, and cybersecurity "to combat new and emerging cyber threats to the security of sensitive information and critical systems".[1] The Cyber-Fraud Initiative is the direct product of a larger ongoing DOJ review to address grave cyber threats in the wake of unprecedented ransomware attacks and digital supply chain compromises. DOJ outlined both punitive and preventative goals in launching the initiative. For example, it intends to use the False Claims Act ("FCA") to motivate companies and contractors to comply with cybersecurity standards. Specifically, DOJ will be actively pursuing FCA actions against government contractors that "hide a breach" rather than "bring it forward and [] report it."[2] Additionally, any company that "knowingly provid[es] deficient cybersecurity products or services [or] knowingly misrepresent[s] their cybersecurity practices or protocols" will be subject to civil action.[3] As the DAG explained, "Where those who are entrusted with government dollars, who are entrusted to work on sensitive government systems, fail to follow required cybersecurity standards, we're going to go after that behavior and extract very hefty, very hefty fines."[4]

But in a notable shift, DOJ also outlined preventative goals of "[b]uilding broad resiliency against cybersecurity intrusions across the government, the public sector and key industry partners" and "[i]mproving overall cybersecurity practices that will benefit the government, private users and the American public."[5]

AN UNCERTAIN ENVIRONMENT

The announcement of the Cyber-Fraud Initiative development reflects a broader focus on cybersecurity across the federal government and ongoing evolution on appropriate cybersecurity standards in a dynamic threat environment. Historically, the government has treated cybersecurity standards as material conditions of government contracts and has used the FCA to pursue cases and damages when a contractor allegedly fails to comply with the standards. Those standards are currently in flux. As we previously noted, President Biden issued an Executive Order in May 2021 that "[t]he Federal Government must adopt security best practices [and] advance toward Zero Trust Architecture."[6] Congress is likewise considering various measures, such as the Cyber Incident Reporting Act, to impose new requirements for cyber incident reporting on critical infrastructure owners and operators. And the SEC has been increasingly focused on using its authorities to regulate cybersecurity.

Although it is not entirely clear what the government intends to do with any new cybersecurity standards (not already announced), we expect DOJ and the government to view the existing standards and any new standards as a "material" aspect of the government's decision to pay a contractor. DOJ will use the FCA against government contractors that (1) do not report cybersecurity "breaches," or (2) otherwise fail to adhere to "required cybersecurity standards." Government contractors may violate the FCA if they do not adhere to the contract's express or implied certification requirements. By using the FCA, DOJ is encouraging whistleblowers and others to report these cybersecurity "failures" as potentially fraudulent conduct. Targeted against individuals and organizations that defraud the government, the FCA creates severe penalties for submitting false claims for payment to the government. The statute provides civil penalties of between approximately $12,000 and $24,000 for each false claim and up to three times the amount of the government's damages. In 2020 alone—when cybersecurity was not a stated priority for DOJ enforcement—DOJ obtained more than $2.2 billion in FCA judgments and settlements. With whistleblowers receiving at least 15-25% of the overall settlement or damage amount, they have every incentive to report alleged cybersecurity failures as potentially fraudulent conduct. These new far-reaching implications apply to *any company* with whom the government contracts.

TAKEAWAYS FOR COMPANIES

Although most companies maintain cybersecurity policies, procedures, and other standards, government contractors now face an increased risk of investigation and litigation from *qui tam* relators or DOJ if their cybersecurity measures are even perceived not to align with those of the government. In a dynamic threat environment, however, federal government expectations for cybersecurity standards may differ significantly across agencies, contracts, and even points in time. Moreover, DOJ's stated goals of "building broad resiliency against cybersecurity intrusions" and "improving overall cybersecurity practices" suggest that enforcement discretion will be used as a means of proactive cybersecurity improvement beyond set past expectations.

Against this new enforcement environment, companies should carefully reevaluate their FCA risk from a legal, technical, and operational perspective. Risks may stem, for instance, from vague contractual provisions, employee misunderstandings on cybersecurity compliance procedures, or information security procedures that are not fully up to date.

ABOUT KING & SPALDING

Celebrating more than 130 years of service, King & Spalding is an international law firm that represents a broad array of clients, including half of the Fortune Global 100, with 1,200 lawyers in 22 offices in the United States, Europe, the Middle East and Asia. The firm has handled matters in over 160 countries on six continents and is consistently recognized for the results it obtains, uncompromising commitment to quality, and dedication to understanding the business and culture of its clients.

ABU DHABI	CHARLOTTE	FRANKFURT	LOS ANGELES	RIYADH	SINGAPORE
ATLANTA	CHICAGO	GENEVA	NEW YORK	SACRAMENTO	TOKYO
AUSTIN	DENVER	HOUSTON	NORTHERN VIRGINIA	SAN FRANCISCO	WASHINGTON, D.C.
BRUSSELS	DUBAI	LONDON	PARIS	SILICON VALLEY	

[1] https://www.justice.gov/opa/pr/deputy-attorney-general-lisa-o-monaco-announces-new-civil-cyber-fraud-initiative
[2] *Id.*
[3] *Id.*
[4] *Id.*
[5] *Id.*
[6] https://www.kslaw.com/news-and-insights/president-bidens-executive-order-to-improve-cybersecurity-issued