Washington Legal Foundation
Advocate for freedom and justice®
2009 Massachusetts Avenue, NW
Washington, DC 20036
202.588.0302

Critical Legal Issues: WORKING PAPER SERIES

DOJ'S CIVIL CYBER-FRAUD INITIATIVE: WHAT CONTRACTORS NEED TO KNOW ABOUT NOVEL USE OF FALSE CLAIMS ACT

Alaap Shah and Stuart M. Gerson
Epstein Becker & Green, P.C.

Washington Legal Foundation
Critical Legal Issues WORKING PAPER Series

Number 224
January 2022

TABLE OF CONTENTS

ABOUT OUR LEGAL STUDIES DIVISION

Since 1986, WLF's Legal Studies Division has served as the preeminent publisher of persuasive, expertly researched, and highly respected legal publications that explore cutting-edge and timely legal issues. These articles do more than inform the legal community and the public about issues vital to the fundamental rights of Americans—they are the very substance that tips the scales in favor of those rights. Legal Studies publications are marketed to an expansive audience, which includes judges, policymakers, government officials, the media, and other key legal audiences.

The Legal Studies Division focuses on matters related to the protection and advancement of economic liberty. Our publications tackle legal and policy questions implicating principles of free enterprise, individual and business civil liberties, limited government, and the rule of law.

WLF's publications target a select legal policy-making audience, with thousands of decision makers and top legal minds relying on our publications for analysis of timely issues. Our authors include the nation's most versed legal professionals, such as expert attorneys at major law firms, judges, law professors, business executives, and senior government officials who contribute on a strictly *pro bono* basis.

Our eight publication formats include the concise COUNSEL'S ADVISORY, succinct LEGAL OPINION LETTER, provocative LEGAL BACKGROUNDER, in-depth WORKING PAPER and CONTEMPORARY LEGAL NOTE, topical CIRCULATING OPINION, informal CONVERSATIONS WITH, balanced ON THE MERITS, and comprehensive MONOGRAPH. Each format presents single-issue advocacy on discrete legal topics.

In addition to WLF's own distribution network, full texts of LEGAL OPINION LETTERS and LEGAL BACKGROUNDERS appear on the LEXIS/NEXIS® online information service under the filename "*WLF*," and every WLF publication since 2002 appears on our website at www.wlf.org. You can also subscribe to receive select publications at www.WLF.org.

To receive information about WLF publications, or to obtain permission to republish this publication, please contact Glenn Lammi, Vice President of Legal Studies, Washington Legal Foundation, 2009 Massachusetts Avenue, NW, Washington, DC 20036, (202) 588-0302, glammi@wlf.org.

ABOUT THE AUTHORS

Alaap Shah is a partner with Epstein Becker & Green, P.C. where he Co-chairs the Privacy, Cybersecurity and Data Asset Management team. As Co-chair, Mr. Shah where he bring his tech-savvy and solutions oriented approach to deftly guide clients through complex and ever-evolving privacy, cybersecurity, medical device, artificial intelligence (AI), interoperability, digital health, telehealth, fraud and abuse, and other laws and regulations.

Stuart M. Gerson, a long-time member of WLF's Legal Policy Advisory Board and a partner at Epstein Becker & Green, P.C., is a former federal prosecutor, Assistant Attorney General for the Civil Division of the Department of Justice, and Acting Attorney General of the United States. His practice involves both cybersecurity and False Claims Act defense.

The authors thank Epstein Becker & Green, P.C. attorneys Jennifer Carney Nelson, Devon Minnick, and Chris Taylor for their contributions to this WORKING PAPER.

DOJ'S CIVIL CYBER-FRAUD INITIATIVE: WHAT CONTRACTORS NEED TO KNOW ABOUT NOVEL USE OF FALSE CLAIMS ACT

INTRODUCTION

Cyberattacks and data breaches continue to make front-page news because of their disruptive impact on the operations, finances, and reputations of companies large and small. The COVID-19 pandemic, during which remote business activity and the use of technology to access and transmit sensitive information increased, has magnified this threat. Some industries, health care as a prime example, have been particularly hard hit.

The Biden administration responded to the growth of cybercrime by championing a national response strategy, particularly to thwart ransomware attacks. In furtherance of this effort the Department of Justice ("DOJ") recently announced an enhanced Civil Cyber-Fraud Initiative (the "DOJ Initiative"). Under this initiative, DOJ plans to leverage its broad enforcement authority under the False Claims Act ("FCA") to pursue cybersecurity-related fraud involving government contracts and federal grantees. This effort will affect every company—running the gamut from defense contractors to providers who participate in federally funded health care programs. And as any government contractor knows, the threat of treble-damages lawsuits isn't limited to DOJ action. The FCA is a vehicle for private "relators" to sue in the name of the United States. Indeed, spurred by financial incentives and an industry tendency to

settle cases, the vast majority of FCA cases are initiated by private relators. Thus, the DOJ Initiative poses significant risks and increased costs associated with company cybersecurity practices.

We first turn our attention to the nature and scope of the DOJ Initiative, the FCA theory that it purports to rely upon, and the avenues of prevention and response that this victim-as-potential-defendant policy suggests. Finally, we examine policy arguments that suggest that the DOJ Initiative might be misplaced.

I. THE DOJ INITIATIVE

In October 2021, Deputy Attorney General Lisa Monaco announced the launch of the DOJ Initiative as a mechanism for combatting "new and emerging cyber threats to the security of sensitive information and critical systems."[1] The DOJ Initiative specifically seeks to punish U.S. companies that do not implement appropriate cybersecurity protocols, and that fail to inform DOJ of incidences of cybercrime. In a somewhat novel offensive tactic, DOJ will use the law as a weapon to extract better cybersecurity practices from a broad range of government contractors and grantees, including payers and providers that enter into financial relationships with the government under various federal programs such as Medicare and Medicaid. DOJ plans to extend its scrutiny to corporate and individual conduct that places

[1] https://www.justice.gov/opa/pr/deputy-attorney-general-lisa-o-monaco-announces-new-civil-cyber-fraud-initiative (last accessed Jan. 14, 2022).

government information or systems at risk by *knowingly*:

- providing deficient cybersecurity products or services,
- misrepresenting cybersecurity practices or protocols, or
- violating obligations to monitor and report cybersecurity incidents and breaches.

Thus, DOJ will, by adding the risk of FCA treble damages, penalize actual or potential victims of cyber attacks and ransomware attacks—a double whammy for those companies already struggling to recover from data breaches and ransomware debilitating their systems and, in some cases, resulting in multi-million-dollar payments and related remediation costs.

According to statements made by Ms. Monaco, DOJ aims to scrutinize any government contractor or grantee that is "entrusted to work on sensitive government systems" that "fail to follow required cybersecurity standards." Though this might seem reasonable, this perspective does not appear to account for those companies who fall victim to a cyber attack due to little or no fault of their own, such as those who suffered a zero-day attack or are severely impacted as a result of a third party hack into one of their trusted vendors. We'll discuss that conflict later.

The scope of enforcement is not yet clear, but the Fraud Section of DOJ's Civil Division's Commercial Litigation Branch leads the DOJ Initiative and is expected to evaluate all manner of cybersecurity noncompliance to determine adverse impacts to federal programs under its jurisdiction. Ms. Monaco was also clear that violators would be subject to "very hefty fines." Given the history of DOJ's FCA enforcement,

this too is unsurprising. DOJ typically recovers from $2 to $5 billion annually in FCA cases.

II. FALSE CERTIFICATION AS THE BASIS FOR ENFORCEMENT

A. Express and Implied False Certification

To establish an actionable FCA lawsuit, the government or relator must show: a false statement or fraudulent course of conduct, which is made or carried out with knowledge of the falsity of such statement or conduct, that is material to the fact of payment, and that involved a request or demand for compensation, in cash or in kind, from the U.S. government. The relationship between an entity suffering a cyber breach and its having submitted a false claim for payment would seem illusive at best. However, that illusion is fractured by the false certification theory upon which DOJ proposes to proceed with respect to cybersecurity.

There are two types of false certifications. An *express* false certification occurs when a company or individual knowingly, falsely certifies that it has complied with a law or contractual term, so long as compliance with that law or term is a requirement for payment. An *implied* false certification occurs when a company or individual knowingly does not disclose that it has violated laws or contractual terms that impact its eligibility to be paid.

In order for the government or a relator to meet the materiality requirement of an implied false certification claim, the claim must not only request payment, but

also make specific representations about the goods or services provided to the government. DOJ thus frequently argues that an entity's failure to disclose that it did not comply with a material law or contractual term "makes those representations misleading half-truths."[2]

Even prior to launch of the Initiative, the DOJ occasionally has utilized the FCA in its investigations related to cybersecurity. In one such case, Cisco Systems, Inc. was alleged to have known security flaws within its video surveillance product that enabled hackers to take control of the environment in which it was installed. That environment included branches of the government and multiple airports and train stations. The complaint invoked the FCA in alleging that Cisco knew of the critical security flaws for several years and failed to notify the government entities that had purchased and continued to use the software. Further, the complaint contended that the software product failed to comply with the security standards imposed on government systems by the Federal Information Security Management Act. The case was filed in 2011 and settled in 2019 for $8.6 million.[3]

In a 2017 case, DOJ alleged false certification under the FCA by an electronic health records ("EHR") company and obtained a significant settlement.[4] DOJ contended that the EHR, eClinicalWorks ("ECW"), falsely obtained certification for its

[2] *See United States ex rel. Escobar,* 136 S. Ct. 1989, 2001 (2016).

[3] *See United States*. *ex. rel. Glenn v. Cisco Systems*, No. 1:11-cv-00400 (W.D. NY 2019).

[4] *See United States ex rel. Delaney v. eClinicalWorks* LLC, 2:15-CV-00095-WKS (D. Vt. 2017).

software when it concealed from its independent certifying entity that its software did not comply with the requirements for certification. The Department of Health and Human Services ("HHS") established the certification requirements for purposes of the EHR Incentive Program to encourage healthcare providers to adopt and demonstrate their "meaningful use" of EHR technology. Because ECW's software contained deficiencies, the government claimed that ECW caused the submission of false claims for federal incentive payments based upon the use of its software. Under the terms of its settlement, ECW had to pay $155 million and enter into a five-year Corporate Integrity Agreement ("CIA") with the HHS Office of Inspector General.[5]

B. *Qui Tam* Risk

Both of the cases discussed above were initiated by whistleblowers, *i.e.*, "relators" eligible under the FCA to receive as much as 25-30% of any amount recovered. Accordingly, there is a clear financial incentive for whistleblowers to bring *qui tam* cases under the FCA. The DOJ Initiative thus likely will encourage whistleblower lawsuits from persons within companies who believe a cybersecurity weakness exists and that a big payout is possible. Companies covered by the Health Insurance Portability and Accountability Act of 1996, as amended ("HIPAA"), might

[5] https://www.justice.gov/opa/pr/electronic-health-records-vendor-pay-155-million-settle-false-claims-act-allegations (last accessed Jan. 14, 2022).

have unique *qui tam* risk emanating from potential violations of implementation specifications detailed under the HIPAA Security Rule.[6]

III. HOW TO BUILD A DEFENSIBLE CYBERSECURITY POSTURE

A. Identifying Standards for "Reasonable and Appropriate" Cybersecurity Controls

Regulators increasingly have required companies to implement reasonable and appropriate security safeguards to maintain the confidentiality, integrity and availability of their sensitive information. In light of the DOJ Initiative, companies should revisit their policies and practices to ensure they are meeting what applicable laws, regulations and industry best practices would consider reasonable and appropriate levels of security. The scope of what constitutes "reasonable and appropriate" practices is ever-changing, and it is unclear what standards DOJ will be insisting upon.

Recent amendments to the Health Information Technology for Economic and Clinical Health Act ("HITECH Act"), 42 U.S.C. § 17931, might offer some insight into what can constitute "reasonable and appropriate" cybersecurity controls.[7] These amendments require that "recognized cybersecurity practices" be considered by the Secretary of HHS in determining any HIPAA-related fines, audit results, or mitigation

[6] 45 C.F.R. § 164.308 (a)(2)—Administrative Safeguard Standard: Assigned Security Responsibility.

[7] Note that these amendments only govern what may be reasonable and appropriate under the HIPAA Security Rule.

remedies. The term *recognized security practices* means "the standards, guidelines, best practices, methodologies, procedures, and processes developed under section 2(c)(15) of the National Institute of Standards and Technology ("NIST") Act, the approaches promulgated under section 405(d) of the Cybersecurity Act of 2015, and other programs and processes that address cybersecurity and that are developed, recognized, or promulgated through regulations under other statutory authorities" to be applied in a manner consistent with the size, scope and complexity of subject organizations.

Further, as the language references "other programs and processes that address cybersecurity and that are developed, recognized, or promulgated through regulations under other statutory authorities," it is likely to also include standards set forth in the following: NIST SP 800-53 Rev. 5, Security and Privacy Controls for Information Systems and Organizations.[8]

In addition, several other government authorities have issued guidance on cybersecurity including, but not limited to the DOJ,[9] HHS,[10] OCR,[11] the Federal Bureau

[8] https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final (last accessed Jan. 14, 2022).

[9] https://www.justice.gov/criminal-ccips/file/1096971/download (last accessed Jan. 14, 2022).

[10] https://healthsectorcouncil.org/hicp/ (last accessed Jan. 14, 2022).

[11] https://www.hhs.gov/hipaa/for-professionals/security/guidance/cybersecurity/index.html (last accessed Jan. 14, 2022).

of Investigation ("FBI"),[12] the Federal Trade Commission,[13] the U.S. Department of the Treasury's Office of Foreign Asset Control,[14] and the Cybersecurity and Infrastructure Security Agency ("CISA").[15] Potentially useful cybersecurity standards established by non-governmental entities include: HITRUST Cybersecurity Framework, which was developed as a healthcare industry standard;[16] ISO/IEC 27001 Information Security Management standard;[17] SOC2 Trust Service Criteria;[18] and OWASP Top 10.[19]

Clearly there is no dearth of best-practices guidance available to companies seeking to build a defensible cybersecurity posture. Nevertheless, it's unclear which of the various standards (or combinations thereof) DOJ would use as the measuring stick under an FCA investigation.

---

[12] https://www.fbi.gov/investigate/cyber/publications (last accessed Jan. 14, 2022).

[13] https://www.ftc.gov/tips-advice/business-center/guidance/start-security-guide-business (last accessed Jan. 14, 2022). It should be noted that the FTC continues to be increasingly involved in cybersecurity issues and has even recently issued guidance regarding remediation of the Log4j security vulnerability by warning that companies have a "duty to take reasonable steps to mitigate known software vulnerabilities." *See* https://www.ftc.gov/news-events/blogs/techftc/2022/01/ftc-warns-companies-remediate-log4j-security-vulnerability (last accessed Jan. 4, 2022).

[14] https://home.treasury.gov/system/files/126/ofac_ransomware_advisory.pdf.

[15] https://www.cisa.gov/cisa-cybersecurity-resources (last accessed Jan. 14, 2022).

[16] https://hitrustalliance.net/ (last accessed Jan. 14, 2022).

[17] https://www.iso.org/isoiec-27001-information-security.html (last accessed Jan. 14, 2022).

[18] https://us.aicpa.org/interestareas/frc/assuranceadvisoryservices/trustdataintegritytaskforce (last accessed Jan. 14, 2022).

[19] https://owasp.org/www-project-top-ten/ (last accessed Jan. 14, 2022).

B. Getting the Government to Decline a *Qui Tam* Lawsuit

While most FCA lawsuits are filed by private-party relators, most large settlements and judgments come in those cases in which the government assumed direct control. Accordingly, a charged company's primary strategy should be to get DOJ to decline the case. While a relator may then continue litigating in the name of the government, the chances of success are substantially diminished.

While the government's decision to intervene or decline depends upon multiple factors including evidence of intent, the magnitude of economic injury, the nature and history of the defendant, *etc.*, a successful defense argument in a cybersecurity case necessarily depends upon showing "reasonable and appropriate" cybersecurity controls. Underlying that position a subject entity will benefit by formulating and presenting a documented record that includes:

- Written policies and procedures that evidence implementation of an applicable legal, regulatory and/or industry standards or frameworks;
- Evidence of delegated security responsibility;
- A written incident-response plan and breach-notification policy;
- Evidence of table top exercises demonstrating company preparedness;
- Evidence of operational implementation of technical security controls, proper system configurations, and routine system updates/patching;
- Evidence of strong authentication and role-based access controls;
- Evidence of secure software development lifecycle and change management practices;
- Periodic technical testing reports such as phishing exercises, vulnerability scans and penetration tests (preferably by an independent third party);
- Evidence of vendor diligence and ongoing management activities;

- Annual risk analysis (preferably by an independent third party);
- Go-forward risk management plan and evidence of remediation step taken;
- Evidence of training including content, participation logs, and any testing results;
- Evidence of system monitoring via log generation and review;
- Maintaining logs of security incidents and data breaches;
- Evidence of a multi-disciplinary team breach response including, investigation, containment, recovery, regulatory reporting and notice analysis, and cooperation with law enforcement; and
- Documenting governmental interests, *e.g.*, promoting public-private partnerships and advancing national security, directed at DOJ's declining to bring or assume an FCA case.

Establishing and documenting a robust cybersecurity program not only reduces the probability of DOJ instituting or taking over an FCA case, it both reduces the practical risk of a material data breach in the first place, and provides the basis for a successful defense of litigation on the merits.

IV. DOES THE DOJ INITIATIVE MAKE LEGAL AND POLICY SENSE?

A. Does the DOJ Cyber Initiative Productively Serve American Needs and Interests?

While cybersecurity has, in the past, largely focused on the need for privacy, recent incidents have demonstrated that, more than anything else, it is an issue of American national security that can only be satisfactorily addressed by a partnership between the government and the private sector. Indeed our national cybersecurity leadership is constantly stressing that need. This suggests that it does not make policy sense for a government agency to create *disincentives* to private cooperation by

encouraging expensive and time-consuming large-scale lawsuits that create market risk for companies that are putative victims of often-international criminals. A quick look at several important cybersecurity case studies suggests that it in fact does not. It also suggests a line of defense that companies might raise in getting DOJ to moderate its tone and to decline to initiate or enter into all but the most egregious FCA cases.

In early 2020, hackers secretly broke into Texas-based SolarWinds' systems and added malicious code into the company's "Orion" software system used by about 33,000 customers. The breach resulted from SolarWinds having unwittingly sent out software updates that included the hacked code. This attack, perpetrated by Russian hackers under Russian government protection, put numerous federal agencies at risk for months. No U.S. security agency discovered the breach. Rather, a private cybersecurity firm, FireEye, discovered the breach and then assisted federal officials in remedying it.

More recently, Colonial Pipeline, which operates the biggest gasoline conduit to the East Coast, supplying upwards of 45% of the East Coast's supply of diesel, gasoline, and jet fuel, was the victim of a ransomware attack that shut down transmission for days and caused the White House to declare a state of emergency in 17 eastern states. This attack was substantially ameliorated in a cooperative effort between Colonial and the FBI, which led to the exposure of the perpetrators and the

recovery of most of the ransom that was paid through an insurer.

And, in December 2021, American business and government experienced the widespread transmission of a bug contained in the vastly-popular "Log4j," an open-source chunk of code that helps software applications keep track of their past activities. The code appears on a large swath of Internet services. According to Jen Easterly, Security Director of CISA, "The log4j vulnerability is the most serious vulnerability that I have seen in my decades-long career."[20] Indeed, within days, our Iranian adversaries were detected making efforts to exploit the Log4j vulnerability.

These incidents, and thousands of others, particularly those involving ransomware, have created untold numbers of victims of computer crimes in the private sector, as well as in federal and state government agencies. These entities collectively have invested many billions of dollars in cybersecurity and adherence to a myriad of best practices described by government law enforcement and standards-setting organizations. Yet, increasingly novel forms of attack have proliferated, and especially among large companies and agencies, even those who maintain state of the art compliance programs, it is impossible to eliminate all human error, some of which provides a gateway to major data breaches.

Moreover, it has become clear that the fundamental threat is to national

[20] CNBC, *Eamon Javers Interview With Jen Easterly* (Dec. 16, 2021), https://www.cnbc.com/video/2021/12/16/log4j-vulnerability-the-most-serious-ive-seen-in-my-decades-long-career-says-cisa-director.html (last accessed Jan. 19, 2022).

security. While so-called "identity theft" is a bellwether among privacy advocates, the fact is that although class-action lawsuits are filed within moments of every major data breach, the individual members of these purported classes rarely can show injury in fact. This has not stanched the flow of litigation, notwithstanding efforts of businesses and others to get the courts more rigidly to enforce standing requirements. But the most demonstrable hit is to American institutions ranging from our elections, to the nature and tone of public discourse, and to the nation's critical infrastructure. If the fact that most of the largest data breach cases have been the result of actions of adversary nation-state-sponsored or protected groups is not enough, recent Russian activities directed at the Ukraine punctuate the threat that our own government continues to face.

This suggests that DOJ's strong threat of employing a hyper-technical application of the FCA might not serve national interests because it will create a disincentive for private companies and institutions to disclose cyber threat vectors and otherwise engage in what the government itself asserts is a necessary and effective partnership with the private sector.

B. Should the Government Encourage FCA Litigation When, in the Typical Data Breach Case, There Is No Demonstrable "Injury in Fact"?

Admittedly, a False Claims Act violation does not depend upon a showing that the government has suffered an economic injury. However, in considering whether to

bring or to intervene in FCA cases, or in encouraging potential *qui tam* relators to initiate them, the government has broad discretion. The exercise of that discretion should reflect the entirety of the government's interests and responsibilities. Cybersecurity has become a preeminent matter of national security that militates a need for cooperation between the public and private sector. That cooperation already is inhibited by the fact that the corporations and other entities that are the victims of cybercrimes, especially those with great monetary assets, already face class action lawsuits. Those lawsuits frequently fail because the putative class members are unable to show no more than speculative injury. However, the DOJ Initiative will be seen by relators and others as encouraging attempts to evade normal Article III standing and injury-in-fact requirements that the government insists be strictly applied in private suits against itself. *See, e.g., Lujan v. Defenders of Wildlife*, 504 U.S. 555 (1992). The Supreme Court has reiterated this standing prerequisite more generally. See *TransUnion LLC v. Ramirez*, 594 U.S. ___ (2021); *Spokeo v. Robins*, 578 U.S. 330 (2016),

Federal circuit courts post-*Spokeo* have been divided over the question of whether plaintiffs in a data breach class action can establish standing if they only allege a heightened "risk of future harm," which is the basic allegation in virtually all

class action data breach cases.[21] However, the view most consistent with Supreme Court precedent, and the one that the government uniformly urges, is that present, not speculative future injury is generally required. The FCA doesn't demand proof of injury at all, but its absence begs the question of whether it makes sense for DOJ to threaten or bring data breach cases under the guise of the FCA when there is no demonstrable present injury and there are countervailing policy interests that the Initiative would inhibit.

The Initiative likely will act to deter actual or potential victims of cyber attacks to share threat vector and data security information with a government that badly needs the private sector's help. Accordingly, it would make good policy sense for DOJ, in consultation with CISA, to clarify the Initiative to reflect that, with the exception of cases that demonstrate gross negligence and demonstrable potential to injure national security, the government will not bring or intervene in an FCA case in which there is no concrete present injury in fact such as economic loss. And where relators have brought FCA cyber cases with no showing of present injury in fact, and where private cooperation with the government as to national security issues is

[21] Compare *In re Horizon Healthcare Services Inc. Data Breach Litigation*, 846 F.3d 625 (3d Cir. 2017); *Galaria v. Nationwide Mut. Ins. Co.*, 663 F. App'x 384 (6th Cir. 2016); *Lewert v. P.F. Chang's China Bistro, Inc.*, 819 F.3d 963 (7th Cir. 2016); *In re Zappos.com, Inc.*, 884 F.3d 893 (9th Cir. 2018); *Tsao v. Captiva MVP Restaurant Partners, LLC,* No. 18-14959 (11th Cir. 2021); *See Attias v. CareFirst Inc.*, No. 16-7108 (D.C. Cir. Aug. 1, 2017), with *Katz v. Pershing, LLC*, 672 F.3d 64 (1st Cir. 2012); *Whalen v. Michaels Stores, Inc.*, 2017 WL 1556116 (2d Cir. 2017); *Beck v. McDonald*, 848 F.3d 262 (4th Cir. 2017); *Peters v. St. Joseph Servs. Corp.*, 74 F. Supp. 3d 847 (S.D. Tex. 2015); *In re: SuperValu, Inc., Customer Data Security Breach Litigation*, 870 F.3d 763 (8th Cir. 2017).

contemplated, the government should exercise its discretion and move to dismiss such actions.

Of course, DOJ might argue that the Supreme Court's decision in *Universal Health Services v. Escobar, supra,* upholding implied certification as a viable FCA theory, ends a discussion that is rendered unnecessary because the FCA doesn't require proof of economic loss. But that argument doesn't account for DOJ's saber-rattling and weaponization of the FCA against crime victims where only the defendant could demonstrate actual harm. We can expect DOJ to claim that responsible use of prosecutorial discretion will keep its actions limited to truly egregious violators. Inasmuch as even the most conscientious enforcers can't restrain *qui tam* relators who bring most FCA cases in any event, DOJ should do more to clarify and temper the Initiative's threat.

* * * *

In sum, the DOJ FCA Initiative is an unnecessary, and potentially counter-productive, measure. While American businesses, already deeply invested in cybersecurity, must prepare themselves for the possibility of novel and risky False Claims Act litigation, DOJ, in conjunction with other national security agencies, should issue guidance illustrating its intention to exercise its discretion in a manner that will not create a disincentive to private sector cooperation with the government to identify and thwart cyber threats.