How Health Care Cos. Can Prepare For DOJ's Cyberfraud Push

By **Kathleen McDermott and Mark Krotoski** (February 23, 2022)

Kathleen McDermott

Mark Krotoski

In late 2021, the U.S. Department of Justice announced its Civil Cyber-Fraud Initiative[1] as part of its effort to combat cybersecurity issues and hold government contractors and grant recipients accountable for putting government information or systems at risk.

This initiative is part of the Biden administration's May 2021 Executive Order No. 14028[2] to modernize cybersecurity.[3]

Among other tools, the initiative will utilize the False Claims Act[4] — the government's principal civil fraud enforcement tool — and its whistleblower provisions to investigate and pursue cybersecurity-related fraud involving government contracts and federal grant recipients.

With enforcement initially occurring largely through civil investigations applying the FCA in the broadest possible way, health care organizations should undertake a priority assessment of their cybersecurity status to ensure that their practices can withstand hacks, whistleblowers and government scrutiny.

Cyber Risk: A Reoccurring Threat With a New Twist

Cyber risk mitigation remains a top priority for organizations, particularly those in vulnerable industries such as health care, as a cyber incident not only causes business disruption and an economic impact, it also could be a potential significant exposure of liability under the FCA and other regulatory risks.

According to an IBM Corp. report, the average cost of a data breach in the health care industry was $9.23 million in 2021, an increase of 29.5% compared to 2020.[5]

Traditionally, the health care industry has not thought about cybersecurity with respect to the FCA, focusing more on risk associated with privacy-related statutes in contract management, risk management, or compliance standards and procedures.

And yet, most stakeholders are contractors, grantees or providers. Government contractors have long had special contract provisions related to cybersecurity, the risk of malware and other security risks, requiring certifications related to basic cybersecurity requirements.

According to Deputy Attorney General Lisa Monaco in an October 2021 press release, the initiative will

> hold accountable entities or individuals that put U.S. information or systems at risk by knowingly providing deficient cybersecurity products or services, knowingly misrepresenting their cybersecurity practices or protocols, or knowingly violating obligations to monitor and report cybersecurity incidents and breaches.

This last category is where there has been the most activity at the state attorney general level, where the victim can be pinned as the wrongdoer if there is a failure to monitor or report incidents and breaches.

DOJ officials also identify other important policy goals that may not be well associated with the traditional FCA objective of recovering money for the public fisc.

The initiative's FCA cyber enforcement goals are expected to focus on:

- Noncompliance with cybersecurity standards on goods and services provided by federal contractors, misrepresentation of security controls and practices, and failure to disclose violations, including failure to adhere to specific contractual requirements and failure to protect government data and unauthorized access;

- Misrepresentation of security controls and practices, such as false representations regarding system security plans and security controls; misrepresentations in the bidding process, known as fraudulent inducement; misrepresentations in periodic reporting and failure to disclose violations; and

- Failure to timely and accurately report suspected breaches of cybersecurity protocols.

It is important to note that a cybersecurity incident investigation is not a civil fraud investigation generated by a whistleblower or a big civil investigative demand under the FCA, and it may require significant updates to existing regulations and contract provisions to meet the relevant statutory definitions in the FCA, notably the definition of "obligation."

The initiative requires looking at cybersecurity from a different lens because of the much greater punitive consequences, and how it will affect enterprise risk management.

Implications for the Health Care Industry

The big question: Is the scope of liability expanded beyond what the health care industry currently has under federal and state privacy statutes?

The answer is yes, because the FCA is a very broad statute, and has both a lower burden of proof and whistleblower provisions that have proved successful in identifying regulatory violations.

Given this, FCA cyber exposure is now a significant parallel exposure to the Health Insurance Portability and Accountability Act and the Health Information Technology for Economic and Clinical Health Act on the federal level and state law breach exposures — except the scope of exposure is much broader, with graver consequences.

To date, this initiative directly affects all health care contractors, whether governed by the Federal Acquisition Regulation or not, as well as health plans, Veterans Affairs Federal Supply Schedule service suppliers, grantees in academic medical centers, and life science companies providing products to health care providers reimbursed by federal funds.

There is no reason to believe that the DOJ and whistleblowers will not push the envelope to

include all health care providers.

Another area that is expected to be affected is an organization's cybersecurity compliance program.

The health industry, for the most part, has predominantly been focused on managing fraud and abuse and regulatory compliance. Cybersecurity is highly technical, complex and not always on the checklist for a workplace compliance program.

As a result of this initiative, cybersecurity, as a practical matter, will become a major engine of the compliance department.

It is expected that breach notices, timeliness of reporting and completeness of disclosures will be expanded as an exposure under the FCA.

Therefore, it is critical for organizations to incorporate cyber notification procedures into more traditional compliance disclosure policies and procedures since, that is going to be the FCA liability.

Monaco said the DOJ would work with cyber experts in a whistleblower capacity, citing the technical complexity of cybersecurity, and the unique position allowing in-house or vendor IT personnel to be aware of potential cybersecurity exposures and noncompliance.

This is an unusual invitation for whistleblower collaboration that is designed to accelerate the civil cyberfraud initiative with immediate investigations and quick results.

The DOJ has set up special hotline reporting to get real-time tips of cyberthreats.

It is not clear that cyberthreats or even breaches will always correspond to provable FCA damages predictably enough to interest the whistleblower bar to invest in whistleblower cyberfraud investigations and filings.

The nature of such threats are often immediate and will require a whistleblower to act first for the public good and determine commercial personal interests later to avoid injury to U.S. information or data.

For the health industry, this reinforces the need to assess IT personnel and vendor issues for FCA whistleblowing, and expressly incorporate cybersecurity issues into compliance disclosure procedures.

FCA Cases and Settlements

While there has been an avalanche of FCA contractor cases, few have been focused on cybersecurity.

In 2020, the U.S. District Court for the District of Columbia dismissed U.S. ex rel. Adams v. Dell Computer Corp., a qui tam case alleging the sale of computer products with undisclosed cybersecurity hardware vulnerabilities.[6]

Interestingly, an Escobar analysis was applied on materiality, and the case was dismissed.

In another qui tam case, U.S. ex rel. Markus v. Aerojet Rocketdyne Holdings Inc., dismissed by the U.S. District Court for the Eastern District of California in 2019, the relator was an

insider — a former senior director of cyber, compliance and controls — who alleged noncompliance with contractual cybersecurity requirements.[7]

The district court allowed some FCA claims to survive motion to dismiss.

Lastly, in U.S. ex rel. Thomas v. Duke University, a $112.5 million FCA settlement[8] was reached in 2019 over false research grant certifications on research results and progress reports.

This case raises the question: Are specific certifications needed, or is cybersecurity inherently material to payment or receipt of government funds?

Looking forward, if cases are filed, they will most likely be litigated, as materiality and liability may not be easy to establish.

Using the FCA for regulatory or contract violations has had mixed success in the courtroom.

Proactive Measures to Manage Risk

Whether this initiative will lead to whistleblower tips and investigation activity, health care organizations should focus pragmatically on why cybersecurity is so critical to their business missions, including employee, patient, government and public trust.

Some specific steps health care organizations can take to mitigate risk include the following:

- Reevaluate cybersecurity response plans, update compliance program disclosure procedures to expressly encourage internal reporting of cyber concerns by employees and contractors, and establish a cybersecurity compliance committee to benchmark all contract and regulatory requirements;

- Assess and update relevant contracts to account for FCA exposure, assess whistleblower management issues and implement training, particularly with respect to ransomware and how to continue servicing clients without interruption;

- Plan an independent review of cybersecurity exposure in compliance program work and evaluate insurance policies for cyber FCA coverage;

- Update notification procedures to include assessment of disclosure to the DOJ's Civil Fraud Section or local U.S. attorney's offices; and

- Organize an incident response team that includes a forensic specialist; public relations team; customer and business relations; outside counsel (legal guidance,

direct investigation); auditor; board of directors; management and other third parties.

Conclusion

The initiative is a prominent, high-profile move by the DOJ that creates added pressure on health care entities.

Health care organizations should treat this DOJ initiative as a starting bell for improving and updating cybersecurity practices.

As a result, an uptick in both cyber reporting and subpoenas related to this can be anticipated.

Health care organizations should use the necessary safeguards, as well as ensure they are working with vendors that do the same.

Kathleen McDermott is a partner at Morgan Lewis & Bockius LLP. She previously served as an assistant U.S. attorney and as a DOJ health care fraud coordinator.

Mark L. Krotoski is a partner at Morgan Lewis. He previously served in the U.S. Department of Justice as assistant chief of the Antitrust Division's National Criminal Enforcement Section and national coordinator for the Computer Hacking and Intellectual Property Program.

[1] https://www.justice.gov/opa/pr/deputy-attorney-general-lisa-o-monaco-announces-new-civil-cyber-fraud-initiative.

[2] https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/.

[3] https://www.whitehouse.gov/briefing-room/statements-releases/2021/08/25/fact-sheet-biden-administration-and-private-sector-leaders-announce-ambitious-initiatives-to-bolster-the-nations-cybersecurity/.

[4] https://www.justice.gov/opa/speech/acting-assistant-attorney-general-brian-m-boynton-delivers-remarks-cybersecurity-and.

[5] https://www.ibm.com/security/data-breach.

[6] In re US ex rel. Adams v. Dell Computer, No. 15-cv-608 (D.D.C. 2020).

[7] In re US ex rel. Markus v. Aerojet Rocketdyne Holdings, Inc., 381 F. Supp. 3d 1240 (E.D. Cal. 2019).

[8] https://www.justice.gov/opa/pr/duke-university-agrees-pay-us-1125-million-settle-false-claims-act-allegations-related.