Published on *The National Law Review* https://natlawreview.com

DOJ Signals Intent to Hold Government Contractors Accountable for Lax Cybersecurity Standards

Article By:

Robert (Rob) M. Duncan

Lindsay K. Gerdes

Michael B. Stuart

It is imperative that companies with government contracts, or those receiving federal grant funding, ensure that they have adequate cybersecurity protocols in place. The announcement by the Department of Justice (DOJ) of the Cyber Fraud Initiative strongly signals its intent to be aggressive in holding government contractors with lax cybersecurity standards and controls accountable. Further, the announcement of the initiative will undoubtedly lead to more qui tam lawsuits filed by private actors seeking to share in any monetary recovery for reporting deficient cybersecurity practices or data breaches. Failing to implement robust cybersecurity measures that are in compliance with federal requirements could result in significant monetary penalties and litigation costs for companies. Additionally, knowingly providing false information to the government could lead to criminal prosecution and fines.

Recently, the Department of Justice (DOJ) announced the creation of two new enforcement programs to combat cyber fraud. On Oct. 6, 2021, the DOJ unveiled a new Civil Cyber Fraud Initiative (the Cyber Fraud Initiative) aimed at using civil enforcement actions under the False Claims Act (FCA) to "combat new and emerging cyber threats to the security of sensitive information and critical systems."[1]

The FCA, first enacted during the Civil War to combat fraud by contractors supplying the military, awards damages and levies penalties against parties who make false claims to the government in connection with obtaining federal funds and property through government programs. The Cyber Fraud Initiative will now hold accountable companies that are government contractors and/or federal grant recipients and that fail to report data breaches or to follow required security standards.[2]

Deputy Attorney General Lisa Monaco warned of "very hefty fines" for such companies and emphasized the DOJ's commitment to protecting whistleblowers who bring those violations and failures forward[3]. She noted, "For too long, companies have chosen silence under the mistaken belief that it is less risky to hide a breach than to bring it forward and to report it."[4]

The FCA also contains a whistleblower provision encouraging private citizens to report suspected misconduct and file suits on behalf of the government (called "*qui tam*" suits) against those who defraud it. The FCA has been described as "one of the most important tools [the government has] to fight healthcare fraud, grant fraud, financial fraud, government contracting fraud, and many other types of fraud on the taxpayer."[5] Private citizens who file successful qui tam suits are eligible to receive a portion of the government's recovery.

According to the DOJ, "the Cyber Fraud Initiative seeks to "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."[6] In an effort to encourage companies to proactively report breaches, Deputy Attorney General Monaco expressed the DOJ's commitment to partnering and helping self-reporting companies.[7] "Victims can help avoid liability through working with law enforcement, and those companies that stand with us, and work with us, will see that we stand with them in the aftermath of an incident," she said.[8] She further remarked, "If companies don't come forward in this threat environment . . . I think legitimate questions will be, and should be asked of companies, 'Why didn't you come forward and help prevent the next victim?"[9]

On the same day, the DOJ announced the creation of a National Cryptocurrency Enforcement Team (the Crypto Team), designed to "tackle complex investigations and prosecutions of criminal misuses of cryptocurrency," including acts of money laundering.[10] The Crypto Team "will also assist in tracing and recovery of assets lost to fraud and extortion, including cryptocurrency payments to ransomware groups."[11] Both the Cyber Fraud Initiative and the Crypto Team stem from the DOJ's review of its existing cyber capabilities with the goal of "enhanc[ing] and expand[ing] the Justice Department's efforts against cyber threats."[12]

The creation of the Cyber Fraud Initiative is consistent with the government's recent approach in using the FCA aggressively as a means to protect the country against cyber threats. Traditionally, "the [FCA] is used by government to tackle civil lawsuits over false claims made in relation to federal funds and property connected with government programs."[13] In recent years, under both the Obama and Trump administrations, the government has successfully used the FCA in bringing cases against various professional industries and corporations, including military contractors, medical professionals, health care providers, and others for billing-related fraud and for submitting false claims.

Notably, in a speech at the Federal Bar Association's Qui Tam Conference in February 2021, Acting Assistant Attorney General Brian M. Boyton outlined the Biden administration's intention to expand the use of the FCA into other areas, including COVID-19-related fraud, fraud targeting seniors, fraud surrounding electronic health records, telehealth, and opioids.[14] In the speech, Boynton also previewed the government's use of the FCA to address cybersecurity, noting, "It is not difficult to image a situation where [FCA] liability may arise" from a government contractor failing "to comply with required security standards."[15]

FOOTNOTES

[1] U.S. DOJ, "Deputy Attorney General Lisa O. Monaco Announces New Civil Cyber-Fraud Initiative," October 6, 2021

[2] Id.

[3] Jason Miller, "DoJ's new Civil Cyber-Fraud Initiative to hold contractors accountable for cybersecurity," Federal News Network, October 6, 2021

[4] Id.

[5] U.S. DOJ, "Acting Assistant Attorney General Brian M. Boynton Delivers Remarks at the Federal Bar Association Qui Tam Conference," February 17, 2021

[6] U.S. DOJ, "Deputy Attorney General Lisa O. Monaco Announces New Civil Cyber-Fraud Initiative," October 6, 2021

[7] U.S. DOJ, "DAG Monaco Speaks at Criminal Division Cybersecurity Roundtable on 'The Evolving Cyber Threat Landscape,'" October 20, 20201

[8] Id.

[9] Id.

[10] U.S. DOJ, "Deputy Attorney General Lisa O. Monaco Announces National Cryptocurrency Enforcement Team," October 6, 2021

[11] Id.

[12] U.S. DOJ, "Deputy Attorney General Lisa O. Monaco Announces New Civil Cyber-Fraud Initiative ," October 6, 2021

[13] Ax Sharma, "US gov't will slap contractors with civil lawsuits for hiding breaches," Ars Technica, October 7, 2021

[14] U.S. DOJ, "Acting Assistant Attorney General Brian M. Boynton Delivers Remarks at the Federal Bar Association Qui Tam Conference," February 17, 2021

[15] Id.

National Law Review, Volume XI, Number 295