DOJ Announces New Cyber-Fraud Initiative Promoting False Claims Act Enforcement Against Contractors and Grantees Failing to Follow Cybersecurity Standards

Written by Anthony D. Mirenda, Stephen Garvey, Natalie Panariello

October 15, 2021

As we anticipated last spring, the Department of Justice (DOJ) has signaled that it will utilize civil enforcement of the False Claims Act (FCA) to address new and emerging cybersecurity threats. On October 6, 2021, Deputy Attorney General Lisa Monaco announced the launch of a new cyber-fraud initiative led by the Fraud Section of DOJ's Commercial Litigation Branch. The new initiative will focus FCA enforcement against federal government contractors or grant recipients who fail to follow required cybersecurity standards. Essentially, DOJ is using the threat of the FCA to increase the pressure on companies to adopt and maintain cybersecurity best practices.

Monaco characterized the cyber-fraud initiative as the "direct result" of a 120-day review of cybersecurity practices launched by the Department in May. Prior to the review's launch, Monaco broadly identified ransomware attacks and data breaches carried out by criminal actors or hostile states, like the 2020 SolarWinds hack, as areas of concern. DOJ asserts that the initiative will incentivize building broad resiliency against cybersecurity intrusions and will ensure that companies investing in meeting cybersecurity standards are not at a competitive disadvantage. At the same time, DOJ emphasized that the initiative will hold government contractors and grantees to their commitments to protect government information and infrastructure. Given this context, last week's announcement makes clear that government contractors who become the victims of cyberattacks may also face FCA liability.

Under the FCA, any person who knowingly submits a false or fraudulent claim for payment to the United States government is liable for treble damages plus a per-claim monetary penalty. In addition to these civil penalties, those who violate the FCA can face criminal prosecution. Among other things, the FCA prohibits knowingly making a false statement material to a claim for payment from the government. Where cybersecurity protections are a material requirement of payment or participation under a government program or contract, the knowing failure to establish and maintain such protections could give rise to FCA liability.

The statute allows civil claims to be brought not only by the government, but also by private parties who sue in the name of the government and are eligible to receive a percentage of the money recovered. This bounty system is a powerful enforcement tool, creating a substantial incentive for whistleblowers and others to bring claims.

FCA cases brought pursuant to DOJ's new initiative may punish victims of cyberattacks for inadequate cybersecurity protections. The most recent ransomware prevention best practices published by the Cybersecurity and Infrastructure Security Agency set out one example of what the government expects companies to adopt.

Foley Hoag offers comprehensive resources to help you minimize the threat of a cyberattack and to help you understand your legal obligations should one occur.

- **If you are a business**, protect yourself against attacks by ensuring that your cybersecurity policies are updated and actively implemented, and build compliance steps into your incident response plan. Foley Hoag's Cybersecurity Incident Response Team and the Privacy & Data Security practice group can advise on safeguarding company records, financial information, and other valuable information assets, and developing an effective incident response plan.
- **If you are a victim**, Foley Hoag's Cybersecurity Incident Response Team and White Collar Crime & Government Investigations practice group can help you navigate your legal obligations after being attacked, including addressing any False Claims Act exposure.

RELATED PRACTICES

- White Collar Crime & Government Investigations
- Privacy & Data Security