Skadden

Cybersecurity and Data Privacy Update

July 2, 2024

If you have any questions regarding the matters discussed in this memorandum, please contact the following attorneys or call your regular Skadden contact.

Bradley A. Klein
Partner / Washington, D.C.
202.371.7320
bradley.klein@skadden.com

Jessie K. Liu
Partner / Washington, D.C.
202.371.7340
jessie.liu@skadden.com

William E. Ridgway
Partner / Chicago
312.407.0449
william.ridgway@skadden.com

David A. Simon
Partner / Washington, D.C.
202.371.7120
david.simon@skadden.com

John A.J. Barkmeyer
Counsel / Washington, D.C.
202.371.7306
john.barkmeyer@skadden.com

One Manhattan West
New York, NY 10001
212.735.3000

Contractors Settle Cyber Fraud Claims Alleging Ignored Security Measures

Two recent settlements under the False Claims Act (FCA):

- Signal enhanced risk around cybersecurity for recipients of federal funds.
- Underscore the need to assess compliance with cybersecurity requirements and contractual obligations.
- Demonstrate the need for contractors to oversee delegated security measures to ensure they meet contractual standards.

Background

On May 13, 2024, the Department of Justice (DOJ) entered into settlements with contractor Guidehouse Inc. and its subcontractor Nan McKay and Associates (NMA), resolving FCA allegations that they failed to meet cybersecurity requirements in Guidehouse's contract to provide technology and services implementing a federally funded New York state emergency rental relief program.[1]

Guidehouse, a consulting firm that advises on a range of topics including cybersecurity, had primary responsibility for the program's implementation as a whole; it hired NMA to develop and maintain the technology product that supported users' online applications to the program. Guidehouse's contract required the company to perform industry-standard cybersecurity tests and scans in the pre-product environment, before the application platform went live. Guidehouse delegated this responsibility to NMA, retaining its own right to conduct application and webserver testing and scanning, but as both of the defendants admitted, NMA could not make one of its testing tools function prior to the launch of the platform as provided in the contract. Guidehouse attempted to perform the testing itself, using a different tool, but also failed to make it function prior to launch.

The platform ultimately became active without either entity performing the testing. The state took the platform offline after 12 hours of operation when it discovered that some applicants' personal information had become accessible by commercial internet search engines, triggering a security breach protocol in the contract.

FCA claims and settlements

DOJ asserted FCA claims premised on two central admissions from the defendants:

- Both defendants admitted that they could have noticed and prevented the accessibility of applicants' personal information to search engines had they tested the platform according to the contract.

[1] DOJ has publicly released the settlements with Guidehouse and with NMA on its website.

Contractors Settle Cyber Fraud Claims Alleging Ignored Security Measures

- Guidehouse also admitted that it used a third-party data cloud software program that the contract did not authorize to store personal information and administer a program "adjacent to" the New York program.

In settlement of the FCA claims, Guidehouse agreed to pay $7.6 million, and NMA agreed to pay $3.7 million.

Implications

These settlements reflect DOJ's increased scrutiny of cybersecurity practices under its Civil Cyber-Fraud Initiative — ongoing since October 2021 — which has resulted in several settlements.[2] These cases underscore the government's willingness to police cybersecurity measures with the punitive remedies of the FCA.

They also reveal that it is not the technology expert alone that bears the risk of such investigations; even a prime contractor that delegates cybersecurity responsibilities to a subcontractor may be at risk if the subcontractor fails to fulfill its duties — here, for more than double the liability of the subcontractor itself. A contractor cannot necessarily trust that its subcontractor's cybersecurity measures are adequate without verifying those measures itself, and the government may demand particular responsibility in these scenarios from contractors, like Guidehouse, who consult elsewhere on cybersecurity issues.

These cases suggest that companies with involvement in federally funded contracts should closely monitor the cybersecurity implications of *all* aspects of their contracts, including an assessment of subcontractors. They should also signal to contractors' security personnel that contractual requirements — rather than industry practice or operational necessities — are the standards by which an organization must measure its FCA liability risk.

[2] For example, read our October 30, 2023, alert: Cyber Fraud Alleged by Former CIO for Purported Noncompliance With DoD Cyber Requirements.