New York Law Journal
SERVING THE BENCH AND BAR SINCE 1888
WWW.NYLJ.COM
An ALM Publication
VOLUME 267—NO. 29
MONDAY, FEBRUARY 14, 2022

Outside Counsel

False Claims Act Liability for Cyber Breaches: Limiting the Risk

By **Laura K. Schwalbe**

Nobody likes admitting they have been hacked. It can scare away customers and investors, invite lawsuits, and lead to regulatory scrutiny. For years, a patchwork of federal and state rules governed when and how organizations disclose cyber breaches. Layered atop those rules, for government contractors and program participants, have been the specific and evolving standards in contracts and rules for reporting cyber incidents and implementing safeguards. But law enforcement has lamented the low levels of reporting and asked the business community to come forward and report breaches, so that law enforcement can better understand and assess cyber threats.

Now, the federal government is changing its approach. The U.S. Department of Justice is turning to threats of severe financial repercussions, expensive litigation, and reputation-busting press releases—in other words, the False Claims Act. On Oct. 6, 2021, the Justice Department's number two official, Deputy Attorney General Lisa Monaco, announced a new Civil Cyber-Fraud Initiative. "For too long," Monaco declared, "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." Monaco announced, "[T]hat changes today" because, as part of the initiative, the Justice Department "will use [its] civil enforcement tools to pursue companies, those who are government contractors who receive federal funds, when they fail to follow required cybersecurity standards—because we know that puts all of us at risk."

The focus of the initiative is the use of the False Claims Act against government contractors, grantees, and program participants who violate mandatory cyber compliance and reporting obligations.

The False Claims Act is a potent tool to ratchet up the consequences of a knowing or reckless failure to comply with material government contract and program rules. The Act imposes treble-damages penalties and personal liability on high-level executives. False Claims Act investigations are often lengthy and expensive. And the False Claims Act includes a whistleblower provision, which rewards private parties (relators) with knowledge of wrongdoing who identify and pursue claims on behalf of the federal government.

Anticipate Denials For Violations

Not every violation of a legal requirement triggers False Claims Act liability, but the federal government appears engaged in an effort to make sure that breaches will trigger such liability. As the law stands, liability may apply when an organization knowingly violates a requirement material to the government's payment decision.

LAURA K. SCHWALBE *is senior associate at Harter Secrest & Emery, where she practices in the areas of privacy and data security, government and internal investigations, commercial litigation and corporate governance and compliance. She can be reached at lschwalbe@hselaw.com.*

To prove materiality, the Justice Department often cites cases in which it has refused to pay contractors or reimburse grantees or program participants for violation of a particular requirement. Because the Justice Department is focused on cyber violations, they are probably pressing agencies to assist them in building a track record of payment denials, even for inadvertent or negligence violations, to shore up the government's materiality position. If so, before organizations see False Claims Act treble damages for knowing or reckless violations of cyber requirements, they are likely to see payment denials.

Understand the Requirements

Now is the time for organizations to develop strategies to ensure cybersecurity compliance and manage and mitigate False Claims Act risks related to inevitable shortfalls in cybersecurity.

Organizations should inventory the cybersecurity requirements they have agreed to in government contracts, grants, or program agreements. Contractors must carefully read their contracts, including any addenda or exhibits and incorporated provisions of law. Grantees must review their grants. And program participants must understand the program rules governing receipt of funds in federally-funded programs.

The Justice Department has highlighted its areas of focus: (1) failures to timely report a breach as required and (2) failures to implement cybersecurity standards. Organizations should pay special attention here and anticipate increasingly emphasized duties to report breaches or implement security protocols.

Organizations should also assess what additional regulatory regimes apply. Sometimes, the government takes the position that compliance with other rules, laws, or regulatory regimes is material to payments. Some government contracts, grants, and program agreements include a blanket "compliance with all applicable laws" provision where an organization certifies it is complying with all applicable laws.

Now is the time for organizations to develop strategies to ensure cybersecurity compliance and manage and mitigate False Claims Act risks related to inevitable shortfalls in cybersecurity."

There are also a number of cybersecurity-related regulations that organizations may not know apply to them. For example, the recently-enacted New York Stop Hacks and Improve Electronic Data Security Act (SHIELD Act) applies to any person or businesses that owns or licenses private information of a New York resident. It expands the definition of what is considered a reportable breach and imposes new data security requirements in the form of reasonable administrative, technical, and physical safeguards.

Audit and Prepare

To ensure they have the necessary infrastructure to comply with cybersecurity requirements, organizations should assess existing internal policies, procedures, and plans. While there are a number of important policies and procedures that are key in this area, three of the most important for these purposes are: (1) a risk assessment; (2) a Written Information Security Program (WISP); and (3) an Incident Response Plan (IRP).

The best risk assessments will bring together knowledgeable individuals from each area of an organization to identify risks, quantify likelihood and severity, and outline mitigation factors. The format of a risk assessment will vary based on the size and type of organization, however many businesses adopt a form similar to NIST SP 800-30, which provides guidance for conducting risk assessments of federal information systems.

A WISP is a wrap document, required in some states, which details an organization's overall information security program. It will typically include an overview of regulatory requirements and exceptions, list and organize existing policies under administrative (or organizational), physical, and technical safeguards, and expressly reference, and incorporate the risk assessment.

Lastly, an IRP details how a business will respond in the event of a cyber incident. Businesses often build the IRP around an established framework, such as NIST SP 800-61,

which contains recognized incident response domains that have been expressly adopted by regulators or tacitly incorporated into regulations. These three documents, the IRP, a risk assessment, and WISP, are among the first things a regulator or litigant will ask to review following a cybersecurity incident and it is important that businesses have robust, accurate, and up-to-date versions of each.

Bringing in an experienced outside consultant to help test processes and procedures can help businesses identify issues and pitfalls before a real incident occurs. Industry and legal experts can provide guidance on whether an organization has adequately catalogued the requirements to which it is subject. Outside experts can take a critical eye to key documents like the WISP and risk assessment to identify holes and weaknesses. IRPs can be tested by experienced outsiders in such a manner that a business feels like it is responding to a real incident.

Insure Against Risks

Even the best organizations fall short at times. To mitigate, organizations should review insurance coverage. It is important to review policies not only for losses arising from breaches and other cyber incidents, but also specifically for False Claims Act liabilities and defense costs.

Because False Claims Act investigations are expensive, organizations should consider purchasing coverage for investigation defense fees triggered by the receipt of a subpoena or target letter as well as considering what exclusions may apply. In particular, as the federal government becomes more aggressive in demanding admissions of wrongdoing, organizations should review the scope of any exclusions of coverage that might be triggered by such admissions.

Listen to Internal And External Concerns

Another procedure organizations should implement is an internal complaint or reporting process. As noted above, the False Claims Act contains a robust whistleblower process. Many whistleblowers try to raise concerns internally and only proceed to a False Claims Act proceeding if they feel their concerns are not taken seriously and addressed.

> The focus of the initiative is the use of the False Claims Act against government contractors, grantees, and program participants who violate mandatory cyber compliance and reporting obligations.

Ensuring a robust process where employees know they can raise concerns and receive a response can provide organizations with the opportunity to detect and address issues and reduce the risk of whistleblower actions.

Educate Leaders On Personal Liability

The False Claims Act is particularly threatening (and effective) because it provides for individual liability. Anyone who submits a false statement or false claim for payment, as well as anyone who causes such a submission, can be personally liable to the same extent as an organization.

Leaders will often expose themselves to such personal liability. Responsible organizations should educate their leaders on this potential liability. Individuals who understand they are personally on the hook may internalize the risks of noncompliance. Organizations should support these individuals with access to the resources they need to feel comfortable about the organization's compliance.

Cybersecurity considerations are already top-of-mind for many business leaders, and businesses that contract with the federal government are aware of False Claims Act liability risks. Businesses, particularly those that contract with the government, should do as much as possible to ensure compliance with the myriad cybersecurity requirements to avoid potential False Claims Act investigations and liability.