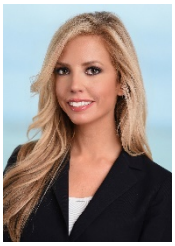
Lawyer Insights

Insurance Tips For Mitigating DOJ Cyber Initiative Risks

By Andrea DeField, Sean O'Connell and Geoffrey Fehling
Published in Law360 | November 19, 2021



The U.S. Department of Justice recently announced its new Civil Cyber-Fraud Initiative — a plan to prosecute cybersecurity-related fraud through civil actions using the False Claims Act.

Fortunately for companies and executives involved in FCA matters, directors and officers, or D&O, and cyber insurance can help defray substantial costs of defense and even liability for settlements of FCA actions alleging failures in cybersecurity procedures, disclosures and controls, like those envisioned by the DOJ's new initiative.

What is the Civil Cyber-Fraud Initiative?

Per the DOJ, this new task force, announced on Oct. 6, "will utilize the False Claims Act to pursue cybersecurity related fraud by government contractors and grant recipients."[1]

The FCA prohibits the knowing submission of false or fraudulent claims for payment to the federal government, as well as false certifications of compliance with material statutory, regulatory or contractual requirements. The FCA also includes a whistleblower provision that allows individuals, known as relators, to file suit on behalf of the government — called qui tam actions — to assist the government in pursuing civil action under the FCA.

In return, relators share in a portion of any recovery and are protected from retaliation. Violators of the FCA are subject to treble damages and civil penalties of up to $23,331 per false claim. Damages can be reduced through negotiation and if the company self-discloses fraudulent activity.

Given that many qui tam actions allege dozens — or even hundreds — of false claims, the corresponding civil penalties and mandatory multiplied damages can be substantial

Since 1986, the federal government has recovered over $64 billion, with $2.2 billion recovered in 2020 alone — not including billions of additional dollars in settlements that are not yet final or did not become final before the end of the fiscal year.[2] Those staggering settlement figures also fail to capture the substantial legal fees and expenses incurred by companies and individuals targeted in investigations and enforcement actions, which in many instances can run into the multiple millions of dollars.

The government's use of the FCA as a vehicle to combat fraudulent and false claims is not new.

The statute dates back to the Civil War era but was strengthened by Congress in 1986 and is now used frequently to combat wrongdoing against companies and, increasingly, individuals in a wide variety of

claims, ranging from health care and procurement fraud to bid rigging and fraud in public assistance programs.

While the DOJ's use of the FCA to regulate fraud in the cybersecurity industry is new, it is a natural expansion of the statute's reach across all business sectors connected to government programs.

In the DOJ's recent press release discussing the initiative, U.S. Deputy Attorney General Lisa Monaco highlighted three types of cybersecurity-related conduct that the DOJ will pursue under the FCA:

- Knowingly providing deficient cybersecurity products or services;
- Knowingly misrepresenting their cybersecurity practices or protocols; and/or
- Knowingly violating obligations to monitor and report cybersecurity incidents and breaches.

In speaking about the cyber fraud initiative, U.S. Acting Assistant Attorney General Brian Boynton recently said that False Claims Act enforcement and whistleblower reporting will help spur compliance by contractors and grantees.[3]

How can insurance help?

Fortunately for companies and their directors and officers named in FCA qui tam actions, insurance can help mitigate the cost of defending against and even settling such actions with regulators. To maximize coverage, policyholders should ensure that they have broad coverage for cyber-related suits and investigations under both their cyber insurance policies and D&O liability policies.

Here are five tips policyholders should consider at renewal to help maximize coverage for potential FCA claims alleging cybersecurity-related fraud.

1. Procure broad investigations coverage.

Oftentimes, the DOJ will issue civil investigative demands, or CIDs, to persons and companies as an information-gathering tool prior to formally filing a False Claims Act action in court. Responding to a CID or subpoena can be extremely expensive and time-consuming, resulting in substantial legal fees and other costs, even where the investigation is closed or the enforcement action does not result in any settlement or adverse ruling.

While certain liability policies can provide coverage for FCA investigations and enforcement actions, many policyholders fail to procure express coverage — or investigate the potential for coverage — for these costs on either or both their cyber or D&O insurance policies.

On cyber policies, coverage for FCA matters is often referred to as regulatory action coverage. While

regulatory action coverage typically is broad enough to apply to the government's CIDs, subpoenas and other information requests, the relevant insuring agreement may nonetheless require allegations of a privacy or security wrongful act or failure, which may not encompass alleged misrepresentations made to a government agency or deficiencies in cybersecurity products and services that are not tied to a breach of the insured's system.

Accordingly, policyholders should request broad investigations coverage, including for informal investigations and subpoenas that do not identify a target or do not identify a purported wrongful act. Policyholders should also seek broad investigations coverage on their D&O policy — a request that will be more difficult for public companies than private companies — since coverage under D&O forms may not require allegations of an actual privacy or security breach in order to trigger coverage.

2. Eliminate exclusions for claims brought "by or on behalf of" governmental entities.

Focusing on the adequacy and scope of coverage grants may not be enough. Policyholders also must carefully review any exclusions or limitations on coverage for governmental actions.

For example, some cyber policies contain exclusions for claims brought by or on behalf of local, state, federal or foreign governments, agencies or offices, which insurers could rely on to preclude coverage for a relator's qui tam action brought on the government's behalf. Any problematic exclusions should be eliminated at renewal or — where elimination is not possible — at least revised to apply only to claims brought by the government in order to not apply where the government chooses not to intervene in a relator's suit.

3. Limit conduct exclusions.

Cyber and D&O liability policies typically include so-called conduct exclusions, which preclude coverage for claims arising out of fraudulent or criminal conduct or the willful or deliberate violation of the law. While some form of conduct exclusion is often unavoidable, it can be narrowed significantly, especially to preserve the insurer's defense cost reimbursement prior to a final, adverse ruling against an insured.

Policyholders should ensure that conduct exclusions in both D&O and cyber policies contain final adjudication requirements that do not bar coverage unless and until it is determined that the insured committed such prohibited conduct by a final, nonappealable adjudication against the insured in the underlying proceeding — as opposed to any proceeding, such as a declaratory judgment brought by the insurer.

Conduct exclusions should also be subject to a severability requirement so that a final adjudication against one insured will not automatically bar coverage for all other insureds, regardless of whether the other insureds committed the prohibited conduct.

4. Confirm that "insured versus insured" exclusions contain a whistleblower claims exception.

Cyber and D&O policies often include "insured versus insured" exclusions, which as the name suggests bar coverage for claims brought by or on behalf of one insured against another insured.

While language varies widely between policies, it is intended to discourage company infighting by removing intracompany disputes from coverage and to avoid collusion. In practice, however, broadly

worded insured versus insured exclusions can apply to a much wider range of circumstances, which is why most policies include numerous carveouts for particular types of claims.

Two modifications in particular are critical to maximizing coverage for companies and directors and officers targeted in qui tam actions.

First, policyholders should ensure that any insured versus insured exclusions be limited to claims brought by the insured company, preserving coverage — especially "Side A" coverage for loss not indemnified by the company — for insured individuals.

Second, exclusions should contain an express carveout for claims brought by an insured acting as a whistleblower. Otherwise, a policy's exclusion prohibiting coverage for claims brought by insureds may be construed to apply to FCA claims in qui tam actions brought by employee whistleblowers.

5. Policies should cover FCA damages.

As stated above, remedies for FCA violations include treble damages, civil penalties and an award of relator's attorney fees. Historically, some insurers have argued that FCA settlements do not constitute covered loss under D&O policies. However, several courts have rejected that defense, finding coverage for defense costs incurred and settlement payments paid in FCA matters.

For example, in the U.S. District Court for the Northern District of Illinois case Astellas US Holdings Inc. v. Starr Indemnity & Liability Co. decided on Oct. 8, an insurer argued that the policyholder's FCA settlement constituted uninsurable restitution or disgorgement, which was excluded from the D&O policy's definition of loss.[4]

The Illinois federal court rejected this argument and held first that the insurer — not the policyholder — should bear the burden of proof where it seeks to avoid coverage for settlement payments based on the definition of "loss," even where language is not contained in an express policy exclusion; and second, that the remedies available to the government under the FCA do not include uninsurable disgorgement.

The court found that the FCA allows only for civil penalties and compensatory damages, and that the settlement payment at issue was insurable, notwithstanding a "restitution" label in the settlement agreement, which is often used in FCA settlements to comply with the Tax Cuts and Job Act.

To help avoid an insurer's argument that treble damages or penalties paid in settlement of an FCA action are uninsurable, corporate policyholders should (1) ensure express coverage for treble damages, fines, and penalties in the definition of "loss"; (2) negotiate a "most favored jurisdiction" clause, such as one stating that multiple damages, civil fines or penalties will be covered where insurable by the applicable law which most favors coverage; and (3) ensure coverage for plaintiff's attorney fees so that insurance will cover the relator's fee claim.

Conclusion

Between 2001 and 2020, the number of government FCA actions more than doubled, from about 400 to more than 900. Increased government spending during the pandemic, such as through the Paycheck Protection Program and other pandemic-related assistance programs, has only heightened the government's attention to potential FCA violations.

Insurance Tips For Mitigating DOJ Cyber Initiative Risks
By Andrea DeField, Sean O'Connell and Geoffrey Fehling
Law360 | November 19, 2021

In 2020, for example, the government initiated 250 FCA actions, nearly double the yearly average. D&O and cyber insurance are important risk mitigation tools available to companies and their officers and directors to combat rising FCA exposures, including those arising from the Civil Cyber-Fraud Initiative.

Notes

1. Press Release, U.S. Dep't of Justice, Deputy Attorney General Lisa O. Monaco Announces New Civil Cyber-Fraud Initiative (Oct. 6, 2021), https://www.justice.gov/opa/pr/deputy-attorney-general-lisa-o-monaco-announces-new-civil-cyber-fraud-initiative

2. See Press Release, U.S. Dep't of Justice, Justice Department Recovers Over $2.2 Billion from False Claims Act Cases in Fiscal Year 2020 (Jan. 14, 2021), https://www.justice.gov/opa/pr/justice-department-recovers-over-22-billion-false-claims-act-cases-fiscal-year-2020.

3. Remarks as Delivered, U.S. Dep't of Justice, Acting Assistant Attorney General Brian M. Boynton Delivers Remarks at the Cybersecurity and Infrastructure Security Agency (CISA) Fourth Annual National Cybersecurity Summit (Oct. 13, 2021), https://www.justice.gov/opa/speech/acting-assistant-attorney-general-brian-m-boynton-delivers-remarks-cybersecurity-and.

4. Astellas US Holdings Inc. v. Starr Indemnity & Liability Co., No. 17-cv-08220 (N.D. Ill. Oct. 8, 2021).

Andrea DeField *is a partner in the firm's Insurance Coverage group in the firm's Miami office. Andrea finds risk management, risk transfer, and insurance recovery solutions for public and private companies. She can be reached at +1 (305) 810-2465 or adefield@HuntonAK.com.*

Sean B. Connell *is a counsel in the firm's White Collar Defense group in the firm's Richmond office. Having directed both criminal and civil Department of Justice investigations, Sean is uniquely situated to provide compliance counseling, conduct internal investigations, navigate and counter government investigations and, if need be, defend government allegations at every stage of litigation. He can be reached at +1 (804) 788-7222 or soconnell@HuntonAK.com.*

Geoffrey B. Fehling *is Counsel in the firm's Insurance Coverage group in the firm's Boston office. Geoff represents corporate policyholders and their officers and directors in insurance coverage disputes involving directors' and officers' (D&O), errors and omissions (E&O), and other professional liability claims, cybersecurity and data breaches, representations and warranties, employee theft and fidelity claims, government investigations, breach of fiduciary duty, environmental liabilities, and property damage. He can be reached at +1 (617) 648-2770 or gfehling@HuntonAK.com.*