Managing Cybersecurity Compliance and False Claims Act Enforcement Risks

The Department of Justice is increasingly using the **False Claims Act** to pursue misrepresentations about cybersecurity practices. Alleged failures to implement mandated controls can now lead to multimillion-dollar settlements and **high-stakes** civil fraud investigations.

WHEN TO TAKE ACTION

You should contact a **white collar crime lawyer** if:

- **You are asked to certify cybersecurity compliance:** Signing attestations without verifiable controls in place creates significant liability.
- **An employee reports a cyber weakness:** Internal whistleblowers can drive **qui tam** suits alleging false statements about readiness.
- **You receive a subpoena regarding a vendor breach:** Misrepresenting a vendor's posture can trigger FCA exposure similar to direct failures.

HOW TO TAKE ACTION

- **Limit and Substantiate Attestations:** Ensure executives only sign statements supported by demonstrable controls and documentation.
- **Strengthen Vendor Oversight:** Require contractual flowdowns and ongoing monitoring to verify promised protections are operating.
- **Improve Internal Reporting:** Investigate reports about cyber weaknesses promptly to reduce the risk of an escalation to a **federal criminal investigation**.
- **Retain Experienced Defense Counsel**: Use Dykema's former federal prosecutors to align your representations with facts before the government begins a **regulatory enforcement** action.

Contact Dykema's White Collar Defense and Government Investigations practice today for a confidential consultation.

Mark Chutkow
Member, Bloomfield Hills
248-203-0715
mchutkow@dykema.com

Jennifer Beidel
Member, Bloomfield Hills
248-203-0506
jbeidel@dykema.com

Leigha Simonton
Member, Dallas
214-462-6444
lsimonton@dykema.com