Government Keeps Ratcheting Up Its Pursuit of Companies and Executives Over Cybersecurity and Privacy Problems

Abraham J. Rein and Laily Sheybani

For decades, the government's primary mode of enforcing data security and privacy obligations was through civil enforcement actions by the Federal Trade Commission (FTC), state Attorneys General (AGs), and/or the Health and Human Services Office for Civil Rights (HHS OCR). But these days, if the government thinks a company—or even an individual executive—has not lived up to its obligations with respect to maintaining the security of sensitive data, the company or individual could face criminal prosecution, a False Claims Act (FCA) action, a Securities and Exchange Commission (SEC) action, or all three, in addition to more traditional enforcement. (All of this, of course, is in addition to the private litigation that inevitably follows a data breach.)

In recent years, a wave of new federal initiatives has expanded enforcement of cybersecurity and privacy rules to levels not previously seen. The Department of Justice (DOJ) now utilizes criminal as well as civil tools against companies and executives. The SEC has developed cybersecurity disclosure rules and is wielding its enforcement powers against individual officers and publicly traded companies, demanding precise, accurate cybersecurity disclosures. Meanwhile, earlier this year, DOJ's National Security Division instituted a sweeping Data Security Program, threatening potential criminal sanctions for violators. DOJ's Civil Division is aggressively pursuing its "Civil Cyber-Fraud Initiative" against government contractors who fail to meet their cybersecurity requirements and, in May 2025, the Criminal Division announced plans of its own to prioritize "procurement fraud" prosecutions. The result is a multi-agency regime in which civil, administrative, and criminal penalties all play a part. Defense counsel will need to understand each agency's investigatory triggers and statutory elements, coordinate privileged internal probes, and rigorously challenge *mens rea*, jurisdictional hooks, and materiality as appropriate.

Executive's Conviction for Insufficient Disclosure of a Data Breach

On March 13, 2025, the Ninth Circuit upheld the landmark conviction of Joseph Sullivan, former Chief Security Officer (CSO) of Uber—the first corporate executive prosecuted and convicted for his company's cybersecurity failures.[1]

Uber was the victim of two successive hacks, collectively exposing hundreds of thousands of driver records. The second hack occurred while the FTC was investigating the first; according to the prosecution, Sullivan withheld relevant information about the second hack from the FTC in connection with that investigation. Further, Sullivan allegedly oversaw a process of negotiation with the hackers involving a $100,000 payment and recharacterizing their hacking as "research" pursuant to Uber's bug bounty program. The government charged Sullivan with obstructing the FTC investigation, and—significantly—misprision of a felony, because he knew about the second hack and did not report it.[2]

The misprision conviction, affirmed by the Ninth Circuit, is of particular concern in an era of rampant ransomware: in the absence of some independent disclosure requirement, executives frequently make the legitimate, considered decision to pay a hacker's ransom and move on, rather than report the crime. Similarly, bug bounty programs[3] are designed to encourage hacking attempts as a way of testing a company's security. Under the *Sullivan* precedent, executives who oversee those activities potentially face no less a risk than *personal criminal liability.*[4]

The case underscores the severity of potential enforcement when things go wrong from a data perspective. Enterprising (or irritated) prosecutors will scrutinize perceived efforts to conceal breaches and

misdirect regulators, and courts appear to permit a prosecution for misprision of a felony where the government can establish that a felony was deliberately hidden by the accused.

DOJ National Security Division's Data Security Program

On October 6, 2025, DOJ's "Data Security Program," which threatens criminal penalties for willful violations, goes into full effect. Announced on January 8, 2025, the program takes the form of regulations codified at 28 C.F.R. Part 202, implementing the International Emergency Economic Powers Act (IEEPA)[5] pursuant to a series of Executive Orders (EOs) declaring a national emergency with respect to foreign adversaries' "malicious cyber-enabled actions."[6] It establishes what are effectively export controls on certain sensitive information, prohibiting any U.S. person or entity from, among other things, engaging in certain types of transactions with designated "countries of concern" (i.e., China, Russia, Iran, North Korea, Cuba, and Venezuela) or individuals and entities associated with those countries, where the transaction involves "access" to certain types of sensitive data.[7] "Access" is defined broadly and includes the mere "ability" to "view" the data, raising the possibility of noncompliance in the case of faulty cybersecurity or privacy practices.[8]

Implementation guidance issued April 11, 2025, instituted a grace period under which civil enforcement would be deprioritized to allow companies to build compliance programs, perform due diligence, and update contracts to come into compliance with the Data Security Program.[9] Since that grace period ended on July 8, 2025, any transaction of any kind that "has the purpose of evading or avoiding, causes a violation of, or attempts to violate any of the prohibitions" of the Program, and any conspiracy to violate the Program, is punishable both criminally and civilly.[10] Civil penalties can be up to $368,136 per violative transaction, or twice the value of each such transaction, whichever is greater. Willful violations are punishable by imprisonment of up to 20 years and a $1 million fine.[11]

DOJ's Civil Cyber-Fraud Initiative

Under the DOJ's "Cyber Fraud Initiative," government contractors who fail to meet their data security obligations are in the crosshairs for a False Claims Act action, which carries the threat of treble damages and draconian per-"claim" penalties.[12] The Cyber Fraud Initiative was announced in October 2021 and has recently ramped up, with DOJ filing its first public intervention in a cyberfraud whistleblower case in August 2024.[13]

As of this writing, while it appears that the Trump administration is no longer using the "Cyber-Fraud Initiative" moniker, settlements of FCA matters involving allegations of government contractors' faulty cyber practices continue apace. On July 14, 2025, General Services Administration (GSA) contractor Hill Associates settled with the government over allegations that it billed federal agencies for the labor of IT personnel who lacked the experience and education required under its contract, and that it billed the government as if it had passed certain technical evaluations when it had not, among other things.[14] The settlement requires the contractor to pay $14.75 million, plus 2.5% of its annual gross revenue in excess of $18.8 million, every year through 2029.[15] In May, Raytheon Companies and Nightwing Group settled cyberfraud allegations for $8.4 million.[16] In March, defense contractor MORSECORP settled for $4.6 million.[17] In February, Health Net Federal Services and Centene Corporation settled for $11 million.[18] Clearly, the government sees value in pursuing this initiative.

While the Cyber-Fraud Initiative as originally conceived is civil in nature, the Trump administration's narrow white-collar *criminal* enforcement priorities, which are purportedly limited to certain "high-impact areas," includes "procurement fraud"—i.e., misleading the government in connection with contracts.[19] Correspondingly, "corporate procurement fraud" was added to the list of areas for which whistleblowers whose tips lead to criminal forfeitures may be eligible for an award.[20] In other words, criminal enforcement of procurement fraud, including surrounding data security and privacy, can be expected to have governmental scrutiny, investigation and prosecution in the coming months.

SEC Enforcement: Cybersecurity Disclosures

On July 26, 2023, the SEC adopted new rules to enhance and standardize disclosures regarding cybersecurity risk management, strategy, governance, and incidents (i.e., data breaches) by public companies that are subject to SEC reporting requirements.[21] Failures to comply with those disclosure requirements can subject companies, along with their individual officers, to SEC enforcement actions.

Indeed, as far back as 2021, the SEC has used its civil monetary penalty powers to punish publicly traded companies that insufficiently disclose cybersecurity risk to the investing public. For example, in October 2023, the SEC sued the CISO of SolarWinds, Timothy Brown, in his individual capacity, over allegations that he was involved in misleading investors about security controls and understating breach risk ahead of revealing the 2020 Sunburst supply-chain hack.[22] Among other things, the SEC charged that SolarWinds' public "security statement"—posted on its website—contradicted internal assessments about weak password policies, incomplete access controls, and missing secure-development lifecycles.[23]

The SEC has also charged four downstream SolarWinds customers—Unisys, Avaya, Check Point, and Mimecast—for making misleading disclosures about their exposure to or the impact of the hack, including negligent risk-factor disclosures and under-reporting the scope of data exfiltrated.[24] Each company agreed to pay penalties ranging from $990,000 to $4 million, underscoring that generic or hypothetical cybersecurity risk language may not satisfy new Regulation S-K Item 106 once a company has actual knowledge of an exploit or intrusion.[25]

Public companies, and their executives, must ensure that cybersecurity disclosures, risk factors, and breach notices faithfully reflect known vulnerabilities, active incidents, and the real-world implications of a breach—lest they may face SEC enforcement for misleading investors.

Conclusion: Key Takeaways for Defense Counsel

The above-discussed enforcement channels are, of course, cumulative of the familiar FTC, state AG, HHS OCR, and private plaintiff threats that victims of cyber and privacy intrusions have previously faced. As a result, now more than ever, defense attorneys need to map the evolving landscape of multi-agency cybersecurity enforcement. Beyond traditional FTC actions, our clients now face potential charges under misprision and obstruction statutes, the False Claims Act, export-control analogies in IEEPA under the DOJ's National Security Program, and SEC fraud provisions. Understanding each agency's investigatory triggers and statutory elements is the first step in formulating an effective defense. Counsel should consider the following practice points:

- Early engagement is critical. Counsel should advise clients to preserve all communications and forensic artifacts[26] from the moment a breach is suspected.

Coordinating a privileged internal investigation, involving cyber-forensics experts, strengthens privilege arguments and positions counsel to challenge assertions of knowing concealment or misrepresentation.

- When criminal exposure arises, scrutinize the *mens rea* requirements of the applicable statutory violations and geographic or territorial hooks that give federal agencies jurisdiction.
- In FCA-driven civil cyber fraud cases, explore the scope of "knowing" misstatements and challenge materiality in contract-compliance representations. The plaintiff's theory in such a case will be that the defendant feigned that its data practices were compliant with contractual requirements when they were not. But to succeed, plaintiff will need to establish not just that a claim was false, but that the false claim was made with *scienter—i.e.*, in the FCA context, that the defendant acted with actual knowledge, deliberate ignorance, or reckless disregard of the claim's falsity.[27] Further, plaintiff will need to meet a "demanding" and "rigorous" burden that the alleged falsity be *material—i.e.*, that it is not an "insignificant regulatory or contractual violation[ ]," but rather that the noncompliance is "so central to the [contracted services] that the [government] would not have paid the[ ] claims if it had known of the[ ] violations."[28] And in certain FCA cases, the plaintiff arguably needs to prove, not only that the violations were material, but that the defendant *knew* they were.[29] These can be steep burdens in cybersecurity cases, which can involve obscure technical details and vague reasonableness standards.
- In SEC-related actions, analyze whether risk disclosures meet the standards for scienter and materiality under SEC Rule 10b-5.[30] Be aware that SEC analysis can differ from the FCA one in key ways. For example, FCA cases can involve empirical evidence of materiality, or lack thereof, in the form of government behavior—if the government continues to pay despite knowing of the noncompliance, for example, that is strong evidence that it was immaterial[31]—whereas in securities matters, the question is more abstract, turning on whether a "reasonable investor" would view the omitted fact as significantly altering the "total mix" of information.[32] Being aware of such nuances allows counsel to calibrate arguments for different agencies as necessary, and align them where possible.
- Parallel civil and administrative proceedings demand coordinated strategies. For example, it is crucial to work closely with civil-litigation colleagues, starting early, to align argument themes, to avoid discovering mid-negotiation that your client's class action defense team's key argument undercuts, for example, your mitigation strategy.
- Similarly, think carefully about privilege waiver in the parallel proceeding context. Some agencies may offer attractive incentives—*e.g.*, cooperation credit or a potential advice-of-counsel defense—to reveal information. But any waiver likely will not be limited by an agency, and the information revealed could be used in related civil litigation or another regulator's enforcement action.[33]
- Where possible, counsel should work to leverage the same voluntary disclosures of data security issues, or overhauls of security and compliance programs implicated by cyber incidents, into mitigation credit with multiple agencies and constituencies.

By anticipating investigative priorities, leveraging privilege, and deploying targeted challenges to statutory elements, defense counsel can help clients navigate this new era of severe, overlapping enforcement.

NOTES:

[1] *United States v. Sullivan*, 131 F.4th 776 (9th Cir. 2025).
[2] *United States v. Sullivan*, No. 3:20-cr-00337-WHO-1, (N.D. Cal. Aug. 20, 2020); *see also* 18 U.S.C. § 1505 (obstruction); 18 U.S.C. § 4 (misprision).

Click here to view and/or print the full notes section for this article.

About the Authors

Abraham J. Rein is Chair of Post & Schell's White Collar Defense and Investigations Practice Group and Chair of the firm's Data Privacy and Cybersecurity Practice. Over his multi-decade career, he has successfully defended corporate and individual clients facing a broad spectrum of federal and state white-collar concerns including False Claims Act matters, matters revolving around research misconduct, theft of trade secrets, Controlled Substances Act violations, health care fraud, mail fraud, and wire fraud, among many others. Recently, he has defended several of the nation's most well-respected scientists and academics in matters involving allegations of ties to foreign governments and misuse of U.S. information. Mr. Rein also defends companies who are facing high-stakes litigation over cybersecurity or privacy missteps and counsels clients on how to ensure compliance with their cybersecurity and data privacy obligations, including walking them through the steps following a breach.

Laily Sheybani is an Associate in Post & Schell's White Collar Defense and Investigations Practice Group. Ms. Sheybani conducts internal investigations and defends individuals, companies, and organizations facing criminal and civil investigations and litigation. Her practice includes matters involving investigations by state and federal regulatory bodies, internal investigations, criminal charges, and alleged fraud. This includes investigations and litigation related to the False Claims Act, the Federal Anti-Kickback Statute and Stark Law, and alleged financial fraud and securities violations. Her clients include individuals and companies in the health care, financial, manufacturing, and construction industries, among others.

Share this article

Notes

[1] *United States v. Sullivan*, 131 F.4th 776 (9th Cir. 2025).
[2] *United States v. Sullivan*, No. 3:20-cr-00337-WHO-1, (N.D. Cal. Aug. 20, 2020); *see also* 18 U.S.C. § 1505 (obstruction); 18 U.S.C. § 4 (misprision).
[3] "Bug bounty programs" are corporate initiatives that offer rewards, typically monetary, to ethical hackers who discover and report data security vulnerabilities to the company. In this way, companies deputize the hacking community to identify and mitigate weaknesses, hopefully before they are exploited by malicious actors. *See, e.g.*, U.S. Dep't of Justice, Crim. Div., Cybersecurity Unit, *A Framework for a Vulnerability Disclosure Program for Online Systems* (Version 1.0, Jul. 2017), https://www.justice.gov/criminal/criminal-ccips/page/file/983996/dl?inline=. Uber's bug bounty program was initially announced in 2016, and at the time it offered rewards up to $10,000 for critical issues. Uber, *Welcome All Bug Bounty Hunters* (Mar. 22, 2016), https://www.uber.com/en-CH/newsroom/bug-bounty-program/.
[4] *United States v. Sullivan*, 131 F.4th 776, 787 n.6 (9th Cir. 2025).
[5] 50 U.S.C. §§ 1701 *et seq*.
[6] EO 13873 (May 15, 2019); EO 14034 (Jun. 19, 2021); EO 14117 (Feb. 28, 2024). By way of further explanation, the IEEPA grants the President certain authorities that may only be exercised to address an "unusual and extraordinary threat with respect to which a national emergency has been declared for purposes of this title." 50 U.S.C. § 1701(b). Among those authorities is the power to "investigate, regulate, or prohibit" certain "transactions" involving foreign interests, 50 U.S.C. § 1702(a)(1); the President is empowered to "issue such regulations, including regulations prescribing definitions, as may be necessary for the exercise of the authorities granted by this title." 50 U.S.C. § 1704. The willful violation of any such regulation is a crime. 50 U.S.C. § 1705(c). In 2019, President Trump declared an emergency for purposes of the IEEPA, via EO 13873. Five years later, in EO 14117, President Biden expanded the scope of that emergency and directed the Attorney General to issue regulations prohibiting certain transactions involving sensitive data. The final rule, codified at 28 C.F.R. Part 202, was published on January 8, 2025. 2024-31486 (90 FR 1636). Those regulations expressly refer to and incorporate the IEEPA criminal enforcement mechanism for willful violations. 28 C.F.R. § 202.1301(a)(3). The DOJ has issued a Compliance Guide and a set of Frequently Asked Questions to help those affected understand the impact of these rules. U.S. Dep't of Justice, Nat'l Security Div, *Data Security Program: Compliance Guide* (Apr. 11, 2025), https://www.justice.gov/opa/media/1396356/dl; U.S. Dep't of Justice, Nat'l Security Div, *Data Security Program: Frequently Asked Questions* (Apr. 11, 2025), https://www.justice.gov/opa/media/1396351/dl.
[7] 28 C.F.R. § 202.601 (2025).
[8] 28 C.F.R. § 202.201 (2025).
[9] U.S. Dep't of Justice, Nat'l Security Div., *Data Security Program: Compliance Guide* (Apr. 11, 2025), https://www.justice.gov/opa/media/1396356/dl.
[10] 28 C.F.R. § 202.304(a); 28 C.F.R. § 202.1301(a).
[11] C.F.R. § 202.1301(a)(3).
[12] U.S. Dep't of Justice, Office of Public Affairs, *Deputy Attorney General Lisa O. Monaco Announces New Civil Cyber-Fraud Initiative* (Oct. 6, 2021), *available at* https://www.justice.gov/archives/opa/pr/deputy-attorney-general-lisa-o-monaco-announces-new-civil-cyber-fraud-initiative; 31 U.S.C. 3729(a)(1) (providing for per-claim penalties and treble damages); 90 FR 2758 (setting penalties for 2025 at $14,308 to $28,618 per claim).
[13] *United States ex rel. Craig v. Georgia Tech Research Corp, et al.*, No. 1:22-cv-02698 (N.D. Ga.); U.S. Dep't of Justice, Office of Public Affairs, *United States Files Suit Against the Georgia Institute of Technology and Georgia Tech Research Corporation Alleging Cybersecurity Violations* (Aug. 22, 2024), https://www.justice.gov/archives/opa/pr/united-states-files-suit-against-georgia-institute-technology-and-georgia-tech-research.
[14] U.S. Dep't of Justice, Office of Public Affairs, *Maryland IT Company Agrees to Pay $14.75M to Resolve Alleged False Claims* (Jul. 14, 2025), https://www.justice.gov/opa/pr/maryland-it-company-agrees-pay-1475m-resolve-alleged-false-claims.
[15] Settlement Agreement between United States Department of Justice and Hill ASC, Inc. (Jul. 14, 2025), https://www.justice.gov/opa/media/1407761/dl.

[16] U.S. Dep't of Justice, Office of Public Affairs, *Raytheon Companies and Nightwing Group to Pay $8.4M to Resolve False Claims Act Allegations Relating to Non-Compliance with Cybersecurity Requirements in Federal Contracts* (May 1, 2025), https://www.justice.gov/opa/pr/raytheon-companies-and-nightwing-group-pay-84m-resolve-false-claims-act-allegations-relating.

[17] U.S. Dep't of Justice, Office of Public Affairs, *Defense Contractor MORSECORP, Inc. Agrees to Pay $4.6 Million to Settle Cybersecurity Fraud Allegations* (Mar. 26, 2025), https://www.justice.gov/opa/pr/defense-contractor-morsecorp-inc-agrees-pay-46-million-settle-cybersecurity-fraud.

[18] U.S. Dep't of Justice, Office of Public Affairs, *Health Net Federal Services, LLC and Centene Corporation Agree to Pay Over $11 Million to Resolve False Claims Act Liability for Cybersecurity Violations* (Feb. 18, 2025), https://www.justice.gov/opa/pr/health-net-federal-services-llc-and-centene-corporation-agree-pay-over-11-million-resolve.

[19] U.S. Dep't of Justice, Crim. Div., Memorandum from Matthew R. Galeotti, Head of Crim. Div., *Focus, Fairness, and Efficiency in the Fight Against White-Collar Crime* (May 12, 2025), https://www.justice.gov/criminal/media/1400046/dl?inline.

[20] *Id*. at 5.

[21] Securities & Exchange Comm'n, *Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure,* Release Nos. 33-11216; 34-97989, 88 Fed. Reg. 51,896 (Aug. 4, 2023).

[22] *SEC v. SolarWinds Corp.*, No. 23-cv-9518-PAE (S.D.N.Y.); Securities & Exchange Comm'n, *SEC Charges SolarWinds and Chief Information Security Officer with Fraud, Internal Control Failures* (Oct. 30, 2023), https://www.sec.gov/newsroom/press-releases/2023-227.

[23] *Id*. (alleging, among other things, violations of 15 U.S.C. § 78j(b); 15 U.S.C. § 78m(a); and 15 U.S.C. § 77q(a)).

[24] Unisys Corporation, Securities Act Release No. 11323, Exchange Act Release No. 101401, SEC File No. 3-22272 (Oct. 22, 2024); Avaya Holdings Corp., Securities Act Release No. 11320, Exchange Act Release No. 101398, SEC File No. 3-22269 (Oct. 22, 2024); Check Point Software Technologies Ltd., Securities Act Release No. 11321, Exchange Act release No. 101399, SEC File No. 3-22270 (Oct. 22, 2024); Mimecast Limited, Securities Act Release No. 11322, Exchange Act Release No. 101400, SEC File No. 3-22271 (Oct 22, 2024).

[25] U.S. Sec. & Exch. Comm'n, Press Release No. 2024-174, *SEC Charges Four Companies With Misleading Cyber Disclosures* (Oct. 22, 2024), https://www.sec.gov/newsroom/press-releases/2024-174.

[26] "Forensic artifacts" in the data breach context refers to digital evidence, *i.e.*, pieces of data such as cached files, metadata, system logs, browser history, remnants of deleted files or data that may be used to reconstruct specifically what happened, when, and how.

[27] *United States ex rel. Schutte v. SuperValu Inc.*, 598 U.S. 739, 749-50, 143 S. Ct. 1391, 1399-400 (2023); 31 U.S.C. § 3729(b)(1).

[28] *Universal Health Servs. v. United States ex rel. Escobar*, 579 U.S. 176, 196, 136 S. Ct. 1989, 2004 (2016); *see also* 31 U.S.C. § 3729(b)(4).

[29] *See, e.g.*, *Escobar*, 579 U.S. at 181 ("What matters is . . . whether the defendant knowingly violated a requirement that *the defendant knows* is material to the Government's payment decision" (emphasis added).).

[30] 17 C.F.R. § 240.10b-5.

[31] *Escobar*, 579 U.S. at 194-95.

[32] *TSC Industries v. Northway, Inc.*, 426 U.S. 438, 449 (1976).

[33] *See, e.g.*, *Westinghouse Elec. Corp. v. Republic of Phil.*, 951 F.2d 1414, 1431 (3d Cir. 1991) (rejecting defense argument that providing privileged internal investigation documents to SEC and DOJ for purposes of cooperating did not waive the privilege as to private plaintiff).