Fourth Edition
July 2026

CYBERSECURITY AND DATA PRIVACY

WHISTLEBLOWER PROTECTIONS

An overview of the protections and rewards available to cybersecurity and data privacy whistleblowers under federal and state law

Matthew LaGarde, Lisa J. Banks, and Catherine Seita

KATZ BANKS KUMIN

WASHINGTON, DC | PHILADELPHIA, PA | SAN FRANCISCO, CA | NEW YORK, NY
202.299.1140 | KATZBANKS.COM

© Copyright 2026

TABLE OF CONTENTS

INTRODUCTION 3

CURRENT PROTECTIONS FOR CYBERSECURITY AND DATA PRIVACY WHISTLEBLOWERS 5

A. Federal Statutes Providing Protections to Cybersecurity and Data Privacy Whistleblowers 5
1. Sarbanes-Oxley and Dodd-Frank Protections 6
2. Protections for Banking and Consumer Finance Whistleblowers 16
3. False Claims Act Protections 18
4. Anti-Money Laundering Act Protections 21
5. Protections for Nuclear Whistleblowers 23
6. Protections for Federal Government Employees 24
7. Protections for Federal Government Contractors 26

B. State Laws Providing Protections to Cybersecurity and Data Privacy Whistleblowers 28
1. Federal Law Bases for State Wrongful Discharge and Whistleblower Retaliation Claims 30
2. State Law Bases for State Wrongful Discharge and Whistleblower Retaliation Claims 33

REWARDS FOR CYBERSECURITY AND DATA PRIVACY WHISTLEBLOWERS 34

A. SEC Whistleblower Program 34
B. CFTC Whistleblower Program 35
C. Qui Tam Lawsuits under the False Claims Act 36
D. Anti-Money Laundering Whistleblower Reward Program 38
E. DOJ Pilot Whistleblower Program 39

THINGS TO THINK ABOUT BEFORE BLOWING THE WHISTLE 40

A. Report a Violation of Law, Not Just Cybersecurity or Data Privacy Vulnerabilities 40
B. Report in Writing to Someone Who Can Address the Problem 40
C. Be Careful About Taking Documents 40
D. Seek Legal Representation 41
E. If Terminated, Diligently Look For New Work 41

ENDNOTES 43

APPENDIX A 65

INTRODUCTION

Cybersecurity and data privacy concerns must remain a paramount concern for industry leaders and policymakers.

Since the original version of this Guide's release more than eight years ago, cybersecurity and data privacy issues have continued to dominate headlines and remain a key concern for individuals, businesses, and the government. Just last year, Charles Borges, former Chief Data Officer of the Social Security Administration (SSA) and a Katz Banks Kumin LLP client, became a front-page story when he blew the whistle on practices of the Department of Government Efficiency (DOGE) that violated SSA data security protocols and left the personal information of hundreds of millions of Americans vulnerable to cyberattacks.[1] Before that, another Katz Banks Kumin client, Peiter "Mudge" Zatko, former head of security at Twitter, made headlines following his disclosures and testimony to the Senate Judiciary Committee about his cybersecurity concerns at Twitter.[2]

Public concern about cybersecurity and data privacy breaches is well warranted. Companies and other institutions have continued to suffer high-profile cybercrime incidents and data breaches in recent years, including Change Healthcare, a healthcare technology provider owned by UnitedHealth Group;[3] Ticketmaster;[4] AT&T;[5] and the University of Pennsylvania.[6]

So too has the American public. The Federal Bureau of Investigation (FBI) reported a record-breaking one million cybercrime complaints in 2025, more than double the number of complaints in 2019, with reported losses of over $20 billion.[7] Foreign hacking has also compromised U.S. national security through large-scale attacks on critical U.S. infrastructure, healthcare systems, the media, and elections.[8]

Given the significant harm caused by cybersecurity and data privacy breaches, federal agencies continue to dedicate significant resources to these issues. For example, the Department of Justice (DOJ) demonstrated its ongoing commitment to combatting cybercrime by announcing the launch of the Civil Cyber-Fraud Initiative in October 2021.[9] The Initiative, led by the Fraud Section of the Civil Division's Commercial Litigation Branch, has continued to hold entities and individuals accountable for failures to protect government data, targeting entities that knowingly misrepresent cybersecurity practices and protocols or knowingly provide deficient cybersecurity products or services. In 2024, the Initiative resolved four cybersecurity-related FCA matters, recovering over $16 million. These cases arose from failures to protect federally funded data in COVID-era programs, unsecured Medicare beneficiary records, and non-compliance with cybersecurity requirements in defense and aerospace contracts.

The Civil Cyber-Fraud Initiative remained active in 2025, with the DOJ settling nine[10] other FCA cases that further underscored the importance of compliance with cybersecurity requirements in government contracts, including:

In February 2025, Health Net Federal Services Inc. and its corporate parent, Centene Corporation, paid over $11 million to resolve claims that the company falsely certified compliance with cybersecurity requirements in a contract with the Department of Defense (DOD) to administer a health benefits program for servicemembers and their families.[11]

In May 2025, Raytheon Companies and Nightwing Group paid $8.4 million to resolve allegations that the companies failed to meet required cybersecurity standards in their DOD contracts and subcontracts.[12]

© Copyright 2026

In July 2025, biotechnology company Illumina, Inc. agreed to pay $9.8 million, resolving allegations that it sold genomic sequencing systems with cybersecurity vulnerabilities to various federal agencies after falsely representing compliance with cybersecurity standards.[13]

In September 2025, Georgia Tech Research Corporation agreed to pay $875,000 to the United States to resolve allegations that it failed to meet cybersecurity requirements in connection with Air Force and Defense Advanced Research Projects Agency contracts.[14]

More recently, in June 2026, the DOJ settled another cybersecurity-related FCA action against defense contractor LOGZONE Inc., which it alleged had submitted false or fraudulent claims for payment on Navy contracts after failing to implement required cybersecurity controls.[15] The company agreed to pay $507,144 to resolve the case.

Governmental regulators have joined law enforcement agencies in addressing cybersecurity. On February 20, 2025, the Securities and Exchange Commission (SEC) announced the creation of the Cyber and Emerging Technologies Unit (CETU), which the Commission said would focus on combatting cyber-related misconduct to protect retail investors from bad actors in the emerging technologies space.[16] The CETU's stated priorities include combating fraud involving AI and emerging technologies, hacking to obtain material nonpublic information, crypto asset fraud, and failures by public issuers and regulated entities to comply with cybersecurity-related regulatory requirements.[17]

Aside from the SEC, the U.S. Federal Trade Commission (FTC) has also aggressively pursued companies for cybersecurity and data privacy failures, bringing enforcement actions and reaching settlements with companies that failed to adequately secure customer data.[18] A number of the FTC's actions in recent years have focused on violations of the Children's Online Privacy Protection Act (COPPA), which places limitations and requirements on online platforms that collect personal information via the internet from children under 13 years old.[19] In 2025, the FTC filed or resolved several COPPA enforcement actions against companies that unlawfully collected children's personal data, including an action resulting in a $10 million settlement with the Walt Disney Company.[20]

The technological landscape driving these threats continues to evolve rapidly. The shift to remote work, the proliferation of cloud computing and connected devices, and the broad adoption of AI tools have each introduced new security risks that organizations are still working to understand and address.[21] Cybersecurity and data privacy concerns must therefore remain a paramount concern for industry leaders and policymakers alike.[22]

Despite the growing importance of these issues, many organizations continue to fail to provide cybersecurity and data privacy the attention and resources they deserve. Indeed, a 2025 survey of executives at large corporations found that 82% of U.S. CEOs ranked cybercrime and cyber insecurity as the top threats that could negatively impact their organization's prosperity, with 52% of CEOs reporting that they were specifically concerned about identity theft and data privacy and 45% reporting the same of vulnerability to cyberattacks.[23] While 46% of survey participants reported that they were increasing their investments in cybersecurity and digital resilience to mitigate risks, these numbers reflect that many companies have a long way to go.

© Copyright 2026

Given the scope of the threat, the public has little choice but to rely on companies and government agencies that store personal information to prevent their websites, applications, or devices from serving as a platform for cybercrime and to protect information in their custody from cyberattacks. Given practical limitations on enforcement agencies, however, and the disregard with which some companies treat cybercrime and data privacy issues, these protections will only achieve their goals if employees alert companies and government agencies to lax cybersecurity standards and cyber vulnerabilities. For this reason, whistleblowers are crucial to ensuring the safety of an organization's employees, customers, and partners.

Unfortunately, retaliation against employees who blow the whistle on cybersecurity problems is all too common. An employee who reports cybersecurity or data privacy problems may face serious harm to their career, including termination. Since most employees cannot afford to risk their jobs, their fear of retaliation deters them from reporting such problems. While Congress has not yet explicitly provided cybersecurity or data privacy whistleblowers with protections against retaliation, a patchwork of state and federal laws can be used to provide these protections and incentives for many cybersecurity and data privacy whistleblowers. This Guide provides a compilation and discussion of the major legal claims available to cybersecurity and data privacy whistleblowers. It also describes the federal programs under which those whistleblowers' reports may lead to monetary rewards. Finally, it provides potential cybersecurity and data privacy whistleblowers with specific suggestions to enhance their legal protections when blowing the whistle.

CURRENT PROTECTIONS FOR CYBERSECURITY AND DATA PRIVACY WHISTLEBLOWERS

While there continues to be no federal statute that explicitly protects employees who blow the whistle on lax cybersecurity or data privacy violations (in contrast, for example, to blowing the whistle about transportation or environmental issues), there are a handful of federal statutes and state laws that can provide cybersecurity and data privacy whistleblowers with a basis for actionable retaliation claims. The availability of such protections, however, varies depending on the facts and circumstances of each case. To provide a basic understanding of potential claims, this section first discusses the federal statutes that may protect a cybersecurity or data privacy whistleblower. It then discusses potential claims under state law that might protect a cybersecurity or data privacy whistleblower.

A. Federal Statutes Providing Protections to Cybersecurity and Data Privacy Whistleblowers

There are at least nine federal statutes that may provide protections to a cybersecurity or data privacy whistleblower, depending on the entity for which the whistleblower works and the wrongdoing the whistleblower reports.[24] Those statutes are:

- The Sarbanes-Oxley Act of 2002, which provides protections to employees who report fraud and securities violations at publicly traded companies;[25]

© Copyright 2026

- The Dodd-Frank Wall Street Reform and Consumer Protection Act, which provides protections to employees who report securities violations to the SEC;[26]

- The Consumer Financial Protection Act of 2010, Title X of the Dodd-Frank Act, which provides protections to employees who report violations of Consumer Financial Protection Bureau rules at consumer financial products or services providers;[27]

- The Financial Institutions Reform Recovery and Enforcement Act of 1989, which provides protections to employees who report legal violations at banks and other depository institutions;[28]

- The False Claims Act of 1863, which provides protections to employees who oppose fraud against the government;[29]

- The Bank Secrecy Act of 1970, as amended by the Anti-Money Laundering Act of 2020, which provides protections to employees who report violations of Department of Treasury laws and regulations;[30]

- The Energy Reorganization Act of 1974, which provides protections to employees in the nuclear industry who oppose violations of that law, the Atomic Energy Act of 1954, or Nuclear Regulatory Commission regulations;[31]

- The Whistleblower Protection Act of 1989, which provides protections to federal government employees who report legal violations, a substantial and specific danger to public health or safety, or gross mismanagement, waste, or abuse;[32] and

- The National Defense Authorization Act for Fiscal Year 2013, which provides protections to employees who report gross mismanagement, waste, abuse, or violations of laws or regulations relating to federal contracts.[33]

Understanding what constitutes protected activity and an actionable adverse action under each of these statutes is essential to the effective assertion of a claim, particularly since cybersecurity and data privacy whistleblowing is not the explicit focus of any of these laws. Additionally, each statute has procedural requirements for asserting a claim. These requirements must be followed or a whistleblower will lose the protections of the statute. Below is a detailed discussion of each statute, including the circumstances in which cybersecurity or data privacy whistleblowing could constitute protected activity, the actions taken against an employee that could constitute an adverse action, and the procedural requirements of each statute.

1. Sarbanes-Oxley and Dodd-Frank Protections

In 2002, in the wake of the infamous accounting fraud scandals of Enron and WorldCom, Congress passed the Sarbanes-Oxley Act of 2002 (SOX), a law designed to curb corporate and accounting misconduct by publicly traded companies. In recognition of the vital and high-profile role of the whistleblowers in those cases, Congress included retaliation protections for employees of publicly traded companies

A cybersecurity whistleblower hoping to claim the protections of SOX and Dodd-Frank must establish that she made a protected disclosure.

© Copyright 2026

in Section 806 of SOX.[34] Eight years later, in the wake of the financial crisis that led to the Great Recession, Congress passed the Dodd-Frank Wall Street Reform and Consumer Protection Act of 2010 (Dodd-Frank) to address deficiencies in existing financial regulations. Dodd-Frank includes enhanced protections for whistleblowers working for publicly traded companies and new protections for those working in the financial industry, for wholly owned subsidiaries and affiliates of publicly traded companies, and for nationally recognized statistical organizations.[35] In the years since the passage of these two laws, cybersecurity has become a critical issue for publicly traded companies and their primary regulator, the SEC, bringing cybersecurity disclosures well within the reasonable boundaries of the whistleblower protections provided by these two statutes.

a) Protected Activity

SOX and Dodd-Frank only protect employees when a whistleblower discloses information about specific types of wrongdoing to specific recipients. SOX provides that no publicly traded company, including its wholly owned subsidiaries or affiliates,[36] may take an adverse action against an employee because the employee provided information regarding mail fraud, wire fraud, bank fraud, securities fraud, a violation of any SEC rule or regulation, or a violation of any federal law relating to fraud against shareholders.[37] SOX protections also extend to employees of private contractors and subcontractors serving public companies,[38] although the wrongdoing identified by the employee may need to relate to or have been engaged in by the public company.[39] A whistleblower is entitled to SOX protections provided she makes such a report to a federal agency, member of Congress, supervisor, or person working for the employer who has the authority to investigate, discover, or terminate misconduct.[40] When a whistleblower has met both of these requirements by providing information about one of the enumerated types of wrongdoing to one of the enumerated recipients, she has engaged in "protected activity" under SOX.

Dodd-Frank, on the other hand, prohibits any employer from taking an adverse action against a whistleblower because she: (a) provided information about securities violations to the SEC; (b) assisted the SEC in an investigation of securities violations; or (c) made disclosures protected under SOX, the Securities Exchange Act of 1934, or any other law, rule, or regulation subject to the jurisdiction of the SEC.[41] To qualify for whistleblower protection under Dodd-Frank, however, an individual must report the misconduct to the SEC.[42] In other words, whistleblowers who only report their concerns internally cannot pursue a retaliation claim under Dodd-Frank. However, because internal whistleblowers *are* protected under SOX, for most whistleblowers, the inability to assert a Dodd-Frank claim only affects potential remedies and procedural safeguards. Dodd-Frank provides more generous monetary remedies and a longer statute of limitations than SOX, as well as the ability to file directly in federal court.[43] That being said, Dodd-Frank does not contain the restrictive definition of "employer" used by SOX, meaning that employees of a non-public company, such as an investment management firm, who report securities violations to the SEC may be entitled to Dodd-Frank protections even if they are not protected by SOX.[44]

The most significant hurdle for a cybersecurity whistleblower who wishes to claim the protections of SOX and Dodd-Frank is establishing that her disclosure falls into one of the statutorily enumerated categories. While a cybersecurity disclosure

© Copyright 2026

may not appear to relate to one of the protected disclosure categories at first blush, there are at least four potential grounds for asserting that a cybersecurity or data privacy disclosure qualifies as protected activity.

(1) Fraud

To the extent a cybersecurity or data privacy whistleblower at a publicly traded company reports activity that can be characterized as fraudulent, this disclosure should qualify as protected activity under SOX. Four of the statutory categories of protected SOX disclosures concern violations of federal fraud statutes, specifically mail, wire, bank, and securities fraud.[45] The Administrative Review Board (ARB) of the Department of Labor (DOL) takes the position that reports of violations of these federal fraud statutes constitute protected activity, regardless of whether the fraud also relates to fraud upon shareholders.[46] Almost all of the federal circuits to have considered the issue have followed this interpretation.[47] All disclosures protected by SOX are also protected by Dodd-Frank, provided that the whistleblower has made a report to the SEC.[48]

An employee need only "reasonably believe" that the information she provides is a violation of one of the enumerated categories.[49] This requires that "(1) [the whistleblower] had a reasonable, subjective belief that the conduct she complained of constituted a violation of the laws listed at section 1514, and (2) a reasonable person of similar experience, training, and factual knowledge would objectively believe that a violation had occurred or was occurring."[50] SOX protections also extend to reports about violations *about to be* committed, provided the employee reasonably believes the violation is likely to occur.[51] Moreover, an employee need not use the word "fraud" in her disclosure to identify fraudulent activity for the purposes of garnering SOX protections.[52]

The following hypothetical example of cybersecurity disclosures meets this standard. An employee working for a publicly traded company learns information indicating that her employer is non-compliant with ISO/IEC 27001, an industry standard for information security management. The employee also discovers that, although the company has known it is non-compliant for years, to secure a major deal, it represented to a client that it was ISO/IEC 27001-compliant. The employee reports this information to her supervisor. In this situation, the company's knowing misrepresentation to the client of its cybersecurity posture as compliant could constitute fraud. If the whistleblower states that she believes that the company's conduct may be fraudulent in her report to her supervisor, she likely has a strong argument that her report is protected.

(2) Securities Fraud and Violations of SEC Disclosure Requirements

Publicly traded companies are prohibited from making false or misleading public statements about material facts. Specifically, Section 10(b) of the Securities Exchange Act of 1934,[53] SEC Rule 10b-5,[54] and Section 17(a) of the Securities Act of 1933[55] prohibit fraudulent practices in connection with the purchase or sale of a security, including the knowing misrepresentation or omission of material facts. In the

© Copyright 2026

securities context, a "material fact" is a term of art referring to a fact that a reasonable investor would have viewed as significantly altering the "total mix" of information available to him.[56] A false or misleading public statement about a company's cybersecurity posture could constitute securities fraud given the potentially catastrophic financial impact of cyberattacks.

In 2018, the SEC took its first enforcement action against a company for misleading investors about cybersecurity. Altaba, the company formerly known as Yahoo! Inc. ("Yahoo"), agreed to pay the SEC $35 million to resolve claims that it misled investors by failing to disclose a cybersecurity breach that enabled hackers to steal the personal data of hundreds of millions of Yahoo users.[57] According to the SEC, the company failed to properly investigate and disclose the breach to investors for more than two years after members of Yahoo's senior management and legal department learned of the breach. During that time, the company filed several quarterly and annual reports that made no mention of the breach, instead making only vague references to the risk of data breaches in general. In the years since, the SEC has charged multiple companies for failing to disclose or issuing misleading statements about cyber breaches.[58] As a recent example, in October 2024, the SEC charged four companies for making materially misleading disclosures related to cybersecurity breaches they had suffered, resulting in a combined total of approximately $6.9 million in civil penalties.[59] Two months later, in December 2024, the SEC announced that it had settled charges against Flagstar Bancorp, Inc. for making materially misleading statements regarding a cybersecurity attack on Flagstar's network in late 2021.[60]

Indeed, the SEC has long warned companies of their obligations to make necessary disclosures of material information about cybersecurity risks and breaches. In 2011, the SEC's Office of Corporation Finance issued guidance that emphasized the importance of cybersecurity disclosures in SEC filings.[61] The guidance acknowledged that there is no specific disclosure requirement for cybersecurity risks and breaches, but emphasized that registrants are required to disclose material information about cybersecurity risks and cyber incidents so that investors have information they would consider important to an investment decision. Registrants are also required to disclose any information about cybersecurity that is necessary to prevent other disclosures from misleading potential investors. The SEC provided several examples of appropriate cybersecurity disclosures depending on the specific circumstances.[62]

In 2018, the SEC issued a second cybersecurity guidance, entitled "Commission Statement and Guidance on Public Company Cybersecurity Disclosures," that supplements the 2011 guidance and became effective on February 26, 2018.[63] The SEC explained that the additional guidance was necessary because of the increasing significance of cybersecurity incidents. In its 2018 Cybersecurity Guidance, the Commission stated that it is "critical that public companies take all required actions to inform investors about material cybersecurity risks and incidents in a timely fashion, including those companies that are subject to material cybersecurity risks but may not yet have been the target of a cyber-attack." While the 2018 Cybersecurity Guidance reiterated much of what was explained in the initial 2011 Cybersecurity Guidance, the Commission added detail on how companies might determine whether a cybersecurity risk or incident was material and provided a list of considerations to assist companies in evaluating their cybersecurity risks.[64]

© Copyright 2026

On July 26, 2023, the SEC adopted final rules specific to cybersecurity risk management within publicly traded companies.[65] The 2023 Cybersecurity Rules became effective on September 5, 2023. These Rules formalized and updated the cybersecurity reporting framework reflected in the 2011 and 2018 guidance documents for companies regulated by the SEC. They also included the following changes to the prior regulatory regime, among others:

- Companies must publicly disclose certain information about a material cybersecurity incident within four business days after determining one has occurred;[66]

- Companies must promptly update any such disclosures with responsive information that comes to light after the initial filing;[67] and

- In their risk disclosures, companies must describe their processes, if any, for identifying and managing cybersecurity risks, including whether they consider cybersecurity as part of their business strategy or capital allocation, whether the board has oversight of cybersecurity risks, and company management's role and expertise in managing cybersecurity risks.[68]

Whistleblowers and their attorneys who are evaluating whether a disclosure would qualify as protected activity should review the 2023 Cybersecurity Rules, as well as the 2011 and 2018 guidance documents carefully.[69]

Securities fraud and violations of SEC disclosure requirements are not limited to cybersecurity concerns. The SEC has also brought enforcement actions against public companies pertaining to data privacy. For instance, in 2019, the SEC settled a case with Facebook, the social media company now known as Meta, for $100 million based on charges that Facebook failed to disclose the misuse of user data for over two years after discovering the issue.[70] The charges related to the so-called "Cambridge Analytica scandal," in which Cambridge Analytica, the now-defunct data analytics company, paid a researcher to collect Facebook data on approximately 30 million Americans to assist with its political advertising strategies.[71] After discovering the abuse, rather than disclosing it to investors, Facebook continued to obfuscate and mislead investors and reporters.[72]

The SEC has adopted new rules designed to close certain data privacy gaps. Specifically, in May 2024, the SEC adopted rules updating Regulation S-P to strengthen customer data privacy protections by, among other things, requiring broker-dealers, registered investment advisers, and other covered entities to notify individuals affected by certain types of data breaches. More on Regulation S-P can be found *infra* in Section II.A.1.a.4.

The following hypothetical demonstrates a report that would be protected because it relates to potential securities fraud and violations of SEC disclosure requirements. An employee of a publicly traded company reports to the company compliance hotline that the company has known for years about a serious cyber vulnerability. The employee reports that, although the data breach has already resulted in the theft of critical intellectual property, the company has refused to correct the problem and has not disclosed either its vulnerability or the breach to the public. Even though the whistleblower did not reference securities fraud or violations of SEC rules and regulations, since her report directly references material public misrepresentations, it should constitute protected activity under the liberal ARB standard that requires a

© Copyright 2026

reasonable belief that the company has violated one or more of the enumerated SOX categories. The employee need only show that her belief was objectively and subjectively reasonable—i.e., that she actually believed fraud had occurred, and that a reasonable person of similar experience, training, and factual knowledge would reach the same conclusion.

That being said, the whistleblower would bolster her claim if she directly stated that she believed the company's failure to publicly report the cyber vulnerability and the breach could constitute securities fraud and result in the company's failure to meet the SEC's disclosure requirements related to cybersecurity. This more explicit statement would preclude an employer from arguing that the whistleblower's report was not about one of SOX's enumerated categories.

Whistleblowers engaging in this form of protected activity, however, should pay close attention to their company's disclosures. In a 2017 case brought by investors of LifeLock, Inc., against the company, the Ninth Circuit affirmed a district court dismissal of the investors' class action suit alleging securities fraud.[73] The investors had alleged, in part, that LifeLock made false statements regarding its compliance with applicable payment card industry data security standards (PCI DSS).[74] The Ninth Circuit, however, found that the company had never affirmatively represented in its statements to shareholders that the application underlying the plaintiffs' allegations *was* compliant with PCI DSS.[75] The Ninth Circuit added that even if the company's statements had been misleading, the plaintiffs had failed to adequately plead that the statements were made with scienter,[76] a necessary element of a securities fraud claim.[77] Accordingly, the Ninth Circuit upheld the district court's determination that the company's failure to notify shareholders that its application was not PCI DSS compliant did not constitute securities fraud.[78]

In April 2022, the Fourth Circuit affirmed the District Court for the District of Maryland's dismissal of allegations that Marriott International engaged in securities fraud.[79] Investors claimed that Marriott omitted material information about cybersecurity vulnerabilities in a series of public statements.[80] The Fourth Circuit held that Marriott's statements, including an SEC submission stating that the "integrity and protection of customer, employee, and company data is critical to us," were, at most, puffery and not false or misleading to the extent necessary to be actionable under the Securities Exchange Act.[81] The Fourth Circuit continued, rejecting the investors' argument that Marriott's statements were "materially misleading" by generally warning of the risk of cybersecurity breaches that had, in fact, already occurred.[82] The Fourth Circuit held that while "forward looking warnings" are actionable if they rise to the level of "misleading omissions about current or past challenges,"[83] Marriott had updated its SEC disclosures to make note that the company had experienced cybersecurity attacks, in addition to generally warning of the risk of future cybersecurity breaches.[84]

More recently, in 2024,[85] the Southern District of New York dismissed most of the claims in an action brought by the SEC against SolarWinds, a multinational information technology and software company, and its chief information security officer. The SEC asserted securities fraud, internal accounting controls, and disclosure controls claims related to allegedly known cybersecurity risks and vulnerabilities.[86] With respect to the securities fraud claims, the SEC alleged that defendants misleadingly touted SolarWinds' cybersecurity practices and products, while understating its cybersecurity risks.[87] Although the court left intact the SEC's claim that a "Security Statement" on the company's website made prior to the cyberattacks

© Copyright 2026

was misleading, it dismissed all other claims.[88] The court found that defendants' statements in press releases, blog posts, and podcasts—conveying, for example, that SolarWinds "places a premium on the security of its products"—were "non-actionable corporate puffery."[89] As to the SEC filings predating the attacks, the court found that SolarWinds' risk disclosures, which the SEC faulted for being "boilerplate and generic," sufficiently alerted the investing public to the cybersecurity risks the company faced and did not need to be updated following cyber intrusions already contemplated by the disclosures.[90] Finally, the court found that the SEC filings from after the attacks—which disclosed that SolarWinds experienced a "cyberattack" and that a "vulnerability" was inserted into its products, but omitted information about the cyber incidents that had occurred prior to the attacks at issue—were not misleading.[91] The SEC announced a settlement resolving the surviving claims against SolarWinds in November 2025.[92]

In contrast to the above cases, in 2021, the Ninth Circuit ruled that investors adequately pleaded a securities violation arising from cybersecurity problems with the Google+ social network website.[93] The decision may reflect recognition by some courts of the serious nature of cybersecurity problems, particularly as cybersecurity relates to data privacy. Indeed, the complaint contextualized the Google+ breach within the SEC enforcement action taken in response to the Cambridge Analytica scandal discussed above.[94] As alleged in the complaint, executives at Google believed that in light of the ongoing scrutiny of Facebook relating to the Cambridge Analytica scandal, disclosure of the securities vulnerabilities described in the complaint would likely lead to immediate regulatory interest.[95] Accordingly, Google failed to notify investors of the breach.[96] The court determined that the complaint plausibly alleged a material omission, citing the SEC's 2018 Cybersecurity Guidance discussed above in support of its conclusion.[97]

(3) Failure to Maintain Disclosure Controls and Procedures

Publicly traded companies are required to maintain disclosure controls and procedures, and management must evaluate the effectiveness of those controls and procedures.[98] As the SEC noted in its 2018 Cybersecurity Guidance, cybersecurity risk management policies and procedures are "key elements of enterprise-wide risk management."[99] The Commission encouraged companies to "adopt comprehensive policies and procedures related to cybersecurity and to assess their compliance regularly," and assess whether they "have sufficient disclosure controls and procedures in place to ensure that relevant information about cybersecurity risks and incidents" is escalated to senior management in a way that permits them to make informed disclosure decisions and certifications.[100] The SEC noted that companies are required under Item 407(h) of Regulation S-K and Item 7 of Schedule 14A to provide shareholders with "a description of how the board administers its risk oversight function," adding that if material cybersecurity risks existed, the description "should include the nature of the board's role in overseeing the management of that risk."[101] As mentioned above, the SEC formalized these disclosure controls in its 2023 Cybersecurity Rules. For example, the 2023 Cybersecurity Rules amended Regulation S-K to provide that registered companies must describe their processes, if any, for identifying and managing cybersecurity risks in their risk disclosures.[102] The regulations further require that companies disclose whether the board has oversight of cybersecurity risk and company management's role and expertise in managing

© Copyright 2026

cybersecurity risk.[103] With these requirements, a whistleblower who has raised concerns about the lack of adequate cybersecurity controls and procedures will have a strong argument that she has engaged in protected activity under SOX (and under Dodd-Frank, if she also reported the issues to the SEC).

Even prior to the 2023 Cybersecurity Rules and the 2018 Cybersecurity Guidance, a federal court in Florida held that complaints of deficient disclosure controls related to information security could serve as a basis for protected activity. In *Thomas v. Tyco Int'l Mgmt. Co., LLC*, the plaintiff notified Tyco of her concerns about, among other things, the lack of involvement of IT and compliance personnel in the disclosure process and Tyco's inability to detect manual manipulations to its financial data.[104] The court held that "[d]ata security, approvals, and segregation of duties are controls that exist to ensure the accuracy of financial reporting. . . . An employee's complaint concerning inadequate internal control over financial reporting can constitute protected activity."[105]

(4) SEC Regulations Protecting Consumer Data

Registered investment companies and registered investment advisers are subject to SEC regulations related to customer data protection, most notably Regulations S-P and S-ID.[106] Under Regulation S-P, known as the "Safeguards Rule," a covered entity is required to notify clients concerning the collection, use, and sharing of nonpublic personal information (NPI).[107] The regulation also limits the disclosure of client NPI to anyone not affiliated with the entity unless the entity specifically notifies the client and the client declines to opt out of having that information shared.[108] The SEC has aggressively enforced the Safeguards Rule. Indeed, in 2021, the SEC announced sanctions against eight investment advisory firms and broker-dealers for violations of the Safeguards Rule, specifically for the companies' alleged failures in their cybersecurity procedures.[109]

On May 16, 2024, the SEC announced the adoption of amendments to the Safeguards Rule to impose requirements beyond notifying customers as to how their financial information is used.[110] As then-SEC Chair Gary Gensler explained, following the adoption of the amendments, "[t]he basic idea for covered firms is if you've got a breach, then you've got to notify."[111] The amendments, which became effective on August 2, 2024, require broker-dealers, investment companies, registered investment advisers, and transfer agents to "develop, implement, and maintain written policies and procedures for an incident response program that is reasonably designed to detect, respond to, and recover from unauthorized access to or use of customer information."[112] The covered institutions must "provide notice as soon as practicable, but not later than 30 days, after becoming aware that an incident involving unauthorized access to or use of customer information has occurred or is reasonably likely to have occurred" and "include details about the incident, the breached data, and how affected individuals can respond to the breach to protect themselves."[113]

Regulation S-ID, known as the "Identity Theft Red Flags Rules," requires covered entities that maintain certain types of accounts for clients to establish and maintain programs that detect, prevent, and mitigate identity theft.[114] As with the Safeguards Rule, the SEC actively enforces violations of this regulation. For example, in September 2018, the SEC reached a settlement with Voya Financial Advisors Inc. to resolve allegations that the company had violated the Safeguards Rule and the Identity Theft Red Flags Rule.[115] The charge represented the SEC's first enforcement

© Copyright 2026

action alleging violations of the Identity Theft Red Flags Rule.[116] In July 2022, the SEC charged JPMorgan, UBS, and TradeStation $1.2 million, $925,000, and $425,000, respectively, for violating the Identity Theft Red Flags Rule, marking its second enforcement action.[117] More recently, in 2025, the SEC reached a $45 million settlement with the broker-dealers Robinhood Securities LLC and Robinhood Financial LLC, which were charged with violating more than 10 separate Securities Laws provisions, including both Regulations S-P and S-ID.[118]

Thus, an employee who reports an employer's failure to have an adequate identity theft program may be eligible for SOX protection, provided that the employer is a publicly traded company or a wholly owned subsidiary or affiliate of one. Unlike the other categories of protected activity, however, Dodd-Frank may protect employees of non-public companies for raising these concerns, so long as those companies are subject to Regulations S-P and S-ID, such as registered investment companies or registered investment advisors.[119]

In thinking about proceeding with a retaliation claim under any of these theories of protected activity, a March 2026 decision by a federal court in California is instructive. In that case, in which the plaintiff asserted SOX retaliation based on reporting cybersecurity deficiencies and failures to protect user data, the court dismissed the complaint upon finding that the plaintiff had failed to adequately allege he engaged in protected activity. The court identified the following as insufficient to constitute protected activity under SOX: (a) broad references in the complaint to the plaintiff having filed a Form TCR (i.e., a tip) with the SEC; (b) allegations contained in documents incorporated by reference into the complaint, such as the plaintiff's OSHA charge; (c) allegations that the defendant engaged in "securities fraud through misrepresentations about [the company's] security capabilities in public filings and statements"; and (d) alleged failures to maintain internal controls related to their cybersecurity practices.[120] The primary throughline in the court's decision was that the complaint lacked non-conclusory allegations to support his claims that he engaged in protected activity. This should serve as a reminder for SOX plaintiffs that in order to survive a motion to dismiss, they must provide non-conclusory facts to support their claims.

b) Adverse Action

Section 806 of SOX states that no company "may discharge, demote, suspend, threaten, harass, or in any other manner discriminate against an employee in the terms and conditions of employment" because the employee engaged in protected activity under SOX.[121] Dodd-Frank has similar language, providing that an employer may not "discharge, demote, suspend, threaten, harass, directly or indirectly, or in any other manner discriminate against, a whistleblower in the terms and conditions of employment."[122]

The ARB has interpreted SOX's statutory language to evince a "clear congressional intent to prohibit a very broad spectrum of adverse action against SOX whistleblowers,"[123] adding that "adverse action under SOX Section 806 must be more expansively construed than [adverse action] under Title VII."[124] In keeping with this position, the DOL has long permitted non-tangible employment actions to form the basis for a SOX retaliation claim, such as outing an employee as a whistleblower or blackballing.[125] In the years since *Menendez*, several federal courts have similarly held that a variety of non-tangible employment actions constitute adverse actions for

© Copyright 2026

purposes of a SOX retaliation claim, including outing, blackballing, and poor performance reviews.[126] Federal courts differ, however, in whether they have adopted the ARB's more liberal standard for adverse action in reaching the conclusion that non-tangible employment actions qualify. Some courts still analyze adverse actions under SOX using the Title VII retaliation standard, which requires that the action be "harmful enough that it well might have dissuaded a reasonable worker from engaging in statutorily protected whistleblowing."[127] In practice, however, it is difficult to identify instances where courts have determined that an action qualifies as an adverse action under the SOX standard, but not under the Title VII standard. A plaintiff need only prove that her protected activity was a contributing factor in her employer's decision to subject her to an adverse action.[128] She does not need to prove that her employer acted with "retaliatory intent" in taking the adverse action.[129]

There is far less guidance about what constitutes an adverse action under Dodd-Frank. Due to the similarities between the adverse action language of SOX and Dodd-Frank, there is reason to believe that courts would apply the same standard to actions brought under the latter statute. However, the ARB has no jurisdiction over Dodd-Frank claims, so its liberal adverse action standard is due no deference in that context. Moreover, what guidance does exist from the courts has not aligned with the ARB's interpretation. While at least one federal court has applied SOX's adverse action analysis in its interpretation of a Dodd-Frank claim,[130] that same court later applied the more restrictive Title VII standard in that same case.[131] Further, other courts across the country have tended to defer to the "materially adverse" standard established for Title VII retaliation claims in analyzing claims brought under Dodd-Frank.[132] These decisions, however, contain almost no analysis of the appropriate adverse action standard, instead adopting the Title VII standard with little discussion.

c) Procedure

In contrast to the overlap between protected activity and adverse actions under SOX and Dodd-Frank, there is virtually no procedural overlap between the two statutes. Under SOX, employees must file claims of retaliation with the DOL's Occupational Safety and Health Administration (OSHA) within 180 days after the date of the adverse action.[133] OSHA then has 60 days to investigate and issue written findings as to whether there is reasonable cause to believe that the employer has retaliated against the employee.[134] Following OSHA's written findings, either party has 30 days to request a hearing with an administrative law judge (ALJ), and the parties have the opportunity to conduct discovery before the hearing.[135] Either party may appeal the ALJ's ruling to the ARB within 14 days of the ALJ's ruling.[136] Both parties then have 60 days to appeal the ARB's ruling to the U.S. Court of Appeals for the jurisdiction either in which the violation allegedly occurred or in which the complainant resided on the date of the violation.[137] If the ARB has not issued a final decision within 180 days of the employee's filing of the complaint, the employee has the right to "kick out" her complaint to an appropriate federal district court.[138] In practice, few cases receive final decisions within 180 days.

Importantly, predispute arbitration agreements are not enforceable with respect to SOX claims, so even if the whistleblower has signed an arbitration clause, her SOX claim cannot be compelled to arbitration.[139]

The procedure for filing complaints under Dodd-Frank is far less complicated. An individual alleging retaliation in violation of Dodd-Frank may file her complaint directly

© Copyright 2026

in an appropriate federal district court.[140] The employee's complaint of retaliation must be filed within six years of the date on which the retaliation occurred or, alternatively, three years of the date when facts material to the right of action were known or reasonably should have been known by the employee (but in no case may the complaint be filed more than 10 years after the date on which the retaliation occurred).[141]

2. Protections for Banking and Consumer Finance Whistleblowers

In the wake of the 1980s Savings and Loans Crisis, Congress passed the Financial Institutions Reform Recovery and Enforcement Act of 1989 (FIRREA), which provides broad protections against retaliation for employees of both banking institutions and banking agencies.[142] Many years later, as noted above, Congress enacted the Dodd-Frank Wall Street Reform and Consumer Protection Act of 2010 in response to a different crisis: the Great Recession. Title X of the Dodd-Frank Act, known as the Consumer Financial Protection Act (CFPA), established the Consumer Financial Protection Bureau (CFPB) to regulate consumer finance products and services and protect consumers from unfair, deceptive, or abusive practices.[143] The CFPA prohibits retaliation against employees of consumer finance product and service providers who report violations of the statute or any other law subject to the jurisdiction of the CFPB.[144] Whistleblowers in banking or other consumer finance sectors who report insufficient data security measures could qualify for protections under these statutes.

a) Protected Activity

FIRREA protects employees of "insured depository institutions"—i.e., any bank for which the Federal Deposit Insurance Corporation (FDIC) insures deposits—and employees of federal banking agencies who engage in protected activity.[145] The basis for protected activity under FIRREA is quite liberal. A report of a *possible* violation of *any* law or regulation, as well as of any gross mismanagement, waste, abuse, or danger to public health or safety, qualifies.[146] In the cybersecurity and data privacy context, for example, this standard would protect a disclosure of insufficient data security if it constituted a possible violation of the Gramm-Leach-Bliley Act (GLBA),[147] which requires financial institutions to protect certain consumer data, or of Section 5 of the Federal Trade Commission Act of 1914 (FTCA),[148] which prohibits unfair or deceptive practices in commerce, including insufficient data security practices.[149]

Critically, FIRREA only protects a whistleblower if she reports externally to a federal banking agency or the U.S. Attorney General (i.e., the DOJ).[150] Internal complaints of violations of law by employees at insured depository institutions do not constitute protected activity under FIRREA.[151] In addition, FIRREA explicitly denies protection to an employee who deliberately caused or participated in the misconduct or knowingly or recklessly provided substantially false information to the banking agency or Attorney General.[152] Employees considering reporting wrongful activity must also be careful not to improperly reveal confidential supervisory information through their reports.[153] Such a disclosure, even in the context of a whistleblower report or to the whistleblower's attorney, could violate the stringent regulations prohibiting the

© Copyright 2026

dissemination of supervisory information and could potentially expose a whistleblower to criminal liability.[154]

As for the CFPA, the statute protects employees who provide information relating to a violation of: (a) any provision of the CFPA; (b) any other provision of law that is subject to the jurisdiction of the CFPB; or (c) any rule, order, standard, or prohibition prescribed by the CFPB.[155] In order for a disclosure to be protected, the employee must make the report to her employer, the CFPB, or any other state, local, or federal government authority or law enforcement agency.[156] The whistleblower need only possess a reasonable belief[157] that the information she disclosed constituted a violation of law.[158]

As is relevant in the cybersecurity context, the CFPB has jurisdiction for enforcing certain provisions of the GLBA. Specifically, the CFPB enforces the sections of the GLBA that relate to governance of NPI by financial institutions.[159] Generally, NPI encompasses any non-publicly available information that (1) a consumer provides to a financial institution to obtain a financial product or service from the institution; (2) results from a transaction between the consumer and the institution involving a financial product or service; or (3) a financial institution otherwise obtains about a consumer in connection with providing a financial product or service.[160] Under the GLBA, subject to certain exceptions, financial institutions are prohibited from disclosing NPI about consumers to nonaffiliated third parties unless (a) the institution meets specific requirements for giving notice and the right to opt out; and (b) the consumer has not elected to opt out of the NPI disclosure.[161] Additionally, the GLBA requires financial institutions to provide notice of its privacy policies and practices to consumers.[162] Thus, if, for example, an employee working at a consumer financial institution reports her reasonable belief that her employer is violating the GLBA by making unauthorized disclosures of consumer NPI, her report should be protected by the CFPA. Similarly, an employee who believes that her employer is misrepresenting its information-sharing policies to customers and reports as much to her employer has likely engaged in protected activity under the CFPA.

b) Adverse Action

FIRREA prohibits depository banks and federal banking regulators from discharging or otherwise discriminating against any employee with respect to compensation, terms, conditions, or privileges of employment because the employee engaged in protected activity.[163] The causation standard under FIRREA is a liberal one, requiring a plaintiff to prove only that her protected activity was a contributing factor in her employer's decision to terminate or otherwise discriminate against her.[164] Courts attempting to define an actionable adverse action under FIRREA have differed, with some adopting the adverse action standard from Title VII discrimination claims[165] and others adopting the standard from Title VII retaliation claims.[166]

While there are few cases analyzing retaliation claims under the CFPA, due to the similarities between the language of the statutes, a court's interpretation of the adverse action element under SOX would likely be instructive as to how that court would analyze adverse actions under the CFPA.[167]

© Copyright 2026

c) Procedure

Under FIRREA, a whistleblower who has experienced retaliation has the right to file a civil action in the appropriate United States district court.[168] The whistleblower must do so within two years of the date of the retaliatory action.[169] The statute requires that a whistleblower simultaneously file a copy of her complaint with the appropriate federal banking agency.[170]

The CFPA, in contrast, requires whistleblowers to exhaust their administrative remedies before filing in court, mirroring the procedural requirements of SOX. Employees must file claims of retaliation with OSHA within 180 days after the date of the adverse action.[171] OSHA then has 60 days to investigate and issue written findings as to whether there is reasonable cause to believe that the employer has retaliated against the employee.[172] Following OSHA's written findings, either party has 30 days to request a hearing with an ALJ, and the parties have the opportunity to conduct discovery before the hearing.[173] Either party may appeal the ALJ's ruling to the ARB within 14 days of the ALJ's ruling.[174] Both parties have 60 days to appeal the ARB's ruling to the U.S. Court of Appeals for the jurisdiction either in which the violation allegedly occurred or in which the complainant resided on the date of the violation.[175] If the ARB has not issued a final decision within 210 days of the employee's filing of the complaint, or within 90 days after the issuance of written findings, the employee has the right to "kick out" her complaint to an appropriate federal district court.[176] As with SOX claims, predispute arbitration agreements are not enforceable with respect to CFPA retaliation claims (with a narrow exception carved out for arbitration provisions in collective bargaining agreements in some circumstances).[177]

3. False Claims Act Protections

The federal False Claims Act (FCA)[178] was passed in 1863 in the midst of the American Civil War in response to "alarming reports of misappropriation of money supposedly spent to aid the war effort."[179] The FCA authorizes private citizens who observe fraud against the government to file a "*qui tam*" claim on behalf of the government and share in any recovery against the wrongdoer.[180] In 1986, the FCA was amended to protect employees who report such fraud from retaliation,[181] and subsequent amendments made in 2009[182] and 2010[183] strengthened the retaliation protection. FCA protections may be available to an employee who reports her employer's failure to maintain adequate cybersecurity or data privacy measures as required by a government contract.

Employees who oppose their government contractor employer's cybersecurity deficiencies may be entitled to protection against retaliation.

a) Protected Activity

The FCA protects employees, contractors, agents, or "associated others" who investigate or file a *qui tam* lawsuit or engage in lawful activities in an attempt to stop government fraud.[184] Originally, whistleblowers were only entitled to protection when they experienced retaliation "because of lawful acts done by the employee on behalf of the employee or others in furtherance of an action under this section[.]"[185] For years, many courts interpreted this to mean that the FCA protections against

© Copyright 2026

retaliation applied only when a plaintiff could demonstrate that FCA litigation was a "distinct possibility" or that she had engaged in conduct that "reasonably could lead to a viable FCA action."[186] The Fraud Enforcement and Recovery Act of 2009 (FERA) amended the FCA to protect whistleblowers from retaliation for "efforts to stop 1 or more violations of [the FCA]."[187] While the legislative history of FERA clearly indicates that Congress intended the Act's protections against retaliation to be broadly construed,[188] it has taken several years for the courts to recognize the broadened scope of protected activity under the statute.[189] Even now, some district courts, relying on pre-amendment precedent, occasionally apply the "distinct possibility" and "viable action" standards that restrict the protections of the statute.[190]

To understand how a private company's cybersecurity and data security challenges could constitute actionable fraud against the government, it is critical to first understand what constitutes a false claim under the FCA. There are two categories of false claims under the FCA: a factually false claim and a legally false claim.[191] A factually false claim occurs when a claimant misrepresents what goods or services it has provided to the government.[192] A legally false claim is based on one of two "false certification" theories of liability: express false certification or implied false certification.[193] Express false certification occurs when a claimant falsely certifies that it is in compliance with regulations that are requirements for government payment.[194] Implied false certification occurs when a claimant submits a request for payment without disclosing that the claimant is in violation of a regulation or requirement that affects its eligibility for payment.[195] To qualify as an implied false certification, the claimant must make specific representations about the goods or services in its submission that are rendered misleading by the claimant's failure to disclose its noncompliance with the regulation or requirement.[196] Critically, the noncompliance must concern a material requirement.[197]

With the federal government's expanding cybersecurity and data privacy requirements, the likelihood that a cybersecurity whistleblower's disclosure might qualify as actionable fraud under the FCA has increased. Over the past decade or so, companies contracting with the government have become subject to a number of heightened cybersecurity requirements, including changes to the Federal Acquisition Regulation (FAR) that have increased cybersecurity standards for companies pursuing contracts with the government.[198] One rule, FAR 52.204-21, requires certain companies with government contracts to implement a lengthy list of procedures designed to safeguard their information systems.[199] In addition to changes to the FAR, the DOD published a rule in the Defense Federal Acquisition Regulation Supplement (DFARS) requiring certain DOD contractors to adhere to the standards set forth in National Institute of Standards and Technology (NIST) Special Publication 800-171, which provides detailed regulations for "Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations."[200] The rule also significantly increased the scope of information that contractors are responsible for securing. Under DFARS 252.204-7012, rather than only being responsible for securing information received from the government, contractors are also responsible for securing information that is "collected, developed, received, transmitted, used, or stored by or on behalf of the contractor in support of the performance of the contract."[201]

In September 2020, the DOD issued an interim final rule to further elaborate on the verification processes for government contractors to ensure that they are protecting

© Copyright 2026

sensitive unclassified information.[202] The rule created a five-year roll-out of the Cybersecurity Maturity Model Certification (CMMC) framework, which provides for different levels of cybersecurity requirements for government contractors.[203] Following industry feedback on the initial iteration of the CMMC framework, a streamlined version of the framework—CMMC 2.0—was announced in November 2021.[204]

The CMMC 2.0 framework contains three levels. Level 1, which applies to government contractors that only handle Federal Contract Information (FCI),[205] requires an annual self-assessment and affirmation of compliance with requirements outlined in FAR 52.204-21.[206] Level 2, which applies to contractors that handle Controlled Unclassified Information (CUI), requires either an assessment by an authorized CMMC Third-Party Assessment Organization (C3PAO) or, in some cases, a self-assessment, every three years and annual affirmation verifying compliance with the requirements in NIST SP 800-171.[207] Level 3, which applies to contractors handling CUI that relates to Advanced Persistent Threats, requires achieving Level 2 CMMC status and undergoing an assessment by the Defense Contract Management Agency's (DCMA) Defense Industrial Base Cybersecurity Assessment Center (DIBCAC) every three years, along with annual affirmation verifying compliance with enhanced security requirements in NIST SP 800-172.[208]

After a lengthy review process, the finalized CMMC framework was published into the federal register on October 15, 2024 as a final rule, which then became effective on December 16, 2024.[209] To implement the finalized CMMC Program, DOD issued a long-awaited final rule on September 10, 2025 that incorporated the Program requirements into new DOD contracts.[210] The CMMC framework began Phase 1 of its implementation, which introduces the Level 1 and Level 2 assessments, on November 10, 2025.[211] Phase 1 is expected to last until November 2026, at which point the next phase of implementation will begin.[212]

Because employers seeking contracts with the DOD and other agencies of the federal government are subject to these requirements, their failure to adhere to those standards may give rise to a viable claim under the FCA for express or implied false certification depending on the specific facts of the case.[213] Cybersecurity professionals who speak out against their government-contractor employer's failure to meet these standards may therefore be entitled to the broadly construed protections against retaliation provided by the FCA.[214]

The following hypothetical demonstrates the kind of report that would be protected by the FCA. A company wins a contract to develop modeling software for a government agency. Late in the development process, a software engineer learns of a critical flaw rendering the software vulnerable to a data breach. She notifies senior leadership at the company of the flaw and explains to them that resolving the issue will require starting over from scratch, requiring months of work and several million dollars. She explains that doing so is necessary, however, to adhere to applicable FARs. Rather than notifying the government agency of the issue and starting over, the company terminates the software engineer and ignores the cybersecurity flaw. Depending on the language of the company's contract with the agency, its subsequent invoice may represent a factually false claim and its material violation of applicable FARs may represent a legally false claim. As a result, the software engineer's efforts to stop the company from defrauding the government will be protected under the FCA.

© Copyright 2026

There are also more straightforward examples of cybersecurity issues that would lead to the submission of false claims to the government. Suppose, for example, that a government contractor wins a bid to develop encryption software for the DOD, but the software that the contractor develops contains serious cybersecurity flaws rendering it so insecure that the government will be unable to use it. If an employee raises concerns about the cybersecurity flaws, she is raising concerns about the contractor failing to fulfill the terms of the contract and is therefore engaging in protected activity under the FCA. Indeed, in 2019, the government successfully prosecuted Cisco Systems for just this type of alleged misconduct.[215]

As discussed above, several DOJ settlements in recent years serve as additional examples of companies being held accountable through *qui tam* actions for failing to adhere to cybersecurity requirements in connection with DOD contracts.[216]

b) Adverse Action

An employee has suffered an adverse action within the bounds of the FCA anti-retaliation provision when that employee is discharged, demoted, suspended, threatened, harassed, or in any other manner discriminated against in the terms and conditions of employment.[217] Retaliation claims under the FCA are scrutinized under the same test as retaliation claims under Title VII: an adverse action is one that might have dissuaded a reasonable worker from engaging in the protected conduct.[218] Tangible employment actions, such as termination, demotion, and pay and benefit cuts, qualify as adverse actions under this standard, as can many other actions, such as written warnings, diminished responsibilities, or auditing an employee's job performance.[219]

c) Procedure

An FCA retaliation plaintiff must bring her claim in federal district court within three years of the date of the retaliation.[220] Unlike FCA *qui tam* actions, FCA retaliation claims under Section 3730(h) do not require a plaintiff to comply with often onerous filing and procedural requirements, such as filing under seal (filing the complaint confidentially with the court) and submitting a disclosure statement, unless a plaintiff is including a retaliation claim with her *qui tam* claim.[221] Additionally, if an employee files suit with both a *qui tam* and retaliation claim and her *qui tam* claim is subsequently dismissed, her Section 3730(h) retaliation claim may survive without it.[222]

4. Anti-Money Laundering Act Protections

While money laundering and cybersecurity may not be intuitively connected, FinCEN, an agency within the Department of Treasury, has long identified cybercrime as an important priority in the fight against money laundering.[223] The Department of Treasury "is particularly concerned about cyber-enabled financial crime, ransomware attacks, and the misuse of virtual assets that exploits and undermines their innovative potential, including through laundering of illicit proceeds."[224]

With the passage of the Anti-Money Laundering Act of 2020 (AMLA), which amended the Bank Secrecy Act of 1970 (BSA), not only did Congress enact a comprehensive set of reforms to anti-money laundering laws in the United States, but it expanded

© Copyright 2026

whistleblower protections that can help protect a cybersecurity whistleblower who reports potential violations of anti-money laundering laws.[225]

a) Protected Activity

The AMLA protects whistleblowers from retaliation for providing information to (i) the Department of Treasury or DOJ; (ii) a federal regulatory or law enforcement agency; (iii) any member or committee of Congress; or (iv) "a person with supervisory authority over the whistleblower, or such other person working for the employer who has the authority to investigate, discover, or terminate misconduct."[226] Under the AMLA, the report may qualify as protected activity even if it is part of the whistleblower's job duties to report on such matters.[227] Protected activity also includes "initiating, testifying in, or assisting in any investigation or judicial or administrative action of the Department of the Treasury or the [DOJ]."[228]

In order to gain whistleblower protection under the AMLA, the whistleblower need only have a reasonable belief that the conduct she is reporting is a violation of any law, rule, or regulation subject to the jurisdiction of the Department of Treasury, or a violation of criminal statutes against money laundering (18 U.S.C. §§ 1956, 1957, 1960).[229] Many such rules and regulations potentially relate to cybersecurity and data privacy. For example, BSA regulations require financial institutions to submit Suspicious Activity Reports (SARs) for suspicious transactions involving $5,000 or more in assets.[230] Through a guidance document issued in 2016, FinCEN explained to financial institutions how BSA regulations and requirements apply to cyber events, cyber-enabled crime, and cyber-related information.[231] FinCEN advised that "[i]f a financial institution . . . has reason to suspect that a cyber-event was intended, in whole or in part, to . . . affect a transaction or a series of transactions, it should be considered part of an attempt to conduct a suspicious transaction or series of transactions."[232] FinCEN further stated that "financial institutions should include available cyber-related information when reporting *any* suspicious activity, including those related to cyber events as well as those related to other activity, such as fraudulent wire transfers."[233] Thus, if an employee of a financial institution reports that their employer is failing to accurately report cyber activity relating to its SARs, that report is likely protected under the AMLA.

b) Adverse Action

The statute has an expansive definition of adverse action and provides that "[n]o employer may, directly or indirectly, discharge, demote, suspend, threaten, blacklist, harass, or in any other manner discriminate against a whistleblower in the terms and conditions of employment or post-employment" because of the employee's engagement in protected activity.[234] In other words, this provision expressly encompasses adverse actions short of termination, such as blacklisting and harassment. It also explicitly encompasses actions committed by the employer during and after the whistleblower's employment.

© Copyright 2026

c) Procedure

To pursue a retaliation claim under the AMLA, a whistleblower must first file a complaint with the DOL.[235] If the DOL does not issue a decision within 180 days of the filing, then the whistleblower may bring an action against her employer in federal district court.[236] Notably, the statute provides that "[n]o predispute arbitration agreement shall be valid or enforceable, to the extent the agreement requires arbitration of a dispute arising under this section."[237] Thus, even if the whistleblower has an agreement with the employer requiring her to arbitrate disputes arising from her employment, she cannot be forced to arbitrate her AMLA retaliation claim. A whistleblower has up to six years after the retaliatory action to file her claim in court or, alternatively, up to three years after the date when the facts material to the retaliation become known to the employee, or reasonably should have been known to her.[238] A successful whistleblower may be entitled to reinstatement, double back pay, compensatory damages (including litigation costs and attorneys' fees), and "any other appropriate remedy."[239]

5. Protections for Nuclear Whistleblowers

The Energy Reorganization Act of 1974 (ERA) protects employees who provide information about or participate in investigations relating to violations of nuclear safety laws and standards.[240] Employees who speak out against cybersecurity vulnerabilities in the nuclear industry may be entitled to the same protections as those who report safety issues.

a) Protected Activity

The ERA protects an employee from discrimination because she: (a) notified her employer of violations of the ERA, the Atomic Energy Act, or Nuclear Regulatory Commission (NRC) regulations; (b) refused to engage in such violations; (c) testified before Congress or at any federal or state proceeding regarding the ERA or Atomic Energy Act; (d) or commenced, testified in, or otherwise participated in an NRC proceeding.[241] While protected activity has traditionally concerned safety issues, such as meltdown risks or nuclear-materials storage, there are NRC regulations relating to cybersecurity. In 2009, NRC issued a nuclear safety standard entitled "Protection of Digital Computer and Communications Systems and Networks."[242] Under this regulation, NRC licensees[243] "shall provide high assurance that digital computer and communication systems and networks are adequately protected against cyber attacks[.]"[244] The regulation and its accompanying regulatory guide,[245] as updated in February 2023,[246] provide for detailed cybersecurity responsibilities to which NRC licensees must adhere.[247] The lengthy guidance documents—the most recent iteration spans some 160 pages—provide granular information to NRC licensees concerning cyber event reporting obligations, best practices to mitigate cyber vulnerabilities, and requirements for maintaining and documenting sufficiently rigorous cybersecurity plans. Per the definition of protected activity stated above, any employee of an NRC licensee has engaged in protected activity under the ERA's anti-retaliation provisions if she opposed practices by her employer that she reasonably believed violated these cybersecurity regulations.

© Copyright 2026

b) Adverse Action

The ERA prohibits an employer from discharging or otherwise discriminating against any employee with respect to her compensation, terms, conditions, or privileges of employment because that employee engaged in protected activity under the ERA.[248] To qualify as an adverse action, the complainant must prove that the action significantly changed her employment status, meaning that the employer's actions were "harmful to the point that they could well have dissuaded a reasonable worker from engaging in protected activity."[249] Adverse actions thus include not only tangible employment actions, such as terminations, demotions, and pay and benefits cuts, but also non-tangible actions such as blacklisting.[250]

c) Procedure

Employees must file complaints under the ERA with the DOL within 180 days of the date the employer made the retaliatory decision and communicated it to the employee.[251] The DOL's OSHA then has 30 days to investigate and issue written findings as to whether there is reasonable cause to believe that the employer has unlawfully retaliated against the employee.[252] Following OSHA's written findings, either party has 30 days to request a *de novo*, on-the-record hearing with an ALJ.[253] Either party may then appeal the ALJ's ruling to the ARB within 10 days of the ruling.[254] Once the ARB has issued a decision, both parties then have 60 days to appeal the ARB's ruling to the United States Court of Appeals for the jurisdiction in which either the violation occurred or the complainant resided on the date of the violation.[255] In addition to these appeal rights, if the DOL has not issued a final decision within one year of the employee's filing of the complaint, the employee has the right to "kick out" her complaint to an appropriate federal district court.[256]

6. Protections for Federal Government Employees

Given the recent high-profile cyberattacks by foreign powers against the United States— not to mention incidents such as the DOGE scandal discussed above, in which Charles Borges blew the whistle on practices of the U.S. government itself that compromised sensitive data on hundreds of millions of Americans—cybersecurity and data privacy are and will continue to be a serious issue for federal employees. The Whistleblower Protection Act (WPA),[257] as amended by the Whistleblower Protection Enhancement Act (WPEA),[258] work together to provide meaningful protections to cybersecurity whistleblowers within the federal government.

Given recent high-profile cyberattacks against the United States, cybersecurity remains a serious issue for federal employees.

a) Protected Activity

As amended by the WPEA, the WPA prohibits adverse personnel actions against employees of the federal government who disclose information based on a reasonable belief of: (a) a violation of any law, rule, or regulation; (b) gross mismanagement, a gross waste of funds, or an abuse of authority; or (c) a substantial and specific danger to public health or safety.[259] Such a disclosure is not protected, however, if it is prohibited by law or executive order.[260] Due to this relatively broad language, to garner protections under the WPA, a federal employee who raises concerns about cybersecurity likely would not need to point to a particular law or regulation she thinks is being violated. Rather, she likely need only indicate in her report that the

© Copyright 2026

cybersecurity lapse at issue constitutes gross mismanagement, abuse of authority, or a substantial danger to public safety.

Such an argument would be significantly bolstered, however, by pointing to a particular law, regulation, or Executive Order calling on an agency to meet certain cybersecurity standards. For example, in 2013, in Executive Order 13636, President Obama called on "[a]gencies with responsibility for regulating the security of critical infrastructure" to adopt a (then yet-to-be-written) Cybersecurity Framework to be created by NIST.[261] In 2014, NIST published that Cybersecurity Framework, which it then updated in 2018.[262] In May 2017, a subsequent Executive Order extended the NIST standards to all federal government agencies.[263] Unless or until the Executive Order is rescinded, an employee at one of those agencies who suffers retaliation because she complained about her agency's failure to timely adopt or adequately implement the NIST standards should be protected against retaliation.

b) Adverse Action

The WPA prohibits a federal agency from taking or failing to take, or threatening to take or fail to take, a personnel action because of the employee's protected activity.[264] A report issued by the U.S. Merit Systems Protection Board (MSPB) provides a helpful list of personnel actions that could constitute an adverse action under the WPA:

- An appointment;
- A promotion;
- An action under chapter 75 of Title 5 or other disciplinary or corrective action, including any behavior intended to modify the employee's behavior in the future, such as a letter of admonishment;
- A detail, transfer, or reassignment;
- A reinstatement;
- A restoration;
- A reemployment;
- A performance evaluation under chapter 43 of Title 5;
- A decision concerning pay, benefits, or awards, or concerning education or training if the education or training may reasonably be expected to lead to an appointment, promotion, performance evaluation, or other action described in this subparagraph, including placing an employee in a leave without pay (LWOP) or absent without leave (AWOL) status, a denial of annual leave, or a denial of an opportunity to earn overtime pay;
- A decision to order psychiatric testing or examination; and
- Any other significant change in duties, responsibilities, or working conditions, including retaliatory investigations.[265]

In 2015, the MSPB held that the creation of a hostile work environment may also constitute a prohibited personnel action under the WPA.[266]

c) Procedure

A federal whistleblower has four potential avenues to pursue her claims under the WPA. First, in some cases, the employee may appeal the adverse action directly to the MSPB, which is known as a "Chapter 77" appeal.[267] Chapter 77 appeals are available to federal employees who suffer certain adverse employment actions because of alleged deficiencies in their conduct[268] or performance.[269] A whistleblower who brings a Chapter 77 appeal is alleging that her employer actually

© Copyright 2026

took an adverse action against her because of her protected activity, not because of any purported deficient conduct or performance.[270] Employees may obtain judicial review of a final order or decision issued by the MSPB.[271] Generally, such petitions to review a final MSPB order or decision are to be filed in the United States Court of Appeals for the Federal Circuit or any other court of appeals of competent jurisdiction.[272]

Second, the employee may file a charge with the U.S. Office of Special Counsel (OSC).[273] If the OSC finds the complaint meritorious, it can seek corrective action from the offending federal agency.[274] If the agency fails to take appropriate corrective action, the OSC can petition the MSPB for corrective action on the employee's behalf.[275] If the MSPB orders corrective action, such corrective action may include that the employee be placed, as nearly as possible, in the position she would have been had the retaliation not occurred, as well as reimbursement for attorney's fees, back pay and related benefits, medical costs incurred, travel expenses, any other reasonable and foreseeable consequential damages, and compensatory damages.[276] Again, employees may seek judicial review of any final MSPB order or decision.[277]

Third, the employee may bring an individual right of action (IRA) to the MSPB if the OSC declines to bring one on her behalf.[278] To bring an IRA, the employee must show: (1) she engaged in whistleblowing activity by making a protected disclosure; (2) based on the protected disclosure, the agency took or failed to take a personnel action (or made such a threat); (3) she sought corrective action from the OSC; and (4) she exhausted corrective action proceedings before the OSC.[279] A federal whistleblower has a right to file an IRA beginning 60 days after the OSC closes its investigation of her claims or 120 days after filing her complaint with the OSC.[280] Such IRA appeals are filed with one of the MSPB's field or regional offices, which then assigns it to an administrative judge (AJ).[281] The whistleblower may then appeal the AJ's decision to the three-member Board of the MSPB on a petition for review (PFR).[282] The whistleblower may also appeal either the AJ's initial decision or the PFR decision to the appropriate U.S. Court of Appeals.[283]

Finally, if the employee is a union member, she can pursue a grievance under her union's negotiated grievance procedures.[284] An aggrieved employee affected by a prohibited personnel action is precluded from choosing both the negotiated and statutory avenues of redress.[285] In other words, a federal employee may pursue a claim for whistleblower retaliation by pursuing a grievance under the union's negotiated procedures or by filing a complaint with the OSC or a direct appeal to the MSPB.[286] However, if the employee chooses the negotiated procedures, she is still entitled to request a review of the final decision by the MSPB, where appropriate.[287] Under the All Circuit Review Act,[288] signed into law in July 2018, whistleblowers proceeding under the WPA anti-retaliation provision may appeal MSPB decisions to *any* U.S. Court of Appeals (not just the Court of Appeals for the Federal Circuit), provided theirs is not a "mixed case," i.e., a case that also involves an allegation of discrimination.[289]

7. Protections for Employees of Federal Contractors

Just as the federal government is a target for cybersecurity attacks, so too are its contractors. The Defense Contractor Whistleblower Protection Act (DCWPA), initially

© Copyright 2026

passed in 1986, created anti-retaliation protections for contractors of the DOD and the National Aeronautics and Space Administration (NASA).[290] The National Defense Authorization Act for Fiscal Year 2013 (NDAA) included a four-year pilot program expanding DCWPA protections to all government contractors.[291] Congress passed, and President Obama signed, a bill making the extended protections permanent on December 14, 2016.[292]

a) Protected Activity

Under the NDAA, an employee of a federal contractor is protected for making disclosures regarding several forms of misconduct by her employer.[293] To be protected by the Act, the employee must disclose information the employee reasonably believes evidences:
gross mismanagement of a Federal contract or grant, a gross waste of Federal funds, an abuse of authority relating to a Federal contract or grant, a substantial and specific danger to public health or safety, or a violation of law, rule, or regulation related to a Federal contract (including the competition for or negotiation of a contract) or grant.[294]

The disclosure must be made to one or more of the following persons or entities:
(A) A Member of Congress or a representative of a committee of Congress.
(B) An Inspector General.
(C) The Government Accountability Office.
(D) A Federal employee responsible for contract or grant oversight or management at the relevant agency.
(E) An authorized official of the DOJ or other law enforcement agency.
(F) A court or grand jury.
(G) A management official or other employee of the contractor, subcontractor, or grantee who has the responsibility to investigate, discover, or address misconduct.[295]

Taken together, an employee of a government contractor who reports "a violation of law, rule, or regulation related to a Federal contract" to a "management official" or other "employee . . . who has the responsibility to investigate, discover, or address misconduct" has engaged in protected activity under the NDAA.

In the cybersecurity context, protected activity under the NDAA could take a number of forms, most of which mirror the sorts of protected activity that would form the basis for an FCA claim. As explained in the section on the FCA, *see supra* Section II.A.3, the FAR requires that certain companies with government contracts implement a series of safeguarding procedures to protect their information systems.[296] The DFARS imposes heightened requirements on certain defense contractors, mandating compliance with the detailed standards set forth in NIST SP 800-171.[297] Under this regulatory framework, defense contractors are responsible for securing both information that is received from the government and information that is "collected, developed, transmitted, received, used, or stored by or on behalf of the contractor in support of the performance of the contract."[298] In 2023, the DOD issued a final rule to enhance the protection of information by implementing a framework to assess contractors' implementation of cybersecurity requirements.[299] More recently, in June 2026, the FAR Council proposed a rule that would simplify cybersecurity requirements by amending the FAR to extend NIST SP 800-171 standards to all covered government contractors—not just defense contractors—handling CUI.[300]

© Copyright 2026

There are also laws applicable to federal contractors pertaining to data privacy. For example, federal contractors that contract to operate a system of records to accomplish agency functions are also subject to the Privacy Act of 1974.[301] The Privacy Act provides safeguards against the misuse of federal agency records and requirements regarding how such records must be collected, maintained, and disseminated.[302] In addition, pursuant to a rule finalized in 2017, federal contractors must also meet training requirements regarding the handling and safeguarding of personally identifiable information.[303]

Because employers seeking contracts with the DOD and other federal agencies are subject to these requirements, their failure to adhere to those standards may give rise to a viable claim under the NDAA, provided that the employee could argue that the regulation "relate[s] to" the contract in question.[304] Cybersecurity and data privacy professionals who speak out against their government-contractor employer's failure to meet these standards may therefore be entitled to the broad protections against retaliation provided by the NDAA. Employees should take care to clarify that they are expressing concerns about the legality of their employer's actions, since some courts have suggested that mere "expressions of concern" or "differences of opinion" about an employer's behavior do not constitute protected activity under the Act.[305]

b) Adverse Action

Under the NDAA, a federal contractor may not discharge, demote, or otherwise discriminate against an employee for engaging in any of the forms of protected activity described above.[306] An employee must show only that her protected activity was a "contributing factor" in the employer's decision to take an adverse employment action.[307]

There are few cases articulating the standard for what constitutes an adverse action under NDAA. At least one District Court has found that, aside from discharge and demotion, an adverse action under the NDAA includes "intentional conduct which resulted in a significant adverse change in duties, responsibilities, or working conditions."[308] It is also likely that a court would apply the Title VII retaliation standard, given the similarities between the language of the two statutes. Under the Title VII standard, an action is adverse if "it well might have dissuaded a reasonable worker from making or supporting a charge of discrimination."[309] This standard includes tangible personnel actions, such as terminations, demotions, and pay or benefits cuts. It also includes harmful actions such as outing a whistleblower,[310] blackballing,[311] or even a series of smaller actions that, taken together, would dissuade a reasonable worker from participating in the protected activity.[312]

c) Procedure

An employee alleging reprisal for protected activity under the law must file a complaint with the Inspector General (IG) of the executive agency involved in the contract at issue.[313] The claim must be filed within three years of the date of the alleged adverse action.[314] The IG then has 180 days to investigate the allegations and submit a report to the complainant, the respondent contractor, and the head of the relevant agency with whom the private party contracted.[315] If the agency denies relief or fails to file an order granting relief within 210 days after the filing of the complaint, the complainant

© Copyright 2026

may file a lawsuit based on the complaint in federal district court.[316] Either the complainant or the respondent may request a jury trial.[317]

B. State Laws Providing Protections to Cybersecurity and Data Privacy Whistleblowers

Cybersecurity and data privacy whistleblowers may also find protections in state law, whether under a statute prohibiting whistleblower retaliation or a common law claim for wrongful discharge in violation of public policy. In all states except Montana, employment is presumed to be "at-will."[318] Generally, under the at-will employment doctrine, "an employee may be terminated for a good reason, bad reason, or no reason at all," but exceptions exist that protect employees under specific circumstances.[319] A common exception to the at-will employment doctrine is a law that prohibits employers from terminating employees for reporting illegal conduct or, more generally, a law prohibiting terminations that violate "public policy." Such prohibitions against wrongful discharges in violation of public policy exist in both statutory and common law form, but courts generally require that the public policy in question be derived from an existing statutory or constitutional provision. Whistleblower retaliation and wrongful discharge laws differ as to what conduct qualifies as protected activity. Some laws only protect whistleblower reports made to law enforcement or another governmental body,[320] while others also protect internal whistleblowing,[321] and many protect whistleblowers who refuse to engage in criminal activity.[322]

States also differ as to whether a federal law can provide the basis for a state wrongful discharge in violation of public policy claim. Over 30 states either have explicitly stated that federal law, not just state law, may provide the source of this public policy or have created broad public policy exceptions which would appear to encompass federal law as the source.[323] However, some states that recognize federal law as a basis for public policy do not allow a state law claim for wrongful termination if there already exists a federal statute providing whistleblower protections.[324] In other states it remains an open question whether courts would consider the public policy expressed in federal statutes, rules, and regulations to be a source of public policy for purposes of a wrongful discharge claim. Given the heterogeneous development of this area of law, there is little reason to believe this question will be resolved uniformly by the states.

Some courts have issued decisions in favor of cybersecurity and data privacy whistleblowers who have pursued whistleblower retaliation or wrongful discharge in violation of public policy claims under state law. For example, in 2009, a federal court in New Jersey denied an employer's motion for summary judgment on a statutory whistleblower retaliation claim based on an employee's refusal to engage in conduct that could have jeopardized confidential information in violation of the New Jersey Identity Theft Protection Act.[325] In 2010, a California appeals court upheld a wrongful termination verdict for a whistleblower who raised concerns about insufficient cybersecurity protections that the employee reasonably believed violated the federal Health Insurance Portability and Accountability Act (HIPAA).[326] In May 2018, a federal court in Washington denied a defendant's motion to dismiss the plaintiff's claim for wrongful discharge in violation of public policy based on the plaintiff's complaints about noncompliance with applicable PCI DSS.[327]

© Copyright 2026

Other states with more restrictive public policy exceptions have rejected such claims. For instance, in 2023, a Wisconsin appellate court affirmed a dismissal of a wrongful discharge claim brought by two whistleblowers who alleged that they were terminated after raising concerns about data security.[328] Specifically, the employees complained "to various superiors" that their employer was failing to comply with data security requirements set forth in the Food, Drug, and Cosmetic Act (FDCA) and failing to safeguard health information in violation of HIPAA.[329] In Wisconsin, however, wrongful discharge in violation of public policy claims are available only when employees are terminated "for refusing a command to violate a public policy as established by a statutory or constitutional provision."[330] Because the employees had only opposed the unlawful activities—but had not themselves been issued a command to break the law, and therefore refused no such command—the court found that they could not sustain a wrongful discharge claim.[331] In 2025, a federal court in Michigan dismissed a wrongful termination claim brought by a plaintiff who alleged that he was asked to "overlook cybersecurity breaches" at his employer and was terminated after filing an HR complaint about "cybersecurity vulnerabilities."[332] The plaintiff argued that his protected activity related to federal laws, including the FTCA and the Cybersecurity Information Sharing Act (CISA).[333] The court rejected his argument on the grounds that he did not allege that his employer asked him to violate the CISA or the FTCA, neither the CISA nor the FTCA provided for a private right of action, and there was no state law or policy preventing employers from terminating employees for internal reporting.[334] Thus, the plaintiff's claim did not meet the standard for wrongful termination claims under Michigan law.

Although some state whistleblower laws protect employees from adverse actions beyond termination, such as demotion or harassment, others only protect whistleblowers who have been fired.[335] While a work environment may become so intolerable that it permits a whistleblower to quit and allege that she was constructively discharged, the standard for constructive discharge is often very challenging to meet.[336] As a result, whistleblowers without a statute protecting them from retaliation beyond discharge may experience significant and ongoing retaliation with no legal recourse.

This section first discusses the various federal laws that may form the public policy upon which a cybersecurity or data privacy whistleblower may be able to rely for a wrongful discharge in public policy claim (or that may serve as the underlying violation supporting a statutory whistleblower retaliation claim). It next reviews a few of the many laws passed by states over the past decade creating cybersecurity requirements in various industries, which may also form the basis for a wrongful termination claim under state law.

1. Federal Law Bases for State Wrongful Discharge and Whistleblower Retaliation Claims

There are a number of federal laws requiring companies or individuals to take certain steps to protect information with which they have been entrusted. In addition to the securities rules and regulations discussed above in Section II.A, these statutes include HIPAA, the GLBA, the FTCA, and the Communications Act of 1934. Cybersecurity and data privacy whistleblowers who complain about violations of the requirements included in these statutes, or in the related regulations issued by the relevant enforcing agencies, may have engaged in protected activity if the applicable state law protects whistleblowers who report violations of federal laws and regulations.

© Copyright 2026

a) Health Insurance Portability and Accountability Act

For cybersecurity and data privacy whistleblowers in the healthcare field, HIPAA may serve as a basis for protected activity.[337] In 2003, the U.S. Department of Health and Human Services (HHS) created the Security Rule, which is a set of HIPAA regulations that establishes national standards to protect individuals' electronic personal health information (e-PHI).[338] The Security Rule requires covered entities—health plans, health care clearinghouses, and any health care provider who transmits health information in electronic form—to maintain a number of safeguards for protecting e-PHI.[339] If an employee who works for a covered entity subject to these regulatory requirements reports violations of the Security Rule and her employer fires her, she may have a claim for wrongful discharge in violation of public policy or under a state whistleblower retaliation law.

In January 2025, HHS proposed an update to increase the cybersecurity for e-PHI by revising the Security Rule to address: changes in the environment in which health care is provided; significant increases in breaches and cyberattacks; common deficiencies the Office for Civil Rights has observed in investigations into Security Rule compliance by covered entities and their business associates; other cybersecurity guidelines, best practices, methodologies, procedures, and processes; and court decisions that affect enforcement of the Security Rule.[340] The proposed rule remains under review.

b) Communications Act of 1934

irst, Section 201(b) of the Communications Act states that "[a]ll charges, practices, classifications, and regulations for and in connection with [interstate or foreign] communication service [by wire or radio], shall be just and reasonable, and any such charge, practice, classification, or regulation that is unjust or unreasonable is declared to be unlawful."[341]

Second, Section 222(a) of the Communications Act states that "[e]very telecommunications carrier has a duty to protect the confidentiality of proprietary information of, and relating to, other telecommunication carriers, equipment manufacturers, and customers[.]"[342]

Finally, Section 222(c)(1) of the Communications Act states that "a telecommunications carrier . . . shall only use, disclose, or permit access to individually identifiable customer proprietary network information in its provision of (A) the telecommunications service from which such information is derived, or (B) services necessary to, or used in, the provision of such telecommunications service[.]"[343]

The FCC has relied on this authority to take action against companies that fail to adequately protect customer information. In August 2024, the FCC announced a $34.6 million settlement with CaptionCall, resolving allegations that the company had unlawfully retained private consumer call content data.[344] Before that, in February 2020, the FCC proposed over $200 million in fines against four of the largest wireless carriers, Verizon, T-Mobile, Sprint, and AT&T, for allegedly failing to protect consumer location data.[345] In April 2015, the FCC ordered AT&T to pay a $25 million fine to settle claims that multiple data breaches resulted in the leakage of hundreds of thousands of customer records, including records containing Social Security numbers.[346] Six months before that, the FCC ordered two telecommunications carriers, TerraCom and YourTel, to pay a collective $10 million fine for allegedly

© Copyright 2026

storing customers' personal information in a method that was accessible through a routine online search.[347] Notably, the FCC need not find a massive breach to conclude that a company has violated the Communications Act. For instance, on November 5, 2015, the FCC fined the cable company Cox Communications for failing to adequately protect customer information, even though the leak affected only a few dozen individuals.[348]

As illustrated by the FCC's enforcement actions, the Communications Act expresses a clear public policy of ensuring data security protections in communication services. If an employee of a telecommunications carrier or contractor blows the whistle on insufficient data-security standards and is terminated as a result, she may have a strong claim for wrongful discharge or whistleblower retaliation under the laws of many states.

c) Gramm-Leach-Bliley Act

The GLBA[349] created the Safeguards Rule,[350] which requires financial institutions to take certain steps to ensure the security and confidentiality of consumer data, including names, addresses and phone numbers, bank and credit card account numbers, income and credit histories, and Social Security numbers.[351] The Safeguards Rule applies to companies that provide financial products or services to consumers, including check-cashing businesses, mortgage brokers, non-bank lenders, personal property or real estate appraisers, and retailers that issue credit cards to consumers.[352] The Safeguards Rule requires financial institutions to:
Designate the employee or employees to coordinate the safeguards;
Identify and assess the risks to customer information in each relevant area of the company's operation, and evaluate the effectiveness of current safeguards for controlling these risks;

Design a safeguards program, and detail the plans to monitor it;
Select appropriate service providers and require them (by contract) to implement the safeguards; and
Evaluate the program and explain adjustments in light of changes to its business arrangements or the results of its security tests.[353]

The Safeguards Rule received a substantial overhaul via a final rule issued by the FTC in December 2021.[354] The rule served several purposes. Among other things, it: (a) imposed granular regulations regarding how financial institutions should create and maintain certain aspects of their information security program, including access controls, authentication, and encryption;[355] (b) added regulations aimed at improving accountability in financial institutions' data security programs, including requiring periodic reports to the institutions' governing bodies;[356] and (c) expanded the definition of a "financial institution" covered by the Safeguards Rule to include entities engaged in activities "incidental" to financial activities, including so-called "finders," i.e., companies that bring together buyers and sellers of a product or service.[357] In 2023, the FTC approved another amendment to the Safeguards Rule, requiring financial institutions to notify the FTC as soon as possible, and no later than 30 days after discovery, of a security breach involving the information of at least 500 consumers.[358] The amendments became effective in May 2024.

In states that protect whistleblowers who report violations of federal law, the GLBA provides a clear statement of public policy in favor of financial institutions taking

© Copyright 2026

significant steps to protect customer information. A financial institution employee who opposes inadequate protections of customer information and is subsequently terminated may have a strong whistleblower retaliation or wrongful termination claim, if the applicable state law allows a federal law to serve as a basis of public policy.

d) Federal Trade Commission Act of 1914

Section 5 of the FTCA prohibits unfair or deceptive acts or practices in commerce, and empowers the FTC to prosecute violations of the statute.[359] The FTCA defines an "unfair" practice as one that causes or is likely to cause "substantial injury to consumers which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition."[360]

The FTC has exercised this authority against companies that fail to adhere to adequate standards for securing consumer data.[361] Courts have upheld the FTC's interpretation that unreasonable data security practices could violate Section 5 of the FTCA. Specifically, in 2015, the Third Circuit upheld the FTC's ability to bring an action against Wyndam Worldwide Corporation for violations of the FTCA based on data security failures that led to three breaches of sensitive consumer data by hackers in less than two years.[362] Since then, the FTC has successfully resolved a series of actions based on companies' failures to secure customer data.[363] Indeed, in 2019, the FTC imposed a landmark $5 billion penalty against Facebook to settle FTC charges that Facebook misled users about their ability to control the privacy of their personal information.[364]

Based on the FTC's actions, an employee who reports data breaches or deceptive communications about deficient cybersecurity has a strong argument that her report was protected if the applicable state law recognizes federal law as a basis for a whistleblower retaliation or wrongful termination in violation of public policy claim.

2. State Law Bases for State Wrongful Discharge and Whistleblower Retaliation Claims

Cybersecurity and data privacy whistleblowers may not need to depend on federal law as a basis for their retaliation claims. States are beginning to pass their own cybersecurity and data privacy laws and, given the public concern about cybersecurity and data security, more states are likely to enact such laws in the future. Most common are security breach notification laws, which exist in some form in every state. Many states also have laws that address data security issues. While those laws generally focus on governmental actors' handling of data, laws are slowly expanding to protect other types of data.

a) Security Breach Notification Laws

Security breach notification laws require entities that have been the subject of a data breach to notify individuals if the breach involved the potential disclosure of personally identifiable information (PII). States define PII differently, but most states define it with terminology similar to that used by Arkansas:

"Personal information" means an individual's first name or first initial and his or her last name in combination with any one (1) or more of the following data elements when either the name or the data element is not encrypted or redacted:
(A) Social Security number;

© Copyright 2026

(B) Driver's license number or Arkansas identification card number;
(C) Account number, credit card number, or debit card number in combination with any required security code, access code, or password that would permit access to an individual's financial account;
(D) Medical information; and
(E) Biometric data.[365]

All 50 states, as well as the District of Columbia, Guam, Puerto Rico, and the Virgin Islands, have passed some form of security breach notification law.[366] The National Conference of State Legislatures has created a comprehensive directory of these laws with links to the statutes themselves.[367] Thus, employees who are terminated because they have opposed their employer's failure to promptly notify customers or clients of a data breach involving the disclosure of PII likely have a strong basis for a state whistleblower retaliation claim and/or a claim of wrongful termination in violation of public policy, provided they are in a state that allows such claims.

b) Other State Cybersecurity and Data Privacy Measures

Several states have passed additional measures relating to cybersecurity and data privacy in recent years. In September 2025, in response to growing concerns about AI, California passed the Transparency in Frontier Artificial Intelligence Act (TFAIA), which recently came into effect.[368] The TFAIA was drafted to "enhance online safety by installing commonsense guardrails on the development" of advanced AI systems, referred to as "frontier models," and contains provisions relating to cybersecurity.[369] Under the law, large AI frontier developers must design, implement, and publish an AI safety and security framework describing, among other things, their cybersecurity practices and approaches to identifying and responding to critical safety incidents, including harm resulting from a frontier model committing cyberattacks.[370] The TFAIA contains a whistleblower provision[371] that prohibits employers from retaliating against covered employees who disclose violations of the law.[372]

Earlier, in 2018, California passed one of the more comprehensive consumer privacy protection laws, the Consumer Privacy Act (CCPA), which gives consumers more control over the personal information that businesses collect about them.[373] This statute provides consumers: the right to know about personal information that a business collects about them and how it is used;[374] the right to delete certain personal information that a business collects;[375] the right to opt out of the sale of personal information;[376] and protections for exercising their rights under the CCPA.[377] Some states have similarly enacted laws to protect consumer information,[378] while others have passed laws to require certain industries to establish and enforce cybersecurity policies and procedures.[379] Whistleblowers who report violations of such state measures may have a basis to argue they were terminated in violation of their states' anti-retaliation statutes or public policy.

© Copyright 2026

REWARDS FOR CYBERSECURITY WHISTLEBLOWERS

While job protection is a crucial component to encourage employees to blow the whistle, some cybersecurity whistleblowers may be entitled to additional rewards. Reward programs administered by the SEC, the DOJ, the U.S. Commodity Futures Trading Commission (CFTC), and the U.S. Treasury Department may all provide substantial monetary rewards for whistleblowers who are able to supply these agencies with information that leads to a successful enforcement action or settlement.

Some cybersecurity and data privacy whistleblowers may be entitled to substantial monetary rewards.

A. SEC Whistleblower Program

Dodd-Frank created a whistleblower program administered by the SEC that entitles an individual who provides the SEC with original information leading to an enforcement action resulting in over $1 million in monetary sanctions to receive an award of 10% to 30% of the amount collected. The SEC launched the program in 2011 and since then has paid more than $2.2 billion to more than 444 individuals.[380] In May 2023, the SEC issued its largest payout to date, awarding a single whistleblower $279 million for information that was "critical to the success of" the SEC's enforcement action and "expanded the scope of misconduct charged."[381] In 2024, the SEC awarded over $255 million, the third highest annual amount for the Whistleblower Program, to 47 individual whistleblowers.[382] The total annual amount awarded saw a notable decline in 2025, with the SEC awarding over $60 million to 48 individual whistleblowers.[383] To qualify for an award under the SEC Whistleblower Program, a whistleblower must "voluntarily provide" the SEC with information concerning a securities violation—i.e., the whistleblower must have provided the information to the SEC before receiving a request, inquiry, or demand to provide it.[384] The information the whistleblower provides must be "original information," meaning that it is derived from the whistleblower's independent knowledge or independent analysis, and must not be already known to the SEC from some other source or exclusively derived from public sources.[385] Whistleblowers are entitled to an award if the information they provide to the SEC leads to an enforcement action that results in more than $1,000,000 in monetary sanctions.[386] SEC whistleblowers may submit a tip anonymously if they submit it through counsel, and the SEC works vigorously to maintain whistleblowers' anonymity throughout the process.

While not all cybersecurity problems rise to the level of securities violations, the SEC has repeatedly stated that cybersecurity is a priority for the Commission. Depending on the scope of the wrongdoing, any of the violations set forth *supra* in Section II.A.1 may form the basis of a successful tip to the SEC. Indeed, in 2022, the SEC brought charges against JPMorgan Securities LLC, UBS Financial Services Inc., and Morgan Stanley Smith Barney for cybersecurity and data privacy lapses.[387] For detailed information about the rules and procedures of the SEC Whistleblower Program, read Lisa Banks and Michael Filoromo's SEC Whistleblower Practice Guide.

© Copyright 2026

B. CFTC Whistleblower Program

Dodd-Frank also directed the CFTC to create a whistleblower program.[388] The rules of the CFTC Program are similar to those of the SEC. An individual who provides the CFTC with original information leading to an enforcement action that results in over $1 million in monetary sanctions is eligible to receive an award of 10% to 30% of the amount collected. Compared to the SEC Whistleblower Program, the CFTC Program is small: the CFTC has granted whistleblower awards amounting to approximately $390 million since it began accepting tips in September 2012.[389] The awards under the CFTC program have been substantial, although the program has awarded few whistleblowers overall. In October 2021, the CFTC awarded a record-breaking $200 million to a single whistleblower who provided specific, timely, and credible information that led to a successful enforcement action and two related actions.[390]

To qualify for an award under the CFTC Whistleblower Program, a whistleblower must "voluntarily provide" the CFTC with information concerning violation of the Commodities Exchange Act and related regulations—i.e., the whistleblower must have provided the information to the CFTC before receiving a request, inquiry, or demand to provide it.[391] The information the whistleblower provides must be "original information," meaning that it is derived from the whistleblower's independent knowledge or independent analysis, is not already known to the CFTC from some other source, and is not exclusively derived from public sources.[392] Whistleblowers are entitled to an award if the information they provide to the CFTC leads to an enforcement action that results in more than $1,000,000 in monetary sanctions.[393] CFTC whistleblowers may submit a tip anonymously, if they submit it through counsel, and the CFTC works vigorously to maintain whistleblowers' anonymity throughout the process.

The intersection between commodities exchange and cybersecurity principally relates to cybersecurity testing and safeguards for the automated systems used by critical infrastructures that the CFTC regulates. The CFTC has adopted rules requiring clear minimum data security requirements for derivatives clearing organizations,[394] swap data repositories,[395] and specified designated contract markets.[396] Cybersecurity whistleblowers who provide the CFTC with original information about the failure of one of these entities to adhere to these cybersecurity standards,[397] or other cybersecurity rules put in place by the CFTC, may be entitled to an award under the CFTC Whistleblower Program. For detailed information about the rules and procedures of the CFTC Whistleblower Program, read Lisa Banks and Michael Filoromo's CFTC Whistleblower Practice Guide.

C. *Qui Tam* Lawsuits under the False Claims Act

The FCA authorizes individuals, known as relators, to file civil suits, known as *qui tam* actions, against persons or entities that defraud the U.S. government. Since its revitalization by an important series of amendments in 1986, the Act has proven tremendously successful, and *qui tam* actions have led to government recovery of over $78 billion.[398]

Under the FCA, a person who has knowingly submitted a fraudulent claim, knowingly made or used falsified records or statements to gain payment of a fraudulent claim, or conspired to do either is liable to the U.S. government for a civil penalty of between

© Copyright 2026

$13,946–$27,894 per claim, plus three times the amount of damages caused by the person's acts.[399] A "claim" under the FCA is a request or demand for federal money or property, including a request made to a non-governmental recipient who the United States will reimburse for all or a portion of that money.[400] For a claim to be "knowingly" made, the person must have actual knowledge of the fraudulent information, or be acting in either deliberate ignorance or reckless disregard.[401] Further, a defendant's knowledge that a claim was fraudulent is based on subjective intent, not whether an objectively reasonable person in the defendant's position would have understood the claim to be fraudulent.[402] The Supreme Court has explained that the proper inquiry into a defendant's subjective intent focuses on what the defendant thought at the time it submitted the false claim, as opposed to what it thought or learned after submission.[403] In most circumstances, a plaintiff must prove an actual false claim for payment from the government was made.[404]

As described *supra* in Sections I and II.A.3, *qui tam* actions involving cybersecurity issues have involved violations of the cybersecurity-related requirements set forth in the FARs and DFARS. [405] Such actions appear to have been based on both of the two "false certification" theories of liability,[406] express and implied.[407] As discussed in Section II.A.3.a above, express false certification occurs when a claimant falsely certifies that it is in compliance with regulations that are material requirements for payment.[408] Implied false certification occurs when a claimant submits a request for payment without disclosing that the claimant is in violation of a regulation or requirement that affects its eligibility for payment.[409] The Supreme Court has held that, to qualify as an implied false certification, the claimant must (1) make specific representations about the goods or services that are (2) rendered misleading by the claimant's failure to disclose its noncompliance with the regulation.[410] This has become known as the "two-part test for falsity." Since the Court's decision, courts have wrestled about whether the two-part test is mandatory or merely one way to demonstrate falsity under the statute.[411]

Critically, the noncompliance must be with a material requirement under either theory.[412] A prospective whistleblower, therefore, would be wise to seek guidance on whether adherence or failure to adhere to the regulation or requirement at issue likely would be deemed "material." Materiality does not have a rigid definition in the context of government contracts, but the Supreme Court has provided a fairly narrow definition of materiality by providing a list of things that are not material:

The materiality standard is demanding. The False Claims Act is not "an all-purpose antifraud statute," or a vehicle for punishing garden-variety breaches of contract or regulatory violations. A misrepresentation cannot be deemed material merely because the Government designates compliance with a particular statutory, regulatory, or contractual requirement as a condition of payment. Nor is it sufficient for a finding of materiality that the Government would have the option to decline to pay if it knew of the defendant's noncompliance. Materiality, in addition, cannot be found where noncompliance is minor or insubstantial.

In sum, when evaluating materiality under the False Claims Act, the Government's decision to expressly identify a provision as a condition of payment is relevant, but not automatically dispositive. Likewise, proof of materiality can include, but is not necessarily limited to, evidence that the defendant knows that the Government consistently refuses to pay claims in the mine run of cases based on noncompliance with the particular statutory, regulatory, or contractual requirement. Conversely, if the Government pays a particular claim in full despite its actual knowledge that certain requirements were violated, that is very strong evidence that those requirements are not material. Or, if the Government regularly pays a particular type of claim in full

© Copyright 2026

despite actual knowledge that certain requirements were violated, and has signaled no change in position, that is strong evidence that the requirements are not material.[413]

Despite the Supreme Court's somewhat narrow construction of materiality, lower courts post-*Escobar* have found less explicit evidence sufficient to allow a case to proceed.[414]

In addition to liability under a false certification theory, a whistleblower could bring a *qui tam* based on allegations that software or hardware sold to the government had a cybersecurity defect so significant that it rendered the product defective. For example, as discussed *supra* Section II.A.3.a, Cisco Systems, a video surveillance company, sold technology to various federal and state governmental agencies, knowing the technology had a significant security flaw and agreed to pay $8.6 million to settle those claims.[415] In 2017, a medical device manufacturer recalled over 400,000 devices due to cybersecurity vulnerabilities that were discovered in the devices.[416] Had similar deficiencies been discovered in, for example, an aircraft a government contractor manufactured for the DOD, it would have rendered the claims the contractor submitted for payment for the aircraft false.

The procedure for filing a *qui tam* action has specific requirements, and failure to meet them is fatal to a relator's claim. The relator must file a civil complaint under seal with the appropriate federal court, and then serve a copy of the complaint, along with a written disclosure of substantially all material evidence and information in the relator's possession, on the U.S. Attorney General and the U.S. Attorney.[417] This procedure allows the government to investigate the relator's claims without the defendant knowing about the investigation. The government has 60 days to decide whether it will join the case, which is known as "intervening."[418] After 60 days, if the government does not take action, the relator may litigate the case on her own. Because 60 days is a fairly short limitations period, and the government is often reviewing many *qui tam* suits at any given time, the government may request that the court grant it additional time.[419] These requests are routinely granted to allow the government sufficient time to investigate the whistleblower's claims.

If the government does not intervene in the action and the relator is successful, then the relator must receive between 25% and 30% of the proceeds of the suit or settlement.[420] On the other hand, if the government intervenes, the relator receives between 15% and 25%, depending on the relator's contribution to the prosecution of the action.[421] Intervention is critical for the success of *qui tam* actions. Ninety percent of cases in which the government intervened have generated recovery, while cases in which the government declined to intervene have failed to generate similar rates of recovery.[422] This favorable success rate in cases of government intervention makes the associated reduction in award palatable for most whistleblowers. If the government chooses to intervene, it will then file a new complaint that automatically becomes the operative complaint as to all claims in which the government has intervened.[423] In August 2024, the DOJ for the first time intervened in an FCA lawsuit[424] as part of the Civil Cyber-Fraud Initiative. The lawsuit alleged that the defendant contractors failed to follow cybersecurity rules incorporated into two DOD contracts when performing on campus research. In September 2025, the DOJ announced that Georgia Tech Research Corporation agreed to pay $875,000 to resolve the allegations, bringing the case to a close.[425]

© Copyright 2026

D. Anti-Money Laundering Whistleblower Reward Program

Under the AMLA, when an anti-money laundering enforcement action brought by the DOJ or the Treasury Department results in monetary sanctions over $1 million, the Secretary of the Treasury "shall pay an award or awards to 1 or more whistleblowers who voluntarily provided original information" that led to a successful enforcement action.[426] Under the AMLA, a whistleblower award shall equal between 10% and 30% of the total resulting monetary sanctions.[427]

A whistleblower will not be entitled to an award if she "(1) knowingly and willfully makes any false, fictitious, or fraudulent statement or representation; or (2) uses any false writing or document knowing the writing or document contains any false, fictitious, or fraudulent statement or entry."[428]

The AMLA Whistleblower Program is administered by FinCEN. For more than five years after the Program was established in 2021, FinCEN did not publish rules or regulations governing how a whistleblower should file a tip under the AMLA Whistleblower Program. Then, on February 13, 2026, FinCEN announced that it launched a new webpage to accept tips from AMLA whistleblowers.[429] On March 30, 2026, FinCEN published its proposed rules to fully implement the AMLA Whistleblower Program.[430] In the Program's current state, however, there is no option to submit an anonymous tip or attach files to the submission.[431] Katz Banks Kumin has filed tips under the Program and can advise prospective AMLA whistleblowers on how best to proceed under the Program.

Under FinCEN's proposed rules, the AMLA Whistleblower Program would cover violations of the BSA and sanctions-related statutes including the International Emergency Economic Powers Act, the Trading with the Enemy Act, and the Foreign Narcotics Kingpin Designation Act.[432] FinCEN also positions the Program as supporting enforcement of the Department of Treasury's Outbound Investment Security Program and, relevant to the areas of cybersecurity and data privacy, the DOJ's new Data Security Program where those matters fall under the scope of the covered statutes.[433] The Data Security Program, which went into effect on April 8, 2025, purports to "address[] the national-security risks posed by the continued efforts of foreign adversaries to use commercial activities to access and exploit U.S. Government-related data and Americans' bulk sensitive personal data."[434]

Thus far, FinCEN has issued no awards under the Program, whether to cybersecurity and data privacy whistleblowers or otherwise. FinCEN sanctions and the ensuing rewards can be considerable, however. For example, in March 2022, FinCEN fined USAA Federal Savings Bank $140 million after the Bank inadequately responded to thousands of potentially suspicious customer transactions.[435] That fine could have led to an award of as much as $42 million—30% of $140 million—for a participating whistleblower. More recently, in February 2025, FinCEN assessed a record $1.3 billion civil penalty against TD Bank for the bank's willful failure to implement and maintain an anti-money laundering program that met the minimum requirements of the BSA, resulting in the widespread failure to identify and report suspicious transactions.[436] Even a whistleblower award at the minimum amount of 10% would have resulted in a $130 million payout. In March 2026, FinCEN assessed an $80 million penalty, the largest ever imposed against a broker-dealer for violating the anti-

© Copyright 2026

money laundering requirements of the BSA, against Canaccord Genuity LLC.[437] This penalty could have resulted in a $24 million whistleblower award. In the technology space, FinCEN has also assessed significant financial penalties against two large crypto exchanges, BitMEX and Bittrex, for failing to implement adequate anti-money laundering controls.[438]

E. DOJ Pilot Whistleblower Program

In August 2024, the DOJ created the Corporate Whistleblower Awards Pilot Program, a new whistleblower program designed to fill some of the gaps not covered by existing ones. The Program, which is operating for a three-year pilot window, provides an avenue for whistleblowers to submit tips concerning corporate misconduct that would not otherwise be eligible for an award through another whistleblower program. Specifically, to participate in this Program, whistleblowers must provide information pertaining to: (1) violations by financial institutions, including schemes involving money laundering and fraud; (2) violations related to foreign corruption and bribery involving companies; (3) violations by or through companies involving payment of bribes or kickbacks to domestic public officials; or (4) violations related to federal health care offenses involving non-public health care benefit programs, fraud against patients and other non-governmental entities in the health care industry, and any other federal violations involving conduct related to health care not covered by the FCA.[439] Whistleblowers must submit original, non-public information to the DOJ, and have the option of doing so anonymously if represented by an attorney.[440]
Where a whistleblower tip leads to an investigation that results in a successful forfeiture of over $1 million, they may be eligible for an award of up to 30% of the first $100 million forfeited; an award of up to 5% of proceeds forfeited in the range of $100 million to $500 million; and no award on proceeds forfeited above $500 million[441]—effectively capping awards at a maximum of $50 million, in contrast to the SEC, CFTC, and AMLA Whistleblower Programs.

So far, the DOJ has yet to issue any awards through the Corporate Whistleblower Awards Pilot Program. However, one can contemplate ways in which a cybersecurity or data privacy tip could be covered under this program. For instance, a tip concerning noncompliance with the GLBA related to deficient data security practices could arguably be covered under the Program. As another example, a report concerning misrepresentations about cybersecurity that amount to fraud against private health insurance providers could be covered by the Program.

II. THINGS TO THINK ABOUT BEFORE YOU BLOW THE WHISTLE

While there is no way to blow the whistle that will prevent an employer from retaliating, there are steps that whistleblowers can take to ensure that they have as many legal protections as possible if the worst happens.

A whistleblower should not sign a severance agreement before discussing her case with a knowledgeable attorney.

© Copyright 2026

A. Report a Violation of Law, Not Just Cybersecurity or Data Privacy Vulnerabilities

The law protects whistleblowers who report violations of laws or who refuse to engage in unlawful conduct. For cybersecurity and data privacy whistleblowers, there may not be an obvious link between the vulnerability they are reporting and a legal violation. Ideally, therefore, a whistleblower should articulate clearly that the issue she is reporting is not simply a cybersecurity or data privacy vulnerability, but also involves actual or potential violations of law. In doing so, it benefits the whistleblower to be as specific as possible about the potential legal violation. Provided the whistleblower has a reasonable belief that the conduct is unlawful, she should be protected even if she is wrong.

B. Report in Writing to Someone Who Can Address the Problem

The substance of a whistleblower's report is critical, and ideally, an employee will have proof of exactly what she reported. Employers frequently defend themselves against retaliation claims by arguing that the employee never reported legal violations, but simply reported a standard IT problem, complained about a business decision, or advocated for an alternative approach. By reporting her concern in writing, a whistleblower will avoid any dispute about the substance of her report. The report should be specific about the facts at issue and why the whistleblower believes the company's conduct may violate the law. The report should not combine that information with complaints about other topics, such as personnel or personality conflicts. Since the report will become critical evidence if the employer retaliates against the whistleblower, the tone of the report should be professional and not insubordinate.

The report should be made to someone who can address the problem, such as a supervisor or a compliance officer. Reports to co-workers will generally not be sufficient to provide a whistleblower with legal protection. It is important to remember that, under some laws, a whistleblower is protected only if she reports the problem externally to law enforcement or other appropriate officials.

C. Be Careful About Taking Documents

Once a whistleblower discovers a problem, she may be tempted to investigate further by reviewing company files and data to uncover the extent of the problem. Such a campaign, however, can backfire and jeopardize the whistleblower's legal protections. A whistleblower can generally review documents and data to which she has access in the normal course of business, but if she searches through a document, computer server, or even a filing cabinet that she does not have a right to access, she may be giving the company a non-retaliatory basis for terminating her, as well as potentially exposing herself to civil and criminal liability. Relatedly, if her employer tells her to halt any further investigation or analysis of the matter, the whistleblower generally should comply. While arguments can be made to defend the whistleblower's further investigation, especially if the whistleblower is considering reporting her concerns to the SEC or filing a *qui tam* action, the whistleblower will be in the strongest position if she fully complies with the company's orders.

© Copyright 2026

A whistleblower may also be tempted to retain incriminating company documents and data if the company discharges the whistleblower after she has blown the whistle. Again, the law governing such conduct is unsettled, so it is best for a whistleblower to consult with a whistleblower attorney about retaining company documents and data.

D. Seek Legal Representation

Given that there are few laws explicitly regulating cybersecurity and no laws explicitly protecting cybersecurity whistleblowers, it is critical for a whistleblower to seek experienced legal representation as soon as possible. If a whistleblower consults with a knowledgeable attorney prior to blowing the whistle, the attorney can advise the whistleblower on which, if any, whistleblower laws might protect her and what she must do to ensure she qualifies for protection. Specifically, the whistleblower will need to know whether internal reporting is protected, what type of law must be implicated in such a report, and how best to word the report to make clear that the cybersecurity issue involves a covered legal violation.

If an employer retaliates against a whistleblower, it is even more imperative that she immediately seek representation. Some laws, such as SOX, require the whistleblower to take legal action within 180 days of termination (or other retaliatory act). The whistleblower also should not sign a severance agreement prior to discussing her case with a knowledgeable attorney. Such an agreement will almost surely release all claims the whistleblower has against her employer, and, depending on the facts of the case, the whistleblower may have a strong claim for more compensation than the employer initially has offered.

E. If Terminated, Diligently Look For New Work

If an employer fires a whistleblower, the whistleblower must start looking for a new job even while pursuing a remedy for her wrongful termination. A whistleblower who wishes to hold a former employer legally responsible for the economic harm resulting from her termination has a legal obligation to make a good-faith, reasonable effort to secure new employment. That being said, the whistleblower is only required to accept a job that is substantially equivalent to the one she lost. It is critical that the whistleblower keep detailed records of all job search efforts to ensure that the employer cannot feasibly claim that her efforts were insufficient.

* * *

Matthew B. LaGarde is a partner with Katz Banks Kumin LLP. Mr. LaGarde focuses his practice on the representation of whistleblowers who have experienced workplace retaliation or wish to report wrongdoing to the government. In addition to this Guide, Mr. LaGarde is an editor for *Whistleblower Law: A Practitioner's Guide*, a treatise first published in 2016 by American Legal Media (ALM) that is updated annually. He has worked on multiple *qui tam* actions alleging that companies were fraudulently billing the government, including a successful *qui tam* lawsuit against a naval husbandry company for fraudulently billing the government that resulted in a $20 million settlement in 2018. He has also filed many whistleblower tips on behalf of clients with the SEC, including several cybersecurity whistleblower tips that remain pending as of the date of publication. He has represented whistleblower clients, including cybersecurity whistleblowers, in state and federal court, in arbitration, and before administrative agencies. Mr. LaGarde has also assisted in securing numerous confidential prelitigation settlements for his whistleblower clients.

© Copyright 2026

Lisa J. Banks is a partner with Katz Banks Kumin LLP. She is the co-chair of the firm's New York whistleblower practice. She regularly represents individuals in whistleblower retaliation cases, SEC and CFTC whistleblower tips, and employment discrimination and sexual harassment claims. She is a member of the governing council of the American Bar Association's Labor and Employment Section, and is the co-author of Whistleblower Law: A Practitioner's Guide, a comprehensive treatise on federal and state whistleblower law.

Catherine Seita is an associate with Katz Banks Kumin LLP. Ms. Seita represents plaintiffs in whistleblower retaliation cases as well as other employment matters, including civil rights discrimination, retaliation, and harassment disputes. She has worked on cases in California court and in arbitration on behalf of whistleblowers who faced workplace retaliation after reporting unlawful conduct. Ms. Seita has also represented many employees in whistleblower retaliation and other matters that resolved confidentially prior to litigation.

Katz Banks Kumin LLP's website at www.katzbanks.com features detailed information about how employees who have blown the whistle on unlawful conduct can fight back against unlawful retaliation and also earn financial rewards where available. Articles in the website's Whistleblower Law section explain both the law and practicalities of whistleblowing as they play out in a wide range of industries and professions. Whistleblower topics include the SEC Whistleblower Program, Corporate and Accounting Fraud, *Qui Tam* Lawsuits under the False Claims Act, IRS Whistleblowers, Compliance Officer Whistleblowers, Consumer Finance Whistleblowing, the Pharmaceutical Industry, Food Safety, the Nuclear Industry, and Consumer Product Safety Whistleblowers, to name just a few. *See* https://www.katzbanks.com/practice-areas/whistleblower-law and https://katzbanks.com/practice-areas/sec-whistleblower-law.

The Katz Banks Kumin website also hosts an informative blog that can help keep whistleblowers and other conscientious employees up to date on new developments in whistleblower law and related news, including broader whistleblower news and developments. *See* https://katzbanks.com/blogs.

III. ENDNOTES

[1] Meryl Kornfield & Hannah Natanson, *He accused DOGE of risking Social Security data. It cost him his career*, Washington Post (last updated Oct. 20, 2025), https://www.washingtonpost.com/politics/2025/10/20/social-security-data-doge-whistleblower/.

[2] S. COMM. ON THE JUDICIARY, *Senate Judiciary Committee Releases Testimony of Twitter Whistleblower Peiter "Mudge" Zatko* (Sept. 13, 2022), www.judiciary.senate.gov/press/dem/releases/senate-judiciary-committee-releases-testimony-of-twitter-whistleblower-peiter-mudge-zatko.

[3] Reed Abelson & Julie Creswell, *Cyberattack Paralyzes the Largest U.S. Health Care Payment System*, N.Y. Times (Mar. 5, 2024), https://www.nytimes.com/2024/03/05/health/cyberattack-healthcare-cash.html.

[4] Sopan Deb, *Ticketmaster Confirms Data Breach. Here's What to Know.*, N.Y. Times (May 31, 2024), https://www.nytimes.com/2024/05/31/business/ticketmaster-hack-data-breach.html.

[5] Jenny Gross & Danielle Kaye, *AT&T Says Phone Data of 'Nearly All' Customers Was Breached in 2022*, N.Y. Times (July 12, 2024), https://www.nytimes.com/2024/07/12/business/att-data-breach.html.

[6] Stephanie Saul, *Penn Data Breach Involves Decades of Student and Alumni Information*, N.Y. Times (Nov. 4, 2025), https://www.nytimes.com/2025/11/04/us/penn-data-breach-donors-students.html.

© Copyright 2026

[7] FED. BUREAU OF INVESTIGATION, INTERNET CRIME COMPLAINT CTR., *Internet Crime Report 2025*, at 3–4 (Apr. 6, 2026), *available at* https://www.ic3.gov/AnnualReport/Reports/2025_IC3Report.pdf.

[8] OFF. OF THE DIR. OF NAT'L INTEL., *Annual Threat Assessment of the U.S. Intelligence Community* (Mar. 25, 2025), *available at* https://www.dni.gov/files/ODNI/documents/assessments/ATA-2025-Unclassified-Report.pdf.

[9] 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/archives/opa/pr/deputy-attorney-general-lisa-o-monaco-announces-new-civil-cyber-fraud-initiative.

[10] U.S. DEP'T OF JUSTICE, *False Claims Act Settlements and Judgments FY 2025 Fact Sheet* (Jan. 16, 2026), https://www.justice.gov/opa/media/1424126/dl.

[11] U.S. DEP'T OF JUSTICE, *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.

[12] U.S. DEP'T OF JUSTICE, *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 (hereinafter "Raytheon Settlement").

[13] U.S. DEP'T OF JUSTICE, *Illumina Inc. to Pay $9.8M to Resolve False Claims Act Allegations Arising from Cybersecurity Vulnerabilities in Genomic Sequencing Systems* (July 31, 2025), https://www.justice.gov/opa/pr/illumina-inc-pay-98m-resolve-false-claims-act-allegations-arising-cybersecurity (hereinafter "Illumina Settlement").

[14] U.S. DEP'T OF JUSTICE, *Georgia Tech Research Corporation Agrees to Pay $875,000 to Resolve Civil Cyber-Fraud Litigation* (Sept. 30, 2025), https://www.justice.gov/opa/pr/georgia-tech-research-corporation-agrees-pay-875000-resolve-civil-cyber-fraud-litigation (hereinafter "Georgia Tech Settlement").

[15] U.S. DEP'T OF JUSTICE, *Alabama Defense Contractor Agrees to Pay $507,144 to Resolve False Claims Act Liability Relating to Cybersecurity Violations* (June 18, 2026), https://www.justice.gov/opa/pr/alabama-defense-contractor-agrees-pay-507144-resolve-false-claims-act-liability-relating.

[16] U.S. SEC. AND EXCH. COMM'N, *SEC Announces Cyber and Emerging Technologies Unit to Protect Retail Investors* (Feb. 20, 2025), https://www.sec.gov/newsroom/press-releases/2025-42.

[17] *Id.*

[18] *See, e.g.*, FED. TRADE COMM'N, *FTC Finalizes Order with GoDaddy over Data Security Failures* (May 21, 2025), https://www.ftc.gov/news-events/news/press-releases/2025/05/ftc-finalizes-order-godaddy-over-data-security-failures.

[19] 15 U.S.C. § 6501 *et seq.*

[20] FED. TRADE COMM'N, *Disney to Pay $10 Million to Settle FTC Allegations the Company Enabled the Unlawful Collection of Children's Personal Data* (Sept. 2, 2025), https://www.ftc.gov/news-events/news/press-releases/2025/09/disney-pay-10-million-settle-ftc-allegations-company-enabled-unlawful-collection-childrens-personal.

[21] Belle Lin, *AI Is Generating Security Risks Faster Than Companies Can Keep Up*, Wall Street Journal (Aug. 10, 2023), https://www.wsj.com/articles/ai-is-generating-security-risks-faster-than-companies-can-keep-up-a2bdedd4.

[22] On the AI front, at least, some legislators have taken action. The AI Whistleblower Protection Act was introduced in the Senate in May 2025. If passed, it would protect employees who, for example, provide information about cybersecurity failures or data breaches that could potentially allow for theft of emerging AI technology. S. 1792, 119th Cong. (2025). State legislators, for their part, have introduced a number of AI-related bills across the country, although these laws may face challenges in the wake of Executive Order 14365, signed by President Trump in December 2025, which aims to establish a unified, federal policy framework for AI.

© Copyright 2026

[23] KPMG, KPMG 2025 U.S. CEO Outlook, at 4 (Oct. 7, 2025), https://kpmg.com/kpmg-us/content/dam/kpmg/pdf/gated/2025/2025-ceo-outlook.pdf.

[24] This is not intended to be an exhaustive list of all federal statutes that could provide protections, since there are other federal whistleblower statutes that could conceivably apply to a cybersecurity and data privacy whistleblower under less common circumstances (e.g., an employee blowing the whistle regarding cybersecurity in the aviation or trucking industries). In our practice, the nine statutes discussed in this paper have been the most common federal statutes to provide protection to cybersecurity and data privacy whistleblowers.

[25] 18 U.S.C. § 1514A.

[26] 15 U.S.C. § 78u-6.

[27] 12 U.S.C. § 5567.

[28] 12 U.S.C. § 1831j.

[29] 31 U.S.C. § 3730(h).

[30] 31 U.S.C. § 5323.

[31] 42 U.S.C. § 5851.

[32] 5 U.S.C. § 2302.

[33] 41 U.S.C. § 4712.

[34] 18 U.S.C. § 1514A.

[35] 15 U.S.C. § 78u-6.

[36] 18 U.S.C. § 1514A(a) (limiting application of SOX to any "company with a class of securities registered under section 12 of the Securities Exchange Act of 1934 (15 U.S.C. 78*l*), or that is required to file reports under section 15(d) of the Securities Exchange Act of 1934 (15 U.S.C. 78*o*(d)) including any subsidiary or affiliate whose financial information is included in the consolidated financial statements of such company, or nationally recognized statistical rating organization (as defined in section 3(a) of the Securities Exchange Act of 1934 (15 U.S.C. 78c)[)], or any officer, employee, contractor, subcontractor, or agent of such company or nationally recognized statistical rating organization").

[37] 18 U.S.C. § 1514A(a)(1).

[38] Lawson v. FMR LLC, 571 U.S. 429 (2014).

[39] *See, e.g.*, Baskett v. Autonomous Rsch. LLP, No. 17-CV-9237 (VSB), 2018 WL 4757962, at *8 (S.D.N.Y. Sept. 28, 2018) (holding that SOX's "contractor provision does not apply where a public company has no involvement in the conduct Congress sought to curtail by passing SOX"); *but see* Gryga v. Henkels & McKoy Grp., Inc., No. 19 C 1276, 2019 WL 3573565, at *4 (N.D. Ill. Aug. 6, 2019) (holding that plaintiff who raised concerns about a contractor's fraudulent activity on projects for a publicly traded company did state a claim under SOX because "a company's shareholders can be equally harmed whether it is the contractor, or the company itself, that causes losses due to fraud").

[40] 18 U.S.C. § 1514A(a)(1).

[41] 15 U.S.C. § 78u-6(h)(1)(A).

[42] Digital Realty Tr., Inc. v. Somers, 583 U.S. 149 (2018).

[43] Dodd-Frank provides a successful litigant with double back pay, a three-year statute of limitations, and the ability to go directly to federal court. 15 U.S.C. § 78u-6(h). In contrast, SOX does not provide a multiplier for back pay, has a 180-day statute of limitations, and requires that a litigant first file with the U.S. Department of Labor. 18 U.S.C. § 1514A.

[44] 15 U.S.C. § 78u-6(h)(1)(A); *see, e.g.*, Ott v. Fred Alger Mgmt., Inc., No. 11 CIV. 4418 LAP, 2012 WL 4767200, at *4 (S.D.N.Y. Sept. 27, 2012) (permitting Dodd-Frank retaliation claim to move forward against privately held investment firm).

© Copyright 2026

[45] 18 U.S.C. § 1514A(a)(1); Seguin v. Northrup Grumman Sys. Corp., ARB No. 16-014, ALJ No. 2012-SOX-37, 2017 WL 2838086, at *3 (Dep't of Labor May 30, 2017) ("The SOX employee protection provisions prohibit . . . retaliat[ion] against an employee . . . because the employee provided . . . information relating to alleged violations of 18 U.S.C. § 1341 (mail fraud), § 1343 (fraud by wire, radio, or television), § 1344 (bank fraud), § 1348 (security fraud), any rule or regulation of the Securities and Exchange Commission, or any provision of federal law relating to fraud against shareholders.").

[46] *See, e.g.*, Sylvester v. Parexel Int'l LLC, ARB No. 07-123, ALJ Nos. 2007-SOX-39 and 42, 2011 WL 2165854, at *17 (Dep't of Labor May 25, 2011) ("When an entity engages in mail fraud, wire fraud, or any of the six enumerated categories of violations set forth in Section 806, it does not necessarily engage in immediate shareholder fraud. . . . [W]e conclude that an allegation of shareholder fraud is not a necessary component of protected activity under SOX Section 806."); Zinn v. Am. Com. Lines Inc., ARB No. 10-029, ALJ No. 2009-SOX-025, 2012 WL 1143309, at *4 (Dep't of Labor Mar. 28, 2012) (citing *Sylvester*); Funke v. Fed. Express Corp., ARB No. 09-004, ALJ No. 2007-SOX-043, 2011 WL 3307574, at *7 (Dep't of Labor July 8, 2011) (citing *Sylvester*).

[47] *See, e.g.*, Nielsen v. AECOM Tech. Corp., 762 F.3d 214, 223 (2d Cir. 2014) (noting that plaintiff needed to allege facts plausibly suggesting that defendant's misconduct implicated "any" of the enumerated provisions in SOX Section 806); Wiest v. Lynch, 710 F.3d 121, 137 (3d Cir. 2013); Lockheed Martin Corp. v. Admin. Rev. Bd., 717 F.3d 1121, 1130–32 (10th Cir. 2013); Nance v. Time Warner Cable, Inc., 433 F. App'x 502, 503 (9th Cir. 2011); Wallender v. Canadian Nat'l Ry. Co., No. 2:13-CV-2603-DKV, 2015 WL 10818741, at *12 (W.D. Tenn. Feb. 10, 2015); Gladitsch v. Neo@Ogilvy, No. 11 CIV. 919 DAB, 2012 WL 1003513, at *7–8 (S.D.N.Y. Mar. 21, 2012); Sharkey v. J.P. Morgan Chase & Co., 805 F. Supp.2d 45, 55–56 (S.D.N.Y. 2011); O'Mahony v. Accenture Ltd., 537 F. Supp.2d 506, 517–18 (S.D.N.Y. 2008); *but see* Livingston v. Wyeth Inc., No. 1:03CV00919, 2006 WL 2129794, at *10 (M.D.N.C. July 28, 2006), *aff'd*, 520 F.3d 344 (4th Cir. 2008) ("To be protected under Sarbanes-Oxley, an employee's disclosures must be related to illegal activity that, at its core, involves shareholder fraud."); Gauthier v. Shaw Grp., Inc., No. 3:12-CV-00274-GCM, 2012 WL 6043012, at *4–5 (W.D.N.C. Dec. 4, 2012).

[48] 15 U.S.C. § 78u-6(h)(1)(A)(iii) ("No employer may discharge, demote, suspend, threaten, harass, directly or indirectly, or in any other manner discriminate against, a whistleblower in the terms and conditions of employment because of any lawful act done by the whistleblower . . . in making disclosures that are required or protected under the Sarbanes-Oxley Act of 2002 (15 U.S.C. 7201 et seq.) . . . ."); *see also* Neely v. Boeing Co., 823 F. App'x 494, 496 (9th Cir. 2020) (employee did not qualify as whistleblower under Dodd-Frank because he did not file a complaint with the SEC).

[49] *Sylvester*, 2011 WL 2165854, at *11–13; *see also* Northrop Grumman Sys. Corp. v. U.S. Dep't of Labor, 927 F.3d 226, 233 (4th Cir. 2019) ("[A]n employee engages in protected activity only when she provides information regarding conduct that she reasonably believes violates one of six categories listed by Congress in § 1514A(a)(1)—mail fraud, wire fraud, bank fraud, securities fraud, any SEC rule or regulation or any federal law relating to fraud against shareholders.").

[50] Johnson v. The Wellpoint Cos., Inc., ARB No. 16-020, ALJ No. 2010-SOX-038, 2017 WL 3953473, at *3 (Dep't of Labor Aug. 31, 2017); *see also* Day v. Staples, Inc., 555 F.3d 42, 55 (1st Cir. 2009); Harp v. Charter Commc'ns, 558 F.3d 722, 723 (7th Cir. 2009); Van Asdale v. Int'l Game Tech., 577 F.3d 989, 1001 (9th Cir. 2009); Allen v. Admin. Rev. Bd., 514 F.3d 468, 477 (5th Cir. 2008).

[51] *Sylvester*, 2011 WL 2165854, at *13; *see also* Wirth v. Salesforce, Inc., 749 F. Supp. 3d 231, 238 (D. Mass. 2024) ("[R]equiring an employee to wait for a violation to occur when an earlier report could have possibly prevented it would defeat the purpose of the statute.").

[52] Inman v. Fannie Mae, ARB No. 08-060, ALJ No. 2007-SOX-47, 2011 WL 2614298, at *6 (Dep't of Labor June 28, 2011) ("[A]n employee can engage in SOX-protected activity without mentioning or complaining about 'fraud.'"); *see also Wiest*, 710 F.3d at 134 ("An employee may not have access to information necessary to form a judgment on certain elements of a generic fraud claim, such as scienter or materiality, and yet have knowledge of facts sufficient to alert the employer to fraudulent conduct. When an employee communicates these facts to a supervisor, the employer has a sufficient basis to suspect that the employee is protected against reprisal for communicating that information."); Rhinehimer v. U.S. Bankcorp Invs., Inc., 787 F.3d 797, 811 (6th Cir. 2015) ("We agree with the Third Circuit that an employee 'should not be unprotected from reprisal because she did not have access to information sufficient to form an objectively reasonable belief that there was an intent to defraud or [that] the information communicated to her supervisor was material to a shareholder's decision.'" (quoting *Wiest*, 710 F.3d at 132)).

[53] 15 U.S.C. § 78j(b).

[54] 17 C.F.R. § 240.10b-5.

© Copyright 2026

[55] 15 U.S.C. § 77q(a).

[56] TSC Indus., Inc. v. Northway, Inc., 426 U.S. 438, 449 (1976); *see* Erica P. John Fund, Inc. v. Halliburton Co., 563 U.S. 804, 811 (2011).

[57] U.S. SEC. AND EXCH. COMM'N, *Altaba, Formerly Known as Yahoo!, Charged With Failing to Disclose Massive Cybersecurity Breach; Agrees to Pay $35 Million* (Apr. 24, 2018), https://www.sec.gov/news/press-release/2018-71.

[58] *See, e.g.*, U.S. SEC. AND EXCH. COMM'N, *SEC Charges Software Company Blackbaud Inc. for Misleading Disclosures About Ransomware Attack That Impacted Charitable Donors* (Mar. 9, 2023), https://www.sec.gov/news/press-release/2023-48; U.S. SEC. AND EXCH. COMM'N, *SEC Charges Pearson plc for Misleading Investors about Cyber Breach* (Aug. 16, 2021), https://www.sec.gov/news/press-release/2021-154.

[59] U.S. SEC. AND EXCH. COMM'N, *SEC Charges Four Companies With Misleading Cyber Disclosures* (Oct. 22, 2024), https://www.sec.gov/newsroom/press-releases/2024-174.

[60] U.S. SEC. AND EXCH. COMM'N, *SEC Charges Flagstar for Misleading Investors About Cyber Breach* (Dec. 16, 2024), https://www.sec.gov/enforcement-litigation/administrative-proceedings/33-11343-s.

[61] U.S. SEC. AND EXCH. COMM'N, *CF Disclosure Guidance: Topic No. 2, Cybersecurity* (2011), *available at* https://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm (hereinafter "2011 Cybersecurity Guidance").

[62] For example, the SEC stated that cybersecurity disclosures should include: (1) a discussion of aspects of the registrant's business or operations that give rise to material cybersecurity risks and the potential costs and consequences; (2) to the extent the registrant outsources functions that have material cybersecurity risks, a description of those functions, and how the registrant addresses those risks; (3) a description of cyber incidents experienced by the registrant that are individually, or in the aggregate, material, including a description of the costs and other consequences; (4) risks related to cyber incidents that may remain undetected for an extended period; and (5) a description of relevant insurance coverage. *Id.*

[63] U.S. SEC. AND EXCH. COMM'N, *Commission Statement and Guidance on Public Company Cybersecurity Disclosures* (2018), *available at* https://www.sec.gov/rules/interp/2018/33-10459.pdf (hereinafter "2018 Cybersecurity Guidance").

[64] For example, the SEC stated that companies should evaluate: (1) the occurrence of prior cybersecurity incidents, including their severity and frequency; (2) the probability of the occurrence and potential magnitude of cybersecurity incidents; (3) the adequacy of preventative actions taken to reduce cybersecurity risks and the associated costs, including, if appropriate, discussing the limits of the company's ability to prevent or mitigate certain cybersecurity risks; (4) the aspects of the company's business and operations that give rise to material cybersecurity risks and the potential costs and consequences of such risks, including industry-specific risks and third-party supplier and service provider risks; (5) the costs associated with maintaining cybersecurity protections, including, if applicable, insurance coverage relating to cybersecurity incidents or payments to service providers; (6) the potential for reputational harm; (7) existing or pending laws and regulations that may affect the requirements to which companies are subject relating to cybersecurity and the associated costs to companies; and (8) litigation, regulatory investigation, and remediation costs associated with cybersecurity incidents. *Id.* at 13–14.

[65] U.S. SEC. AND EXCH. COMM'N, *Final Rule: Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure* (July 26, 2023), *available at* https://www.sec.gov/files/rules/final/2023/33-11216.pdf (hereinafter, "2023 Cybersecurity Rules").

[66] U.S. SEC. AND EXCH. COMM'N, Form 8-K, Item 1.05 and General Instructions § B.1, *available at* https://www.sec.gov/files/form8-k.pdf.

[67] *Id.*

[68] 17 C.F.R. § 229.106.

[69] The SEC introduced another set of proposed cybersecurity rules on March 15, 2023 that would have imposed requirements on broker-dealers, clearing agencies, and other so-called "market entities" to address their cybersecurity risks. *See* U.S. SEC. AND EXCH. COMM'N, *SEC Proposes New Requirements to Address Cybersecurity Risks to the U.S. Securities Markets* (Mar. 15, 2023), https://www.sec.gov/news/press-release/2023-52. On June 17, 2025, however, the Commission formally withdrew the notice of proposed

© Copyright 2026

rulemaking. U.S. SEC. AND EXCH. COMM'N, *Notice of Withdrawal of Proposed Regulatory Actions* (June 17, 2025), *available at* https://www.sec.gov/files/rules/final/2025/33-11377.pdf.

[70] U.S. SEC. AND EXCH. COMM'N, *Facebook to Pay $100 Million for Misleading Investors About the Risks It Faced from Misuse of User Data* (July 24, 2019), https://www.sec.gov/news/press-release/2019-140.

[71] *Id.*

[72] *Id.*

[73] In re LifeLock, Inc. Sec. Litig., 690 F. App'x 947 (9th Cir. 2017).

[74] *Id.* at 952.

[75] *Id.*

[76] The Supreme Court has defined scienter as "a mental state embracing intent to deceive, manipulate, or defraud." Ernst & Ernst v. Hochfelder, 425 U.S. 185, 193 n.12 (1976). The precise definition of "scienter" in the context of securities fraud actions varies depending on the jurisdiction, but generally includes some level of "reckless disregard" in excess of ordinary negligence. *See generally* Greebel v. FTP Software, Inc., 194 F.3d 185, 198–201 (1st Cir. 1999) (discussing varying definitions of scienter among the circuits); *see also* In re Gen. Elec. Sec. Litig., 844 F. App'x 385, 388 (2d Cir. 2021) ("Scienter can be pleaded with adequate particularity through allegations showing either (1) that defendants had the motive and opportunity to commit fraud, or (2) strong circumstantial evidence of conscious misbehavior or recklessness." (internal quotation marks omitted)); In re Triangle Cap. Corp. Sec. Litig., 988 F.3d 743, 751 (4th Cir. 2021) (including "severe recklessness" in the definition of scienter, meaning "an act so highly unreasonable and such an extreme departure from the standard of ordinary care as to present a danger of misleading the plaintiff to the extent that the danger was either known to the defendant or so obvious that the defendant must have been aware of it").

[77] *LifeLock*, 690 F. App'x at 953.

[78] *Id.* at 956; *but see* Singleton v. Intellisist, Inc., No. C17-1712RSL, 2018 WL 2113973, at *3 (W.D. Wash. May 8, 2018) (finding that plaintiff stated a claim for wrongful discharge by alleging that he was terminated in retaliation for his whistleblowing concerning PCI DSS violations), *reconsideration denied,* No. C17-1712RSL, 2018 WL 3032662 (W.D. Wash. June 19, 2018). This decision serves as a reminder that whistleblowers for whom federal statutes do not provide a remedy should consider possible remedies under state law. *See* Section II.B, *infra*.

[79] In re Marriott Int'l, Inc., 31 F.4th 898 (4th Cir. 2022).

[80] *Id.* at 901.

[81] *Id.* at 902 n.1.

[82] *Id.* at 904–05.

[83] *Id.* at 904 (quoting In re Alphabet, Inc. Sec. Litig., 1 F.4th 687, 703–04 (9th Cir. 2021)).

[84] *Id.* at 905.

[85] The events from which this action arose occurred prior to the 2023 Cybersecurity Rules becoming effective.

[86] Sec. & Exch. Comm'n v. SolarWinds Corp., 741 F. Supp. 3d 37 (S.D.N.Y. 2024).

[87] *Id.* at 48–49.

[88] *Id.* at 49–50.

[89] *Id.* at 89.

[90] *Id.* at 91–92.

[91] *Id.* at 102–03.

© Copyright 2026

[92] U.S. SEC. AND EXCH. COMM'N, *SolarWinds Corp. and Timothy G. Brown* (Nov. 20, 2025), https://www.sec.gov/enforcement-litigation/litigation-releases/lr-26423.

[93] In re Alphabet, Inc. Sec. Litig., 1 F.4th 687, 709 (9th Cir. 2021), *cert. denied*, 142 S. Ct. 1227 (Mar. 7, 2022) (No. 21-594).

[94] *Id.* at 695.

[95] *Alphabet*, 1 F.4th at 696–97.

[96] *Id.*

[97] *Id.* at 703.

[98] 17 C.F.R. §§ 240.13a-15, 240.15d-15.

[99] *See* 2018 Cybersecurity Guidance, *supra* n.63, at 18.

[100] *Id.*

[101] *Id.* at 17–18.

[102] 17 C.F.R. § 229.106(b).

[103] 17 C.F.R. § 229.106(c).

[104] 262 F. Supp. 3d 1328, 1332 (S.D. Fla. 2017).

[105] *Id.* at 1336–37 (citing *Commission Guidance Regarding Management's Report on Internal Control Over Financial Reporting Under Section 13(a) or 15(d) of the Securities Exchange Act of 1934*, Release Nos. 33-8810; 34-55929; FR-77; File No. S7-24-06, 72 Fed. Reg. 35343 n.27 (June 27, 2007); Wiggins v. ING U.S., Inc., No. 3:14-CV-01089 (JCH), 2015 WL 8779559, at *7 (D. Conn. Dec. 15, 2015)).

[106] 17 C.F.R. §§ 248.30, 248.201.

[107] 17 C.F.R. §§ 248.1, 248.4–6.

[108] 17 C.F.R. § 248.10.

[109] U.S. SEC. AND EXCH. COMM'N, *SEC Announces Three Actions Charging Deficient Cybersecurity Procedures* (Aug. 30, 2021), https://www.sec.gov/news/press-release/2021-169.

[110] U.S. SEC. AND EXCH. COMM'N, *SEC Adopts Rule Amendments to Regulation S-P to Enhance Protection of Customer Information* (May 16, 2024), https://www.sec.gov/newsroom/press-releases/2024-58.

[111] *Id.*

[112] *Id.*

[113] *Id.*

[114] 17 C.F.R. § 248.201.

[115] U.S. SEC. AND EXCH. COMM'N, *SEC Charges Firm With Deficient Cybersecurity Procedures* (Sept. 26, 2018), https://www.sec.gov/news/press-release/2018-213.

[116] *Id.*

[117] U.S. SEC. AND EXCH. COMM'N, *SEC Charges JPMorgan, UBS, and TradeStation for Deficiencies Relating to the Prevention of Customer Identity Theft* (July 27, 2022), https://www.sec.gov/newsroom/press-releases/2022-131.

[118] U.S. SEC. AND EXCH. COMM'N, *Two Robinhood Broker-Dealers to Pay $45 Million in Combined Penalties for Violating More Than 10 Separate Securities Law Provisions* (Jan. 13, 2025), https://www.sec.gov/newsroom/press-releases/2025-5.

© Copyright 2026

[119] 15 U.S.C. § 78u-6(h)(1)(A); *see also* Ott v. Fred Alger Mgmt., Inc., No. 11 CIV. 4418 LAP, 2012 WL 4767200, at *4 (S.D.N.Y. Sept. 27, 2012) (permitting Dodd-Frank retaliation claim to move forward against privately held investment firm).

[120] Baig v. Meta Platforms, Inc., No. 25-CV-07604-LB, 2026 WL 821002, at *4–7 (N.D. Cal. Mar. 23, 2026).

[121] 18 U.S.C. § 1514A(a).

[122] 15 U.S.C. § 78u-6(h)(1)(A).

[123] Menendez v. Halliburton, Inc., ARB No. 09-002, ALJ Case No. 2007-SOX-005, 2011 WL 4915750, at *9 (Dep't of Labor Sept. 13, 2011).

[124] *Id.* at *10.

[125] *See, e.g.*, *id.* at *12–16 (outing and blackballing a whistleblower is an adverse action); Fricka v. Nat'l R.R. Passenger Corp., ARB No. 14-047, ALJ No. 2013-FRS-035, 2015 WL 7904894, at *4–5 (Dep't of Labor Nov. 24, 2015) (applying identical adverse action standard to separate anti-retaliation statute and finding that misclassification of injury could constitute adverse action); Williams v. Am. Airlines, Inc., ARB No. 09-018, ALJ No. 2007-AIR-004, 2010 WL 5535815, at *6 & n.51 (Dep't of Labor Dec. 29, 2010) (noting in the context of a statute with a "virtually identical" definition of adverse employment action that the definition was "intended to include, as a matter [of] law, reprimands (written or verbal), as well as counseling sessions . . . which are coupled with a reference to potential discipline"); McClendon v. Hewlett Packard, Inc., ALJ No. 2006-SOX-29, 2006 WL 6577175, at *79–81 (Dep't of Labor Oct. 5, 2006) (transfer to a position with significantly different job responsibilities constituted adverse action); Hendrix v. Am. Airlines, Inc., ARB No. 2004-SOX-23, ALJ No. 2004-AIR-10, 2004 WL 5345479, at *13 (Dep't of Labor Dec. 9, 2004) (placing an employee on a layoff list constituted an adverse action, despite subsequent removal from list).

[126] *See, e.g.*, Halliburton, Inc. v. Admin. Rev. Bd., 771 F.3d 254, 259–62 (5th Cir. 2014) (holding that "outing" a whistleblower to his colleagues could constitute an adverse action under SOX); Erhart v. Bofl Holding, Inc., 269 F. Supp. 3d 1059, 1075–76 (S.D. Cal. 2017) (making threats and derogatory statements about an employee was adverse action); Guitron v. Wells Fargo Bank, N.A., No. C 10-3461 CW, 2012 WL 2708517, at *16 (N.D. Cal. July 6, 2012) (holding that paid administrative leave and poor performance review were adverse actions), *aff'd*, 619 F. App'x 590 (9th Cir. 2015); Kolchinsky v. Moody's Corp., No. 10 CIV. 6840 PAC, 2012 WL 639162, at *6 (S.D.N.Y. Feb. 28, 2012) (holding that exclusion from meetings, demotion, reduced salary and bonuses, transfer to a support role without possibility of promotion, suspension, and termination were each adverse actions).

[127] *See, e.g.*, Halliburton, 771 F.3d at 260; Allen v. Admin. Rev. Bd., 514 F.3d 468, 476 n.2 (5th Cir. 2008); Quast v. MidAmerican Energy Co., No. 4-14-CV-00278, 2016 WL 4536460, at *12 (S.D. Iowa Feb. 8, 2016); Bogenschneider v. Kimberly Clark Glob. Sales, LLC, No. 14-CV-743-BBC, 2015 WL 3948137, at *3 (W.D. Wis. June 29, 2015).

[128] 29 C.F.R. § 1980.104(e)(1).

[129] Murray v. UBS Sec., LLC, 601 U.S. 23, 24 (2024).

[130] Ott v. Fred Alger Mgmt., Inc., No. 11 CIV. 4418 LAP, 2012 WL 4767200, at *6–7 (S.D.N.Y. Sept. 27, 2012); *see also* Yang v. Navigators Grp., Inc., 674 F. App'x 13, 14 (2d Cir. 2016) ("The parties agree that the elements of a Dodd-Frank claim, while not identical, are sufficiently similar for the SOX standard to control review on this appeal.").

[131] Ott v. Fred Alger Mgmt., Inc., No. 11 CIV. 4418 LAP, 2016 WL 5407663, at *9–10 (S.D.N.Y. Sept. 27, 2016).

[132] *See, e.g.*, Edwards v. First Tr. Portfolios L.P., No. 3:23-CV-2239-BN, 2025 WL 256993, at *11 (N.D. Tex. Jan. 21, 2025); Slawin v. Bank of Am. Merch. Servs., 491 F. Supp. 3d 1334, 1339–40 (N.D. Ga. 2020); Thomas v. Tyco Int'l Mgmt. Co., LLC, 416 F. Supp. 3d 1340, 1367 (S.D. Fla. 2019); Miglani v. Edwards Lifesciences, LLC, No. 8:17-CV-00418-JLS-DFM, 2018 WL 6265007, at *3 (C.D. Cal. Jan. 8, 2018); Price v. UBS Fin. Servs., Inc., No. CV 2:17-01882, 2017 WL 5667994, at *3 (D.N.J. Nov. 27, 2017); Grimm v. Best Buy Co., No. 16-CV-1258 (DWF/HB), 2017 WL 9274874, at *4 (D. Minn. Apr. 19, 2017), *R&R adopted*, No. CV 16-1258 (DWF/HB), 2017 WL 2345585 (D. Minn. May 30, 2017); Hall v. Teva Pharm. USA, Inc., 214 F. Supp. 3d 1281, 1288 (S.D. Fla. 2016).

[133] 18 U.S.C. § 1514A(b)(2)(D).

[134] 29 C.F.R. § 1980.105(a).

© Copyright 2026

[135] 29 C.F.R. §§ 1980.106(a), 1980.107.

[136] 29 C.F.R. § 1980.110(a).

[137] 29 C.F.R. § 1980.112(a).

[138] 18 U.S.C. § 1514A(b)(1)(B).

[139] 18 U.S.C. § 1514A(e)(2).

[140] 15 U.S.C. § 78u-6(h)(1)(B)(i).

[141] 15 U.S.C. § 78u-6(h)(1)(B)(iii).

[142] 12 U.S.C. § 1831j.

[143] 12 U.S.C. § 5481 *et seq.*

[144] 12 U.S.C. § 5567.

[145] 12 U.S.C. § 1831j(a). The covered federal banking entities are the FDIC, the Board of Governors of the Federal Reserve System, the Federal Housing Finance Agency, the Comptroller of the Currency, federal home loan banks, and Federal Reserve banks. 12 U.S.C. §§ 1831j(a)(2), 1831j(e).

[146] *Id.*

[147] 15 U.S.C. § 6801 *et seq.*

[148] 15 U.S.C. § 45.

[149] 15 U.S.C. § 45(a)(1). The specific coverage of these laws in relation to cybersecurity is discussed in detail in Section II.B.1.

[150] 12 U.S.C. § 1831j(a)(1).

[151] *Id.*; *see also* Lippert v. Cmty. Bank, Inc., 438 F.3d 1275, 1279–80 (11th Cir. 2006); Haug v. PNC Fin. Servs. Grp., Inc., 930 F. Supp. 2d 871, 884–85 (N.D. Ohio 2013).

[152] 12 U.S.C. § 1831j(d).

[153] Confidential supervisory information means information "created or obtained in furtherance of the [Federal Reserve Board of Governors' or any Federal Reserve Bank's] supervisory, investigatory, or enforcement activities," including "reports of examination, inspection, and visitation; confidential operating and condition reports; supervisory assessments; investigative requests for documents or other information; and supervisory correspondence or other supervisory communications." 12 C.F.R. § 261.2(b)(1). Further, "any portion of a document in the possession of any person . . . that contains or would reveal confidential supervisory information is confidential supervisory information." *Id.*

[154] *See* 12 C.F.R. § 261.20 (providing that confidential supervisory information is the property of the Federal Reserve Board of Governors); 18 U.S.C. § 641 (providing that theft of federal property is subject to a fine or imprisonment of up to ten years).

[155] 12 U.S.C. § 5567(a)(1).

[156] *Id.*

[157] There is little case law examining what constitutes protected activity under the CFPA, but courts have applied the SOX standard, i.e., that reasonable belief has subjective and objective components, to CFPA retaliation claims. *See* Veard v. F&M Bank, 704 F. App'x 469, 474 (6th Cir. 2017).

[158] 12 U.S.C. § 5567(a)(1).

[159] CONSUMER FIN. PROT. BUREAU, *Gramm-Leach-Bliley Act (GLBA) Examination Procedures* (last updated Oct. 28, 2016), *available at* https://files.consumerfinance.gov/f/documents/102016_cfpb_GLBAExamManualUpdate.pdf.

© Copyright 2026

[160] *Id.* at 4.

[161] *Id.* at 1.

[162] *Id.*

[163] 12 U.S.C. § 1831j(a)(1).

[164] *See* 5 U.S.C. § 1221(e)(1); 12 U.S.C. § 1831j(f) (adopting § 1221 standard); *see also* Becotte v. Coop. Bank, No. CV 15-10812-RGS, 2017 WL 886967, at *5 (D. Mass. Mar. 6, 2017).

[165] In 2024, the Supreme Court clarified that, while an action must be "materially" adverse so as to deter employees from engaging in protected activity in Title VII retaliation cases, in the discrimination context, the harm need not be "significant"—there merely needs to have been *some* harm. Muldrow v. City of St. Louis, Mo., 601 U.S. 346, 347 (2024).

[166] *Compare, e.g.*, Fruge v. Bd. of Governors of Fed. Rsrv. Sys., No. 1:20-CV-02811 (CJN), 2022 WL 5166031, at *16–17 (D.D.C. Oct. 5, 2022) (noting similarities between FIRREA adverse action definition and that of Title VII discrimination provision, and adopting adverse action standard from Title VII discrimination provision), *with* Waiting v. Blue Hills Bank, No. CV 14-14742-IT, 2017 WL 1074952, at *10 (D. Mass. Feb. 8, 2017) (applying "materially adverse" adverse action standard from Title VII retaliation claims without analysis), *R&R adopted*, No. 14-CV-14742-IT, 2017 WL 1054485 (D. Mass. Mar. 20, 2017).

[167] *See, e.g.*, Real-Loomis v. Bryn Mawr Tr. Co., No. 2:20-CV-0441-JDW, 2022 WL 17477552, at *2 (E.D. Pa. Dec. 6, 2022) (analyzing CFPA and SOX claims together).

[168] 12 U.S.C. § 1831j(b).

[169] *Id.*

[170] *Id.*

[171] 12 U.S.C. § 5567(c)(1)(A).

[172] 29 C.F.R. § 1985.105(a).

[173] 29 C.F.R. §§ 1985.106(a), 1985.107.

[174] 29 C.F.R. § 1985.110(a).

[175] 29 C.F.R. § 1985.112(a).

[176] 12 U.S.C. § 5567(c)(4)(D)(i).

[177] 12 U.S.C. § 5567(d).

[178] 31 U.S.C. § 3729 *et seq.*

[179] James B. Helmer Jr., *False Claims Act: Incentivizing Integrity for 150 Years for Rogues, Privateers, Parasites and Patriots*, 81 U. CIN. L. REV. 1261, 1264–65 (2013) (footnotes omitted).

[180] *See* 31 U.S.C. §§ 3729(a), 3730(b).

[181] Pub. L. No. 99-562, 100 Stat. 3153 (1986).

[182] Pub. L. No. 111-21 § 4, 123 Stat. 1617, 1621–25 (2009).

[183] Pub. L. No. 111-203, § 1079A (c)(1), 124 Stat. 1376 (2010).

[184] 31 U.S.C. § 3730(h).

[185] Pub. L. No. 99-562, § 4, 100 Stat. 3153 (1986).

[186] U.S. ex rel. Karvelas v. Melrose-Wakefield Hosp., 360 F.3d 220, 236 (1st Cir. 2004) (collecting cases), *abrogated on other grounds by* Allison Engine Co. v. U.S. ex rel. Sanders, 553 U.S. 662 (2008).

[187] Pub. L. No. 111-21, § 4(d), 123 Stat. 1617, 1624–25 (2009), codified as 31 U.S.C. § 3730(h)(1).

© Copyright 2026

[188] *See* S. COMM. ON JUDICIARY, FALSE CLAIMS AMENDMENTS ACT OF 1986, S. REP. NO. 345, at 35 (1986), *REPRINTED IN* 1986 U.S.C.C.A.N. 5266, 5299 ("Protected activity should . . . be interpreted broadly."); 155 CONG. REC. E1295-03, E1300 (daily ed. June 3, 2009) (statement of Rep. Berman) ("[T]his subsection protects not only steps taken in furtherance of a potential or actual qui tam action, but also steps taken to remedy the misconduct through methods such as internal reporting to a supervisor or company compliance department and refusals to participate in the misconduct that leads to the false claims, whether or not such steps are clearly in furtherance of a potential or actual qui tam action.").

[189] *See* Mooney v. Fife, 118 F.4th 1081, 1092 (9th Cir. 2024) ("[A]n employee's efforts to stop 1 or more violations need not lead to a lawsuit or to the distinct possibility of a lawsuit." (internal quotation marks omitted)); U.S. ex rel. Ascolese v. Shoemaker Constr. Co., 55 F.4th 188, 194–96 (3d Cir. 2022) (discussing broadened scope of FCA anti-retaliation provision following FERA amendments and finding that reporting concerns of fraud internally constituted protected activity under the FCA); Hickman v. Spirit of Athens, Alabama, Inc., 985 F.3d 1284, 1288–89 (11th Cir. 2021) (recognizing broadened scope of protected activity under FERA amendments but declining to expressly overrule pre-FERA precedent because it did not affect outcome); Singletary v. Howard Univ., 939 F.3d 287, 297 (D.C. Cir. 2019) (plaintiff established she engaged in protected activity because she alleged "facts showing that she took lawful measures to stop or avert what she reasonably believed would be a violation of the False Claims Act" by reporting conditions that were non-compliant with federal funding programs of her laboratory to her employer); Guilfoile v. Shields, 913 F.3d 178, 189 (1st Cir. 2019) ("Put colloquially, rather than plausibly pleading the existence of a fire -- the actual submission of a false claim -- a plaintiff alleging FCA retaliation need only plausibly plead a reasonable amount of smoke -- conduct that could reasonably lead to an FCA action based on the submission of a false claim."); U.S. ex rel. Reed v. KeyPoint Gov't Sols., 923 F.3d 729, 738 (10th Cir. 2019) (recognizing effect of FERA amendments in expanding scope of protected activity); U.S. ex rel. Crockett v. Complete Fitness Rehab., Inc., 721 F. App'x 451, 460 (6th Cir. 2018) (plaintiff's objections to supervisor's demands that she provide patients with more therapy than necessary or appropriate and complaints that supervisor did so to increase profits from Medicare were protected under the FCA); U.S. ex rel. Chorches for Bankr. Est. of Fabula v. Am. Med. Response, Inc., 865 F.3d 71, 95–98 (2d Cir. 2017) (discussing FERA amendments and finding that refusal to participate in fraudulent scheme was protected under the FCA); U.S. ex rel. Bias v. Tangipahoa Parish Sch. Bd., 816 F.3d 315, 323 (5th Cir. 2016) (plaintiff engaged in protected activity under the FCA by reporting suspected misappropriation of government funds internally); Young v. CHS Middle East, LLC, 611 F. App'x 130, 132–34 (4th Cir. 2015) (plaintiffs' internal complaints that, *inter alia*, using expired medicines was illegal and violated the contract were deemed protected activity under the FCA); Halasa v. ITT Educ. Servs., Inc., 690 F.3d 844, 847–48 (7th Cir. 2012) (discussing FERA amendments and finding that internal reports of false claims were protected under the statute); U.S. ex rel. Lupo v. Quality Assurance Servs., Inc., 242 F. Supp. 3d 1020, 1028 (S.D. Cal. 2017) ("Relator was not required to specifically communicate an intention to bring an FCA action; section 3730(h) protects other steps, as well, including internal reporting."); Hinton v. Integra LifeSciences Holdings Corp., No. 18-CV-00244-SRB, 2022 WL 1036777, at *9 (W.D. Mo. Apr. 6, 2022) (finding that internal reports to whistleblower hotline represented "efforts to stop" FCA violations and therefore were protected).

[190] *See, e.g.*, Eder v. City of Burleson, No. 3:23-CV-00948-K, 2024 WL 4771408, at *2 (N.D. Tex. Nov. 13, 2024); Scibetta v. AcclaiMed Healthcare, No. 3:16-CV-02385-PGS-DEA, 2021 WL 5450296, at *8 (D.N.J. Nov. 22, 2021); McClinton on behalf of United States v. Southerncare, Inc., No. 3:16-CV-128-CWR-FKB, 2021 WL 2587162, at *5 (S.D. Miss. June 23, 2021); Jacquez v. GEO Int'l Mgmt., LLC, No. EP-20-CV-00183-KC, 2021 WL 2908880, at *7 (W.D. Tex. June 2, 2021).

[191] United States v. Eastwick Coll., 657 F. App'x 89, 93–94 (3d Cir. 2016) (quoting U.S. ex rel. Wilkins v. United Health Grp., Inc., 659 F.3d 295, 305 (3d Cir. 2011)).

[192] *Id.*

[193] U.S. ex rel. Bergman v. Abbot Labs., 995 F. Supp. 2d 357, 366 (E.D. Pa. 2014).

[194] *Id.*

[195] *Id.*; *see also* United States v. Aerojet Rocketdyne Holdings, Inc., 381 F. Supp. 3d 1240, 1248–49 (E.D. Cal. 2019) ("[R]elator's complaint alleges possible material nondisclosures . . . such as AR's failure to report its status on all required controls, its alleged misstatements as to partial compliance with protection measures, and the fact that the company cherrypicked what data it chose to report. . . . Accepting these allegations as true, the government may not have awarded these contracts if it knew the full extent of the company's noncompliance, because how close AR was to full compliance was a factor in the government's decision to enter into some contracts.").

[196] Universal Health Servs. v. U.S. ex rel. Escobar, 579 U.S. 176, 188–90 (2016).

© Copyright 2026

[197] *Id.* at 191; s*ee, e.g.*, United States v. Aerojet Rocketdyne Holdings, Inc., 381 F. Supp. 3d 1240, 1248–49 (E.D. Cal. 2019) (holding that a defense contractor's noncompliance with regulations for safeguarding against cybersecurity threats was material to the government's decision to pay the contractor).

[198] Federal Acquisition Regulation; Basic Safeguarding of Contractor Information Systems, 81 Fed. Reg. 30439 (May 16, 2016) (codified at 48 C.F.R. pts. 4, 7, 12, and 52).

[199] 48 C.F.R. § 52.204-21 (hereinafter "FAR 52.204-21").

[200] Defense Federal Acquisition Regulation Supplement: Network Penetration Reporting and Contracting for Cloud Services, 81 Fed. Reg. 72986 (October 21, 2016) (codified at 48 C.F.R. pts. 202, 204, 212, 239, and 252); *see* NAT'L INST. SCI. & TECH, Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations, Rev. 3 (last updated May 14, 2024), https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171r3.pdf (hereinafter "NIST SP 800-171").

[201] 48 C.F.R. § 252.204-7012 (hereinafter "DFARS 252.204-7012").

[202] Defense Federal Acquisition Regulation Supplement: Assessing Contractor Implementation of Cybersecurity Requirements, 85 Fed. Reg. 61505 (Sept. 29, 2020).

[203] *Id.* at 61510.

[204] Cybersecurity Maturity Model Certification (CMMC) 2.0 Updates and Way Forward, 86 Fed. Reg. 64100 (Nov. 17, 2021).

[205] FCI refers to "information, not intended for public release, that is provided by or generated for the Government under a contract to develop or deliver a product or service to the Government, but not including information provided by the Government to the public (such as on public Web sites) or simple transactional information, such as necessary to process payments." 48 C.F.R. § 52.204-21(a).

[206] U.S. DEP'T OF DEF., *About CMMC*, https://dodcio.defense.gov/cmmc/About/ (last visited May 26, 2026).

[207] CUI refers to "information the Government creates or possesses, or that an entity creates or possesses for or on behalf of the Government, that a law, regulation, or Government-wide policy requires or permits an agency to handle using safeguarding or dissemination controls," but does not include classified information "or information a non-executive branch entity possesses and maintains in its own systems that did not come from, or was not created or possessed by or for, an executive branch agency or an entity acting for an agency." 32 C.F.R. § 2002.4(h).

[208] An Advanced Persistent Threat is "adversary that possesses sophisticated levels of expertise and significant resources which allow it to create opportunities to achieve its objectives by using multiple attack vectors including, for example, cyber, physical, and deception." NIST SP 800-171 at 85.

[209] Cybersecurity Maturity Model Certification (CMMC) Program (Oct. 15, 2024), 89 Fed. Reg. 83092 (codified at 32 C.F.R. pt. 170).

[210] Defense Federal Acquisition Regulation Supplement: Assessing Contractor Implementation of Cybersecurity Requirements, 90 Fed. Reg. 43560 (Sept. 10, 2025) (codified at 48 C.F.R. pts. 204, 212, 217, and 252).

[211] U.S. DEP'T OF DEF., *About CMMC*, https://dodcio.defense.gov/cmmc/About/ (last visited May 26, 2026).

[212] *Id.*

[213] *See, e.g.*, Jefferson v. Sci. Applications Int'l Corp., No. CV 24-1692 (SLS), 2025 WL 1305245, at *3–4 (D.D.C. May 6, 2025) (denying motion to dismiss FCA retaliation claim alleging employee was terminated from government contractor employer after complaining about noncompliance with cybersecurity standards in relation to DOD contract); U.S. ex rel. Decker v. Penn. State Univ., No. 22-cv-03895-PD (E.D. Penn. filed Oct. 5, 2022) (*qui tam* case unsealed on September 1, 2023, in which the relator, the former Chief Information Officer of Penn State's Applied Research Lab, alleged that Penn State falsely certified to the DOD that, *inter alia*, it was compliant with NIST SP 800-171).

[214] 31 U.S.C. § 3730(h).

[215] *See* Katie Benner & Katie Conger, *Cisco to Pay $8.6 Million to Settle Government Claims of Flawed Tech*, N.Y. TIMES (July 31, 2019), https://www.nytimes.com/2019/07/31/technology/cisco-tech-flaw-

© Copyright 2026

sales.html; *see also* ATT'Y GEN. OF N.C., *Attorney General Josh Stein Reaches $6 Million Settlement with Cisco Systems* (Aug. 1, 2019), https://ncdoj.gov/attorney-general-josh-stein-reaches-6-million-set/; ATT'Y GEN. OF N.Y., *Attorney General James Secures $6 Million from Cisco Systems in Multistate Settlement* (Aug. 1, 2019), https://ag.ny.gov/press-release/2019/attorney-general-james-secures-6-million-cisco-systems-multistate-settlement.

[216] *See* Raytheon Settlement, *supra* n.12; Illumina Settlement, *supra* n.13; Georgia Tech Settlement, *supra* n.14.

[217] 31 U.S.C. § 3730(h).

[218] *See, e.g.*, Brunelle v. PeaceHealth, No. 3:22-CV-05499-TMC, 2024 WL 4529267, at *15 (W.D. Wash. Oct. 18, 2024) (citing Burlington N. & Santa Fe Ry. Co. v. White, 548 U.S. 53, 68 (2006)); Difiore v. CSL Behring, U.S., LLC, 171 F. Supp. 3d 383, 393 (E.D. Pa. Mar. 17, 2016).

[219] *See* Pitts v. Howard Univ., 111 F. Supp. 3d 9, 23 (D.D.C. 2015) (diminished responsibilities); Clinkscales v. Walgreen Co., No. CA 8:10-2290-TMC, 2012 WL 80543, at *6 (D.S.C. Jan. 11, 2012) (written warnings); Turner v. DynMcDermott Petroleum Operations Co., No. CIV.A. 06-1455, 2010 WL 4363403, at *3 (E.D. La. Oct. 21, 2010) (performance audit); *see also Difiore*, 171 F. Supp. 3d at 394–95 (holding that multiple actions that would not constitute adverse actions in isolation may be taken together to constitute adverse actions).

[220] 31 U.S.C. § 3730(h)(3).

[221] U.S. ex rel. Pilon v. Martin Marietta Corp., 60 F.3d 995, 1000 (9th Cir. 1995).

[222] U.S. ex rel. Ramseyer v. Century Healthcare Corp., 90 F.3d 1514, 1522 (10th Cir. 1996), *superseded by statute as stated in* Tompkins v. U.S. Dep't of Veterans Affs., 16 F.4th 733 (10th Cir. 2021).

[223] *See e.g.*, U.S. DEP'T OF TREASURY, Financial Crimes Enforcement Network, Advisory to Financial Institutions on Cyber-Events and Cyber-Enabled Crime, No. FIN-2016-A005 (Oct. 25, 2016), https://www.fincen.gov/sites/default/files/advisory/2016-10-25/Cyber%20Threats%20Advisory%20-%20FINAL%20508_2.pdf (hereinafter "FinCEN Cyber Advisory"); U.S. DEP'T OF TREASURY, Financial Crimes Enforcement Network, Anti-Money Laundering and Countering the Financing of Terrorism National Priorities (June 30, 2021), https://www.fincen.gov/sites/default/files/shared/AML_CFT%20Priorities%20(June%2030%2C%202021).pdf (hereinafter "FinCEN AML Priorities").

[224] FinCEN AML Priorities, *supra* n.223, at 4.

[225] 31 U.S.C. § 5311 *et seq*.

[226] 31 U.S.C. § 5323(g)(1)(A); 31 U.S.C. § 5323(g)(1)(C) (protected activity includes providing information regarding conduct that the whistleblower "reasonably believes" constitutes a covered violation to a person with supervisory authority over the whistleblower or to "another individual working for the employer" who the whistleblower reasonably believes has the authority to investigate, discover, or terminate the misconduct or take any other action to address it).

[227] *See* 31 U.S.C. § 5323(a)(5)(A) (defining whistleblower as any individual or individuals who report covered violations, "including as part of the job duties of the individual or individuals").

[228] 31 U.S.C. § 5323(g)(1)(B).

[229] 31 U.S.C. § 5323(g)(1)(C).

[230] 12 C.F.R. § 21.11(c).

[231] FinCEN Cyber Advisory, *supra* n.223.

[232] *Id.* at 4.

[233] *Id.* at 6.

[234] 31 U.S.C. § 5323(g)(1).

[235] 31 U.S.C. § 5323(g)(2)(A).

© Copyright 2026

[236] 31 U.S.C. § 5323(g)(2)(B).

[237] 31 U.S.C. § 5323(j)(2).

[238] 31 U.S.C. § 5323(g)(3)(B)(ii).

[239] 31 U.S.C. § 5323(g)(3)(C).

[240] 42 U.S.C. § 5851.

[241] 42 U.S.C. § 5851(a)(1); *see also* Procedures for the Handling of Retaliation Complaints Under the Employee Protection Provisions of Six Environmental Statutes and Section 211 of the Energy Reorganization Act of 1974, 76 Fed. Reg. 2808, 2819 (Jan. 18, 2011) ("[T]he reporting of possible violations of NRC regulations is protected activity under the ERA.").

[242] 10 C.F.R. § 73.54.

[243] Licensees include persons or entities who "conduct any or all of the following activities:

- Construct, operate, and decommission commercial reactors and fuel cycle facilities.
- Possess, use, process, export and import nuclear materials and waste, and handle certain aspects of their transportation.
- Site, design, construct, operate, and close waste disposal sites."

Licensing, U.S. NUCLEAR REGUL. COMM'N, https://www.nrc.gov/about-nrc/regulatory/licensing (last visited May 26, 2026).

[244] 10 C.F.R. § 73.54(a).

[245] U.S. NUCLEAR REGUL. COMM'N, *Cyber Security Programs for Nuclear Facilities* (Jan. 2010), *available at* https://www.nrc.gov/docs/ml0903/ml090340159.pdf.

[246] U.S. NUCLEAR REGUL. COMM'N, *Cyber Security Programs for Nuclear Power Reactors* (Feb. 2023), *available at* https://katzbanks.com/wp-content/uploads/nrc-cybersecurity-guide-feb-2023.pdf.

[247] U.S. NUCLEAR REGULATORY COMM'N, *Backgrounder on Cyber Security*, https://www.nrc.gov/reading-rm/doc-collections/fact-sheets/cyber-security-bg (last visited May 26, 2026).

[248] 42 U.S.C. § 5851(a)(1).

[249] Overall v. Tenn. Valley Auth., ARB No. 04-073, ALJ Case No. 99-ERA-25, 2007 WL 2141757, at *6 (Dep't of Labor July 16, 2007).

[250] *See* Remusat v. Bartlett Nuclear, Inc., ALJ Case No. 94-ERA-36, 1996 WL 171434, at *3 (Dep't of Labor Feb. 26, 1996) ("[T]he blacklisting of current or former employees is prohibited under the ERA . . . an employer's reference to participation in protected activity in the course of providing an employment reference violates the ERA[.]").

[251] 29 C.F.R. § 24.103(d)(2).

[252] 29 C.F.R. § 24.105(a).

[253] 29 C.F.R. §§ 24.106(a), 107(b).

[254] 29 C.F.R. § 24.110(a).

[255] 29 C.F.R. § 1980.112(a).

[256] 42 U.S.C. § 5851(b)(4).

[257] 5 U.S.C. § 2302.

[258] Pub. L. No. 112-199, 126 Stat. 1465 (2012).

[259] 5 U.S.C. § 2302(b)(8).

[260] *Id.*

© Copyright 2026

[261] Exec. Order No. 13636, Improving Critical Infrastructure Cybersecurity, 78 Fed. Reg. 11739, 11743–44 (Feb. 12, 2013), *available at* https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity.

[262] NAT'L INST. OF STANDARDS AND TECH., *Framework for Improving Critical Infrastructure Cybersecurity* (Apr. 16, 2018), *available at* https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf.

[263] Exec. Order No. 13800, Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure, 82 Fed. Reg. 22391 (May 11, 2017), *available at* https://trumpwhitehouse.archives.gov/presidential-actions/presidential-executive-order-strengthening-cybersecurity-federal-networks-critical-infrastructure/.

[264] 5 U.S.C. § 2302(b)(8).

[265] MERIT SYS. PROT. BD., *Whistleblower Protections for Federal Employees*, at 34–35 (Sept. 2010), *available at* https://www.mspb.gov/studies/studies/Whistleblower_Protections_for_Federal_Employees_557972.pdf (hereinafter "MSPB Report").

[266] *See* Savage v. Dep't of the Army, 2015 M.S.P.B. 51, ¶ 23 (Sept. 3, 2015).

[267] 5 U.S.C. § 7701.

[268] 5 U.S.C. § 7513(d). The covered adverse actions for this provision are removal, suspension for more than 14 days, a reduction in grade, a reduction in pay; and a furlough of 30 days or less. 5 U.S.C. § 7512.

[269] 5 U.S.C. § 4303(e). The covered adverse actions for this provision are reduction in grade and removal. *Id.*

[270] 5 U.S.C. § 7701(c).

[271] 5 U.S.C. § 7703(a).

[272] 5 U.S.C. § 7703(b).

[273] 5 U.S.C. § 1214(a)(1)(A).

[274] 5 U.S.C. § 1214(b)(2)(B).

[275] 5 U.S.C. § 1214(b)(2)(C).

[276] 5 U.S.C. § 1214(g).

[277] 5 U.S.C. § 1214(c)(1).

[278] 5 U.S.C. § 1221(a).

[279]5 C.F.R. § 1209.2(b)(1); *see* MSPB Report, *supra* n.265, at 45.

[280] 5 U.S.C. § 1214(a)(3).

[281] MSPB Report, *supra* n.265, at 47.

[282] *Id.*

[283] *Id.*

[284] 5 U.S.C. § 7121.

[285] 5 U.S.C. § 7121(d); *see* CONG. RSCH. SERV., *The Whistleblower Protection Act: An Overview*, at 13–14 (Mar. 12, 2007), *available at* https://www.everycrsreport.com/files/20070312_RL33918_d264fd9594f248085a9c6d9f922eb084f5437e56.pdf.

[286] *Id.*

[287] *Id.*

© Copyright 2026

[288] Pub. L. No. 115-195, 132 Stat. 1510 (2018).

[289] 5 U.S.C. § 7703(b).

[290] 10 U.S.C. § 2409 (renumbered § 4701).

[291] Pub. L. No. 112–239, 126 Stat. 1632 (2013).

[292] An Act to Enhance Whistleblower Protection for Contractor and Grantee Employees, Pub. L. No. 114-261, 130 Stat. 1362 (2016).

[293] 41 U.S.C. § 4712.

[294] 41 U.S.C. § 4712(a)(1).

[295] 41 U.S.C. § 4712(a)(2).

[296] FAR 52.204-21.

[297] DFARS 252.204-7012.

[298] *Id.*

[299] Defense Federal Acquisition Regulation Supplement: Use of Supplier Performance Risk System (SPRS) Assessments (DFARS Case 2019-D009), 88 Fed. Reg. 17336 (Mar. 22, 2023) (codified at 48 C.F.R. pts. 204, 208, 209, 212, 213, 215, 216, and 252).

[300] Federal Acquisition Regulation: Revolutionary Federal Acquisition Regulation Overhaul Parts 1, 2, 4, 33, 39, 40, and 53, 91 Fed. Reg. 37550 (June 23, 2026) (to be codified at 48 C.F.R. pts. 1, 2, 4, 33, 39, 40, 52, and 53).

[301] 5 U.S.C. § 552a(m).

[302] 5 U.S.C. § 552a.

[303] 48 C.F.R. § 24.301.

[304] 41 U.S.C. § 4712(a)(1).

[305] *See* U.S. ex rel. Cody v. Mantech Int'l Corp., 207 F. Supp. 3d 610, 622 (E.D. Va. 2016) (under analogous DCWPA provision); Kavanagh v. M.S.P.B., 176 F. App'x 133, 135 (Fed. Cir. 2006) (under analogous WPA provision); *see also* U.S. ex rel. Toledo v. HCA Holdings, Inc., No. 21-20620, 2023 WL 2823899, at *2–3 (5th Cir. Apr. 7, 2023) (affirming dismissal of NDAA retaliation claim because employee complaints could have been interpreted as "mistakes or possible computer glitches" and employee "admit[ted] that she never used words like *fraud* or *illegal* when raising concerns" (emphasis in original)); Fuerst v. Hous. Auth. of City of Atlanta, 38 F.4th 860, 875 (11th Cir. 2022) (finding that plaintiff "fell short of establishing a reasonable belief that her disclosure evidenced gross mismanagement, or, really, anything more than a dispute with her boss about negotiation tactics").

[306] 41 U.S.C. § 4712(a)(1).

[307] Armstrong v. The Arcanum Grp., Inc., 897 F.3d 1283, 1287 (10th Cir. 2018).

[308] Wooten v. La Salle Corr., 748 F. Supp. 3d 1363, 1378 (M.D. Ga. 2024).

[309] Burlington N. & Santa Fe Ry. Co. v. White, 548 U.S. 53, 68 (2006) (internal citations and quotation marks omitted).

[310] *See* Halliburton, Inc. v. Admin. Rev. Bd., 771 F.3d 254, 259–62 (5th Cir. 2014) (in SOX case, applying the *Burlington Northern* standard and holding that plaintiff suffered an adverse action when defendant revealed to plaintiff's colleagues that he was a whistleblower).

[311] *See* Kissinger-Campbell v. Harrell, No. 8:08-CV-568-T-27TBM, 2009 WL 103274, at *4, *6 (M.D. Fla. Jan. 14, 2009) (in FLSA case, applying the *Burlington Northern* standard and holding that plaintiff suffered an adverse action when defendant contacted plaintiff's prospective employers to prevent her from obtaining new employment).

© Copyright 2026

[312] *See* Difiore v. CSL Behring, U.S., LLC, 171 F. Supp. 3d 383, 394 (E.D. Pa. 2016) (in an FCA case, applying the *Burlington Northern* standard, court noted "none of these actions, on its own, rises to the level of an adverse employment action. . . . However, viewing these actions in the aggregate, I find that Plaintiff has presented sufficient evidence . . . that may allow a jury to conclude that the cumulative effect of these actions might have dissuaded a reasonable worker from engaging in protected conduct"); *see also* Babb v. Dep't of Veterans Affs., 992 F.3d 1193, 1196 (11th Cir. 2021) (holding that retaliatory hostile work environment claims under Title VII should be evaluated using the *Burlington Northern* standard).

[313] 41 U.S.C. § 4712(b)(1).

[314] 41 U.S.C. § 4712(b)(4).

[315] 41 U.S.C. § 4712(b)(1)–(2).

[316] 41 U.S.C. § 4712(c)(2).

[317] *Id.*

[318] NAT'L CONF. ON STATE LEGISLATURES, *The At-Will Presumption and Exceptions to the Rule*, https://www.ncsl.org/labor-and-employment/at-will-employment-overview (last visited May 26, 2026).

[319] Engquist v. Oregon Dep't of Agr., 553 U.S. 591, 606 (2008) (internal quotation marks omitted).

[320] *See, e.g.*, Maryland (Wholey v. Sears Roebuck Co., 803 A.2d 482, 496 (Md. 2002)); New York (N.Y. Civ. Serv. Law § 75-b).

[321] *See, e.g.*, California (Cal. Lab. Code § 1102.5(b)); Massachusetts (Shea v. Emmanuel Coll., 682 N.E.2d 1348, 1350 (Mass. 1997)); New Hampshire (N.H. Rev. Stat. § 275-E:2); Oklahoma (Darrow v. Integris Health, Inc., 176 P.3d 1204, 1215 (Okla. 2008)); Rhode Island (R.I. Gen. Laws § 28-50-3).

[322] *See, e.g.*, Indiana (Meyers v. Meyers, 861 N.E.2d 704, 707 (Ind. 2007)); Maryland (Parks v. Alpharma, Inc., 25 A.3d 200, 210 (Md. 2011)); New Jersey (N.J. Stat. Ann. § 34:19-3); Tennessee (Tenn. Code Ann. § 50-1-304); Texas (Sabine Pilot Serv., Inc. v. Hauck, 687 S.W.2d 733, 735 (Tex. 1985)); Virginia (Rowan v. Tractor Supply Co., 559 S.E.2d 709, 711 (Va. 2002)).

[323] *See* States Likely to Permit Federal Law to Form Basis for Public Policy Exception, attached hereto as Appendix A.

[324] *See, e.g.*, Perez v. Hosp. Ventures-Denver LLC, 298 F. Supp. 2d 1110, 1111 (D. Colo. 2004); Lopez v. Burris Logistics Co., 952 F. Supp. 2d 396, 405 (D. Conn. 2013), *on reconsideration* (Sept. 23, 2013); O'Neill v. Major Brands, Inc., No. 4:06CV0141 TCM, 2006 WL 1134476, at *2 (E.D. Mo. Apr. 26, 2006); Palmerini v. Fid. Brokerage Servs. LLC, No. 12-CV-505-JD, 2013 WL 3786145, at *1 (D.N.H. July 18, 2013); Gall v. Quaker City Castings, Inc., 874 F. Supp. 161, 164 (N.D. Ohio 1995). Similarly, some states do not allow a wrongful discharge claim to proceed where there already exists a *state* law providing an adequate remedy. *See, e.g.*, Hull v. Ivey Imaging LLC, No. CIVIL 08-744-HU, 2008 WL 5071100, at *2 (D. Or. Nov. 21, 2008).

[325] Zungoli v. United Parcel Srvc., Inc., Civ. No. 07-2194, 2009 WL 1085440, at *5 (D.N.J. Apr. 22, 2009).

[326] Cutler v. Dike, No. B210624, 2010 WL 3341663, at *10 (Cal. Ct. App. Aug. 26, 2010).

[327] Singleton v. Intellisist, Inc., No. C17-1712RSL, 2018 WL 2113973, at *3 (W.D. Wash. May 8, 2018), *reconsideration denied*, 2018 WL 3032662 (W.D. Wash. June 19, 2018).

[328] Travers v. EyeKor, Inc., 988 N.W.2d 295, 2023 WL 2169778, at *1 (Ct. App. Wis. Feb. 23, 2023) (table decision).

[329] *Id.*

[330] *Id.* at *3 (citing Bushko v. Miller Brewing Co., 396 N.W.2d 167, 170 (Wis. 1986)).

[331] *Id.*

[332] Kamal v. Ford Motor *Co.*, No. 24-12073, 2025 WL 1691193, at *1 (E.D. Mich. June 16, 2025), *appeal dismissed*, No. 25-1579, 2025 WL 2709800 (6th Cir. Aug. 27, 2025).

[333] *Id.* at *2.
[334] *Id.* at *2–3.

© Copyright 2026

[335] *Compare* N.Y. Lab. Law § 740 *with* Tenn. Code Ann. § 50-1-304.

[336] *See, e.g.*, Smith v. Del. State Univ., 47 A.3d 472, 477–478 (Del. 2012) (finding that an employee who is constructively discharged can pursue a claim under Delaware's Whistleblower Act as if she had been formally discharged, but here, employee failed to offer sufficient evidence of constructive discharge).

[337] 42 U.S.C. § 1320d *et seq.*

[338] 45 C.F.R. § 160.101 *et seq.*; *see also* U.S. DEP'T OF HEALTH AND HUMAN SERVS., *The Security Rule*, http://www.hhs.gov/hipaa/for-professionals/security/index.html (last visited May 26, 2026); U.S. DEP'T OF HEALTH AND HUMAN SERVS., *Summary of the HIPAA Security Rule*, http://www.hhs.gov/hipaa/for-professionals/security/laws-regulations/index.html (last visited May 26, 2026).

[339] *Id.*

[340] HIPAA Security Rule To Strengthen the Cybersecurity of Electronic Protected Health Information, 90 Fed. Reg. 30983 (Jan. 6, 2025) (to be codified at 45 C.F.R. pts. 160 and 164).

[341] 47 U.S.C. § 201(b).

[342] 47 U.S.C. § 222(a).

[343] 47 U.S.C. § 222(c)(1).

[344] FED. COMMC'NS COMM'N, *FCC Announces $34.6 Million Consumer Privacy Investigation Settlement* (Aug. 19, 2024), https://www.fcc.gov/consumer-governmental-affairs/fcc-announces-346-million-consumer-privacy-investigation-settlement.

[345] FED. COMMC'NS COMM'N, *FCC Proposes Over $200M in Fines for Wireless Location Data Violations* (Feb. 28, 2020), https://www.fcc.gov/document/fcc-proposes-over-200m-fines-wireless-location-data-violations.

[346] Brian Fung, *AT&T will pay $25 million after call-center workers sold customer data*, WASH. POST (Apr. 8, 2015), https://www.washingtonpost.com/news/the-switch/wp/2015/04/08/att-will-pay-25-million-after-call-center-workers-sold-customer-data/.

[347] FED. COMMC'NS COMM'N, *FCC Plans $10 Million Fine for Carriers that Breached Consumer Privacy* (Oct. 24, 2014), https://apps.fcc.gov/edocs_public/attachmatch/DOC-330136A1.pdf.

[348] FED. COMMC'NS COMM'N, *Cox Communications to Pay $595,000 to Settle Data Breach Investigation* (Nov. 5, 2015), https://apps.fcc.gov/edocs_public/attachmatch/DOC-336222A1.pdf.

[349] 15 U.S.C. § 6801 *et seq.*

[350] The SEC's "Safeguards Rule," Regulation S-P, as discussed above, applies the requirements to protect customer information to SEC-regulated entities.

[351] 16 C.F.R. § 314.2(o); *see* FED. TRADE COMM'N, *FTC Safeguards Rule: What Your Business Needs to Know*, https://www.ftc.gov/business-guidance/resources/ftc-safeguards-rule-what-your-business-needs-know (last visited May 26, 2026) (hereinafter "FTC Privacy Primer").

[352] 16 C.F.R. § 314.1(b); *see also* FTC Privacy Primer, *supra* n.350.

[353] 16 C.F.R. § 314.4.

[354] Standards for Safeguarding Customer Information, 86 Fed. Reg. 70272 (Dec. 9, 2021) (codified at 16 C.F.R. pt. 314).

[355] 16 C.F.R. § 314.4(c).

[356] 16 C.F.R. § 314.4(i).

[357] 16 C.F.R. § 314.2(h).

[358] Standards for Safeguarding Customer Information, 88 Fed. Reg. 77499 (Nov. 13, 2023) (codified at 16 C.F.R. pt. 314).

© Copyright 2026

[359] 15 U.S.C. §§ 41, 45(a)(1).

[360] 15 U.S.C. § 45(n).

[361] *See, e.g.*, FED. TRADE COMM'N, *FTC Finalizes Order with Flo Health, a Fertility-Tracking App that Shared Sensitive Health Data with Facebook, Google, and Others* (June 22, 2021), https://www.ftc.gov/news-events/press-releases/2021/06/ftc-finalizes-order-flo-health-fertility-tracking-app-shared; FED. TRADE COMM'N, *FTC Finalizes Settlement with Photo App Developer Related to Misuse of Facial Recognition Technology* (May 7, 2021), https://www.ftc.gov/news-events/press-releases/2021/05/ftc-finalizes-settlement-photo-app-developer-related-misuse; *see also* In the Matter of LabMD, Inc., Opinion of the Commission, Docket No. 9357 (July 29, 2016). An appellate court later struck down the FTC's order against LabMD, not due to any perceived deficiency in the FTC's findings of LabMD's liability, but due to a lack of specificity in its ordered remedy. LabMD, Inc. v. Fed. Trade Comm'n, 894 F.3d 1221, 1237 (11th Cir. 2018).

[362] F.T.C. v. Wyndham Worldwide Corp., 799 F.3d 236, 240 (3d Cir. 2015).

[363] *See, e.g.*, FED. TRADE COMM'N, *FTC Takes Action Against General Motors for Sharing Drivers' Precise Location and Driving Behavior Data Without Consent* (Jan. 16, 2025), https://www.ftc.gov/news-events/news/press-releases/2025/01/ftc-takes-action-against-general-motors-sharing-drivers-precise-location-driving-behavior-data; FED. TRADE COMM'N, *FTC Finalizes Order Banning Mobilewalla from Selling Sensitive Location Data* (Jan. 14, 2025), https://www.ftc.gov/news-events/news/press-releases/2025/01/ftc-finalizes-order-banning-mobilewalla-selling-sensitive-location-data; FED. TRADE COMM'N, *FTC Gives Final Approval to Settlement with Emergency Travel Services Provider Related to Allegations It Failed to Secure Sensitive Data* (Feb. 5, 2021), https://www.ftc.gov/news-events/press-releases/2021/02/ftc-gives-final-approval-settlement-emergency-travel-services; FED. TRADE COMM'N, *PayPal Settles FTC Charges that Venmo Failed to Disclose Information to Consumers About the Ability to Transfer Funds and Privacy Settings; Violated Gramm-Leach-Bliley Act* (Feb. 27, 2018), https://www.ftc.gov/news-events/press-releases/2018/02/paypal-settles-ftc-charges-venmo-failed-disclose-information; FED. TRADE COMM'N, *Electronic Toy Maker VTech Settles FTC Allegations That it Violated Children's Privacy Law and the FTC Act* (Jan. 8, 2018), https://www.ftc.gov/news-events/press-releases/2018/01/electronic-toy-maker-vtech-settles-ftc-allegations-it-violated; FED. TRADE COMM'N, *FTC Approves Final Order in Oracle Java Security Case* (Mar. 29, 2016), https://www.ftc.gov/news-events/press-releases/2016/03/ftc-approves-final-order-oracle-java-security-case.

[364] *See* FED. TRADE COMM'N, *FTC Imposes $5 Billion Penalty and Sweeping New Privacy Restrictions on Facebook* (July 24, 2019), https://www.ftc.gov/news-events/news/press-releases/2019/07/ftc-imposes-5-billion-penalty-sweeping-new-privacy-restrictions-facebook.

[365] Ark. Code § 4-110-103.

[366] *See* NAT'L CONF. ON STATE LEGISLATURES, *Security Breach Notification Laws*, http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx (last visited May 26, 2026).

[367] *Id.*

[368] S.B. 53 (Cal. 2025).

[369] GOVERNOR OF CAL., *Governor Newsom signs SB 53, advancing California's world-leading artificial intelligence industry* (Sept. 29, 2025), https://www.gov.ca.gov/2025/09/29/governor-newsom-signs-sb-53-advancing-californias-world-leading-artificial-intelligence-industry/.

[370] Cal. Bus. & Prof. Code § 22757.12.

[371] Cal. Lab. Code § 1107.

[372] The TFAIA and other state legislation passed to regulate AI may, however, be challenged following Executive Order 14365, which establishes a process through which such state measures may be preempted. *See* Exec. Order No. 14365, Ensuring a National Policy Framework for Artificial Intelligence, 90 Fed. Reg. 58499 (Dec. 11, 2025), *available at* https://www.whitehouse.gov/presidential-actions/2025/12/eliminating-state-law-obstruction-of-national-artificial-intelligence-policy/.

[373] Cal. Civ. Code § 1798.100 *et seq.*

[374] Cal. Civ. Code §§ 1798.100, 1798.110.

© Copyright 2026

[375] Cal. Civ. Code § 1798.105.

[376] Cal. Civ. Code § 1798.120.

[377] Cal. Civ. Code § 1798.125.

[378] *See, e.g.*, Colo. Rev. Stat. § 6-1-1301 (giving consumers the right to opt out of the sale of their personal data and placing new obligations on covered entities to safeguard personal data); Me. Rev. Stat. Ann. tit. 35-A, § 9301 (prohibiting broadband internet access services from using, disclosing, selling, or permitting access to customers' personal information without their express, affirmative consent); Nev. Rev. Stat. § 603A (prohibiting website or online service operators from selling consumers' information if so directed by the consumer); Va. Code § 59.1-575 *et seq*. (providing consumers the right to delete and opt out of the sale of their personal data).

[379] *See, e.g.*, Ark. Code § 23-29-510 (requiring mortgage brokers, bankers, or servicers to establish, implement and enforce "written physical security and cybersecurity policies and procedures reasonably designed to ensure the confidentiality, integrity, and availability of physical and electronic records and information"); Iowa Code § 507F.1 *et seq.* (providing for state standards for data security, and the investigation and notification of cybersecurity events, for any insurance licensee in the state of Iowa).

[380] U.S. SEC. AND EXCH. COMM'N, *Securities and Exchange Commission Office of the Whistleblower Annual Report to Congress for Fiscal Year 2024* (Nov. 15, 2024), https://www.sec.gov/files/fy24-annual-whistleblower-report.pdf (hereinafter "SEC FY 2024 Report").

[381] U.S. SEC. AND EXCH. COMM'N, *SEC Issues Largest-Ever Whistleblower Award* (May 5, 2023), https://www.sec.gov/news/press-release/2023-89.

[382] SEC FY 2024 Report, *supra* n.379 at 1.

[383] U.S. SEC. AND EXCH. COMM'N, *Securities and Exchange Commission Office of the Whistleblower Annual Report to Congress for Fiscal Year 2025* (Feb. 11, 2026), https://www.sec.gov/files/fy25-annual-whistleblower-report.pdf.

[384] U.S. SEC. AND EXCH. COMM'N, Whistleblower Frequently Asked Questions, *available at* https://www.sec.gov/enforcement-litigation/whistleblower-program/whistleblower-frequently-asked-questions (last visited May 26, 2026).

[385] *Id*.

[386] *Id*.

[387] U.S. SEC. AND EXCH. COMM'N, *SEC Announces Enforcement Results for FY22* (Nov. 15, 2022), https://www.sec.gov/news/press-release/2022-206.

[388] 7 U.S.C. § 26.

[389] *See* U.S. COMMODITY FUTURES TRADING COMM'N, *The Whistleblower Program*, *available at* https://www.whistleblower.gov/ (last visited May 26, 2026).

[390] U.S. COMMODITY FUTURES TRADING COMM'N, *CFTC Awards Nearly $200 Million to a Whistleblower* (Oct. 21, 2021), https://www.cftc.gov/PressRoom/PressReleases/8453-21.

[391] *See* U.S. COMMODITY FUTURES TRADING COMM'N, *Whistleblower Program Overview*, *available at* https://www.whistleblower.gov/overview (last visited May 26, 2026).

[392] *Id*.

[393] *Id*.

[394] The CFTC defines a "derivatives clearing organization" as "an entity that enables each party to an agreement, contract, or transaction to substitute, through novation or otherwise, the credit of the DCO for the credit of the parties; arranges or provides, on a multilateral basis, for the settlement or netting of obligations; or otherwise provides clearing services or arrangements that mutualize or transfer credit risk among participants." U.S. COMMODITY FUTURES TRADING COMM'N, *Clearing Organizations*, http://www.cftc.gov/industryoversight/clearingorganizations/index.htm (last visited May 26, 2026).

© Copyright 2026

[395] As the CFTC explains, "[s]wap data repositories ('SDRs') are new entities created by the [Dodd-Frank Act] in order to provide a central facility for swap data reporting and recordkeeping." U.S. COMMODITY FUTURES TRADING COMM'N, *Data Repositories*, http://www.cftc.gov/industryoversight/datarepositories/index.htm (last visited May 26, 2026).

[396] 17 C.F.R. §§ 39.18, 39.34; *see* U.S. COMMODITY FUTURES TRADING COMM'N, *CFTC Unanimously Approves Proposed Enhanced Rules on Cybersecurity for Derivatives Clearing Organizations, Trading Platforms, and Swap Data Repositories* (Dec. 16, 2015), http://www.cftc.gov/PressRoom/PressReleases/pr7293-15. The CFTC defines "designated contract markets" as "boards of trade (or exchanges) that operate under the regulatory oversight of the CFTC," and explains that they are "most like traditional futures exchanges, which may allow access to their facilities by all types of traders, including retail customers." U.S. COMMODITY FUTURES TRADING COMM'N, *Designated Contract Markets*, https://www.cftc.gov/IndustryOversight/TradingOrganizations/DCMs/index.htm (last visited May 26, 2026).

[397] *See, e.g.*, U.S. COMMODITY FUTURES TRADING COMM'N, *CFTC Orders Registrant to Pay $1.5 Million for Violations Related to Cyber Breach* (Sept. 12, 2019), https://www.cftc.gov/PressRoom/PressReleases/8008-19 (CFTC imposed sanctions against Phillip Capital Inc. for allowing cyber criminals to breach its email systems, access customer information, and withdraw $1 million in customer funds).

[398] U.S. DEP'T OF JUSTICE, *False Claims Act Settlements and Judgments Exceed $2.9B in Fiscal Year 2024* (Jan. 15, 2025), https://www.justice.gov/archives/opa/pr/false-claims-act-settlements-and-judgments-exceed-29b-fiscal-year-2024.

[399] 31 U.S.C. § 3729(a)(1).

[400] U.S. ex rel. Bilotta v. Novartis Pharm. Corp., 50 F. Supp. 3d 497, 508–09 (S.D.N.Y. 2014) (citing 31 U.S.C. § 3729(b)(2)).

[401] *Id.* (citing 31 U.S.C. § 3729(b)).

[402] U.S. ex rel. Schutte v. SuperValu Inc., 598 U.S. 739, 749 (2023).

[403] *Id.* at 755.

[404] U.S. ex rel. Aflatooni v. Kitsap Physicians Serv., 314 F.3d 995, 1002 (9th Cir. 2002).

[405] *See, e.g.*, Raytheon Settlement, *supra* n.12; Illumina Settlement, *supra* n.13; Georgia Tech Settlement, *supra* n.14.

[406] *See* U.S. ex rel. Bergman v. Abbot Labs., 995 F. Supp. 2d 357, 366 (E.D. Pa. 2014).

[407] *See, e.g.*, Am. Compl. at 45, U.S. ex rel. Doe v. Raytheon Co. et al., No. 21-cv-2343 (D.D.C. Oct. 25, 2024) ("Raytheon's claims for payment were rendered false and/or fraudulent because . . . of express false certifications[.]"); Compl.-in-Intervention at 81–83, U.S. ex rel. Craig v. Georgia Tech Rsch. Corp. et al., No. 1:22-cv-02698 (N.D. Ga. Aug. 22, 2024) (alleging that defendants submitted invoices to DOD for payment without disclosing defendants' failure to comply with cybersecurity rules and regulations, implicating the implied theory).

[408] *Id.*

[409] *Id.*

[410] Universal Health Servs. v. U.S. ex rel. Escobar, 579 U.S. 176, 188–90 (2016). The Court summarized its holding as follows: "[W]e hold that the implied certification theory can be a basis for liability, at least where two conditions are satisfied: first, the claim does not merely request payment, but also makes specific representations about the goods or services provided; and second, the defendant's failure to disclose noncompliance with material statutory, regulatory, or contractual requirements makes those representations misleading half-truths." *Id.* at 190.

[411] *See, e.g.*, United States v. Stephens Inst., 909 F.3d 1012, 1018 (9th Cir. 2018).

[412] *Universal Health Servs.*, 579 U.S at 192.

[413] *Id.* at 194–95.

© Copyright 2026

[414] *See, e.g.*, U.S. ex. rel. Streck v. Eli Lilly & Co., 152 F.4th 816, 847 (7th Cir. 2025) (upholding FCA award and finding it was not dispositive that government learned how defendant was calculating the average manufacturer price it received for drugs covered by Medicaid but continued to contract with defendant anyway); United States v. Molina Healthcare of Illinois, Inc., 17 F.4th 732, 743–44 (8th Cir. 2021) (allegations that defendant continued to submit enrollment forms that indicated enrollees had access to services to which they did not were material and sufficiently stated a claim for implied false certification); United States v. Brookdale Senior Living Cmtys., Inc., 892 F.3d 822, 835–36 (6th Cir. 2018) (finding that delay in physician certification of necessity was material); U.S. ex rel. Campie v. Gilead Scis., Inc., 862 F.3d 890, 906–07 (9th Cir. 2017) (finding it material that defendant had manufactured its drugs at unregistered facilities, resulting in drug impurities, and rejecting defendant's argument that the issues were not material because the government continued to pay for the medications after it learned of FDA violations); U.S. ex rel. Miller v. Weston Educ., Inc., 840 F.3d 494, 504–05 (8th Cir. 2016) (finding that failure to comply with recordkeeping requirement was material when payment was conditioned on the requirement in three different ways and because "[a] reasonable person would attach importance to a promise to do what is necessary to ensure funds go where they are supposed to go").

[415] Katie Benner & Katie Conger, *Cisco to Pay $8.6 Million to Settle Government Claims of Flawed Tech*, N.Y. Times (July 31, 2019), https://www.nytimes.com/2019/07/31/technology/cisco-tech-flaw-sales.html.

[416] Michael Mezher, *Abbott Recalls 465,000 Pacemakers for Cybersecurity Patch*, REGUL. AFFS. PROF'L SOC'Y (Aug. 30, 2017), https://www.raps.org/resource/abbott-recalls-465000-pacemakers-for-cybersecurit.html.

[417] 31 U.S.C. § 3730(b); *see Provisions for the Handling of Qui Tam Suits Filed Under the False Claims Act*, U.S. ATT'Y CRIM. RES. MANUAL 932, https://www.justice.gov/archives/jm/criminal-resource-manual-932-provisions-handling-qui-tam-suits-filed-under-false-claims-act (last visited May 26, 2026).

[418] 31 U.S.C. § 3730(b)(2).

[419] 31 U.S.C. § 3730(b)(3).

[420] 31 U.S.C. § 3730(d)(2).

[421] 31 U.S.C. § 3730(d)(1).

[422] David Freeman Engstrom, *Public Regulation of Private Enforcement: Empirical Analysis of DOJ Oversight of Qui Tam Litigation Under the False Claims Act*, 107 NW. U. L. REV. 1689, 1720 (2013).

[423] U.S. ex rel. Sansbury v. LB & B Assocs., Inc., 58 F. Supp. 3d 37, 46 (D.D.C. 2014).

[424] U.S. ex rel. Craig v. Georgia Tech Research Corporation et al., No. 1:22-cv-02698 (N.D. Ga.).

[425] *See* Georgia Tech Settlement, *supra* n.14.

[426] 31 U.S.C. § 5323(b)(1).

[427] *Id.*

[428] 31 U.S.C. § 5323(h).

[429] *See* U.S. DEP'T OF TREASURY, *Treasury Accepting Whistleblower Tips on Fraud, Money Laundering, Sanctions Violations* (Feb. 13, 2026), https://home.treasury.gov/news/press-releases/sb0394.

[430] *See* FIN. CRIMES ENF'T NETWORK, *FinCEN Proposes Rule to Pay Whistleblowers* (Mar. 30, 2026), https://www.fincen.gov/news/news-releases/fincen-proposes-rule-pay-whistleblowers.

[431] *See* FIN. CRIMES ENF'T NETWORK, *Contact, available at* https://ois.fincen.gov/contact/ (last visited May 26, 2026).

[432] Whistleblower Incentives and Protections, 91 Fed. Reg. 16328 (April 1, 2026).

[433] *Id.*

[434] U.S. DEP'T OF JUSTICE, *Data Security* (last updated Sept. 24, 2025), https://www.justice.gov/nsd/data-security.

© Copyright 2026

[435] *See, e.g.*, FIN. CRIMES ENF'T NETWORK, *FinCEN Announces $140 Million Civil Money Penalty against USAA Federal Savings Bank for Violations of the Bank Secrecy Act* (Mar. 17, 2022), https://www.fincen.gov/news/news-releases/fincen-announces-140-million-civil-money-penalty-against-usaa-federal-savings.

[436] *See* FIN. CRIMES ENF'T NETWORK, *FinCEN Assesses Record $1.3 Billion Penalty against TD Bank* (Oct. 10, 2024), https://www.fincen.gov/news/news-releases/fincen-assesses-record-13-billion-penalty-against-td-bank.

[437] *See* FIN. CRIMES ENF'T NETWORK, *FinCEN Assesses Historic $80 Million Penalty Against Canaccord Genuity LLC for Securities Fraud-Related Bank Secrecy Act Violations* (Mar. 6, 2026), https://www.fincen.gov/news/news-releases/fincen-assesses-historic-80-million-penalty-against-canaccord-genuity-llc.

[438] *See* FIN. CRIMES ENF'T NETWORK, *FinCEN Announces $100 Million Enforcement Action Against Unregistered Futures Commission Merchant BitMEX for Willful Violations of the Bank Secrecy Act* (Aug. 10, 2021), https://www.fincen.gov/news/news-releases/fincen-announces-100-million-enforcement-action-against-unregistered-futures; FIN. CRIMES ENF'T NETWORK, *FinCEN Announces $29 Million Enforcement Action Against Virtual Asset Service Provider Bittrex for Willful Violations of the Bank Secrecy Act* (Oct. 11, 2022), https://www.fincen.gov/news/news-releases/fincen-announces-29-million-enforcement-action-against-virtual-asset-service.

[439] *Id.* at 5–6.

[440] *Id.* at 1, 12.

[441] *Id.* at 6–7.

© Copyright 2026

APPENDIX A

States That May Permit Federal Law to Form Basis for Public Policy Exception.

Arkansas:	Northport Health Servs., Inc. v. Owens, 158 S.W.3d 164, 174 (Ark. 2004) (citing Sterling Drug, Inc. v. Oxford, 743 S.W.2d 380, 386 (Ark. 1988));
California:	Cal. Lab. Code § 1102.5(b); Tameny v. Atlantic Richfield Co., 610 P.2d 1330, 1335 (Cal. 1980);
Connecticut:	Conn. Gen. Stat. § 31-51m; Faulkner v. United Techs. Corp., Sikorsky Aircraft Div., 693 A.2d 293, 295 (Conn. 1997) (citing Morris v. Hartford Courant Co., 513 A.2d 66, 67 (Conn. 1986));
Colorado:	Cejka v. Vectrus Sys. Corp., 291 F. Supp. 3d 1231, 1245 (D. Colo. 2018); Rocky Mountain Hosp. & Med. Serv. v. Mariani, 916 P.2d 519, 524–25 (Colo. 1996);
Delaware:	19 Del. Code §§ 1702–1703;
District of Columbia:	D.C. Code § 1-615.52(a)(6); Coleman v. District of Columbia, 828 F. Supp. 2d 87, 96 (D.D.C. 2011);
Florida:	Fla. Stat. §§ 112.3187–112.3195; Fla. Stat. § 448.102;
Hawaii:	Parnar v. Americana Hotels, Inc., 652 P.2d 625, 631 (Haw. 1982);
Illinois:	740 Ill. Comp. Stat. 174/15;
Indiana:	Walt's Drive-A-Way Serv., Inc. v. Powell, 638 N.E.2d 857, 858 (Ind. Ct. App. 1994);
Iowa:	Hagen v. Siouxland Obstetrics & Gynecology, P.C., 23 F. Supp. 3d 991, 1008 (N.D. Iowa 2014), rev'd and remanded, 799 F.3d 922 (8th Cir. 2015);
Kansas:	Palmer v. Brown, 752 P.2d 685, 689 (Kan. 1988);
Kentucky:	Firestone Textile Co. Div., Firestone Tire & Rubber Co. v. Meadows, 666 S.W.2d 730, 732–33 (Ky. 1983);
Maine:	26 Me. Rev. Stat. §§ 831 et seq.;
Maryland:	See Parks v. Alpharma, Inc., 25 A.3d 200, 213–16 (Md. 2011) (analyzing wrongful discharge claim using federal law as basis for public policy, but dismissing claim on other grounds); Yuan v. Johns Hopkins Univ., 135 A.3d 519, 532 (Md. Ct. Spec. App. 2016) (same), cert. granted, 144 A.3d 706 (2016); King v. Marriott Inter., Inc., 866 A.2d 895, 902 (Md. Ct. Spec. App. 2005) (same); McIntyre v. Guild, Inc., 659 A.2d 398, 405 (Md. Ct. Spec. App. 1995) (same).
Massachusetts:	Dineen v. Dorchester House Multi-Serv. Ctr., Inc., No. CIV.A. 13-12200-LTS, 2014 WL 458188, at *4 (D. Mass. Feb. 3, 2014);

© Copyright 2026

Michigan:	Mich. Comp. L. §§ 15.361 et seq.; Garavaglia v. Centra, Inc., 536 N.W.2d 805, 808 (Mich. App. 1995);
Minnesota:	Minn. Stat. §§ 181.931 et seq.;
Missouri:	Fleshner v. Pepose Vision Inst., P.C., 304 S.W.3d 81, 92 (Mo. 2010);
Montana:	Mont. Code §§ 39-2-901 et seq.;
New Hampshire:	N.H. Rev. Stat. §§ 275-E:1 et seq.; Scannell v. Sears Roebuck & Co., No. CIV 06-CV-227-JD, 2006 WL 2570601, at *4 (D.N.H. Sept. 6, 2006);
New Jersey:	N.J. Stat. § 34:19-3; Brown v. City of Long Branch, 380 F. App'x 235, 240 (3d Cir. 2010);
New York:	N.Y. Lab. Law § 740;
North Carolina:	Coman v. Thomas Mfg. Co., 381 S.E.2d 445 (N.C. 1989);
North Dakota:	N.D. Cent. Code § 34-01-20;
Ohio:	Ohio Rev. Code § 4113.52(A)(1); Kulch v. Structural Fibers, Inc., 677 N.E.2d 308, 328–29 (Ohio 1997);
Oregon:	Ore. Rev. Stat. § 659A.199;
Pennsylvania:	Field v. Phila. Elec. Co., 565 A.2d 1170, 1182 (Pa. 1989);
Rhode Island:	R.I. Gen. L. §§ 28-50-1 et seq.;
South Carolina:	Nolte v. Gibbs Int'l, Inc., 515 S.E.2d 101, 103 (S.C. Ct. App. 1999);
Tennessee:	Tenn. Code § 50-1-304; Reynolds v. Ozark Motor Lines, Inc., 887 S.W.2d 822, 824 (Tenn. 1994);
Utah:	Rackley v. Fairview Care Ctrs., Inc., 23 P.3d 1022, 1027 (Utah 2001);
Virginia:	Va. Code § 40.1-27.3;
Washington:	Thompson v. St. Regis Paper Co., 685 P.2d 1081, 1090 (Wash. 1984); and
West Virginia:	Wiley v. Asplundh Tree Expert Co., 4 F. Supp. 3d 840, 844–45 (S.D. W.Va. 2014).

© Copyright 2026