Cybersecurity Whistleblower Protections

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

By Alexis Ronickher & Matthew LaGarde

March 2019

KATZ BANKS KUMIN

WASHINGTON, DC | 202.299.1140 | KATZBANKS.COM

TABLE OF CONTENTS

INTRODUCTION

Since this Guide's initial release two years ago, cybersecurity has continued to dominate the headlines as a key concern for individuals, businesses, and the government. By some counts, nearly a billion individuals were affected by cybercrime in 2017.[1] For companies, cybercrime will have a dramatic impact on business moving forward, with some studies suggesting that companies risk losing roughly $5.2 trillion in the next five years due to cybersecurity attacks.[2] Foreign hacking has also compromised U.S. national security with large-scale attacks on the U.S. energy sector, critical U.S. infrastructure, and our elections.[3]

In response to this growing problem, governmental regulators have joined law enforcement agencies in addressing the issue. In 2018, the U.S. Securities and Exchange Commission (SEC) reached a $35 million settlement with Altaba, the company formerly known as Yahoo!, for allegedly misleading investors by failing to properly investigate and disclose the breach of approximately 3 billion accounts. Also in 2018, the SEC announced insider trading charges against an Equifax executive who sold his vested Equifax stock options after learning that the company had a breach that compromised the personal information of 143 million Americans and prior to the company disclosing that fact. In 2017 and 2018, the U.S. Federal Trade Commission (FTC) also aggressively pursed companies related to cybersecurity failures, bringing enforcement actions and reaching settlements with companies that failed to adequately secure customer data.

Regardless of how aggressive law enforcement and regulators work to prevent or prosecute cybercrime, they cannot do so alone because of the rapid development and evolving nature of cyber technology, such as mobile devices, cloud computing, and the internet of things. Law enforcement and regulatory agencies have very limited resources to handle this ever-widening problem, requiring them to prioritize the most critical needs, leaving many cybercrimes and cyber vulnerabilities unaddressed. The public, therefore, has little choice but to rely on companies and government agencies that store sensitive information to prevent their websites, applications, or devices from serving as a platform for cybercrime and to protect information in their custody from cyberattacks.

Companies and government agencies can only provide this protection if their employees alert them to lax cybersecurity standards and cyber vulnerabilities. Unfortunately, retaliation against employees who blow the whistle on cybersecurity problems is all too common. Often the outcome for an employee who reports a cybersecurity problem is career stagnation or even termination. Since most Americans cannot afford to risk their jobs, their fear of retaliation deters them from reporting cybersecurity problems. If we hope to change this culture of fear and encourage whistleblowing, employees need to know that they have legal protections for blowing the whistle as well as potential rewards for reporting cybercrime and cybersecurity vulnerabilities to the government. While Congress has not yet explicitly provided cybersecurity whistleblowers with such protections, there is a patchwork of state and federal laws that can be used to provide these protections and incentives for many cybersecurity whistleblowers.

> Cybersecurity whistleblowers have both legal protections and reward incentives.

This Guide provides a compilation and discussion of the major legal claims available to cybersecurity whistleblowers. It also provides a description of the federal programs under which cybersecurity whistleblowers' reports may lead to monetary rewards. Finally, it provides potential cybersecurity whistleblowers with specific suggestions to enhance their legal protections when blowing the whistle.

CURRENT PROTECTIONS FOR CYBERSECURITY WHISTLEBLOWERS

While there is no federal statute that explicitly protects employees who blow the whistle on lax cybersecurity (in contrast, for example, to blowing the whistle about transportation or environmental issues), there are a handful of federal statutes and state laws which can provide cybersecurity 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 whistleblower. It then discusses state law claims for wrongful termination in violation of public policy, and provides information about some of the federal and state sources of public policy upon which a cybersecurity whistleblower might base such a claim.

A. Federal Statutes Providing Protections to Cybersecurity Whistleblowers

There are at least seven federal statutes that may provide protections to a cybersecurity whistleblower, depending on the entity for which the whistleblower works and the wrongdoing the whistleblower reports.[4] Those statutes are:

- The Sarbanes-Oxley Act, which provides protections to employees who report fraud and securities violations at publicly traded companies;[5]
- The Dodd-Frank Act, which provides protections to employees who report securities violations to the SEC;[6]
- The Financial Institutions Reform Recovery and Enforcement Act, which provides protections to employees who report legal violations at banks and other depository institutions;[7]
- The False Claims Act, which provides protections to employees who oppose fraud against the government;[8]
- The Energy Reorganization Act, which provides protections to employees in the nuclear industry who oppose violations of that law, the Atomic Energy Act or Nuclear Regulatory Commission regulations;[9]
- The Whistleblower Protection Act, 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;[10] 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.[11]

At least 7 federal statutes may provide protections to cybersecurity whistleblowers.

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 whistleblowing is not the explicit focus of any of these laws. Additionally, each statute has procedural requirements for asserting a claim, which must be followed or a whistleblower will lose those protections. Below is a detailed discussion of each statute, detailing the circumstances in which cybersecurity whistleblowing could constitute protected activity, the actions taken against an employee that constitute an adverse action, and the procedural requirements of the 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),[12] 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. Eight years later, in the wake of the financial crisis that led to the Great Recession, Congress passed the Dodd-Frank Act of 2010 (Dodd-Frank)[13] to address deficiencies in existing financial regulations. In Dodd-Frank, lawmakers included 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. 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, making 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,[14] may take an adverse action against an employee because the employee provided information regarding mail fraud, wire fraud, bank fraud, securities fraud, shareholder fraud, or any violation of an SEC rule or regulation.[15] SOX protections also extend to employees of private contractors and subcontractors serving public companies,[16] although the wrongdoing identified by the employee generally must either relate to or have been engaged in by the public company.[17] A whistleblower is entitled to SOX protections provided she makes such a report to a federal agency, a member of Congress, a supervisor, or a person working for the employer who has the authority to investigate, discover, or terminate misconduct.[18] When a whistleblower has met both these requirements, she has engaged in "protected activity" under SOX. According to the Administrative Review Board of the Department of Labor (ARB), the body responsible for adjudicating the SOX anti-retaliation provisions, these protections can extend in some cases to protected actions that occur outside of the United States.[19]

Dodd-Frank, on the other hand, prohibits any employer from taking an adverse action against a whistleblower because she provided information about securities violations to the SEC, assisted the SEC in an investigation of securities violations, or made disclosures protected under SOX,the Securities Exchange Act of 1934, and any other law, rule, or regulation subject to the jurisdiction of the SEC.[20] Dodd-Frank does not contain the restrictive definition of "employer" used by SOX; thus, if an employee of a non-public company, such as an investment

4 Categories of Protected Activity

1. Fraud
2. Securities violations
3. Internal controls
4. SEC Regulations S-P and S-ID

management firm, reports securities violations to the SEC, she may be entitled to Dodd-Frank protections.[21] In 2018, the Supreme Court held in *Digital Realty Tr., Inc. v. Somers* that the Dodd-Frank's anti-retaliation provision protects whistleblowers who report to the SEC.[22] In other words, whistleblowers who only report their concerns internally cannot pursue a retaliation claim under Dodd-Frank. 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, in that Dodd-Frank provides more generous monetary remedies, a longer statute of limitations, and the ability to file directly in federal court.[23]

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

i) Fraud

To the extent a cybersecurity 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 are violations of federal fraud statutes, specifically mail, wire, bank, and securities fraud.[24] The ARB and the majority of federal courts have held that reports of violations of these federal fraud statutes constitutes protected activity.[25] All disclosures protected by SOX are also protected by Dodd-Frank, provided that the whistleblower has made a report to the SEC.[26]

An employee need only "reasonably believe" that the information she provides is a violation of one of the enumerated categories.[27] This requires an employee to believe that "(1) she 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."[28] Moreover, an employee need not use the word "fraud" to identify fraudulent activity for the purposes of garnering SOX protections.[29]

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

ii) 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,[30] SEC Rule 10b-5,[31] and Section 17(a) of the Securities Act of 1933,[32] prohibit fraudulent practices in connection with the purchase or sale of a security, including the knowing misrepresentation or omission of material facts. In the securities context, a "material fact" is a term of art that means a fact that a reasonable investor would have viewed as significantly altering the "total mix" of information available to the investor.[33] 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 related to cybersecurity. Altaba – the company formerly known as Yahoo! Inc. –agreed to pay the SEC $35 million to resolve claims that it misled investors by failing to disclose the cybersecurity breach that enabled hackers to steal the personal data of hundreds of millions of Yahoo users.[34] According to the SEC, for more than two years after members of Yahoo's senior management and legal department learned of the breach, the company failed to properly investigate and disclose the breach to investors. 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.

The SEC has long warned companies that they had 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.[35] 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 necessary to prevent other disclosures from misleading potential investors. The SEC provided several examples of appropriate cybersecurity disclosures depending on the specific circumstances.[36]

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.[37] The SEC explained that the additional guidance was necessary in light 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."

In the 2018 Cybersecurity Guidance, the SEC reiterated much of what it explained in the initial 2011 Cybersecurity Guidance. The Commission, however, 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 risk.[38] Whistleblowers and their attorneys who are evaluating whether a disclosure would qualify as protected activity should review both the 2011 and 2018 guidance carefully.

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 the vulnerability has already resulted in the theft of critical intellectual property, yet the Company refused to correct the problem and has not disclosed either its vulnerability or the breach to the public. Since the whistleblower's report directly references material public misrepresentations, even though she did not reference securities fraud or violations of SEC rules and regulations, it would constitute protected activity under the liberal ARB standard that requires a reasonable belief 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 could result in the company's failure to meet the SEC's disclosure requirements related to cybersecurity. This more explicit report would preclude an employer's argument that the whistleblower's report was not about one of SOX's enumerated categories. Additionally, the more explicit report would ensure that the whistleblower met the standard applied by the minority of federal courts that require a complaint to relate to fraud against shareholders.[39] Finally, by citing violations of SEC disclosure requirements, this more specific report provides a basis for protection that does not implicate the specialized materiality requirement for securities fraud, which can make it more challenging to assert a reasonable belief of fraud under that statute.

Whistleblowers engaging in this form of protected activity, however, should pay close attention to their company's disclosures. In a recent 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.[40] The investors had alleged, in part, that LifeLock made false statements regarding its compliance with applicable payment card industry data security standards (PCI DSS).[41] The Ninth Circuit, however, found that the company had never affirmatively represented in its statements to shareholders that the application that was the subject of the plaintiffs' allegations *was* compliant with PCI DSS standards.[42] 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,[43] a necessary element of a securities fraud claim.[44] 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.[45]

iii) 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.[46] The 2018 Cybersecurity Guidance states that cybersecurity risk management policies and procedures are "key elements of enterprise wide risk management."[47] The Commission encouraged companies to "adopt comprehensive policies and procedures related to cybersecurity and to assess their compliance regularly," and to ensure that 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.[48] 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."[49]

With this guidance from the SEC, there is a strong argument that an employee has made a protected disclosure under SOX (and under Dodd-Frank, if they also report the issues to the SEC) by reporting that relevant information about a cybersecurity risk or incident is not getting to the appropriate personnel to allow the necessary disclosure decisions and certification.[50]

Even prior to 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*,[51] 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.[52] 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."[53]

iv) SEC Regulations Protecting Consumer Data

Registered investment companies and registered investment advisers are subject to SEC regulations related to customer data protection, most notably Regulation S-P and Regulation S-ID.[54] 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).[55] 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.[56] 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.[57] The SEC actively enforces violations of these regulations. For example, in June 2016, the SEC levied a penalty of $1 million against Morgan Stanley Smith Barney LLC for cybersecurity violations that violated the Safeguards Rule.[58] More recently, 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.[59] The charge represented the SEC's first enforcement action alleging violations of the Identity Theft Red Flags Rule.

To be eligible for SOX protection, an employee who reports an employer's failure to have an adequate identity theft program, the employer needs to be 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, provided they are subject to Regulations S-P and S-ID, such as registered investment companies or registered investment advisors.[60]

b) Adverse Action

Section 806 of SOX states that no company "may discharge, demote, 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.[61] 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."[62]

> Under both Dodd-Frank & SOX, no company may discharge, demote, threaten, harass, or in any other manner discriminate against an employee for engaging in protected activity.

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,"[63] adding that "adverse action under SOX Section 806 must be more expansively construed than [adverse action] under Title VII of the Civil Rights Act of 1964."[64] In keeping with this position, the Department of Labor 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.[65] Federal courts in recent years have also held that a variety of non-tangible employment actions constitute adverse actions for purposes of a SOX retaliation claim, including outing, blackballing, and poor performance reviews.[66] Although federal courts have recognized that non-tangible employment actions qualify as adverse actions, some have been unwilling

to adopted ARB's more liberal standard for adverse action and instead still analyze adverse actions under SOX using the Title VII standard requiring that the action be "harmful enough that it well might have dissuaded a reasonable worker from engaging in statutorily protected whistleblowing."[67] In practice, however, it is difficult to identify instances where courts have determined that an action qualifies as an adverse actions under the SOX standard but not the Title VII standard.

Under SOX, a whistleblower has 180 days to file a complaint with OSHA.

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, however, there is reason to believe that the same standard would be applied to actions brought under the latter statute. Indeed, at least one federal court has applied SOX's adverse action analysis in its interpretation of a Dodd-Frank claim.[68] That being said, the ARB has no jurisdiction over Dodd-Frank claims, so its liberal adverse-action standard would not be due any deference.

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 for retaliation with the Department of Labor's Occupational Safety and Health Administration (OSHA) within 180 days after the date of the adverse action.[69] 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.[70] Following OSHA's written findings, either party has 30 days to request a hearing with an administrative law judge (ALJ), during which time the parties will have the opportunity to conduct limited discovery.[71] Either party may also appeal the ALJ's ruling to the ARB within 14 days of the ALJ's ruling.[72] 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.[73] 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.[74] In practice, few cases have final decisions within 180 days.

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 in an appropriate federal district court.[75] The employee's complaint of retaliation must be filed within three years of the date when facts material to the right of action are known or reasonably should have been known by the employee.[76]

2. Protections for Employees of Banks and Other Depository Institutions

In the wake of the 1980s Savings and Loans Crisis, Congress passed the Financial Institutions Reform Recovery and Enforcement Act of 1989 (FIRREA),[77] which provides broad protections against retaliation for employees of both banking institutions and banking agencies. A banking whistleblower who reports insufficient data security could qualify for this protection.

a) Protected activity

FIRREA protects employees of "insured depository institutions"—i.e., depository banks—and employees of federal banking regulators who engage in protected activity.[78] 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. In the cybersecurity 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,[79] which requires financial institutions to protect certain consumer data, or of Section 5 of the Federal Trade Commission Act of 1914,[80] which prohibits unfair or deceptive practices in commerce, including insufficient data security.[81]

Critically, FIRREA only protects a whistleblower if she reports externally to a federal banking agency or the U.S. Attorney General (i.e., the U.S. Department of Justice).[82] Internal complaints of violations of law by employees at insured depository institutions do not constitute protected activity under FIRREA.[83] 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.[84]

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.[85] 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.[86]

No courts have articulated the standard for what constitutes an adverse action under FIRREA; however, it is likely that a court would apply the Title VII standard given the similarities between the two statutes' language. 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."[87] This standard includes not just tangible personnel actions, such as terminations, demotions, and pay or benefits cuts. It also includes harmful actions such as outing a whistleblower,[88] blackballing,[89] or even a series of smaller actions that, taken together, would dissuade a reasonable worker from participating in the protected activity.[90]

c) Procedure

Under FIRREA, a whistleblower has the right to file a civil action in the appropriate United States district court.[91] The whistleblower must do so within two years of the date of the retaliatory action.[92] The statute requires that a whistleblower simultaneously file a copy of her complaint with the appropriate federal banking agency.[93]

3. False Claims Act Protections

The federal False Claims Act (FCA)[94] 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."[95] 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.[96] In 1986, the FCA was amended to protect employees who reported such fraud from retaliation,[97] and subsequent amendments made in 2009[98] and 2010[99] strengthened the retaliation protection. This protection may be available for an employee who reports her employer's failure to comply with federal regulations relating to cybersecurity.

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.[100] Originally, whistleblowers were only entitled to protection when they experienced retaliation "because of lawful acts done by the employee on behalf of the employer or others in furtherance of an action under this section[.]"[101] For years, many courts interpreted this to mean that the FCA protections against 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."[102] 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],"[103] While the legislative history of FERA clearly indicates that Congress intended the Act's protections against retaliation to be broadly construed,[104] courts continue to disagree about the scope of what activities constitute protected activity. In the wake of the FERA amendments many courts have recognized the broadened scope of protected activity under the statute.[105] Unfortunately, several courts, apparently relying on pre-amendment precedent, have continued to apply the "distinct possibility" and "viable action" standards that restrict the protections of the statute.[106]

> The intersection between cybersecurity and government fraud is narrow, but growing.

The intersection between cybersecurity and fraud against the federal government is relatively narrow, but growing. There are two categories of false claims under the FCA: a factually false claim and a legally false claim.[107] A factually false claim occurs when a claimant misrepresents what goods or services it has provided to the government.[108] A legally false claim is based on "a false certification" theory of liability, of which there are two.[109] Express false certification occurs when a claimant falsely certifies that it is in compliance with regulations that are requirements for payment.[110] 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.[111] 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.[112] Critically, the noncompliance must be with a material requirement.[113] With the federal government's expanding cybersecurity requirements, it is increasingly likely that a cybersecurity whistleblower's disclosure might implicate this category of fraud.

Companies contracting with the government have become subject to a number of heightened cybersecurity requirements in recent years. A recent change to the Federal Acquisition Regulations (FARs) increased cybersecurity standards for companies pursuing contracts with the government.[114] The summary of the regulation provides that the rule "is just one step in a series of coordinated regulatory actions being taken or planned to strengthen protections of information systems."[115] Among other things, the rule requires that certain companies seeking government contracts comply with 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."[116] The Department of Defense (DOD) recently implemented a similar rule requiring that DOD contractors adhere to the new NIST SP 800-171 standards.[117] The DOD regulations also significantly increase the scope of information that contractors are responsible for securing; rather than only being responsible for securing information received from the government, contractors will also be responsible for securing information that is "collected, developed, received, used, or stored by or on behalf of the contractor in support of the performance of the contract."[118]

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. 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.[119]

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 the U.S. Census Bureau. 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, in order to adhere to applicable FARs. Rather than notifying the Census Bureau 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 Census Bureau, 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.

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 won a bid to develop encryption software for the Department of Defense. If an employee raised concerns about serious cybersecurity flaws that would render the software so insecure as to render the government unable to use it, she would be escalating concerns about the contractor failing to fulfill the terms of the contract and therefore engaging in protected activity under the FCA.

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.[120] Retaliation claims under the FCA are scrutinized under the same test as retaliation claims under Title VII: whether the "adverse action is one that might have dissuaded a reasonable worker from engaging in the protected conduct."[121] Tangible employment actions, such as termination, demotion, and pay and benefit cuts, qualify as adverse actions under this standard. So too, however, may other adverse actions, such as written warnings, diminished responsibilities, or auditing an employee's job performance.[122]

c) Procedure

An FCA retaliation plaintiff must bring her claim in federal district court within three years of the date of the retaliation. 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 and submitting a disclosure statement, unless a plaintiff is including a retaliation claim with her qui tam claim.[123] Additionally, if an employee files suit with both a qui tam and retaliation claim, if her qui tam claim is dismissed, her Section 3730(h) retaliation claim may survive without it.[124]

4. Protections for Nuclear Whistleblowers

The Energy Reorganization Act of 1978 (ERA)[125] protects employees who provide information about or participate in investigations relating to violations of nuclear safety laws and standards. 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 notified her employer of violations of the ERA, the Atomic Energy Act, or Nuclear Regulatory Commission (NRC) regulations, she refused to engage in such violations, or she otherwise participated in an NRC proceeding.[126] 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."[127] Under this regulation, NRC licensees[128] "shall provide high assurance that digital computer and communication systems and networks are adequately protected against cyber-attacks[.]"[129] The regulation and its accompanying regulatory guide1[30] provide detailed

cybersecurity responsibilities to which NRC licensees must adhere.[131] Any employee of an NRC licensee has engaged in protected activity under the ERA's anti-retaliation provisions if she opposes practices by her employer that she reasonably believed violated these cybersecurity regulations.

b) Adverse Action

The ERA prohibits an employer from discharging any employee 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.[132] 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."[133] 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.[134]

c) Procedure

Employees must file complaints under the ERA with the Department of Labor (DOL) within 180 days of the date the employer made the retaliatory decision and communicated it to the employee.[135] The DOL's Occupational Safety and Health Administration (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.[136] Following OSHA's written findings, either party has 30 days to request a *de novo*, on-the-record hearing with an administrative law judge (ALJ).[137] Either party may then appeal the ALJ's ruling to the DOL's ARB within 10 days of the ruling.[138] 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 allegedly occurred or the complainant resided on the date of the violation.[139] 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.[140]

5. Protections for Federal Government Employees

Given the recent high-profile cyberattacks by foreign powers against the United States, cybersecurity is and will continue to be a serious issue for federal employees. The Whistleblower Protection Act (WPA)[141] and the Whistleblower Protection Enhancement Act (WPEA)[142] work together to provide meaningful protections to cybersecurity whistleblowers within the federal government.

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 about a violation of any law, rule, or regulation; about gross mismanagement, a gross waste of funds, or an abuse of authority; or about a substantial and specific danger to public health or safety.[143] Such a disclosure is not protected, however, if it is prohibited by law or executive order. 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 need only indicate in her report that the 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 13,636, 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 the National Institute of Standards and Technology (NIST).[144] In 2014, NIST published that Cybersecurity Framework.[145] In May 2017, a subsequent Executive Order extended the NIST standards to all federal government agencies.[146] 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.[147] A report issued by the U.S. Merit Systems Protection Board (MSPB), the body responsible for adjudicating WPA claims, 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.[148]

The WPEA, which was passed after the MSPB report, added "security clearance harassment" as a prohibited personnel action under the WPA, meaning that agencies may no longer retaliate against federal employees by stripping them of their security clearance.[149] In 2015, the MSPB held that the creation of a hostile work environment may also constitute a prohibited personnel action under the WPA.[150]

c) Procedure

A federal whistleblower has four potential avenues to pursue her claims under the WPA. First, the employee may appeal the adverse action directly to the MSPB, which is known as a "Chapter 77" appeal.[151] Chapter 77 appeals are available to federal employees who suffer an adverse employment action because of alleged deficiencies in an employee's conduct[152] or performance.[153] A whistleblower who brings a Chapter 77 appeal is alleging that an employer took an adverse action against her because of her protected activity, not because of any purported deficient conduct or performance.[154]

Second, the employee may file a charge with the U.S. Office of Special Counsel (OSC). If the OSC finds the complaint meritorious, it can seek corrective action from the offending federal agency. If the agency fails to take appropriate corrective action, OSC can institute an action with the MSPB on the employee's behalf.[155]

Third, the employee may bring an individual right of action (IRA) to the MSPB if the OSC declines to bring one on her behalf. 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 OSC; and (4) she exhausted corrective action proceedings before OSC.[156] 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.[157] An employee files an IRA with one of the MSPB's field or regional offices which then assigns it to an administrative judge (AJ).[158] The whistleblower may then appeal the AJ's decision to either a three-member Board of the MSPB or to the appropriate U.S. Court of Appeals.[159] If the whistleblower elects to appeal to the MSPB, she may then appeal its decision to the appropriate U.S. Court of Appeals.[160]

Finally, if the employee is a union member, she can pursue a grievance under her union's negotiated grievance procedures.[161] As a result of the 1994 WPA amendments, an aggrieved employee affected by a prohibited personnel action is precluded from choosing more than one of the available avenues of redress.[162] 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.[163] However, if the employee chooses the grievance procedures, she is still entitled to request a review of the final decision by the MSPB, where appropriate.[164] Under the All Circuit Review Act,[165] signed into law in July 2018, whistleblowers will have the power to appeal MSPB decisions to *any* U.S. Court of Appeals, which will provide federal employees the ability to seek out appellate courts who have shown a willingness to fairly consider whistleblowers' retaliation claims.[166]

6. Protections for Federal Government 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 passed in 1986, created anti-retaliation protections for contractors of the Department of Defense (DOD) and the National Aeronautics and Space Administration (NASA).[167] The National Defense Authorization Act for Fiscal Year 2013 (NDAA) included a four-year pilot program expanding DCWPA protections to all government contractors.[168] Congress passed and President Obama signed a bill making the extended protections permanent on December 14, 2016.[169]

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. 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.[170]

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 Department of Justice 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.[171]

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, a Federal Acquisition Regulation (FAR) rule requires that certain companies seeking government contracts comply with 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."[172] The DOD implemented a similar rule requiring its contractors to adhere to the NIST SP 800-171 standards.[173] DOD also significantly increased the scope of information that contractors are responsible for securing; rather than only being responsible for securing information received from the government, contractors will also be responsible for securing information that is "collected, developed, received, used, or stored by or on behalf of the contractor in support of the performance of the contract."[174]

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. Cybersecurity 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.[175] 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 does not constitute protected activity under the Act.[176]

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.[177] An employee must show only that her protected activity was a "contributing factor" in the employer's decision to take an adverse employment action.[178]

No courts have articulated the standard for what constitutes an adverse action under NDAA; however, it is likely that a court would apply the Title VII standard given the similarities between the two statutes' language. 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."[179] This standard includes not just tangible personnel actions, such as terminations, demotions, and pay or benefits cuts. It also includes harmful actions such as outing a whistleblower,[180] blackballing,[181] or even a series of smaller actions that, taken together, would dissuade a reasonable worker from participating in the protected activity.[182]

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.[183] The claim must be filed within three years of the date of the alleged adverse action.[184] 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.[185] If the agency denies relief or fails to file an order granting relief within 210 days after the filing of the complaint, the complainant may file a lawsuit based on the complaint in federal district court, without regard to the amount in controversy.[186] Either the complainant or the respondent may request a jury trial.[187]

B. State Laws Prohibiting Wrongful Termination in Violation of Public Policy

Cybersecurity whistleblowers may also find protection under their state's wrongful discharge law. In all states except Montana, employment is presumed to be "at-will."[188] 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.[189] A common exception is a law that prohibits 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. Wrongful discharge laws differ as to what conduct qualifies as protected activity. Some require a whistleblower to report misconduct to law enforcement or other governmental body,[190] while others protect internal whistleblowing,[191] and many protect whistleblowers who refuse to engage in criminal activity.[192]

States also differ as to whether a federal law can provide the basis for a state wrongful discharge claim. Over 30 states either have explicitly stated that federal 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.[193] 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.[194] 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 state courts have issued decisions in favor of cybersecurity whistleblowers' ability to pursue claims under state wrongful discharge laws. 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 Healthcare Information Portability and Accountability Act (HIPAA).[195] In a 2009 case in New Jersey, a court denied an employer's motion for summary judgment in a statutory wrongful termination claim based on an employee's refusal to engage in conduct that could have jeopardized confidential information in violation of a state statute known as the New Jersey Identity Theft Protection Act.[196] Similarly, in a May 2018 decision issued by a federal court in Washington,[197] the court denied the defendant's motion to dismiss plaintiff's claim for wrongful discharge in violation of public policy based on plaintiff's complaints about compliance with applicable payment card industry data security standards (PCI DSS).[198]

Although state wrongful discharge laws protect whistleblowers who have been fired, they do not protect whistleblowers from other adverse actions, such as demotion or harassment. 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 difficult to meet. 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 whistleblower may be able to rely. Then it reviews a few of the many laws passed by states in recent years 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 Public Policy

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 the Health Insurance Portability and Accountability Act, the Gramm-Leach-Bliley Act, the Communications Act of 1934, and the Federal Trade Commission Act of 1914. Cybersecurity whistleblowers who complain about their companies' violations of the requirements included in these statutes or the related regulations issued by their enforcing agencies may have engaged in protected activity if their state law protects whistleblowers who report violations of federal laws and regulations.

a) Health Insurance Portability and Accountability Act

For cybersecurity whistleblowers in the healthcare field, the Health Insurance Portability and Accountability Act (HIPAA)[199] may serve as a basis for protected activity. 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).[200] The Security Rule requires covered entities—health plans, health care clearinghouses, and any health care provider who transmits health information in electronic form[201]—to maintain a number of safeguards for protecting e-PHI.[202] If an employee who works for a covered entity subject to these regulatory requirements reports violations and her employer fires her, she may have a claim for wrongful discharge.

b) Communications Act of 1934

Cybersecurity whistleblowers who report conduct that violates the Communications Act of 1934[203] may have a basis for protected activity. The Federal Communications Commission (FCC) has interpreted three sections of the Communications Act to require telecommunications companies to meet adequate data security standards.

First, 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."[204]

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[.]"[205]

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[.]"[206]

The FCC has relied on this authority to take action against companies that fail to adequately protect customer information. 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 social security numbers.[207] Six months before that, the FCC ordered two telecommunications carriers, TerraCom and YourTel, to pay a collective $10 million fine for allegedly storing customers' personal information in a method that was accessible through a routine online search.[208] Importantly, the FCC demonstrated that it does not require a massive breach to violate the Communications Act. On November 6, 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.[209]

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

c) Gramm-Leach-Bliley Act

The Gramm-Leach-Bliley Act (GLBA) created the Safeguards Rule, 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.[210] The Safeguards Rule applies to companies that provide financial products or services to consumers, including check-cashing businesses, data processors, mortgage brokers, nonbank lenders, personal property or real estate appraisers, and retailers that issue credit cards to consumers.[211] 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.[212]

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 significant steps to protect customer information. A financial institution employee who opposes lax protections of customer information and is subsequently terminated may have a strong wrongful termination claim if 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 Federal Trade Commission Act of 1914 (FTCA) makes unfair or deceptive acts or practices in commerce unlawful and empowers the Federal Trade Commission (FTC) to prosecute violations.[213] 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."[214]

The FTC has exercised this authority against companies that fail to adhere to adequate standards for securing consumer data.[215] Courts have upheld the FTC's interpretation that unreasonable data security practices could violate Section 5 of the FTCA. Specifically, in 2015, the U.S. Court of Appeals for 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.[216] Since then the FTC has successfully resolved a series of actions based on companies' failure to secure customer data.[217]

Based on the FTC's actions, an employee who reports data breaches or deceptive communications about lax cyber security has a strong argument that her report was protected activity if the state recognizes federal law as a basis for public policy.

2. State Law Bases for Public Policy

Cybersecurity whistleblowers may not need to depend on federal law as a basis for public policy in their wrongful termination claims. States are beginning to pass cybersecurity laws and, given the public concern about cybersecurity, more states are likely to enact such laws in the future. Most common are security-breach notification laws, which exist in some form in almost every state. Many states also have laws that address data-security issues, although currently those primarily focus on governmental actors' handling 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 terms similar to those 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;
> (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; and
> (D) Medical information[.][218]

As of March 2018, 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. The National Conference of State Legislatures has created a comprehensive directory of these laws with links to the statutes themselves.[219] 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 claim of wrongful termination in violation of public policy provided they are in a state that allows such claims.

b) Other State Cybersecurity Measures

Several states have passed additional measures relating to data security in recent years. For example, in June 2015, Connecticut passed S.B. 949, which imposes requirements on companies that contract with the state government to establish procedures for securing and protecting all confidential information.[220] Likewise, Virginia passed S.B. 1121 in 2015, a slightly more substantial law providing that "the director of every department in the executive branch of state government shall be responsible for securing the electronic data held by his department and shall comply with the requirements of the Commonwealth's information technology security and risk-management program[.]"[221] And, in March 2016, Wyoming passed S.F. 38, "requiring agencies to adopt policies for data collection, access, security and use as specified; directing the state chief information officer to develop guidelines for local governments for data collection, access, security and use; providing a definition; requiring a report; and providing for an effective date."[222] Other states have passed measures that, at least to date, do not create cybersecurity requirements and thus are unlikely to serve as a strong basis of "public policy" for a wrongful termination claim.[223]

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 U.S. Securities and Exchange Commission (SEC), the U.S. Commodity Futures Trading Commission (CFTC), and the U.S. Department of Justice (DOJ), 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.

Whistleblowers can receive substantial rewards through government reward programs.

A. SEC Whistleblower Program

The Dodd-Frank Act created a whistleblower program administered by the SEC which entitles an individual who provides the SEC with original information leading to an enforcement action that results 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 as of March 2019, had paid more than $326 million to 59 whistleblowers.[224]

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. 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. 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. 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 in Section II.A.1 may form the basis of a successful tip to the SEC. For detailed information about the rules and procedures of the SEC Whistleblower Program, read David Marshall's SEC Whistleblower Practice Guide.

B. CFTC Whistleblower Program

The Dodd-Frank Act also directed the U.S. Commodity Futures Trading Commission (CFTC) to create a whistleblower program. 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 issued just ten awards since it began accepting tips in September 2012.[225] One of those awards, however, was for approximately $30,000,000,[226] and the Program has the funds and the potential to continue to administer sizable awards to whistleblowers who provide valuable information.

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. 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. 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. 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,[227] swap data repositories,[228] and specified designated contract markets.[229] Cybersecurity whistleblowers who provide the CFTC with original information about the failure of one of these entities to adhere to these cybersecurity standards, 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' CFTC Whistleblower Practice Guide.

C. Qui Tam Lawsuits under the False Claims Act

The False Claims Act (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 $42.5 billion.[230]

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 $5,000 and $10,000 per claim, plus three times the amount of damages caused by the person's acts.[231] 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.[232] 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.[233] In most circumstances, a plaintiff must prove an actual false claim for payment from the government was made.[234]

As discussed more fully in Section II.A.3, it is likely that a qui tam action involving cybersecurity issues would involve violations of the cybersecurity-related requirements set forth in the Federal Acquisition Regulation (FAR), the Defense Federal Acquisition Regulation Supplement (DFARS), or the recently issued Department of Defense (DOD) rule expanding cybersecurity requirements for DOD contractors.[235] Such an action would be based on "a false certification" theory of liability, of which there are two.[236] Express false certification occurs when a claimant falsely certifies that it is in compliance with regulations that are material requirements for payment.[237] 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.[238] 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.[239] 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.[240]

Critically, the noncompliance must be with a material requirement under either theory.[241] Materiality does not have a rigid definition in the context of government contracts. In *Escobar*, the Supreme Court provided a list of materiality pitfalls that attorneys considering filing qui tams should endeavor to avoid.[242] Despite concerns about the effect of the narrow conception of materiality reflected in *Escobar*, its practical impact has been mixed and lower courts continue to allow FCA claims to move forward based on imperfect evidence of materiality.[243] A prospective whistleblower would be wise to seek legal guidance on whether adherence or failure to adhere to the regulation or requirement at issue likely would be deemed "material."

In addition to liability under a false certification theory, a whistleblower could bring a qui tam based on allegations that software or hardware the government purchased had a cybersecurity defect so significant that it rendered the product defective. For example, a medical device manufacturer in 2017 recalled over 400,000 devices due to cybersecurity vulnerabilities that were discovered in the devices.[244] Had similar deficiencies been discovered in, for example, an aircraft a government contractor manufactured for the Department of Defense, 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.[245] 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 the government "intervening."[246] 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.[247] 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.[248] 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.[249] 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.[250] 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.[251]

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. Report a Violation of Law, Not Just Cybersecurity Vulnerabilities

The law protects whistleblowers who report violations of laws or who refuse to engage in unlawful conduct. For cybersecurity whistleblowers, there may not be an obvious link between the cybersecurity vulnerability they are reporting and a legal violation. It is critical, therefore, for a cybersecurity whistleblower to articulate clearly that the issue she is reporting is not simply a cybersecurity 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 an employee needs to have proof of exactly what she reported. Employers frequently defend themselves against retaliation claims by arguing that the employee never reported legal violations, but rather simply reported a standard IT problem, complained about a business decision, or merely advocated 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 launch a clandestine investigation into company files 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 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. 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.

A whistleblower may also be tempted to retain incriminating company documents 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.

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.

5 Things to Think about Before you Blow the Whistle:

1. Report Legal Violations, Not Just Cybersecurity Vulnerabilities
2. Put it in Writing
3. Don't Steal Documents
4. Find Legal Representation
5. If Fired, Look for New Work

E. If Terminated, Diligently Look For New Work

If an employer fires a whistleblower, the whistleblower must start looking for a new job, while at the same time pursuing a remedy for her wrongful termination. The 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 viably claim that her efforts were insufficient.

Alexis Ronickher is a partner with the whistleblower and employment law firm of Katz Banks Kumin, in Washington, D.C. She specializes in representing clients in whistleblower and sexual harassment cases, as well as other employment matters, including civil rights discrimination and retaliation and Title IX violations. Ms. Ronickher has litigated cases nationwide in federal and state courts, as well as in administrative hearings. She represented a hair stylist in a sexual harassment and retaliation trial that resulted in a jury verdict of $2.3 million in favor of her client. In 2018, she represented whistleblowers in a successful *qui tam* lawsuit against a naval husbandry company for fraudulently billing the government that resulted in a $20 million settlement, and in 2014 she represented a whistleblower in a *qui tam* and retaliation lawsuit that resulted in a $10 million settlement. Ms. Ronickher has also represented numerous other employees and whistleblowers in cases that have successfully resolved confidentially prior to or during litigation.

Matthew B. LaGarde is an associate with Katz Banks Kumin. He assisted with the research and preparation of this paper.

RESOURCES

Government Resources

Securities and Exchange Commission: https://www.sec.gov/

Occupational Safety and Health Administration (OSHA): https://www.osha.gov/

Department of Labor – Administrative Review Board: https://www.dol.gov/arb/welcome.html

Federal Communications Commission: https://www.fcc.gov/

Federal Trade Commission: https://www.ftc.gov/

Cybersecurity Information Sharing Act of 2015: https://www.congress.gov/bill/114th-congress/senate-bill/754

Katz Banks Kumin Resources

Katz Banks Kumin'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

Cybersecurity Whistleblowers: http://www.katzbanks.com/practice-areas/whistleblower-law/cybersecurity-whistleblower

SEC Whistleblower Program: http://www.katzbanks.com/practice-areas/sec-whistleblower-law

Qui Tam Lawsuits under the False Claims Act: http://www.katzbanks.com/practice-areas/whistleblower-law/qui-tam-whistleblower-incentives

The Nuclear Industry Whistleblowers: http://www.katzbanks.com/practice-areas/whistleblower-law/nuclear-environmental

Sarbanes-Oxley Act: http://www.katzbanks.com/resources/sarbanes-oxley

Financial Industry Whistleblower Information: http://www.katzbanks.com/resources/financial-industry-whistleblower

Dodd-Frank Act: http://www.katzbanks.com/practice-areas/whistleblower-law/dodd-frank-act-whistleblower-incentives

Practice Guides

SEC Whistleblower Practice Guide: http://www.katzbanks.com/resources/sec-whistleblower-practice-guide

CFTC Whistleblower Practice Guide: http://www.katzbanks.com/resources/guide-navigating-cftc-whistleblower-program

Katz Banks Kumin'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 http://www.katzbanks.com/practice-areas/whistleblower-law/ and http://www.katzbanks.com/practice-areas/sec-whistleblower-law.

The Katz Banks Kumin website also hosts an informative Whistleblower Law Blog that can help keep whistleblowers and other conscientious employees up to date on new developments in whistleblower law and related news separate with broader whistleblower news and developments. See http://www.katzbanks.com/blogs.

ENDNOTES

[1]SYMANTEC, *2017 Norton Cyber Security Insights Report* (Jan. 2018), available at https://www.symantec.com/about/newsroom/press-kits/ncsir-2017.

[2]ACCENTURE, *Securing the Digital Economy: Reinventing the Internet for Trust* (Jan. 17, 2019), available at https://newsroom.accenture.com/news/cybercrime-could-cost-companies-us-5-2-trillion-over-next-five-years-according-to-new-research-from-accenture.htm.

[3]Daniel R. Coats, *Worldwide Threat Assessment of the U.S. Intelligence Community*, OFFICE OF THE DIR. OF NAT'L INTELLIGENCE (Feb. 13, 2018), available at https://www.dni.gov/files/documents/Newsroom/Testimonies/2018-ATA---Unclassified-SSCI.pdf.

[4]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 whistleblower under less common circumstances (e.g., an employee blowing the whistle regarding cybersecurity in aviation or trucking). In our practice, the seven statutes we discuss have been the most common federal statutes to provide protection to cybersecurity whistleblowers.

[5]18 U.S.C. § 1514A.

[6]15 U.S.C. § 78u-6.

[7]12 U.S.C. § 1831j.

[8]31 U.S.C. § 3730(h).

[9]42 U.S.C. § 5851.

[10]5 U.S.C. § 2302.

[11]41 U.S.C. § 4712.

[12]18 U.S.C. § 1514A.

[13]15 U.S.C. § 78u-6.

[14]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. § 781), or that is required to file reports under section 15(d) of the Securities Exchange Act of 1934 (15 U.S.C. § 78o(c) 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").

[15]18 U.S.C. § 1514A(a)(1).

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

[17]*See, e.g.*, Baskett v. Autonomous Research LLP, No. 17-CV-9237 (VSB), 2018 WL 4757962, at *8 (S.D.N.Y. Sept. 28, 2018).

[18]*Id.*

[19]*See* Blanchard v. Exelis Sys. Corp., ARB No. 15-031, 2017 WL 3953474 (Dep't of Labor Aug. 29, 2017).

[20]15 U.S.C. § 78u-6(h)(1)(A)(iii).

[21]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).

[22]Digital Realty Tr., Inc. v. Somers, 138 S. Ct. 767, 778 (2018).

[23]Dodd-Frank provides a successful litigant with double back pay, a statute of limitations of three years, and the ability to go directly to federal court. 15 U.S.C. § 78u-6(h). In contrast, SOX does not have a multiplier for economic damages, 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.

[24]18 U.S.C. § 1514A(a)(1); Seguin v. Northrup Grumman Systems 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.").

[25]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."); Wiest v. Lynch, 710 F.3d 121, 138 (3d Cir. 2013); Lockheed Martin Corp. v. Admin. Review Bd., 717 F.3d 1121, 1130–32 (10th Cir. 2013); 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); Wallender v. Canadian Nat'l Ry. Co., No. 2:13-CV-2603-DKV, 2015 WL 10818741, at *12 and n.18 (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); Zinn v. Am. Commercial Lines Inc., ARB No. 10-029, ALJ No. 2009-SOX-025, 2012 WL 1143309, at *4 (Dep't of Labor Mar. 28, 2012); 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*). Some courts, however, have not adopted the *Sylvester* holding and still require that protected activity be related to shareholder fraud. *See, e.g.*, Nielsen v. AECOM Tech. Corp., 762 F.3d 214, 223 (2d Cir. Aug. 8, 2014); Nance v. Time Warner Cable, Inc., 433 F. App'x 502, 503 (9th Cir. 2011); Gauthier v. Shaw Group, Inc., No. 3:12-CV-00274-GCM, 2012 WL 6043012, at *4–5 (W.D.N.C. Dec. 4, 2012).

[26]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.) . . . .")

[27]*Sylvester*, 2011 WL 2165854, at *11–13.

[28]Johnson v. The Wellpoint Companies, Inc., ARB No. 16-020, ALJ No. 2010-SOX-38, 2017 WL 3953473, at *3 (Dep't of Labor Aug. 31, 2017).

[29]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.'").

[30]15 U.S.C. § 78j(b).

[31]17 C.F.R. § 240.10b-5.

[32]15 U.S.C. § 77q(a).

[33]TSC Indus., Inc. v. Northway, Inc., 426 U.S. 438, 449 (1976); Erica P. John Fund, Inc. v. Halliburton Co., 563 U.S. 804, 810 (2011).

[34]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.

[35]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 "CF Disclosure Guidance").

[36]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.*

[37]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").

[38]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.*

[39]*See, e.g.*, Nielsen v. AECOM Tech. Corp., 762 F.3d 214, 223 (2d Cir. Aug. 8, 2014); Nance v. Time Warner Cable, Inc., 433 F. App'x 502, 503 (9th Cir. 2011); Gauthier v. Shaw Group, Inc., No. 3:12-CV-00274-GCM, 2012 WL 6043012, at *4–5 (W.D.N.C. Dec. 4, 2012).

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

[41]*Id.* at 952.

[42]*Id.*

[43]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).

[44]*In re Lifelock,* 690 F. App'x at 954–55.

[45]*Id.; but see* Singleton v. Intellisist, Inc., No. C17-1712RSL, 2018 WL 2113973, at *3 (W.D. Wash. May 8, 2018) (denying motion to dismiss claim that plaintiff's complaints about PCI compliance constituted protected activity for the purposes of plaintiff's claim of wrongful discharge in violation of Washington public policy), *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.*

[46]*See* 17 C.F.R. §§ 240.13a-15, 240.15d-15.

[47]*See* 2018 Cybersecurity Guidance, *supra* note 37, at 18.

[48]*Id.*

[49]*Id.* at 17–18.

[50]See Current Protections for Cybersecurity Whistleblowers A.1.a.

[51]262 F. Supp. 3d 1328 (S.D. Fla. 2017).

[52]*Id.*

[53]*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. 35,343 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)).

[54]17 C.F.R. §§ 248.30; 248.201.

[55]17 C.F.R. §§ 248.1; 248.4–6.

[56]17 C.F.R. § 248.10.

[57]17 C.F.R. § 248.201.

[58]Morgan Stanley Smith Barney LLC, Admin. Proceeding No. 3-17280 (Sec. and Exch. Comm'n, June 8, 2016).

[59]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.

[60]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).

[61]18 U.S.C. § 1514A(a).

[62]15 U.S.C. § 78u-6(h)(1)(A).

[63]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).

[64]*Id.* at 17.

[65]*See, e.g., id.* (outing and blackballing is an adverse action); Levi v. Anheuser Busch Cos., Inc., ARB No. 08-086, ALJ No. 2008-SOX-28, 2009 WL 6496732, at *3–4 (Dep't of Labor Sept. 25, 2009) (failure to hire may be an adverse employment action but the complainant in this case did not prove he was not hired because of his protected activity); Gattegno v. Prospect Energy Corp., ARB No. 06-118, ALJ No. 2006-SOX-8, 2008 WL 2265209, at *12 (Dep't of Labor May 29, 2008) (constructive discharge); Grove v. EMC Corp., ALJ No. 2006-SOX-99, 2007 WL 7135739, at *16 (Dep't of Labor July 2, 2007) (hostile work environment may be an adverse employment action but it was not sufficiently alleged here); Reines v. Venture Bank and Venture Fin. Grp., ALJ No. 2005-SOX-112, 2007 WL 7139504, at *52–54 (Dep't of Labor Mar. 13, 2007) (demotion/reduced responsibilities); McClendon v. Hewlett Packard, Inc., ALJ No. 2006-SOX-29, 2006 WL 6577175, at *79–81 (Dep't of Labor Oct. 5, 2006) (transfer); Allen v. Stewart Enters., Inc., ARB No. 06-081, ALJ No. 2004-SOX-60 to 62, 2006 WL 6583250, at *12–13 (Dep't of Labor July 27, 2006) (logging increased error rates and relocation were not adverse employment actions in this case); Hughart v. Raymond James & Assocs., Inc., ALJ No. 2004-SOX-9, 2004 WL 5308719, at *47 (Dep't of Labor Dec. 17, 2004) (failure to promote); 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) (placement on a layoff list); McIntyre v. Merrill, 2003-SOX-23, 2004 WL 5032618, at *9 (Dep't of Labor Jan. 16, 2004) (blacklisting).

[66]*See, e.g.,* Halliburton, Inc. v. Admin. Review Bd., 771 F.3d 254, 259 (5th Cir. 2014) (holding that "outing" a whistleblower to his colleagues could constitute an adverse action under SOX); Guitron v. Wells Fargo Bank, N.A., No. C 10-3461 CW, 2012 WL 2708517, at *16 (N.D. Cal. July 6, 2012), *aff'd,* 619 F. App'x 590 (9th Cir. 2015) (holding that suspension and poor performance review were adverse actions); 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).

[67]*See, e.g.,* Allen v. Admin. Review Bd., 514 F.3d 468, 476 n.2 (5th Cir. 2008); Quast v. MidAmerican Energy Co., No. 4-14-CV-00278, 2016 WL 4536460 (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).

[68]Ott v. Fred Alger Mgmt., Inc., No. 11 CIV. 4418 LAP, 2012 WL 4767200, at *5 (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.").

[69]18 U.S.C. § 1514A(b)(2)(D).

[70]29 C.F.R. § 1980.105(a).

[71]29 C.F.R. § 1980.106–107.

[72]29 C.F.R. § 1980.110(a).

[73]29 C.F.R. § 1980.112(a).

[74]18 U.S.C. § 1514A(b)(1)(B).

[75]15 U.S.C. § 78u-6(h)(1)(B)(i).

[76]15 U.S.C. § 78u-6(h)(1)(B)(iii)(I)(bb).

[77]12 U.S.C. § 1831j.

[78]12 U.S.C. § 1831j(a)(2). The covered federal banking entities are: the Board of Governors of the Federal Reserve System, the Federal Housing Finance Agency, the Comptroller of the Currency, federal home loan banks, Federal Reserve banks, and the Federal Deposit Insurance Corporation. 12 U.S.C. § 1831j(e).

[79]15 U.S.C. §§ 6801 *et seq.*

[80]15 U.S.C. § 45.

[81]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.

[82]18 U.S.C. §1831j(a)(1).

[83]*See* 12 U.S.C. § 1831j(a)(1); *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).

[84]12 U.S.C. § 1831j(d).

[85]12 U.S.C. § 1831j(a)(1).

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

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

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

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

[90]Difiore v. CSL Behring, U.S., LLC, 171 F. Supp. 3d 383, 394 (E.D. Pa. 2016) (in a False Claims Act 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, albeit barely, 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").

[91]12 U.S.C. § 1831j(b).

[92]*Id.*

[93]*Id.*

[94]31 U.S.C. §§ 3729-3733.

[95]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).

[96]*See* 37 U.S.C. § 3729(a), 3730(b).

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

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

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

[100]31 U.S.C. § 3730(h) (2010).

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

[102]U.S. ex rel. Karvelas v. Melrose-Wakefield Hosp., 360 F.3d 220, 236 (1st Cir. 2004) (collecting cases).

[103]Pub. L. No. 111-21, § 4(d), 123 Stat. 1617, 1624–25 (May 20, 2009).

[104]*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.").

[105]*See* U.S. ex rel. Grant v. United Airlines Inc., 912 F.3d 190, 200–02 (4th Cir. 2018); U.S. ex rel. Chorches for Bankr. Estate of Fabula v. Am. Med. Response, Inc., 865 F.3d 71, 95–98 (2d Cir. 2017); Jones-McNamara v. Holzer Health Sys., 630 F. App'x 394, 409 n.6 (6th Cir. 2015); Halasa v. ITT Educ. Servs., Inc., 690 F.3d 844, 847–48 (7th Cir. 2012); *see also* U.S. ex rel. Kietzman v. Bethany Circle of King's Daughters of Madison, Indiana, Inc., 305 F. Supp. 3d 964, 981–82 (S.D. Ind. 2018); Moore v. Univ. of Kansas, 118 F. Supp. 3d 1242, 1257 (D. Kan. 2015) ("The amendment seems to sweep within its scope all conduct, complaints and reports intended to stop a FCA violation."); Malanga v. New York Univ., No. 14CV9681, 2018 WL 333831, at *2–3 (S.D.N.Y. Jan. 9, 2018); Laird v. Spanish Fork Nursing & Rehab. Mgmt., LLC, No. 2:14CV850, 2015 WL 3792622, at *3 (D. Utah June 18, 2015) (plaintiff's refusal to follow orders to backdate clinical assessments (believing added charges would therefore be false and create fraudulent billings to CMS) and stating she would not commit fraud were sufficient to state a claim for retaliatory discharge).

[106]*See, e.g.,* Hicks v. D.C., 306 F. Supp. 3d 131, 157 (D.D.C. 2018); Reynolds v. Winn-Dixie Raleigh, Inc., 85 F. Supp. 3d 1365, 1374 (M.D. Ga.), *aff'd,* 620 F. App'x 785 (11th Cir. 2015); Strubbe v. Crawford Cty. Mem'l Hosp., No. C15-4034-LTS, 2017 WL 8792692, at *6 (N.D. Iowa Dec. 6, 2017); Reid v. Temple Univ. Hosp. Episcopal Campus, No. CV 17-2197, 2017 WL 5157620, at *4 (E.D. Pa. Nov. 7, 2017); U.S. ex rel. King v. Solvay S.A., No. CIV.A. H-06-2662, 2015 WL 4256402, at *3 (S.D. Tex. July 14, 2015) (quoting Mann v. Heckler & Koch Defense, Inc., 630 F.3d 338, 344 (4th Cir. 2010)); Cestra v. Mylan, Inc., No. CIV.A. 14-825, 2015 WL 2455420, at *3 (W.D. Pa. May 22, 2015).

[107]U.S. ex rel. Wilkins v. United Health Grp., Inc., 659 F.3d 295, 305 (3d Cir. 2011) (quoting U.S. ex rel. Conner v. Salina Reg'l Health Ctr., Inc., 543 F.3d 1211, 1217 (10th Cir. 2008)).

[108]*Id.*

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

[110]*Id.*

[111]*Id.*

[112]Universal Health Servs. v. U.S. ex rel. Escobar, 136 S. Ct. 1989, 2000–01 (2016).

[113]*Id.* at 2002.

[114]Federal Acquisition Regulation, Basic Safeguarding of Contractor Information Systems, 81 Fed. Reg. 30439 (May 16, 2016).

[115]*Id.* at 30440.

[116]*Id.*

[117]Defense Federal Acquisition Regulation Supplement: Network Penetration Reporting and Contracting for Cloud Services, 81 Fed. Reg. 51739 (Aug. 26, 2015); 80 Fed. Reg. 81472 (Dec. 30, 2015). This regulation became effective on December 31, 2017.

[118]81 Fed. Reg. at 51743.

[119]31 U.S.C. § 3730(h).

[120]*Id.*

[121]Difiore v. CSL Behring, U.S., LLC, 171 F. Supp. 3d 383, 393 (E.D. Pa. Mar. 17, 2016) (citing Burlington N. & Santa Fe Ry. Co. v. White, 548 U.S. 53, 68 (2006)).

[122]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).

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

[124]U.S. ex rel. Ramseyer v. Century Healthcare Corp., 90 F.3d 1514, 1522 (10th Cir. 1996).

[125]42 U.S.C. § 5851.

[126]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.").

[127]10 C.F.R. § 73.54.

[128]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 REGULATORY COMM'N, http://www.nrc.gov/about-nrc/regulatory/licensing.html (last visited March 15, 2019).

[129]10 C.F.R. § 73.54(a).

[130]U.S. NUCLEAR REGULATORY COMM'N, CYBER SECURITY PROGRAMS FOR NUCLEAR FACILITIES (Jan. 2010), *available at* http://pbadupws.nrc.gov/docs/ML0903/ML090340159.pdf.

[131]*Backgrounder on Cyber Security,* U.S. NUCLEAR REGULATORY COMM'N, http://www.nrc.gov/reading-rm/doc-collections/fact-sheets/cyber-security-bg.html (last visited March 15, 2019).

[132]42 U.S.C. § 5851(a)(1).

[133]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).

[134]Remusat v. Bartlett Nuclear, Inc., ALJ Case No. 94-ERA-36, 1996 WL 171434, at *3 (Dep't of Labor Feb. 26, 1996).

[135]29 C.F.R. § 24.103(d)(2).

[136]29 C.F.R. § 24.105(a).

[137]29 C.F.R. § 24.106–107.

[138]29 C.F.R. § 24.110(a).

[139]29 C.F.R. § 1980.112(a).

[140]42 U.S.C. § 5851(b)(4).

[141]5 U.S.C. § 2302.

[142]Pub. L. No. 112-199, 126 Stat. 1465.

[143]5 U.S.C. § 2302(b)(8).

[144]Exec. Order No. 13,636, Improving Critical Infrastructure Cybersecurity, 78 Fed. Reg. 11739, 11743–44 (Feb. 12, 2013), *available at* https://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity.

[145]NAT'L INST. OF STANDARDS AND TECH., Framework for Improving Critical Infrastructure Cybersecurity (Feb. 12, 2014), *available at* http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf.

[146]Exec. Order No. 13,800, Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure, 82 Fed. Reg. 22,391 (May 11, 2017), *available at* https://www.whitehouse.gov/presidential-actions/presidential-executive-order-strengthening-cybersecurity-federal-networks-critical-infrastructure/.

[147]5 U.S.C. § 2302(b)(8).

[148]MERIT SYS. PROT. BD., Whistleblower Protections for Federal Employees (Sept. 2010), *available at* https://www.mspb.gov/mspbsearch/viewdocs.aspx?docnumber=557972&version=559604&application=ACROBAT (hereinafter "MSPB Report").

[149]Pub. L. No. 112-199, 126 Stat. 1465.

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

[151]5 U.S.C. § 7701.

[152]5 U.S.C. § 7513.

[153]5 U.S.C. § 4303.

[154]5 U.S.C. § 7701(a).

[155]5 U.S.C. § 1214(b)(2).

[156]5 U.S.C. § 1214(a)(3); *see also* MSPB Report, *supra* note 148, at 45.

[157]5 U.S.C. § 1221(a).

[158]MSPB Report, *supra* note 148, at 47.

[159]MSPB Report, *supra* note 148, at 47.

[160]MSPB Report, *supra* note 148, at 47.

[161]5 U.S.C. § 7121.

[162]5 U.S.C. § 7121(d); *see* also CONG. RESEARCH SERV., The Whistleblower Protection Act: An Overview, at 13–14 (Mar. 12, 2007), *available at* https://www.fas.org/sgp/crs/natsec/RL33918.pdf.

[163]*Id.*

[164]*Id.*

[165]Pub. L. No. 115-195, 132 Stat. 1510 (July 7, 2018).

[166]*Id.*

[167]10 U.S.C. § 2409.

[168]41 U.S.C. § 4712.

[169]An Act to Enhance Whistleblower Protection for Contractor and Grantee Employees, Pub. L. No. 114-261, 130 Stat. 1362 (1970).

[170]41 U.S.C. § 4712(a)(1).

[171]41 U.S.C. § 4712(a)(2).

[172]Federal Acquisition Regulation, Basic Safeguarding of Contractor Information Systems, 81 Fed. Reg. 30439, 30440 (May 16, 2016).

[173]Defense Federal Acquisition Regulation Supplement: Network Penetration Reporting and Contracting for Cloud Services, 81 Fed. Reg. 51739 (Aug. 26, 2015); 80 Fed. Reg. 81472 (Dec. 30, 2015). This regulation became effective on December 31, 2017.

[174]81 Fed. Reg. at 51743.

[175]31 U.S.C. § 3730(h).

[176]*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).

[177]41 U.S.C. § 4712(a)(1).

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

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

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

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

[182]Difiore v. CSL Behring, U.S., LLC, 171 F. Supp. 3d 383, 394 (E.D. Pa. 2016) (in a False Claims Act 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, albeit barely, 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").

[183]41 U.S.C. § 4712(b)(1).

[184]41 U.S.C. § 4712(b)(4).

[185]41 U.S.C. § 4712(b)(2)(A).

[186]41 U.S.C. § 4712(c)(2).

[187]*Id.*

[188]See Nat'l Conference ON STATE LEGISLATURES, *The At-Will Presumption and Exceptions to the Rule,* http://www.ncsl.org/research/labor-and-employment/at-will-employment-overview.aspx (last visited March 15, 2019).

[189]Engquist v. Oregon Dep't of Agr., 553 U.S. 591, 606 (2008).

[190]*See, e.g.,* Florida (Fla. Stat. §§ 112.3187–112.3195; Fla. Stat. § 448.102); Maryland (Wholey v. Sears Roebuck Co., 803 A.2d 482, 496 (Md. 2002)); New York (N.Y. Civ. Serv. Law § 75-b); Rhode Island (R.I. Gen. Laws § 28-50-3).

[191]*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:1 *et seq.*); Oklahoma (Darrow v. Integris Health, Inc., 176 P.3d 1204, 1210 (Okla. 2008)).

[192]*See, e.g.,* Indiana (Meyers v. Meyers, 861 N.E.2d 704, 707 (Ind. 2007)); Maryland (Parks v. Alpharma, Inc., 25 A.3d 200, 209–11 (Md. 2011)); New Jersey (N.J. Stat. Ann. § 34:19-3); Tennessee (Tenn. Code Ann. § 50-1-304); Virginia (Rowan v. Tractor Supply Co., 559 S.E.2d 709, 711 (Va. 2002)).

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

[194]*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); Gall v. Quaker City Castings, Inc., 874 F. Supp. 161, 164 (N.D. Ohio 1995); Hull v. Ivey Imaging LLC, No. CIVIL 08-744-HU, 2008 WL 5071100, at *2 (D. Or. Nov. 21, 2008); Palmerini v. Fid. Brokerage Servs. LLC, No. 12-CV-505-JD, 2013 WL 3786145, at *1 (D.N.H. July 18, 2013).

[195]Cutler v. Dike, No. B210624, 2010 WL 3341663 (Cal. Ct. App. Aug. 26, 2010).

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

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

[198]*Id.* at *3.

[199]42 U.S.C. §§ 1320d *et seq.*

[200]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 March 15, 2019); 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 March 15, 2019).

[201]*Id.*

[202]These safeguards include: (1) "Access Control," i.e., technical policies and procedures that allow only authorized persons to access electronic protected health information (e-PHI); (2) "Audit Controls," i.e., hardware, software, and/or procedural mechanisms to record and examine access and other activity in information systems that contain or use e-PHI;' (3) "Integrity Controls," i.e., policies and procedures to ensure that e-PHI is not improperly altered or destroyed, and electronic measures enabling the company to confirm that e-PHI has not been improperly altered or destroyed;' and (4) "Transmission Security," i.e., technical security measures that guard against unauthorized access to e-PHI that is being transmitted over an electronic network. *Id.* (citations omitted).

[203]47 U.S.C. §§ 151 et seq.

[204]47 U.S.C. § 201(b).

[205]47 U.S.C. § 222(a).

[206]47 U.S.C. § 222(c)(1).

[207]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/.

[208]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.

[209]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.

[210]15 U.S.C. §§ 6801 et seq.; 16 C.F.R. § 313(o); see also FED. TRADE COMM'N, *Financial Institutions and Customer Information: Complying with the Safeguards Rule,* https://www.ftc.gov/tips-advice/business-center/guidance/financial-institutions-customer-information-complying (last visited March 15, 2019) (hereinafter "FTC Privacy Primer").

[211]16 C.F.R. § 313(k); see also FTC Privacy Primer, *supra note* 210.

[212]*Id.*

[213]15 U.S.C. §§ 41; 45(a)(1).

[214]15 U.S.C. § 45(n).

[215]*See, e.g.,* FED. TRADE COMM'N, *FTC Charges D-Link Put Consumers' Privacy at Risk Due to the Inadequate Security of Its Computer Routers and Cameras* (Jan. 5, 2017), https://www.ftc.gov/news-events/press-releases/2017/01/ftc-charges-d-link-put-consumers-privacy-risk-due-inadequate; Fed. Trade Comm'n v. D-Link Corp., Case No. 3:17-cv-00039-JD (N.D. Cal.). *See also* FED. TRADE COMM'N, *FTC Files Complaint Against LabMD for Failing to Protect Consumers' Privacy* (Aug. 29, 2013), https://www.ftc.gov/news-events/press-releases/2013/08/ftc-files-complaint-against-labmd-failing-protect-consumers; 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, 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. The FTC eventually issued an order requiring that LabMD notify affected consumers, establish a comprehensive information security program reasonably designed to protect the security and confidentiality of the personal consumer information in its possession, and obtain independent assessments regarding its implementation of the program. LabMD, Inc. v. Fed. Trade Comm'n, 894 F.3d 1221, 1237 (11th Cir. 2018).

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

[217]*See, e.g.,* 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; 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, *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.

[218]Ark. Code § 4-110-103.

[219]See NAT'L CONFERENCE ON STATE LEGISLATURES, *Security Breach Notification Laws,* http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx (last visited March 15, 2019).

[220]S.B. 949, Pub. Act 15-142 (Conn. 2015).

[221]S.B. 1121, Ch. 261, Reg. Sess. (Va. 2015).

[222]S.F. 39, Ch. 35, Reg. Sess. (Wyo. 2016).

[223]*See, e.g.:*

Florida: H.B. 1033, Ch. 2016-138, Laws of Fla. (2016) (imposed a series of requirements on the state's Agency for State Technology to create a framework for the rest of the state government to follow to ensure that it follows best cybersecurity practices);
Maryland: S.B. 542, Ch. 358, Reg. Sess. (Md. 2015) (established the State Cybersecurity Council to "review and conduct risk assessments to determine which local infrastructure sectors are at the greatest risk of cyber attacks and need the most enhanced cybersecurity measures" and "identify categories of critical infrastructure as critical cyber infrastructure if cyber damage or unauthorized cyber access to the infrastructure could reasonably result in catastrophic consequences," among other initiatives);
Washington: S.B. 6528, 64th Leg., Reg. Sess. (Wash. 2016) (imposed a requirement on the state's Chief Information Officer to "implement a process for detecting and responding to security incidents" and "develop plans and procedures to ensure the continuity of operations for IT resources in the event of a security incident").

[224]U.S. SEC. AND EXCH. COMM'N, *SEC Awards Almost $4 Million to Overseas Whistleblower* (Sept. 24, 2018), https://www.sec.gov/news/press-release/2018-209.

[225]See U.S. COMMODITY FUTURES TRADING COMM'N, *CFTC Announces First Whistleblower Award to a Foreign Whistleblower* (July 16, 2018), https://www.cftc.gov/PressRoom/PressReleases/7755-18 (noting that this was the sixth award); U.S. COMMODITY FUTURES TRADING COMM'N, *CFTC Announces Multiple Whistleblower Awards Totaling More than $45 Million* (Aug. 2, 2018), https://www.cftc.gov/PressRoom/PressReleases/7767-18 (announcing three additional awards).

[226]U.S. COMMODITY FUTURES TRADING COMM'N, *CFTC Announces Its Largest Ever Whistleblower Award of Approximately $30 Million* (July 12, 2018), https://www.cftc.gov/PressRoom/PressReleases/7753-18.

[227]The CFTC defines a "derivatives clearing organization" as "a clearinghouse, clearing association, clearing corporation, or similar 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 March 15, 2019).

[228]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 March 15, 2019).

[229]17 C.F.R. §§ 39.18; 39.34 (2016); see also 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,* http://www.cftc.gov/IndustryOversight/TradingOrganizations/DCMs/index.htm (last visited March 15, 2019).

[230]U.S. DEP'T OF JUSTICE, *Fraud Statistics – Overview* (Sept. 30, 2018), https://www.justice.gov/civil/page/file/1080696/download.

[231]31 U.S.C. § 3729(a)(1).

[232]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)).

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

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

[235]Defense Federal Acquisition Regulation Supplement: Network Penetration Reporting and Contracting for Cloud Services, 81 Fed. Reg. 51739 (Aug. 26, 2015); 80 Fed. Reg. 81472 (Dec. 30, 2015). This regulation became effective on December 31, 2017.

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

[237]*Id.*

[238]*Id.*

[239]Universal Health Servs. v. U.S. ex rel. Escobar, 136 S. Ct. 1989, 2000–01 (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 2001.

[240]*See, e.g.,* United States v. Stephens Inst., 901 F.3d 1124, 1130 (9th Cir. 2018).

[241]*Universal Health Servs.*, 136 S. Ct. at 2002.

[242]The Court stated, "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. . . . [I]f 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 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." *Id.* at 2003–04.

[243]*See, e.g.,* United States v. Brookdale Senior Living Communities, Inc., 892 F.3d 822, 836 (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.").

[244]Michael Mezher, *Abbott Recalls 465,000 Pacemakers for Cybersecurity Patch,* REGULATORY AFFAIRS PROF'L SOC'Y (Aug. 30, 2017), https://www.raps.org/regulatory-focus%E2%84%A2/news-articles/2017/8/abbott-recalls-465,000-pacemakers-for-cybersecurity-patch.

[245]31 U.S.C. § 3730(b); *see also Provisions for the Handling of Qui Tam Suits Filed Under the False Claims Act,* U.S. ATTORNEY CRIMINAL RES. MANUAL 932, https://www.justice.gov/jm/criminal-resource-manual-932-provisions-handling-qui-tam-suits-filed-under-false-claims-act (last visited March 15, 2019).

[246]31 U.S.C. § 3730(b).

[247]31 U.S.C. § 3730(b).

[248]31 U.S.C. § 3730(d)(2).

[249]31 U.S.C. § 3730(d)(1).

[250]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).

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

APPENDIX A

States Likely to 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:	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;
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);
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);
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.;
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);
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).