THOMSON REUTERS

Westlaw®

Protecting cybersecurity whistleblowers

By Marilyn Robb, Esq., *Katz, Marshall & Banks LLP*

OCTOBER 12, 2020

Cybersecurity is essential for the safety of individual consumers and investors, the integrity of business and government, and national security. Law enforcement and regulators work to prevent and prosecute cybercrime, but robust cybersecurity must begin with responsible businesses and government agencies.

Companies and government agencies must securely 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.

Employees in both the public and private sectors who report and expose cybersecurity problems may have legal protections for blowing the whistle, and also may be entitled to potential rewards[1] for reporting cybercrime and cybersecurity vulnerabilities to the government.

A myriad of federal statutes can provide cybersecurity whistleblowers[2] with a basis for actionable retaliation claims. The availability of these protections varies according to the facts of each case, and the type of employer.[3]

I. EMPLOYEES OF PUBLICLY TRADED COMPANIES

The Sarbanes-Oxley Act of 2002 (SOX)[4] and the Dodd-Frank Act of 2010 (Dodd Frank)[5] protect employees who blow the whistle on some cybersecurity problems. SOX protects employees of publicly traded companies, or of contractors and subcontractors that serve publicly traded companies.[6]

Dodd-Frank's anti-retaliation provision applies both to public and private companies. Unlike SOX, however, it does not protect whistleblowers who only report their concerns internally, but does protect whistleblowers who report to the SEC.[7]

Publicly traded companies may be prohibited from making false or misleading public statements about their cybersecurity measures. Section 10(b) of the Securities Exchange Act of 1934, 15 U.S.C.A. § 78j(b); SEC Rule 10b-5, 17 C.F.R. § 240.10b-5; and Section 17(a) of the Securities Act of 1933, 15 U.S.C.A. § 77q(a), 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 fact that a reasonable investor would have viewed as significantly altering the "total mix" of information available to the investor.[8] Under this standard, a false or misleading public statement about a company's cybersecurity posture could constitute securities fraud.

The SEC has warned companies that they have obligations to disclose material information about cybersecurity risks and breaches.

For example, in 2018, Altaba (the company formerly known as Yahoo! Inc.) paid 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.[9]

> A myriad of federal statutes can provide cybersecurity whistleblowers with a basis for actionable retaliation claims.

Public companies should inform investors about material cybersecurity risks and incidents in a timely fashion. An employee who reports a company's failure to disclose either a serious cybervulnerability or a cybersecurity breach may be engaging in protected activity.[10]

An employee who makes such reports internally is protected by SOX, and an employee who also reports to the SEC is protected by Dodd-Frank in addition to SOX.

Courts are becoming increasingly concerned with the value of this kind of consumer data, and the impact of a possible breach. In 2018, a breach in Marriot's computer system gave hackers access to 5.2 million hotel guests' financial information.

Consumers filed suit in federal court in Maryland. In denying Marriot's motion to dismiss, the district court emphasized the value of this consumer data in the economy. The court cited statements by U.S. Attorney General William Barr connecting the cyberattack to the Chinese military and suggesting that China's spies may use the data for unknown intelligence purposes.

If employees of publicly traded companies report similar data breaches or risks of similar data breaches, this ruling supports the argument that the report would be material, and therefore, protected activity.

It is sometimes difficult to know whether an employer's failure to disclose certain information constitutes a breach of its obligation to disclose material information. In May 2020, a district court in Virginia ordered Capital One Financial Corp. to disclose a cybersecurity firm's forensic analysis of its massive 2019 data breach.

The publicly traded bank has been sued after a cyberattack exposed the sensitive data of more than 100 million people. The court's order to disclose the analysis suggests that the forensic analysis likely would constitute material information. Therefore, if any employee reported Capital One's failure to disclose such information to investors, they likely engaged in protected whistleblowing activity.

SOX and Dodd-Frank prohibit employers from taking a wide range of adverse employment actions against an employee because the employee engaged in protected activity.

As noted above, an employee who reports an employer's cybervulnerabilities may be protected under SOX, if the employer is a publicly traded company or a wholly owned subsidiary or affiliate of one.

Dodd-Frank also protects such employees, provided they report the violations to the SEC, and may protect employees of non-public companies for raising these concerns if they are registered investment companies or registered investment advisors subject to SEC regulations related to customer data protection.

SOX and Dodd-Frank prohibit employers from taking a wide range of adverse employment actions against an employee because the employee engaged in protected activity. Such adverse actions include termination, suspension, demotion, harassment, and may also include non-tangible employment actions such as poor performance reviews.

II. EMPLOYEES OF PRIVATELY HELD BANKS AND OTHER DEPOSITORY INSTITUTIONS

The Financial Institutions Reform Recovery and Enforcement Act of 1989 ("FIRREA")[11] 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.

FIRREA protects employees of depository banks and employees of federal banking regulators who report a wide range of potential wrongdoing. In the cybersecurity context, this standard would protect reports of a possible violation of the Gramm-Leach-Bliley Act,[12] which requires financial institutions to protect certain consumer data, or of Section 5 of the Federal Trade Commission Act of 1914,[13] which prohibits unfair or deceptive practices in commerce, including insufficient data security.

To be protected under FIRREA, employees must report these potential violations externally to a federal banking agency or the U.S. Department of Justice.[14]

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 the above described protected activity.[15]

III. EMPLOYEES OF THE FEDERAL GOVERNMENT

The Whistleblower Protection Act (WPA)[16] and the Whistleblower Protection Enhancement Act (WPEA)[17] together provide meaningful protections to cybersecurity whistleblowers within the federal government.

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.[18]

Whistleblowing is not protected, however, if the disclosure is prohibited by law or executive order in the interest of national defense or the conduct of foreign affairs.[19]

The Whistleblower Protection Act and the Whistleblower Protection Enhancement Act together provide meaningful protections to cybersecurity whistleblowers within the federal government.

To engage in activity protected by the WPA, a federal employee who raises concerns about cybersecurity may point to a particular law or regulation that he or she reasonably believes is being violated, or may indicate that the cybersecurity lapse at issue constitutes gross mismanagement, abuse of authority, or a substantial danger to public safety.

An employee's claim that she or he engaged in protected activity would be particularly strong if he or she reports that the relevant agency is not complying with a particular law, regulation, or Executive Order calling on that agency to meet certain cybersecurity standards.

One such Executive Order was promulgated in 2013 and expanded in 2017. In Executive Order 13,636, President Obama called on "[a]gencies with responsibility for regulating the security of critical infrastructure" to adopt cybersecurity

standards established by the National Institute of Standards and Technology (NIST).[20]

In May 2017, a subsequent Executive Order extended the NIST standards to all federal government agencies.[21] Under this Executive Order, an employee at an agency who reports noncompliance with the NIST standards has engaged in protected activity under the WPA.

The WPA prohibits a federal agency from taking, failing to take, or threatening to take or fail to take, a personnel action because of an employee's protected activity.

Prohibited personnel actions under the WPA include, but are not limited to: disciplinary or corrective action; a detail, transfer, or reassignment; a performance evaluation; a decision concerning pay, benefits, awards, education or training, or; other significant change in duties, responsibilities, or working conditions.[22]

IV. EMPLOYEES OF FEDERAL CONTRACTORS

A. Actions to prevent government fraud

The False Claims Act (FCA)[23] 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.[24] The FCA also protects employees who report such fraud from retaliation.

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]."[25]

Companies contracting with the government are subject to a number of heightened cybersecurity requirements, including Federal Acquisition Regulations (FARs) establishing increased cybersecurity standards.[26]

This rule requires that certain companies seeking government contracts comply with the standards set forth in NIST Special Publication 800-171, which provides detailed regulations for "Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations."[27]

The Department of Defense (DOD) implemented a similar rule requiring that DOD contractors adhere to the new NIST SP 800-171 standards.[28] This regulation became effective on December 31, 2017. The DOD regulations also significantly increase the scope of information that contractors are responsible for securing.[29]

Employees who report the failure of a government contractor to comply with these standards may be protected from retaliation.

The FCA prohibits employers from retaliating against employees who engage in such protected activity by terminating, demoting, suspending, threatening, harassing, or in any other manner discriminating against the employee in the terms and conditions of employment.[30]

B. Employees of defense contractors

The National Defense Authorization Act for Fiscal Year 2013 (NDAA) protects an employee of a Defense Department contractor, subcontractor or grant recipient who discloses 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.[31]

In 2015, the DOD implemented a rule requiring its contractors to adhere to the NIST SP 800-171 standards described above.[32] The DOD also significantly increased the scope of information that contractors are responsible for securing.

Contractors are responsible for securing information received from the government, as well as information that is "collected, developed, received, used, or stored by or on behalf of the contractor in support of the performance of the contract."[33]

Employers seeking contracts with the DOD and other federal agencies are subject to these requirements, and employees who report their employer's failure to meet these standards may be protected from retaliation.

The NDAA prohibits a federal contractor from discharging, demoting, or otherwise discriminating against an employee for engaging in any of the forms of protected activity described above.

However, to be protected by the NDAA, the disclosure must be made to: a member of Congress or a representative of a committee of Congress; an Inspector General; the Government Accountability Office; a federal employee responsible for contract or grant oversight or management at the relevant agency; an authorized official of the Department of Justice or other law enforcement agency; a court or grand jury, or a management official or other employee of the contractor, subcontractor, or grantee who has the responsibility to investigate, discover, or address misconduct.[34]

The NDAA prohibits a federal contractor from discharging, demoting, or otherwise discriminating against an employee for engaging in any of the forms of protected activity described above.[35]

V. CONCLUSION

There is no single federal statute that protects employees who blow the whistle on inadequate cybersecurity protections. However, there are a handful of statutes and other laws on which a cybersecurity whistleblower may rely to create an actionable claim for whistleblower retaliation.

Under these statutes, employees should be able to make such reports without fear of retaliation, and as a result, sensitive consumer data and national security information is more likely to be protected. Because of the complexity and uncertainty of the extent of protections in this area, employees who are considering reporting cybersecurity concerns should seek legal advice about whether they would be protected from potential retaliation.

Notes

[1] https://bit.ly/3np2MPn

[2] https://bit.ly/3nxbNpm

[3] A more in-depth analysis of the overview below may be found in Cybersecurity Whistleblower Protections: An overview of the protections and rewards available to cybersecurity whistleblowers under federal and state law by Alexis Ronickher & Matthew LaGarde, available at https://bit.ly/2GOV6ow.

[4] 18 U.S.C.A. § 1514A

[5] 15 U.S.C.A. § 78u-6

[6] *See Lawson v. FMR LLC*, 571 U.S. 429, 444 (2014).

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

[8] *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).

[9] *See* 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://bit.ly/36KeVZ3.

[10] https://bit.ly/2I2DkPi

[11] 12 U.S.C.A. § 1831j

[12] 15 U.S.C.A. §§ 6801 et seq.

[13] 15 U.S.C.A. § 45(a)(1)

[14] *See* 18 U.S.C.A. §1831j(a)(1).

[15] *See* 12 U.S.C.A. § 1831j(a)(1).

[16] 5 U.S.C.A. § 2302

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

[18] 5 U.S.C.A. § 2302(b)(8).

[19] *See id.*

[20] *See* Exec. Order No. 13636, Improving Critical Infrastructure Cybersecurity, 78 Fed. Reg. 11739, 11743–44 (Feb. 12, 2013), available at https://bit.ly/33IAoj6.

[21] See 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://bit.ly/3ilhyx9.

[22] 5 U.S.C.A. § 2302(a)(2)(A).

[23] 9431 U.S.C.A. §§ 3729-3733

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

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

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

[27] *See id.* at 30440.

[28] *See* 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).

[29] *See* 81 Fed. Reg. at 51743.

[30] *See* 31 U.S.C. § 3730(h).

[31] *See* 41 U.S.C. § 4712(a)(1).

[32] *See* 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).

[33] *See* 481 Fed. Reg. at 51743

[34] *See* 41 U.S.C. § 4712(a)(2).

[35] *See* 41 U.S.C. § 4712(a)(1).

This article was published on Westlaw Today on October 12, 2020.

ABOUT THE AUTHOR

Marilyn Robb is an associate at **Katz, Marshall & Banks LLP**, a plaintiff-side employment and whistleblower law firm based in Washington, D.C. Prior to joining KMB, she clerked for Judge Duane Benton on the U.S. Court of Appeals for the 8th Circuit. Robb received her J.D. from Harvard Law School, and B.A. from Columbia University. She can be reached at robb@kmblegal.com.