# Blowing the Whistle on Data Breaches and Cybersecurity Flaws

**Ms. Hamsa Mahendranathan**
Associate at Constantine Cannon LLP
hmahendranathan@constantinecannon.com

**Mr. Chris McLamb**
Associate at Constantine Cannon LLP
cmclamb@constantinecannon.com

With increasing dependence on technology, cybersecurity has emerged as a critical issue for customers, investors, and government regulators. Data breaches and other cybersecurity incidents can have devastating effects. In 2018, the Council of Economic Advisers estimated that malicious cyber activity cost the U.S. economy up to $109 billion dollars in 2016 alone. (1)

Typically, the public only learns of such flaws and malicious actions months or even years after the fact. Companies may deliberately conceal known breaches or vulnerabilities from the public and their customers. Where companies seek to hide information, whistleblowers can play a critical role in exposing cybersecurity flaws and data breaches.

Under certain circumstances, a whistleblower can even receive an award for bringing timely information about computer hacks, data breaches, and software vulnerabilities to the government. However, there is no single agency that regulates cybersecurity. Instead, whistleblowers must navigate a complex web of overlapping laws to find the best place to bring their information. An experienced whistleblower attorney can provide critical guidance in that assessment. Below we describe some of the key laws covering rewards for cybersecurity whistleblowers in the United States.

**Blowing the Whistle on Cybersecurity Failures in Government Contracts**

The United States government imposes cybersecurity requirements on government contractors.(2) In 2016, the Department of Defense, General Services Administration, and NASA amended the Federal Acquisition Regulation to add a new subpart and contract clause on safeguarding information systems containing federal contract information. As a baseline, FAR now requires contractors and subcontractors to comply with basic cybersecurity controls established in National Institute of Standards and Technology Special Publication 800-171.

Other US federal contracts require more rigorous cybersecurity standards. The US Department of Defense's FAR supplement now requires certain defense contractors to report cyber incidents within 72 hours of their discovery. In addition, government contracts often impose further requirements for the protection of classified information or for compliance with agency-specific information-security requirements.

A contractor's failure to comply with cybersecurity-related contract terms can give rise to liability under the federal False Claims Act, (3) which empowers whistleblowers to report fraud and misconduct in government contracts and programs. The FCA allows whistleblowers to bring a lawsuit on the government's behalf and share in the government's recovery.

Successful whistleblower actions have been brought regarding failures by information technology companies to comply with government standards, although no recoveries yet involve the cybersecurity standards specifically.

- In April, 2019, IT supplier **Fortinet** agreed to pay more than **$500,000 (4)** to resolve an FCA case brought by a whistleblower alleging that it routinely supplied the government with products made in China and then doctored the products' labels to make it appear that they complied with the federal Trade Agreements Act. In announcing the settlement, the government emphasized that it was "committed to combatting procurement fraud and cyber risk within U.S. Department of Defense programs."
- In 2017, electronic health records (EHR) vendor **eClinicalWorks** agreed to pay **$155 million (5)** to resolve claims that it misrepresented the capabilities of its software to fraudulently obtain certification required for government payment. While not involving security standards, EHR fraud cases (6) demonstrate the government's interest in pursuing vendors for misrepresenting software capabilities.
- In 2015, **NetCracker Technology Corp.**,(7) which provided telecommunications network support to the Department of Defense, agreed to pay **$11.4 million** to settle claims that it used employees without security clearances to perform contract work that it knew required clearances.

**SEC Cybersecurity Regulation Can Support a Claim to the SEC Whistleblower Program**

The US Securities and Exchange Commission has also become increasingly focused on cybersecurity, and whistleblowers that report cybersecurity incidents or vulnerabilities to the SEC could be entitled to a reward under the SEC Whistleblower Program (8). In 2018, the SEC published guidance on how public companies should disclose cybersecurity incidents and

risks to investors. In the guidance, the SEC explained that companies face a wide range of cyber risks, from stolen access credentials and phishing, to malware and distributed denial-of-service attacks. Whatever their form, cyberattacks can significantly harm companies by destroying assets, interfering with critical systems, or disclosing sensitive intellectual property or consumer data.

Given these risks, the SEC advised public companies to promptly disclose all material cyber risks and incidents. The SEC identified several factors companies should consider when formulating disclosures:

- The severity and frequency of prior incidents
- The probability of occurrence and potential magnitude of future incidents
- The adequacy and costs of preventative measures
- 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
- The potential for reputational harm
- Existing or pending laws and regulations relating to cybersecurity and their associated costs
- Litigation, investigation, and remediation costs associated with cybersecurity incidents

In explaining these factors, the SEC cautioned companies to "**avoid generic cybersecurity-related disclosure and provide specific information that is useful to investors**." The SEC also noted that directors, officers, and other corporate insiders can violate the antifraud provisions of the securities laws if they trade on material nonpublic information about a company's cybersecurity risks and incidents.

Other entities regulated by the SEC are subject to industry-specific rules. For example, the SEC has issued specialized regulations and guidance for registered broker-dealers, investment companies, and investment advisers who must safeguard confidential investor records and information. Likewise, the SEC promulgated specific rules to enhance the technology infrastructure of entities directly supporting U.S. securities markets, such as stock and options exchanges and registered clearing agencies.

Regulated entities that violate these rules may be subject to SEC fines. For example:

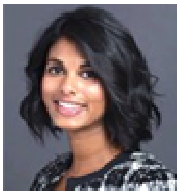
- In 2018, **Yahoo** paid a **$35 million** SEC penalty (9) to settle charges that it misled investors by failing to disclose one of the world's largest data breaches in which hackers stole personal data relating to hundreds of millions of user accounts
- In 2016, **Morgan Stanley Smith Barney** paid a **$1 million** SEC penalty (10) to settle charges that it failed to adequately secure customer information.

The SEC whistleblower program encourages those with knowledge of violations of cybersecurity laws and regulations to share this information with the SEC. If the SEC collects monetary sanctions of more than $1 million, eligible whistleblowers can receive an award of between 10 percent and 30 percent of the amount collected by the government.

**References:**


(1). https://www.whitehouse.gov/articles/cea-report-cost-malicious-cyber-activity-u-s-economy/
(2) https://constantinecannon.com/practice/whistleblower/whistleblower-types/government-contract-fraud/
(3) https://constantinecannon.com/practice/whistleblower/whistleblower-types/whistleblower-reward-laws/fca/
(4) https://constantinecannon.com/2019/04/18/catch-of-the-week-false-claims-act-case-against-cybersecurity-company/
(5) https://constantinecannon.com/2017/06/01/electronic-health-records-vendor-pays-big-settle-false-claims-act-charges/
(6) https://constantinecannon.com/practice/whistleblower/whistleblower-types/healthcare-fraud/electronic-health-records-ehr-fraud/
(7) https://constantinecannon.com/2015/11/06/doj-catch-of-the-week-netcracker-technology-corp/
(8) https://constantinecannon.com/practice/whistleblower/whistleblower-types/whistleblower-reward-laws/sec/
(9) https://constantinecannon.com/2018/06/01/april-24-2018/
(10) https://constantinecannon.com/2016/08/01/june-8-2016-2/


**About the authors**




Hamsa Mahendranathan is as an associate in Constantine Cannon LLP's New York office. She predominantly represents whistleblowers under the federal False Claims Act, numerous state law equivalents, and the whistleblower programs of the Securities and Exchange Commission and Commodity Futures Trading Commission. Prior to joining Constantine Cannon, she practiced at Mayer Brown LLP where she focused on complex commercial litigation involving large financial institutions.

Hamsa received her J.D. from Columbia Law School in 2012. While there, she was a Wien National Scholar, a Harlan Fiske Stone Moot Court Semifinalist, and a Moot Court Editor. She also interned for the Honorable Theodore H. Katz (Ret.), a United States Magistrate Judge in the Southern District of New York, and spent a summer representing indigent defendants sentenced to death in Louisiana at the Capital Appeals Project.

Chris McLamb is an associate in Constantine Cannon LLP's San Francisco office. He represents whistleblowers in qui tam lawsuits brought under the Federal and various state False Claims Acts, as well as claims made under the whistleblower programs of the Internal Revenue Service, Securities and Exchange Commission, Commodity Futures Trading Commission, and Department of Transportation. He has also represented local governments in False Claims Act matters.

Outside of work, Chris serves on the Board of Directors of the American Constitution Society's Bay Area Lawyer Chapter. Chris graduated from Stanford Law School, where he was an articles editor of the Stanford Law Review and a Public Interest Fellow. While in law school, Chris represented children with disabilities as part of Stanford's Youth and Education Law Project.