[IS] OPINIONS
Politics
(https://insidesources.com/category/politics/)

# Blowing the Whistle on Cybersecurity Fraud

Posted to Politics (https://insidesources.com/category/politics/) July 23, 2021 by Renée Brooker (https://insidesources.com/author/renee-brooker/)

Whistleblowers deserve every billion they get from a wide range of generous federal whistleblower reward programs. In recent weeks, Sens. Chuck Grassley and Ron Wyden underscored their support for the concept, introducing the IRS Whistleblower Program Improvement Act (https://www.grassley.senate.gov/imo/media/doc/summary_-_irs_whistleblower_program_improvement_act_of_2021.pdf) to strengthen that agency's existing initiative that recovers funds from wealthy tax cheaters.

One area that is especially ripe for fraud and lucrative whistleblowing is the massive new federal spending on cybersecurity.

As cyber incidents involving the nation's infrastructure, government agencies and private businesses escalate, President Joe Biden is prioritizing the protection (https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/) of the government's information technology and expanding its cybersecurity efforts. Key to that is the Department of Justice's (DOJ's) reinvigorated pursuit of cyber fraud, using the False Claims Act (https://www.justice.gov/opa/speech/remarks-deputy-assistant-attorney-general-michael-d-granston-aba-civil-false-claims-act) as a powerful weapon or, as it is often referred to, the whistleblower law.

That law enables the U.S. to sue government contractors where cybersecurity protection is a material requirement of payment under their contracts. Proof of a knowing failure to address this protection gives rise to False Claims Act liability, and individuals who expose that failure can be awarded 15-30 percent of recovered funds.

Over a recent four-year period, the government recovered $11.4 billion in fraud prosecutions and distributed more than $1.54 billion in reward payments.

Some common fraud schemes committed by government contractors include:

- Obtaining contracts by making false representations in bidding documents;
- Delivering services to the government that do not meet contract specifications while certifying that they do;
- Bid-rigging or kickbacks; and,
- Misrepresenting the cost of a project or "underbidding" contracts.

Cybersecurity breaches pose an immediate, dire threat to the nation, as seen in the recent Colonial Pipeline breach by foreign criminals. Government agencies pay large companies huge sums to prevent cybersecurity breaches from happening. The Government Accountability Office reports (https://www.gao.gov/assets/gao-21-422t.pdf) the federal government invests over $100 billion annually on IT and cybersecurity. Biden's budget to Congress also includes billions for cybersecurity with a huge chunk of that targeted for the Department of Defense.

Based on experience with other major crisis-response funding programs, we know that large-scale fraud will eat away at this national cybersecurity expenditure. It is critical for the government to identify program failures, deter future abuses and claw back misspent money.

DOJ's primary means to uncover cyber fraud is via reporting by whistleblowers, who can be software developers, company technology or information officers, IT security analysts, engineers, architects, administrators, or consultants – anyone with knowledge of the cyber breaches, incidents, or fraud.

In one recent case (https://ag.ny.gov/press-release/2019/attorney-general-james-secures-6-million-cisco-systems-multistate-settlement), an employee of a surveillance system distributor for a government contractor reported that the software had significant flaws that made it vulnerable to hackers. The contractor knew this and failed to report the defects to the government. The whistleblower was paid over $1.7 million for reporting this fraud.

In another instance, one of the nation's largest vendors of electronic health records (EHR) software paid $155 million for misrepresenting its product's capabilities. That whistleblower received a $30 million reward (https://www.fraudfighters.net/wp-content/uploads/2021/06/Electronic-Health-Records-Vendor-to-Pay-155-Million-to-Settle-False-Claims-Act-Allegations-_-OPA-_-Department-of-Justice.pdf).

Another entity paid a $250,000 False Claims Act settlement when two whistleblowers reported that a health care system falsely attested that it conducted and reviewed security risk EHR analyses when it did not.

A $50,000 reward (https://www.justice.gov/usao-ks/pr/kansas-hospital-agrees-pay-250000-settle-false-claims-act-allegations) was paid out.

The False Claims Act protects whistleblowers from retaliation by their employers, who may not discharge, demote, suspend, threaten, harass or discriminate against an employee for their actions.

During my time as a prosecutor enforcing the False Claims Act, I saw many companies knowingly failing to provide services they had promised to the government. Until a whistleblower steps forward and instigates a government investigation, those firms typically continue to engage in illegal conduct.

Sometimes False Claims Act resolutions impose additional requirements on the settling party. The reporting of cybersecurity fraud can thus have the lasting effect of stopping future misconduct.

Whistleblowers are keepers of democracy's flame, illuminating wrongs, safeguarding vital enterprises and bringing justice to bear in the best interest of American taxpayers.

---

## About the Author

**Renée Brooker (https://insidesources.com/author/renee-brooker/)**

Renée Brooker, a partner at the Washington law firm Tycko & Zavareei LLP, represents whistleblowers. She was an Assistant Director at the U.S. Department of Justice in the national office that supervises False Claims Act whistleblower cases in all 94 federal trial courts. She wrote this for InsideSources.com.

More from Inside Sources