

Department of Justice “Cyber-Fraud” Case Tracker (Dec. 2025)

Case	Summary	Settlement Date	Settlement Amount	Links
CHS	Comprehensive Health Services LLC (CHS), a provider of global medical services, was alleged to have violated the False Claims Act (FCA) by falsely representing to the State Department and the Air Force that it complied with contract requirements relating to the provision of medical services at State Department and Air Force facilities in Iraq and Afghanistan. Settlement also resolves two qui tam actions: United States ex rel. Watkins et al. v. CHS Middle East, LLC, 1:17-cv-04319 (E.D. N.Y.); United States ex rel. Lawler et al. v. Comprehensive Health Services, Inc. et al, 1:20-cv-00698 (E.D. N.Y.).	02/25/22	\$930,000	Press Release Settlement
Aerojet Rocketdyne	Aerojet Rocketdyne Inc., a provider of propulsion and power systems for launch vehicles, missiles and satellites and other space vehicles, has agreed to pay \$9 million to resolve allegations that it violated the FCA by misrepresenting its compliance with cybersecurity requirements in certain federal government contracts. Settlement also resolves qui tam action United States ex rel. Brian Markus v. Aerojet Rocketdyne Holdings Inc., et al., Case No. 2:15-cv-02245-WBS-AC (E.D.Cal.).	07/08/22	\$9,000,000	Press Release Statement of Interest Settlement
Jelly Bean	Jelly Bean Communications Design LLC (Jelly Bean) and Jeremy Spinks were alleged to have violated the FCA by failing to secure personal information on a federally funded Florida children's health insurance website, which Jelly Bean created, hosted, and maintained.	03/14/23	\$293,771	Press Release Settlement
Verizon	Verizon Business Network Services LLC was alleged to have violated the FCA by failing to completely satisfy certain cybersecurity controls in connection with an information technology service provided to federal agencies.	09/05/23	\$4,091,317	Press Release Settlement
Insight Global	Staffing company Insight Global LLC was alleged to have violated the FCA by failing to implement adequate cybersecurity measures to protect health information obtained during COVID-19 contact tracing. Settlement also resolves quit tam action United States ex rel. Seilkop v. Insight Global LLC, no. 1:21-cv-1335 (M.D. Pa.).	04/24/24	\$2.7 million	Press Release Settlement
Guidehouse / Nan McKay	Consulting companies Guidehouse Inc. and Nan McKay and Associates were alleged to have violated the FCA by failing to meet cybersecurity requirements in contracts intended to ensure a secure environment for low-income New Yorkers to apply online for federal rental assistance during the COVID-19 pandemic. Settlement also resolves a qui tam action United States ex rel. Elevation 33, LLC v. Guidehouse Inc., and Nan McKay and Associates, Inc., no. 1:22-cv-206 (N.D.N.Y.).	05/13/24	\$7.6 million / \$3.7 million	Press Release Guidehouse Settlement Nan McKay Settlement
AFDS	ASRC Federal Data Solutions LLC (AFDS) was alleged to have violated the FCA in connection with a government contract related to its storage of unsecured personally identifiable information of Medicare beneficiaries.	10/15/24	\$306,722	Press Release Settlement

If you have any questions about this tracker, contact [Sandeep Kathuria](#) at Ice Miller, LLP. | [icemiller.com](#) © 2025 Ice Miller LLP – Attorney Advertising Material – This publication is intended for general information purposes only and does not and is not intended to constitute legal advice. The reader should consult with legal counsel to determine how laws or decisions discussed herein apply to the reader's specific circumstances.

Case	Summary	Settlement Date	Settlement Amount	Links
Penn State	The Pennsylvania State University (Penn State) was alleged to have violated the FCA by failing to comply with cybersecurity requirements in fifteen contracts or subcontracts involving the Department of Defense (DoD) or National Aeronautics and Space Administration (NASA). Settlement also resolves qui tam action U.S. ex rel. Decker v. Pennsylvania State University, No. 2:22-cv-03895 (E.D. Pa.).	10/22/24	\$1,250,000	Press Release Settlement
HNFS	Health Net Federal Services Inc. (HNFS) and its corporate parent Centene Corporation, were alleged to have falsely certified compliance with cybersecurity requirements in a contract with the U.S. Department of Defense (DoD) to administer the Defense Health Agency's (DHA) TRICARE health benefits program. This settlement resolves those claims.	02/2025	\$11,253,400	Press Release Settlement
MORSE	MORSECORP, Inc. (MORSE) was alleged to have violated the FCA by failing to comply with cybersecurity requirements in its contracts with the Departments of the Army and Air Force. Settlement also resolves qui tam action United States ex rel. Berich v. MORSECORP, Inc., et al., No. 23-cv-10130-GAO (D. Mass.).	03/14/2025	\$4,600,000	Press Release Settlement
Raytheon/ Nightwing	Raytheon Company (Raytheon), RTX Corporation, and Nightwing Group LLC, and Nightwing Intelligence Solutions LLC (collectively, Nightwing) were alleged to have violated the FCA by failing to implement security requirements required by contracts on systems used to perform unclassified work for the Department of Defense. The settlement resolves conduct that allegedly occurred between 2015 and 2021, prior to Nightwing's acquisition of the business. Settlement also resolves qui tam action U.S. ex rel. Doe v. Raytheon Co. et al., No. 21-cv-2343 (D.D.C.).	04/09/2025	\$8,400,000	Press Release Settlement
Hill ASC	Hill ASC Inc., doing business as Hill Associates, of Rockville, Maryland, was alleged to have violated the FCA by billing federal agencies for labor of information technology personnel who did not have the experience or education required under the contract and for cybersecurity services and other services that were not within the scope of the contract as well as by failing to provide government customers with required information about discounts for prompt payment. The settlement resolves conduct that allegedly occurred between 2018 and 2023.	07/14/2025	\$14,750,000	Press Release Settlement
Illumina	Illumina, Inc., was alleged to have violated the FCA by selling federal agencies certain genomic sequencing systems with cybersecurity vulnerabilities, without having an adequate security program and sufficient quality systems to identify and address those vulnerabilities. The settlement also resolves qui tam action U.S. ex rel. et al. v. Illumina Inc., 1:23-cv-00372 (D. R.I.).	07/22/2025	\$9,800,000	Press Release Settlement
Aero Turbine/ Gallant	Aero Turbine Inc., and Gallant Capital Partners LLC, were alleged to have violated the FCA by knowingly submitting or causing others to submit false or fraudulent claims for payment on a contract with the Department of the Air Force that did not comply with the contract's cybersecurity requirements.	07/31/2025	\$1,750,000	Press Release Settlement
Georgia Tech / GTRC	Georgia Institute of Technology (Georgia Tech) and Georgia Tech Research Corporation (GTRC) were alleged to have violated the FCA and federal common law by failing to meet cybersecurity requirements in connection with U.S. Department of Defense (DoD) contracts. Settlement also resolves qui tam action U.S. ex rel. Craig v. Georgia Tech Research Corp. et al., No. 1:22-cv-02698 (N.D. Ga.).	09/29/2025	\$875,000	Press Release Settlement

If you have any questions about this tracker, contact [Sandeep Kathuria](#) at Ice Miller, LLP. | [icemiller.com](#) © 2025 Ice Miller LLP – Attorney Advertising Material – This publication is intended for general information purposes only and does not and is not intended to constitute legal advice. The reader should consult with legal counsel to determine how laws or decisions discussed herein apply to the reader's specific circumstances.

Case	Summary	Settlement Date	Settlement Amount	Links
Hillmer	On Dec. 9, 2025, a federal grand indicted Danielle Hillmer, a former senior manager at a Virginia-based government contractor, on charges of major government fraud, wire fraud, and obstructing federal audits for allegedly carrying out a multi-year scheme to mislead federal agencies about the security of a cloud-based platform used by the U.S. Army and other government customers. In this case, the employee's actions were brought to the government's attention by the employer following an internal review. The case is USA v. Hillmer, 1:25CR00383 (D. D.C.).			Press Release
Swiss Automation	Swiss Automation Inc., an Illinois-based precision machining business that supplies alloy and metal parts to commercial and government customers, has agreed to pay \$421,234 to resolve alleged FCA violations. Swiss Automation is alleged to have failed to provide adequate cybersecurity for certain drawings of parts that the company machined and supplied to Department of Defense (DoD) prime contractors. The settlement also resolves qui tam action United States of America, et al v. Swiss Automation, Inc., 1:22CV04328 (N.D. Ill.) pursuant to which the whistleblower, a former quality-control manager at Swiss Automation, will receive \$65,291 of the settlement amount.	12/05/2025	\$421,234	Press Release Settlement

If you have any questions about this tracker, contact [Sandeep Kathuria](#) at Ice Miller, LLP. | [icemiller.com](#) © 2025 Ice Miller LLP – Attorney Advertising Material – This publication is intended for general information purposes only and does not and is not intended to constitute legal advice. The reader should consult with legal counsel to determine how laws or decisions discussed herein apply to the reader's specific circumstances.