INSPECTOR GENERAL'S FRAUD WATCH

MAY 2026

The VA OIG fights fraud through close collaboration with VA personnel, federal law enforcement partners, the Department of Justice, and multiple fraud task forces, including the Fraud Task Force established by the President's March 2026 Executive Order. VA OIG staff investigate and deter fraudulent and criminal conduct and disrupt complex fraud schemes that impact veterans' healthcare, education, and benefits.

Recent enforcement actions and audit reports included below highlight this impact. You can find more information on the VA OIG's oversight work, along with full investigative updates and reports, by visiting the VA OIG website.

Investigations – Recent Activity and Ongoing Cases

Compensation Benefits Fraud

Compensation benefits fraud involves individuals' submission of fraudulent claims for payment of VA disability benefits.

- A VA OIG and Social Security Administration OIG investigation revealed that a nonveteran fraudulently obtained more than $860,000 in VA compensation payments and $163,669 in VHA health benefits by assuming the identity of an actual Vietnam war veteran for more than 25 years. Following the veteran's death in 2018, the defendant continued the scheme by falsely claiming the death had been reported in error and successfully persuaded agencies to resume benefit payments. The fraud continued until 2023, when the defendant's attempts to obtain additional benefits led to the discovery of the scheme. The defendant was sentenced in the Eastern District of Washington to 30 months' imprisonment and 36 months' supervised release and was ordered to pay restitution of approximately $1,025,544 after previously pleading guilty to false representation of a Social Security number, wire fraud, and theft of government funds. The defendant was also previously found guilty at a bench trial of aggravated identity theft.

- A VA OIG investigation resulted in charges alleging that a veteran and his wife fraudulently obtained compensation benefits and Caregiver Support Program benefits through false representations of the veteran's physical capabilities. The total loss to VA was approximately $962,000. The veteran and his wife were indicted in the Eastern District of Tennessee on charges of conspiracy to commit wire fraud and theft of government funds.

- A VA OIG investigation resulted in charges alleging that another veteran and his wife fraudulently obtained compensation benefits and Caregiver Support Program benefits through false representations of the veteran's physical capabilities. The total loss to VA was almost $677,000. The wife pleaded guilty in the Eastern District of Washington to healthcare fraud. Trial for the veteran is scheduled for November 2026.

- A VA OIG investigation revealed that a veteran submitted fraudulent claims to VA claiming the loss of the use of his feet. The defendant made numerous statements to VA in which he further claimed to be unable to ambulate without the aid of a walker, unable to participate in any household chores, and that he required extensive personal hygiene assistance. Due to these fraudulent claims, the defendant received VA compensation benefits totaling almost $470,000, a special adaptive housing grant for over $99,000, and an adaptive vehicle grant for approximately $21,000. The defendant was sentenced in the Western District of Louisiana to 60 months' supervised release and ordered to pay restitution of approximately $125,000 after previously pleading guilty to theft of government funds. The restitution was for the special adaptive housing grant and adaptive vehicle grant that the defendant fraudulently received from VA. The judge also ordered the remaining overpayments of almost $470,000 to be recouped by VA by garnishing the defendant's legitimate VA benefits.

- A VA OIG and US Postal Inspection Service investigation revealed that a defendant unlawfully gained access to the bank account of a veteran who was rated at 100 percent service-connected for blindness and suffered from dementia. Between 2021 and 2024, the defendant stole approximately $225,000 of the veteran's VA disability compensation benefits which he used for personal purchases. The defendant was sentenced in the District of New Hampshire to 21 months' imprisonment and 36 months' supervised release and was ordered to pay restitution of $225,200 after previously pleading guilty to bank fraud.

- A VA OIG investigation resulted in charges alleging that the son of a deceased veteran diverted VA compensation benefits totaling approximately $223,000 that had been intended for the veteran. The defendant was indicted in the Southern District of Mississippi for theft of government property or funds.

- A multiagency investigation resulted in charges alleging that a Jamaican national fraudulently received a Permanent Resident Card (Green Card) when she entered into an fraudulent marriage with an Active-Duty U.S. Army soldier. It is alleged the defendant subsequently enlisted in the United States Army, became a naturalized U.S. Citizen, and was then medically retired from the U.S. Army. It is further alleged the defendant applied for and began receiving VA service-connected disability benefits to which she was not entitled due to her fraudulent marriage. The loss to VA was approximately $130,000. The defendant was arrested after being indicted in the Western District of Missouri on charges to include conspiracy, making a materially false statement under oath, unlawful procurement of citizenship or naturalization on an immigration document, and mail fraud. This investigation was conducted by VA OIG, Army Criminal Investigations Division, Department of Homeland Security OIG, and Immigrations and Customs Enforcement.

- A VA OIG and FBI investigation resulted in charges alleging that a VA-contracted medical provider accepted bribes from veterans in exchange for fraudulent medical records in support of their applications for VA disability compensation benefits. The defendant was indicted in the Middle District of Georgia on charges of bribery and abetting and aiding wire fraud.

Computer Fraud

Computer crime, also known as cybercrime, refers to illegal activities committed using computers or digital networks to steal, damage, or manipulate information for personal, financial, or political gain.

- A multiagency investigation resulted in charges alleging that two defendants conspired to delete databases used to store U.S. government information. Following the termination of their employment as federal contractors, the defendants allegedly sought to harm the company and its more than 45 federal government customers, including VA OIG, by accessing computers without authorization, issuing commands to prevent others from modifying the databases before deletion, deleting databases, stealing information, and destroying evidence of their unlawful activities. One of the defendants was found guilty at trial by a federal jury in the Eastern District of Virginia on charges of conspiracy to

commit computer fraud, password trafficking, and possession of a firearm by a prohibited person. The other defendant previously pleaded guilty and is awaiting sentencing. This investigation was conducted by the Federal Deposit Insurance Corporation OIG, Department of Homeland Security OIG, and Homeland Security Investigations with assistance provided by VA OIG and 19 other law enforcement agencies.

COVID-19 Program Fraud

COVID-19 fraud involves the submission of fraudulent applications for payments under the Small Business Administration's small business pandemic relief programs to include the Payroll Protection Program and Economic Impact Disaster Loan Program. These programs were created through the Coronavirus Aid, Relief, and Economic Security (CARES) Act, which was signed into law in March 2020 in response to the economic fallout from the COVID-19 pandemic.

- A VA OIG and Small Business Administration (SBA) OIG investigation resulted in charges alleging that two current Dayton VA Medical Center employees, one former Dayton VA Medical Center employee, and another defendant obtained multiple fraudulent SBA-backed Paycheck Protection Program and Economic Injury Disaster loans for non-functional businesses and businesses that reported inflated numbers of employees. The defendants were indicted in the Southern District of Ohio on charges of conspiracy to commit wire fraud and wire fraud. The estimated loss to the government for entire fraud scheme was about $1.4 million. Of this amount, over $120,000 was received by VA employees.

- A VA OIG investigation revealed that a former St. Louis VA Regional Office employee, while employed by VA, obtained fraudulent Paycheck Protection Program loans for businesses that never had any earnings and were not in operation as claimed by the defendant. The defendant was sentenced in the Eastern District of Missouri to 60 months' supervised release and was ordered to pay restitution of over $41,000 to the Small Business Administration after previously pleading guilty to false statements.

- A VA OIG investigation revealed that a former Ann Arbor VA Healthcare System employee applied for and received two Paycheck Protection Program loans in the amount of $41,664 by submitting fraudulent bank statements and making other false representations regarding his business operations. The defendant also received $19,880 in COVID Emergency Rental Assistance (CERA) funds after submitting falsified and altered documentation to the Michigan State Housing Development Authority (MSHDA).

The CERA program, administered by MSHDA, was designed to support Michigan residents struggling with rent and utilities due to pandemic-related financial hardships. The defendant was sentenced in the 3rd Circuit Court of Wayne County (Michigan) to 2 to 15 years' imprisonment and was ordered to pay restitution of over $63,000.

- A VA OIG investigation resulted in charges alleging that a West Roxbury VA Medical Center employee applied for and received two Paycheck Protection Program loans in the amount of $41,666 for a purported sole proprietorship by submitting fraudulent tax documents. The defendant allegedly spent the loan proceeds on personal expenses and subsequently submitted loan forgiveness applications that falsely claimed the entire loan amounts were spent on payroll. Based on this misrepresentation, the loans were forgiven. The defendant was charged in the District of Massachusetts with wire fraud.

Fiduciary Fraud

VA's Fiduciary Program was established to protect veterans and other beneficiaries who are unable to manage their financial affairs due to injury, disease, or age-related issues. Fiduciary fraud involves the theft of benefits by a VA-appointed fiduciary who is supposed to manage VA beneficiaries' finances in their best interests.

- A VA OIG investigation revealed that a former VA-appointed fiduciary misappropriated VA funds intended for her veteran son, who is permanently disabled. During her five years as a fiduciary, the defendant misappropriated VA funds and used them for her own benefit by transferring the money to her personal bank account, purchasing a vehicle that her son never used, paying bills, and taking trips even when her son was not living with her. The defendant was sentenced in the Southern District of Mississippi to 37 months' imprisonment, 36 months' supervised release, and restitution of approximately $276,000 after previously pleading guilty to misappropriation by fiduciary.

Healthcare Fraud

Healthcare fraud by VA-paid healthcare providers and vendors in the community is the intentional misrepresentation of information to gain payment, inconsistent with the type, scope, or nature of the treatment, service, or product provided.

- A multiagency investigation resulted in charges alleging that the Chief Executive Officer of a healthcare software company and others conspired to use telemarketers and medical providers to generate templated doctors' orders for medically unnecessary orthotic braces and other items in exchange for kickbacks. Medicare, VA, and other insurers were billed

more than $1 billion and subsequently paid more than $360 million based on these false and fraudulent claims. The loss to VA was more than $3 million. The defendant was found guilty following a four-week trial in the Southern District of Florida of conspiracy to commit healthcare fraud and wire fraud, conspiracy to pay and receive healthcare kickbacks, conspiracy to defraud the United States, and false statements in connection with health care matters. This investigation was conducted by VA OIG, the FBI, Department of Health and Human Services OIG, and Defense Criminal Investigative Service.

- A multiagency investigation revealed that the former Chief Financial Officer of a spinal device company entered into a kickback scheme to bribe surgeons to use the company's products in exchange for sham consulting fees. Six surgeons, including a former Bronx VA Medical Center physician and a non-VA surgeon who was paid through the Veterans Choice Program, previously entered into civil settlements in connection with this investigation in which they acknowledged receiving kickbacks from the defendant's company in exchange for using their surgical products. The former VA physician caused VA to purchase approximately $1 million in surgical products from the company. The former VA physician's settlement totaled $330,668, of which $103,785 was allocated to VA. The founder of the spinal device company who served as Chief Executive Officer was previously sentenced in connection with this investigation. The Chief Financial Officer, meanwhile, pleaded guilty in the District of Massachusetts to conspiracy to violate the Anti-Kickback Statute. This investigation was conducted by VA OIG, Department of Health and Human Services OIG, the FBI, and U.S. Postal Inspection Service.

- A VA OIG, Department of Health and Human Services OIG, and FBI investigation revealed that the owner of a marketing company worked with overseas call centers to exploit and pressure elderly Americans to provide their personal and health insurance information and to accept medically unnecessary braces. The defendant also paid sham telemedicine companies to obtain signed orders from doctors and nurse practitioners who never treated the patients and subsequently sold the orders to marketers and medical supply companies who then submitted claims to Medicare and CHAMPVA. This resulted in approximately $200 million in illegal durable medical equipment claims, including approximately $87,000 to CHAMPVA. The defendant was sentenced in the Middle District of Florida to 196 months' imprisonment and 36 months' supervised release and

was order to pay restitution of approximately $110.7 million and to forfeit approximately $17 million in assets after previously being found guilty at trial.

Workers Compensation Benefits Program Fraud

Federal workers' compensation programs, administered by the Office of Workers' Compensation Programs (OWCP) at the U.S. Department of Labor, provide medical care, wage replacement, and rehabilitation benefits to employees injured or made ill due to their job duties. OWCP fraud involves when federal employees intentionally submit false information or conceal facts to obtain workers' compensation benefits from the U.S. Department of Labor.

- A VA OIG investigation revealed that beginning in December 2018, a former Little Rock VA Medical Center nurse began receiving OWCP benefits after claiming to suffer from Post-Traumatic Stress Disorder and other mental issues stemming from her VA employment. The defendant subsequently obtained an advanced nursing degree which required her to complete 548 hours of clinical rotations in direct patient care. The defendant also opened two healthcare practices in Texas, applied to numerous healthcare related jobs, and worked as a temporary assignment nurse for multiple healthcare companies. The defendant failed to report some of these employment activities and misrepresented her involvement in others to OWCP. While receiving OWCP benefits, the defendant had numerous medical evaluations during which she was found to be totally incapacitated and unable to work, which OWCP relied upon to keep her in the program. The loss to VA was over $466,000. The defendant pleaded guilty in the Eastern District of Arkansas to making a false statement to obtain federal employee's compensation.

Current number of ongoing investigations: 1,004

Audits – Recently Issued Reports and Ongoing Projects

Review of VBA's Process for System Overrides (Published May 27, 2026)

The VA Office of Inspector General (OIG) sought to assess whether Veterans Benefits Administration (VBA) claims processors were appropriately overriding warnings and calculator results within the Veterans Benefits Management System for Rating (VBMS-R). The review focused on overrides processed between April 1 and September 30, 2024, and evaluated compliance with applicable laws, policies, and procedures.

The OIG found that while many overrides were properly executed, an estimated 9,900 were not warranted or lacked valid justification. These unwarranted override decisions occurred (1) because VBA did not conduct regular quality reviews that would provide feedback to processors, (2) because of the absence of clear guidance on what constitutes a valid override justification, and (3) because of limited functionality in two VBMS-R oversight tools. These deficiencies hindered VBA's ability to perform efficient oversight and could lead to quality reviewers examining cases that did not actually involve an override.

Actions by VBA claims processors caused about $67,200 in improper disability benefits payments and unnecessary exam costs, with the potential to affect future disability benefits payments or result in unnecessary exam costs. The OIG briefed VBA on the review's progress in March 2025, and VBA agreed with the sample review results. In December 2025, the OIG officially briefed VBA on the findings. Although VBA later took steps to enhance aspects of its override process by releasing a new reporting dashboard in February 2026, the OIG did not review or test it.

To address the issues the OIG identified and strengthen the VBMS-R override process, the OIG made five recommendations focused on improving guidance, oversight, and system functionality. VBA agreed to implement all five recommendations.

Inspection of Information Security at the VA Saginaw Healthcare System in Michigan (Published May 28, 2026)

The VA OIG's information security inspection program assesses whether VA facilities are meeting federal security requirements related to three high-risk control areas: configuration management, security management, and access. For this inspection, the OIG selected the VA Saginaw Healthcare System in Michigan and found deficiencies in all three areas.

Configuration management controls, which identify and manage security features for all hardware and software components of an information system, were deficient in system baseline configurations and vulnerability scanning and remediation and had unauthorized software hosted on the network.

Security management controls had one deficiency. Although a physical security issue had been previously identified, OIT staff had not developed a plan of action to address it.

Access controls had five deficiencies. The OIG found that the healthcare system staff did not implement required controls for privileged accounts, did not maintain audit logs for local databases, did not consistently verify and document identity of vendors or contractors before granting them access to systems, and did not ensure all networked medical devices were protected by access control lists for their virtual local area networks. The team also identified fire hazards in two telecommunications rooms. As a result, the facility risks unauthorized access, disruption, and destruction of critical information technology resources.

In response to the OIG's findings, healthcare system staff eliminated the identified fire hazards. To address the other deficiencies, the OIG made 10 recommendations to VA, and VA concurred.

Current number of ongoing audits and reviews: 60

Fraud Awareness Training

DATE	TOPIC AND LOCATION
5/12/2026	Fraud Awareness Training to VARO Huntington Employees
5/12/2026	Fraud Awareness Training to VARO Huntington Employees
5/13/2026	Fraud Awareness Training to VARO Huntington Employees
5/13/2026	Fraud Awareness Training to VARO Huntington Employees
5/14/2026	Fraud Awareness Training to VAMC Spokane Employees
5/20/2026	Corruption training for Contracting Personnel from VA Regional Procurement Office – Network Contracting Office
5/21/2026	Fraud Awareness Training to Chair of the VISN Disruptive Behavior Board
5/21/2026	Fraud Awareness Training to VISN 10 Leadership
5/28/2026	Fraud Awareness Training to VA Northern California Healthcare System Community Care Employees
5/28/2026	Fraud Awareness Training to VAMC San Diego Employees