



US DEPARTMENT OF VETERANS AFFAIRS OFFICE OF INSPECTOR GENERAL

INSPECTOR GENERAL'S FRAUD WATCH SEPTEMBER 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

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.

- On September 11, 2026, the owner of a marketing company was sentenced in the Middle District of Florida to five years' probation and was ordered to pay restitution of approximately \$14.3 million. A VA OIG, Health and Human Services (HHS) OIG, and FBI investigation revealed that the defendant exploited elderly victims through overseas call centers, obtained medically unnecessary braces, and paid sham telemedicine companies for fraudulent orders. The scheme resulted in \$37 million in illegal durable medical equipment claims to government healthcare programs.
- On September 11, 2026, in the District of Massachusetts, an eye practice and physician owner agreed to pay \$350,000 to resolve allegations they caused the submission of false claims in violation of the False Claims Act. An investigation by VA OIG, HHS OIG, Social Security Administration (SSA) OIG, IRS, US Postal Inspection Service, FBI, and the Department of Labor Employee Benefits Security Administration revealed that a mobile diagnostics company entered into improper agreements through which physicians

were paid bribes and kickbacks to order unnecessary transcranial doppler tests. Three former non-VA physicians and three executives of the mobile diagnostics company were charged, convicted, and sentenced in this case. Additionally, two practices and their physician owners entered into civil settlements in the District of Massachusetts. Government healthcare programs were billed over \$70 million through this scheme; of that amount, VA's Community Care Program was billed over \$400,000.

- On September 24, 2026, a defendant was found guilty on nine counts of healthcare fraud, violating the antikickback statute, and money laundering in the Northern District of Texas. The defendant paid beneficiaries to participate in a "study" and submit referrals, then billed federal programs for treatments not rendered. TRICARE paid \$17,075,566 and VA was billed for over \$89,000.
- On September 24, 2026, the owner of a homecare company pleaded guilty to healthcare fraud and conspiracy to commit money laundering in the Southern District of Ohio. The defendant used software to circumvent Medicaid location tracking and bill for services not rendered. Estimated loss to VA was \$494,192.
- On September 30, 2026, an acupuncture clinic owner agreed to a \$500,000 civil settlement in the Middle District of Florida to resolve allegations of billing VA's third-party administrators for services not rendered.

Fiduciary and Caregiver 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. VA caregiver fraud occurs when an individual misuses VA caregiver benefits, such as submitting false claims, billing for services not provided, or exploiting a veteran's benefits for personal gain.

- On September 4, 2026, a former home healthcare worker pleaded guilty in the Eastern District of Missouri to fraud in connection with an access device. A VA OIG, SSA OIG, and Missouri Department of Health and Senior Services investigation revealed that the defendant used a veteran's debit card to make unauthorized personal purchases while serving as the veteran's caregiver. The alleged loss to the veteran was approximately \$321,517.

Compensation Benefits Fraud

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

- On September 2, 2026, a veteran pleaded guilty in the Southern District of West Virginia to theft of government funds. The defendant fraudulently obtained \$354,813 in VA disability benefits by falsely claiming post-traumatic stress disorder from Army service.
- On September 15, 2026, a veteran pleaded guilty in the Western District of Missouri to theft of government funds. The defendant submitted false military discharge forms and fabricated medical records to obtain VA compensation, including a false ALS (amyotrophic lateral sclerosis) diagnosis. The estimated loss to VA was \$164,363.

COVID-19 Program Fraud

COVID-19 fraud involves the submission of fraudulent applications for payments under the Small Business Administration's (SBA) small business pandemic relief programs including the Payroll Protection Program and the Economic Injury 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.

- On September 1, 2026, a VA field examiner was indicted in the Southern District of Indiana on a charge of wire fraud. A VA OIG proactive investigation revealed the defendant allegedly defrauded the government by obtaining two SBA-backed Paycheck Protection Program (PPP) loans and two Economic Injury Disaster Loans (EIDL) for nonexistent businesses. The total loss to the government was estimated at \$101,433.
- On September 8, 2026, a VA medical center employee in Orlando, Florida, pleaded guilty to conspiracy to commit wire fraud in the Middle District of Florida. The defendant and spouse obtained PPP and EIDL loans for a nonexistent business and used the funds for personal expenses.

VA Loan Guaranty Fraud

VA provides home loan guaranty benefits and other housing-related programs to help veterans, servicemembers, and eligible surviving spouses become homeowners.

- On September 16, 2026, four defendants were indicted in the Northern District of Texas for conspiracy involving VA-backed mortgage fraud. The defendants falsified employment and income on loan applications. The potential loss to VA was \$541,971.

Pension Benefits Fraud

VA pension benefits are available to wartime veterans or their survivors who meet certain age or disability requirements and have limited income and net worth. VA pension beneficiaries who need help with daily activities or are housebound may be eligible for additional monetary payments. Veterans are targets of wide-ranging “pension poaching” schemes that attempt to steal their assets.

- On September 21, 2026, the ex-girlfriend of a veteran pleaded guilty in the Eastern District of Missouri to wire fraud and aggravated identity theft. The defendant redirected the veteran’s VA pension benefits to her own account. The potential loss to the veteran was \$91,211.

Service-Disabled Veteran-Owned Small Business Fraud

Service-disabled veteran-owned small business (SDVOSB) fraud involves ineligible individuals or companies improperly obtaining, performing, or benefiting from contracts reserved for small businesses owned and controlled by service-disabled veterans. Fraud schemes often involve misrepresenting ownership or control of a company or using an SDVOSB as a “pass-through” entity to secure government contracts for an otherwise ineligible business.

- On September 24, 2026, a defendant pleaded guilty in the Middle District of Pennsylvania to conspiracy to commit major fraud against the United States. A VA OIG, Defense Criminal Investigative Service, SBA OIG, and Army Criminal Investigation Division investigation revealed that the defendant conspired to fraudulently obtain a SDVOSB set-aside construction contract valued at approximately \$5.3 million at the Salem VA Medical Center. The defendant and co-conspirators allegedly concealed the use of another company's employees by placing them on the SDVOSB's payroll to falsely represent compliance with federal contract requirements.

Current ongoing investigations: 962

Current referrals: 646

Audits – Recently Issued Reports

Fiscal Year 2026 Risk Assessment of VA's Charge Card Programs

(September 29, 2026)

The VA Office of Inspector General (OIG) conducted a risk assessment of VA's three charge card programs, which cover purchase cards for supplies and services; travel cards for official travel expenses; and fleet cards for fuel, maintenance, and repair of government-owned and operated vehicles. The assessment is mandated by the Government Charge Card Abuse Prevention Act of 2012 to identify significant governance risks of illegal, improper, or erroneous purchases and other conditions that could affect program integrity. During the assessment period (April 1, 2025, through March 31, 2026), VA processed nearly \$6.5 billion in purchase, travel, and fleet card transactions.

In FY 2026, the OIG assessed the Purchase Card Program and the Travel Card Program as medium risk for illegal or improper purchases. Data analysis of transactions completed during the assessment period, the volume and value of spending, and OIG investigations and reviews identified patterns of card transactions that deviated from the Federal Acquisition Regulation and VA policies and procedures. In contrast, the Fleet Card Program was assessed as low risk.

The assessment also identified governance and control weaknesses that may warrant future OIG oversight. These include the absence of an agencywide process to consolidate monitoring results and verify corrective actions, recurring control deficiencies, approving officials with excessive workloads, and elevated risks associated with selected travel card transactions.

The team discussed the most recent risk ratings with VA senior leaders in August 2026. VA acknowledged the results and offered clarifying information for underlying factors that may have affected the purchase card programs during the assessment period.

Audit of Processing of Community Care Requests for Services

(September 24, 2026)

The VA Office of Inspector General (OIG) examined how quickly the Veterans Health Administration (VHA) reviewed and responded to community care providers' requests for additional services for veterans. These requests are submitted when a community provider determines that a veteran needs more or different care than VA initially approved.

Under the MISSION Act, veterans may receive care from community providers when eligibility criteria are met, such as long drive times, long wait times, or when VA facilities cannot provide the needed service. When community providers ask for more care, VHA must make a decision and notify both the veteran and provider within three business days.

The OIG reviewed nearly 2.6 million requests entered in the Consult Toolbox—the system VHA uses to manage documentation and workflows for VA and community care—between October 1, 2024, and January 31, 2026. The audit found that VA medical facilities often did not meet the required three-business-day standard. Only about 1.2 million requests were decided on time, and only about 1.4 million resulted in notifications to either the veteran or the provider. On average, notifications took about 12 days from the date of receipt—four times longer than required. This can adversely delay or disrupt veterans' care or result in unauthorized care.

The audit identified several barriers to meeting the three-business-day standard, including backlogs, staff shortages, manual processes, and multiple systems and steps needed to process requests. Inconsistent oversight of this process also led to inconsistent data entry and limited national data to support accountability.

VHA is undergoing major changes to its community care operations, including a new Office of Veterans Community Care and upcoming network contract updates. The OIG issued six recommendations to help VHA strengthen oversight and improve the timeliness of decisions so veterans receive the care they need without unnecessary delays.

[Review of the Major Construction Project for the New VA Medical Center in Louisville, Kentucky](#)

(September 24, 2026)

The VA Office of Inspector General (OIG) conducted this review to assess whether VA effectively governed the major medical center construction project in Louisville, Kentucky, specifically whether the project adhered to its initially authorized schedule and budget. Because federal law requires cost estimates but not schedules for authorization, the OIG evaluated schedule performance using Office of Management and Budget (OMB) Circular A-11 guidance, which calls for establishing and monitoring schedule baselines.

The Louisville project is at least 13 years behind its initial plan and is expected to be completed in November 2027. Its projected cost has grown from the 2007 draft business case estimate of \$418.8 million to more than \$1.1 billion. The OIG found that VA did not implement the required acquisition governance framework, did not provide Congress a complete project cost estimate until FY 2016, and did not submit a business case to OMB. Because VA could not demonstrate compliance with OMB's business case submission requirements, the OIG reported the over \$1 billion authorized for the project as a questioned cost.

Project delays and cost growth stemmed from ineffective planning, repeated scope changes, and failure to follow required acquisition and capital programming processes. VA did not effectively use advance planning funds, delayed initiating required environmental reviews, and used a

phased environmental assessment dependent on external agencies. Uncertainty, public concern, and outdated traffic studies ultimately required a full environmental impact statement, which extended the review. VA also did not consistently apply change management controls, did not update business case submissions as required, and understated total project costs by nearly \$160 million through unreported obligations and VA requested changes that are required before the new facility can open.

VA concurred with the OIG's seven recommendations to reinforce compliance with law, regulation, and policy.

Inspection of Information Security at the Lovell Federal Healthcare System in Illinois
(September 10, 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 control. For this inspection, the OIG selected the Lovell Federal Healthcare System in Illinois and found deficiencies in all three areas.

For configuration management, VA staff did not remediate multiple high- and critical-severity vulnerabilities within VA-defined time frames and had not developed required action plans. Also, some devices were not configured according to approved security baselines. These issues increase the risk of unauthorized access and operational disruption.

Security management had one deficiency: The healthcare system did not set access to network accounts to be automatically removed for temporary staff (specifically, student accounts) in line with VA and federal requirements. This could affect veteran care or the healthcare system's operations. It could also result in a breach of personal health information, which could lead to a financial and reputational loss to VA, an agency entrusted to protect sensitive veteran data. In February 2026, after the OIG team notified the facility of this issue, facility staff entered correct expiration dates for individuals. They also created standard operating procedures for establishing appropriate expiration dates for these temporary accounts.

Finally, regarding access control, the OIG found the Lovell Federal Healthcare System in Illinois can improve boundary protection, physical key management, emergency power, electrical grounding, and temporary records destruction. Inadequate access controls can result in unauthorized access to, modification of, or disclosure of sensitive data and programs and disruption of critical operations.

The OIG made seven recommendations to improve the healthcare system's information security, two of which were closed based on sufficient evidence provided by VA's Office of Information and Technology.

Review of Minor Construction and Nonrecurring Maintenance Projects at the Fayetteville VA Medical Center in Arkansas

(September 9, 2026)

The VA Office of Inspector General (OIG) examined how the Fayetteville VA Medical Center in Arkansas managed five minor construction and nonrecurring maintenance projects. These projects are intended to update facilities, improve safety, and ensure veterans receive care in modern, well-maintained buildings.

The review was prompted by a hotline complaint in March 2024. The OIG found that the medical center's contracting officer's representatives—employees responsible for overseeing the projects—did not consistently provide complete design requirements, prepare detailed statements of work, or keep records of design reviews. They also had not received needed training. These gaps contributed to delays and higher costs across all five projects.

Three of the projects were still under construction as of January 2026. Delays ranged from one year to more than seven years, and combined project costs grew from an originally approved \$34.5 million to about \$100 million. The OIG determined that most of the \$64.5 million increase could have been avoided through clearer communication and stronger project oversight. The delays also created additional costs for storing equipment, maintaining security, and providing laundry services.

The review confirmed that several awarded contracts exceeded the government's cost estimates and that delays on one project affected the medical center's ability to move forward with another. The OIG did not substantiate an allegation that the facility had more contract terminations than others in the region.

The OIG made four recommendations to help ensure timely completion of future projects, including better training and documentation practices. The medical center and regional leaders agreed with the findings. The OIG closed recommendation 1 and will monitor corrective actions and close the others once sufficient evidence of improvement is provided.

Review of Supply Chain Management at the VA Augusta Health Care System in Georgia

(September 2, 2026)

The VA Office of Inspector General (OIG) reviewed supply chain management practices at the VA Augusta Health Care System in Georgia. The review was initiated after the VA Secretary, a VISN leader, and a healthcare system leader raised concerns in March 2026 regarding persistent supply chain issues threatening operations and patient care. The review assessed whether facility leaders effectively oversaw supply chain operations and adhered to Veterans Health Administration policies from March through June 2026. The assessment focused on four areas

with recurring weaknesses: supply chain leadership, expendable supplies inventory, nonexpendable equipment inventory, and warehouse and distribution controls.

The OIG found that the facility did not consistently meet requirements for managing critical supplies and equipment. Oversight weaknesses increased the risk of missing equipment, expired products, and disruptions to patient care. These issues aligned with deficiencies previously identified by the OIG at VA facilities nationwide.

Notably, facility staff reported four operating room closures between October 2025 and February 2026—including one lasting 27 days—due to incomplete supply kits, expired supplies, and unreliable restocking processes. The OIG found significant inventory inaccuracies stemming from limited barcode scanning and handwritten logs. In a sample of 35 nonexpendable equipment items, five valued at about \$25,000 could not be located or accounted for.

The OIG also observed unsafe and disorganized storage conditions in the facility's warehouses and found more than 50 pallets of expired, excess, damaged, or obsolete supplies. The healthcare system awarded a \$3.2 million contract for an inventory management system but never fully installed or used it, and the OIG found system equipment abandoned in a warehouse.

The OIG made seven recommendations to improve the healthcare system's controls over supply chain management operations to support accountability and stewardship of taxpayer dollars.

[Review of Contracted Backup Services for the Veterans Crisis Line](#)

(September 1, 2026)

The Veterans Crisis Line (VCL) provides 24/7, confidential suicide prevention support to all veterans, regardless of whether they are enrolled in VA benefits or health care and regardless of discharge status. In this review, the VA OIG found that VA paid about \$11.2 million for VCL call responder backup services that were not provided. The review began after earlier OIG work raised concerns that VA may have paid for more than a year of contracted services that the contractor and subcontractor did not deliver.

The \$32.5 million contract required the contractor to route calls to VCL, answer at least 10 percent of VCL calls, and answer all VCL calls in the event of an emergency to help veterans at risk of suicide. When the original subcontractor stopped providing backup services, which represented about \$20.5 million (63 percent) of the total contract value, the contractor hired a replacement. However, that subcontractor could not begin work because it had not met federal security requirements and did not have enough staff. Furthermore, the contractor did not train call responders to meet contract terms. VA officials knew about these issues within months of the new subcontract starting but continued to approve payments for nearly a year.

Because services were not delivered, the OIG questioned the full \$11.2 million paid. This report highlights the need for stronger oversight of VA contracts and reinforces the importance of verifying security compliance before services begin.

The OIG recommended that the VA Office of General Counsel determine whether VA should recover the \$11.2 million paid for services not received and that VA evaluate and take any needed actions to make sure information system security requirements are accurately determined for contracts that involve sensitive information. VA concurred with the first recommendation and concurred in principle with the second.

Current ongoing audits and reviews: 36

Current ongoing healthcare hotline inspections and national reviews: 25

VA Office of Inspector General
INSPECTOR GENERAL'S FRAUD WATCH

Fraud Awareness Training

TOPIC	LOCATION	DATE
Fraud Awareness Brief	Harlingen, TX VAMC	9/1/2026
Fraud Awareness Brief	McAllen, TX CBOC	9/2/2026
Fraud Awareness Brief	Phoenix, AZ National Cemetery Administration	9/3/2026
Fraud Awareness Brief	Tucson, AZ VAMC	9/10/2026
Fraud Awareness Brief	Buffalo, NY VAMC	9/10/2026
Fraud Awareness Brief	San Francisco, CA VAMC senior leaders	9/10/2026
Fraud Awareness Brief	Syracuse, NY VAMC	9/16/2026
Fraud Awareness Brief	San Francisco, VA VAMC	9/17/2026
Fraud Awareness Brief	Bridgeville, PA National Cemetery	9/24/2026
Fraud Awareness Brief	Clarksburg, WV National Cemetery	9/24/2026
Fraud Awareness Brief	Salt Lake City, UT VAMC	9/28/2026
Fraud Awareness Brief	Buffalo, NY VAMC	9/30/2026