June 1, 2026

The Honorable John Joyce, M.D.
Chairman
Subcommittee on Oversight and Investigations
Committee on Energy and Commerce
U.S. House of Representatives
2125 Rayburn House Office Building
Washington, DC 20515

Dear Chairman Joyce:

Thank you for the opportunity to provide responses to additional questions for the record following the Subcommittee on Oversight and Investigations hearing titled "Common Schemes, Real Harm: Examining Fraud in Medicare and Medicaid," held on February 3, 2026.

Please find my responses below.

Respectfully submitted,

Jessica Tillipman

Jessica Tillipman
Associate Dean for Government Procurement Law Studies &
Government Contracts Advisory Council Distinguished Professorial Lecturer in Law
The George Washington University Law School
jtillipman@law.gwu.edu
202-994-2896

Responses to Additional Questions for the Record

From The Honorable Earl L. "Buddy" Carter (R-GA)

1. From a government contracts perspective, what vulnerabilities in Medicare supplier enrollment allow foreign-controlled shell companies to exploit the system, and how could enhanced disclosure requirements or penalties for nondisclosure prevent such fraud?

One of the most effective responses to foreign-controlled shell companies is to close the domestic corporate anonymity loophole. A foreign actor seeking to bill Medicare while concealing ownership and control need not use a foreign reporting company. An exempt U.S. entity will suffice.

From a government contracting perspective, the vulnerability is familiar. Federal procurement has long treated ownership, control, affiliation, and foreign influence as critical issues, not mere paperwork. Small-business eligibility, responsibility determinations, exclusion screening, and foreign ownership, control, or influence reviews all depend on the government's ability to identify who owns, controls, or benefits from an entity seeking federal funds. Medicare and Medicaid face the same structural problem in a different program setting. They rely on front-end enrollment disclosures and certifications, but verification remains fragmented and often occurs only after money has moved. Back-end enforcement, including audits, investigations, exclusions, civil and criminal enforcement, and whistleblower incentives, can identify misrepresentations after the fact, but it cannot fully compensate for ownership opacity at the point of entry.

As the Government Accountability Office (GAO) has explained:

> Federal programs face heightened fraud risks when beneficial ownership information is opaque for private companies that compete for government contracts or apply for grants or benefits. In addition to financial losses, impact from such fraud can be nonfinancial, such as threats to national security or public safety.[1]

Operation Gold Rush, the largest health care fraud case by loss amount that the Department of Justice (DOJ) has ever charged, illustrates this problem.[2] According to DOJ, the indictment alleges that a transnational criminal organization based in Russia and elsewhere purchased dozens of U.S. durable medical equipment companies that already had the ability to submit claims to Medicare and Medicare supplemental insurers. The organization allegedly paid foreign nationals and others to serve as nominee owners, created fictitious corporate records showing those nominees in control, and concealed that the companies were actually controlled by foreign-

[1] *See* U.S. Gov't Accountability Off., GAO-25-107143, Fraud in Federal Programs: FinCEN Should Take Steps to Improve the Ability of Inspectors General to Determine Beneficial Owners of Companies (2025), https://www.gao.gov/assets/gao-25-107143.pdf.

[2] *See* Press Release, U.S. Att'y's Office, E.D.N.Y., 11 Defendants Indicted in Multi-Billion Health Care Fraud Scheme, the Largest Case by Loss Amount Ever Charged by the Department of Justice (June 30, 2025), https://www.justice.gov/usao-edny/pr/11-defendants-indicted-multi-billion-health-care-fraud-scheme-largest-case-loss-amount.

based leadership. The same ownership fiction then migrated into the banking system. DOJ alleges that the organization armed nominee owners, many of whom were not lawfully present in the United States, with false documentation purporting to show that they beneficially owned and controlled the companies, allowing them to open accounts and disguise the true ownership and control of both the entities and the accounts. The organization allegedly submitted more than $10.6 billion in fraudulent Medicare claims. The Centers for Medicare & Medicaid Services (CMS) and the Department of Health and Human Services Office of Inspector General (HHS-OIG) prevented the organization from receiving the vast majority of that amount, but the scheme still resulted in approximately $41 million in Medicare payments and nearly $900 million in payments from Medicare supplemental insurers. DOJ further alleges that proceeds were siphoned through shell companies and overseas bank accounts in China, Singapore, Pakistan, Israel, and Turkey, and laundered through cryptocurrency. As of June 30, 2025, the government had seized approximately $27.7 million in fraud proceeds, subject to criminal forfeiture and civil forfeiture.

Operation Gold Rush shows why this is not simply an enrollment-form problem. In a scheme like this, the same concealed-control structure runs through billing, banking, and laundering, and makes the proceeds hard to recover once they move offshore. A congressional response focused only on foreign reporting companies would miss the gap Operation Gold Rush allegedly exploited: foreign control can be exercised through ordinary U.S. entities when domestic beneficial ownership reporting is unavailable.

Why CMS cannot solve ownership opacity alone

Two critical responses to foreign exploitation of Medicare and Medicaid, therefore, lie partly outside of CMS's ordinary enrollment process. The first is corporate transparency: ensuring that beneficial ownership information (BOI) is collected and available for verification before a supplier enrolls or begins billing.[3] The second is asset recovery: preserving the capacity to trace and reclaim proceeds once they move offshore.

Strengthening enrollment verification within CMS is critical, but CMS cannot, by itself, reach ownership concealed at the time of entity formation or proceeds that have already moved offshore. Those levers reside principally with Congress, the Treasury Department, and DOJ, and they can be strengthened without waiting for CMS to reengineer its systems. In practice, the risk is not limited to a false enrollment application. It can also include nominee owners, shell entities, or transactions involving already-enrolled suppliers that conceal who actually owns, controls, or benefits from billing privileges.[4]

---

[3] *See* U.S. Gov't Accountability Off., GAO-25-107143*,* Fraud in Federal Programs: FinCEN Should Take Steps to Improve the Ability of Inspectors General to Determine Beneficial Owners of Companies (2025), https://www.gao.gov/assets/gao-25-107143.pdf ("With this information and such relationships hidden, bad actors may target federal programs—and by extension, taxpayer dollars—to improperly receive federal contracts or fraudulently access federal benefits").

[4] *See* Press Release, U.S. Att'y's Office, S.D. Fla., National Health Care Fraud Enforcement Action Results in 193 Defendants Charged and Over $2.75 Billion in False Claims (June 27, 2024), https://www.justice.gov/usao-sdfl/pr/national-health-care-fraud-enforcement-action-results-193-defendants-charged-and-over (describing allegations that a defendant arranged the purchase of an already-

The exposure this Subcommittee is examining sits in the gap between general corporate transparency policy and the ownership-verification tools, data access, and enforcement capacity available in Medicare and Medicaid. Closing that gap would strengthen anti-fraud efforts across federal programs because federal agencies often rely on overlapping provider, supplier, and contractor populations.

Enforcement actions like Operation Gold Rush point to a deeper structural problem: there is still no single, reliable mechanism for CMS to determine, on a cross-program basis, who ultimately owns or controls a supplier at enrollment, at a change of ownership, at revalidation, and while billing continues. Verifying ownership spans four stages: state business formation, federal beneficial ownership reporting where applicable, bank account opening, and health program enrollment. Each has its own checks, but no single institution is responsible for keeping BOI accurate, current, and consistent across them. The result is a system that relies on after-the-fact investigation to reconstruct ownership that was never verified at the ultimate beneficial owner level or shared in a form CMS could use for enrollment and billing decisions.

The narrowed CTA/BOI backstop

A company is formed through a state filing office, and the process is largely ministerial. Formation documents require basic identifying information, including the company name, registered agent information, and an authorized signature, and may require additional address or contact information.[5] They generally do not require disclosure of the company's beneficial owners. GAO identified this weakness *two decades ago*, finding that most states collected limited ownership information and that state officials generally reviewed filings for required fields rather than verifying the identities of company officials.[6] More recently, GAO found that state ownership and control filings continue to vary and may identify officers, directors, managers, or members who are not the individuals who actually own or substantially control the entity.[7] Nominee and shelf company services can compound the problem by placing other names in the record, so that even the names on file need not belong to the people who actually control the entity.[8]

Congress addressed this gap directly when it enacted the Corporate Transparency Act (CTA), which requires covered "reporting companies" to report their beneficial owners to the Financial

enrolled Medicare DME supplier and installed a nominee as the sole listed officer to conceal the company's beneficial owners).

[5] *See* U.S. Gov't Accountability Off., GAO-06-376, Company Formations: Minimal Ownership Information Is Collected and Available (2006), https://www.gao.gov/assets/gao-06-376.pdf.

[6] *Id.*

[7] *See* U.S. Gov't Accountability Off., GAO-26-107967, Corporate Transparency: Treasury Should Address Gaps in Ownership Information Resulting from Expanded Exemptions (2026), https://www.gao.gov/products/gao-26-107967.

[8] *See* U.S. Gov't Accountability Off., GAO-06-376, Company Formations: Minimal Ownership Information Is Collected and Available (2006), https://www.gao.gov/assets/gao-06-376.pdf; Fin. Action Task Force & Egmont Grp., Concealment of Beneficial Ownership (July 2018), https://egmontgroup.org/wp-content/uploads/2021/09/2018_Concealment_of_Beneficial_Ownership.pdf.

Crimes Enforcement Network (FinCEN).[9] After a period of regulatory and judicial uncertainty, FinCEN's March 2025 interim final rule removed BOI reporting obligations for entities created in the United States and for U.S. persons, narrowing the CTA reporting requirement to foreign entities registered to do business in a U.S. State or Tribal jurisdiction that are not otherwise exempt.[10] Pending legislation would codify aspects of this narrowed approach and go further by requiring FinCEN to delete certain previously collected BOI within 90 days, including information relating to U.S. persons and entities outside the revised foreign-focused reporting regime.[11]

To be clear, there were genuine concerns about how the CTA was calibrated, including its compliance burden on small businesses. The CTA already exempted twenty-three categories of entities before 2025, largely because they were otherwise regulated or already reported similar information to a government authority. But exempting the ordinary domestic LLC and corporation, the population the statute was drafted to reach, moves beyond calibration and into a loophole so large that it effectively nullifies the statute's central requirement for the U.S. entities that make up almost all of the corporate landscape. Indeed, GAO recently found that the expanded exemption applies to over 99 percent of entities that previously were required to report.[12] GAO recommended that the Treasury Department identify potential actions to address risks posed by the domestic reporting company and U.S.-person exemptions, and to provide Congress and law enforcement with highly useful ownership information. Treasury, with concurrence from DOJ and the Department of Homeland Security, disagreed, determining that, despite the risks of illicit finance, requiring domestic companies to report beneficial ownership information is not sufficiently useful to justify the burden.

This creates a reporting gap that is available precisely to the individuals and entities most relevant to your question. A foreign actor who wants to bill Medicare while concealing control need not route the scheme through a foreign reporting company. Instead, that actor can form or acquire an ordinary U.S. company, which is now exempt from CTA reporting, and operate through it. The same gap is available to purely domestic bad actors, so a response aimed only at foreign actors would miss the broader vulnerability. The consequence is that, just as CMS is trying to strengthen ownership transparency in its own enrollment systems, the federal corporate transparency regime has been narrowed, weakening the federal backstop for identifying who truly owns or controls ordinary U.S. entities.

Limits of FinCEN access and financial institution CDD

[9] *See* 31 U.S.C. § 5336.
[10] *See* Fin. Crimes Enf't Network, FinCEN Removes Beneficial Ownership Reporting Requirements for U.S. Companies and U.S. Persons, Sets New Deadlines for Foreign Companies (Mar. 21, 2025), https://www.fincen.gov/news/news-releases/fincen-removes-beneficial-ownership-reporting-requirements-us-companies-and-us.
[11] *See* Senate Bill Takes Aim at Corporate Transparency Act, Thomson Reuters Checkpoint (May 6, 2026), https://tax.thomsonreuters.com/news/senate-bill-takes-aim-at-corporate-transparency-act/.
[12] *See* U.S. Gov't Accountability Off., GAO-26-107967, Corporate Transparency: Treasury Should Address Gaps in Ownership Information Resulting from Expanded Exemptions (2026), https://www.gao.gov/products/gao-26-107967.

Access limits compound the reporting gap. Specifically, FinCEN's BOI database is not designed as a routine enrollment-screening tool for CMS or state Medicaid administrators. Under FinCEN's access rule, BOI may be disclosed to federal agencies engaged in national security, intelligence, or law-enforcement activities, and to state, local, and tribal law-enforcement agencies only with a court order authorizing the request in a criminal or civil investigation.[13] Financial institutions may obtain it only for customer due diligence, and only with the reporting company's consent.[14] HHS-OIG and federal prosecutors can therefore seek this information when acting in an investigative or enforcement capacity, but CMS enrollment staff and state Medicaid agencies acting in an ordinary program-administration capacity do not fit neatly within the authorized-recipient categories. GAO has further reported that FinCEN has not yet specified bulk-download capabilities for the registry, even though inspectors general said such a capability could facilitate matching the data against other sources.[15] The result is that even the remaining federal source of reported ownership information is difficult to use at the enrollment stage, where it could help prevent fraud before payment.

That places a greater strain on covered financial institutions, which were never designed to bear this burden alone. Banks and other financial institutions are often described as gatekeepers, and FinCEN's customer due diligence rule under the Bank Secrecy Act requires covered financial institutions to maintain procedures reasonably designed to identify and verify the beneficial owners of legal-entity customers.[16] But that safeguard is only a partial backstop. It operates downstream, after a state has already created the entity, and it still relies substantially on customer-provided information.[17] GAO has found that it does not capture beneficial ownership at the time of formation, and not all transactions pass through a covered financial institution.[18] In February 2026, FinCEN narrowed that safeguard by granting exceptive relief from the requirement to identify and verify beneficial owners each time an existing legal-entity customer opens a new account, while preserving initial account-opening checks and risk-based updating.[19] Customer due diligence remains a meaningful obligation, but it cannot substitute for verified ownership information collected at formation and enrollment.

Enrollment, disclosure duties, and penalties

---

[13] *See* 31 C.F.R. § 1010.955(b)(1), (b)(2). *See also* Fact Sheet: Beneficial Ownership Information Access and Safeguards Final Rule, Fin. Crimes Enf't Network (Dec. 20, 2023), https://www.fincen.gov/news/news-releases/fact-sheet-beneficial-ownership-information-access-and-safeguards-final-rule.
[14] *See* 31 C.F.R. § 1010.955(b)(4)(i).
[15] *See* U.S. Gov't Accountability Off., GAO-25-107143, Fraud in Federal Programs: FinCEN Should Take Steps to Improve the Ability of Inspectors General to Determine Beneficial Owners of Companies (2025), https://www.gao.gov/assets/gao-25-107143.pdf.
[16] *See* 31 C.F.R. § 1010.230.
[17] *Id.*
[18] *See* U.S. Gov't Accountability Off., GAO-26-107967, Corporate Transparency: Treasury Should Address Gaps in Ownership Information Resulting from Expanded Exemptions (2026), https://www.gao.gov/products/gao-26-107967.
[19] *See* Exceptive Relief from Requirement to Identify and Verify Beneficial Owners at Each Account Opening (FIN-2026-R001), FinCEN (Feb. 13, 2026), https://www.fincen.gov/system/files/2026-02/FinCEN-Order-CCDExceptiveRelief.pdf.

Enrollment is the program's gatekeeping step, the point at which Medicare decides whether to grant billing privileges. Although CMS requests ownership and management-control information and applies risk-based screening, the system remains fundamentally application-driven rather than built on independent verification of BOI. That is where ownership opacity can pose a billing risk. Nominee ownership, the mechanism alleged in Operation Gold Rush, is the clearest illustration: the listed owner may exist, sign documents, and appear in the record, while the individuals who control the company remain concealed.

CMS has tools to address certain high-risk enrollment patterns, including screening, revalidation, revocation, payment suspension, and temporary enrollment moratoria for certain provider types.[20] Those safeguards are useful, but they are also piecemeal because the underlying transparency problem they must navigate remains a challenge.[21] Blunt interventions, including moratoria or broad enhanced-oversight periods, may slow some abusive entry strategies, but they do not solve the underlying ownership transparency problem and can impose significant costs on legitimate providers and beneficiaries.[22]

Your question asks specifically about enhanced disclosure and penalties for nondisclosure. Both are worth pursuing, but the order matters. Penalties work only when there is a clear duty to disclose the information at issue. Medicare and Medicaid already impose ownership and control disclosure obligations,[23] and false or misleading enrollment information can support denial or revocation of enrollment, payment suspension, overpayment recovery, civil monetary penalties, exclusion, and, where the facts support it, criminal exposure under false statement, health care fraud, or money laundering statutes.[24] The remaining gap is not simply a lack of penalties. The current law does not consistently require, verify, and share ultimate beneficial ownership information early enough to prevent concealed-control structures from becoming billing entities.

The concern about foreign-controlled shell companies is well-founded. But the loopholes these actors exploit are weaknesses in U.S. corporate transparency and program integrity laws. The anonymity begins at home, so a response calibrated only to foreign actors misses the domestic deficiencies that enable concealment and leaves the system vulnerable to domestic bad actors as well. Closing those domestic loopholes is necessary to address bad actors, whether they are operating from the United States or abroad.

---

[20] *See* 42 C.F.R. §§ 405.371, 424.515, 424.518, 424.527, 424.535, 424.570.
[21] *See* U.S. Dep't of Health & Hum. Servs., Off. of Inspector Gen., OEI-04-11-00591, Medicare: Vulnerabilities Related to Provider Enrollment and Ownership Disclosure (2016); U.S. Gov't Accountability Off., GAO-25-107143, Fraud in Federal Programs: FinCEN Should Take Steps to Improve the Ability of Inspectors General to Determine Beneficial Owners of Companies (2025).
[22] *See* 42 C.F.R. § 424.570; Medicare, Medicaid, and Children's Health Insurance Programs: Announcement of Nationwide Temporary Moratorium on Enrollment of Hospices, 91 Fed. Reg. 27,946 (May 15, 2026); Medicare, Medicaid, and Children's Health Insurance Programs: Announcement of Nationwide Temporary Moratoria on Enrollment of Home Health Agencies (HHAs), 91 Fed. Reg. 27,954 (May 15, 2026).
[23] *See* 42 U.S.C. § 1320a-3, 42 C.F.R. §§ § 420.206 (Medicare), 455.104, 455.105, 455.106 (Medicaid).
[24] *See* 42 C.F.R. §§ 424.530(a)(4), 424.535(a)(4), 405.371; 42 U.S.C. §§ 1320a-7, 1320a-7a; 18 U.S.C. §§ 1035, 1347, 1956.

Of course, none of this makes ownership transparency a cure-all. A reporting requirement is self-reported, and a determined actor can falsify ownership information, as the allegations in Operation Gold Rush illustrate. But a centralized, penalty-backed registry still adds leverage: it would create a single ownership record that program-integrity officials could cross-check against enrollment and banking filings, flagging discrepancies and false statements that carry penalties of their own.

Asset recovery after proceeds move offshore

The second structural weakness is back-end recovery. Even with stronger front-end controls, some fraud will be detected only after payment, and proceeds that have already moved offshore must still be traced and recovered. Recovery depends on specialized capacity: financial intelligence, international cooperation, forfeiture tools, and the ability to connect Medicare-paid funds to accounts, entities, and individuals across jurisdictions.

A recent enforcement action is illustrative of this challenge. As part of the 2025 National Health Care Fraud Takedown, the Department of Justice charged five defendants, including two owners and executives of Pakistani marketing organizations, in connection with an alleged $703 million scheme involving durable medical equipment companies and laboratories.[25] The defendants allegedly caused false claims to be submitted to Medicare and Medicare Advantage plans for products and services that beneficiaries did not request, need, receive, or consent to receive. The scheme allegedly operated through facially legitimate billing entities whose actual ownership and control were concealed behind nominees. DOJ also alleged that certain defendants conspired to conceal and launder proceeds from bank accounts they controlled in the United States to overseas accounts. According to DOJ, Medicare and Medicare Advantage plans paid approximately $418 million on claims connected to the alleged scheme, while the government seized approximately $44.7 million from related bank accounts. Those allegations do not establish the final recoverable amount, but they illustrate the practical difficulty of clawing back proceeds of fraud once they have moved through domestic and foreign accounts.

In early 2025, DOJ redirected parts of its money laundering and asset recovery infrastructure toward enforcement against cartels and transnational criminal organizations. Specifically, the Attorney General directed the Criminal Division's Money Laundering and Asset Recovery Section (MLARS) to prioritize investigations, prosecutions, and asset forfeiture actions targeting cartels and transnational criminal organizations, and disbanded Task Force KleptoCapture, the Department's Kleptocracy Team, and the Kleptocracy Asset Recovery Initiative.[26] To be clear, those disbanded initiatives targeted foreign official corruption, sanctions evasion, and related money laundering, not health care fraud forfeiture. MLARS retains authority to pursue forfeiture in health care fraud matters, and the underlying legal authorities to recover fraud proceeds

[25] *See* U.S. Dep't of Just., Off. of Pub. Affs., *National Health Care Fraud Takedown Results in 324 Defendants Charged in Connection with Over $14.6 Billion in Alleged Fraud* (June 30, 2025), https://www.justice.gov/opa/pr/national-health-care-fraud-takedown-results-324-defendants-charged-connection-over-146.
[26] *See* Memorandum on Total Elimination of Cartels and Transnational Criminal Organizations (Feb. 5, 2025), https://www.justice.gov/ag/media/1388546/dl?inline.

remain intact. The narrower concern is capacity. Complex offshore health care fraud schemes also require cross-border asset tracing, financial intelligence, and coordination with foreign authorities. Redirecting specialized asset recovery resources may therefore create a foreseeable capacity risk in large health care fraud matters involving foreign actors, nominee entities, offshore accounts, and layered laundering structures.

Conclusion and recommendations

To conclude, the solution is not simply to invent new penalties, but to align existing tools with ownership transparency: making complete and accurate beneficial ownership disclosure, including disclosure of foreign beneficial owners, an explicit and enforceable condition of enrollment and continued billing. Unlike many Medicare and Medicaid integrity reforms, which require better execution of existing authority rather than new legislation, this requires Congress to act. Congress should restore a calibrated domestic beneficial ownership reporting requirement and consider the feasibility of a defined, purpose-limited pathway for appropriate federal and state health program-integrity officials to use reported ownership information for enrollment and payment-integrity screening, subject to privacy, cybersecurity, correction, audit, and due process safeguards. Congress should also preserve the capacity to trace and recover fraud proceeds moved through cross-border structures by funding dedicated cross-border asset tracing and recovery capacity, preserving forfeiture and international cooperation authorities, and requiring regular reporting on cross-border recovery activity.

The Honorable Debbie Dingell (D-MI)

1. How can we strengthen the integrity of Medicare and Medicaid without jeopardizing access to care for beneficiaries and overburdening already overworked providers?

Integrity controls are critical to preventing fraud, but poorly designed controls can cost access and provider time without a corresponding reduction in fraud. The goal is better targeting rather than greater enforcement across the board: classify the conduct accurately, match the tool to the risk, deliberately choose between pre-payment and post-payment review, and monitor beneficiary access whenever a broad control is put in place, so that most providers, *who are not engaged in fraud*, are not buried under unnecessary administrative burden.

First, as I noted in my written testimony, classification of the conduct is foundational.[27] Fraud is a legal conclusion, distinct from improper payments, waste, abuse, and administrative error.[28]

---

[27] *See* Jessica Tillipman, *Common Schemes, Real Harm: Examining Fraud in Medicare and Medicaid*, Hearing Before the Subcomm. on Oversight & Investigations of the H. Comm. on Energy & Commerce, 119th Cong. (Feb. 3, 2026) (statement of Jessica Tillipman, Government Contracts Advisory Council Distinguished Professorial Lecturer in Government Contracts Law, Practice & Policy, George Washington University Law School), https://www.congress.gov/119/meeting/house/118917/witnesses/HHRG-119-IF02-Wstate-TillipmanJDJ-20260203.pdf.

[28] *See* Ctrs. for Medicare & Medicaid Servs., Fiscal Year 2025 Improper Payments Fact Sheet (Jan. 15, 2026), https://www.cms.gov/newsroom/fact-sheets/fiscal-year-2025-improper-payments-fact-sheet (stating that improper payment measurement is not a measure of fraud and that not all improper payments

Conflating fraud with these other categories distorts the picture, misdirects scarce program integrity resources, and imposes an unnecessary burden on Medicare, Medicaid, and compliant providers. Accurate classification is itself a form of burden control: treating a documentation or billing error as fraud can invite an enforcement response that is harsher than the conduct warrants. Claims about provider burden and beneficiary access should be tested empirically against appeals and reversal rates, claim delays, provider participation, and access indicators, rather than accepted or dismissed categorically.

Second, the selection of the appropriate response tool must be risk-based. A well-designed compliance program does not apply uniform scrutiny to every transaction. It identifies risks, prioritizes them, and focuses resources where exposure is greatest. The same logic applies to program integrity. Higher-risk providers, services, and transactions warrant more scrutiny and resources, while lower-risk activity warrants less.[29] Treating low-risk claims, providers, and services as equally suspect under-resources the actual risks, imposes unnecessary friction on compliant providers, and overuses the most intensive tools, which can itself threaten access by pushing legitimate providers out or destabilizing those that serve high-need populations. The available responses range from provider education and targeted claims screening before payment to audit, recoupment, payment suspension, revocation, and referral to DOJ, all proportionate to the seriousness of the conduct. They are not interchangeable—each has a different predicate, evidentiary threshold, and procedural consequence, so the choice among them should depend on what the facts support.

Third, timing is critical. Some claims, enrollments, and payments cannot be fully verified before action is taken. Emergency and pandemic-era health program flexibilities illustrate the problem: when continuity of care requires rapid payment or enrollment, front-end verification may be deliberately lighter.[30] The question is whether the government then routes those transactions into heightened, risk-based post-payment or post-enrollment review, or simply accepts the residual risk.

The same discipline should apply to enrollment moratoria. Moratoria may be lawful and, in extreme cases, necessary where there is evidence of a serious risk of fraud. But they are blunt instruments. They restrict lawful market entry rather than verify ownership, billing legitimacy, or medical necessity, and they often signal that more precise front-end controls were not built in time. Used too readily, moratoria shift the cost of program integrity failure onto legitimate providers and beneficiaries. They should therefore remain temporary emergency measures, not routine program integrity tools: time-limited, evidence-based, access-monitored, and subject to meaningful exceptions where beneficiary access would otherwise be impaired.

---

are attributable to fraud or abuse); U.S. Gov't Accountability Off., GAO-24-106608, Improper Payments and Fraud: How They Are Related but Different (2023), https://www.gao.gov/products/gao-24-106608 (explaining that improper payments and fraud are related but not interchangeable).

[29] *See* 42 C.F.R. § 424.518(a) (requiring Medicare contractors to screen enrollment transactions based on CMS's risk assessment and assignment to limited, moderate, or high screening levels).

[30] *See* U.S. Gov't Accountability Off., GAO-23-105494, Medicare: CMS Needs to Address Risks Posed by Provider Enrollment Waivers and Flexibilities (2022), https://www.gao.gov/products/gao-23-105494.

Technology is one of the most promising tools available for Medicare and Medicaid program integrity, but it cannot substitute for human judgment. Claims analytics, network analysis, identity matching, and AI-enabled anomaly detection can identify suspicious billing patterns, link related entities, flag ownership inconsistencies, and prioritize high-risk providers for review far faster than manual processes alone. CMS already uses claims analytics to identify anomalous billing, prioritize leads, and support administrative actions. GAO recently reported that CMS estimated its administrative actions prevented $11.9 billion in potentially fraudulent Medicare payments from fiscal years 2022 through 2024, and described a catheter-billing scheme in which data analytics helped identify 15 providers that allegedly attempted to bill Medicare for more than $4 billion for items that were not medically necessary or not supplied.[31] But that example also shows the proper role of technology: analytics-generated leads for review, suspension, revocation, or referral. They did not replace the legal and clinical judgment required to deny payment, remove a provider, or pursue enforcement.

That leads to another issue: data quality. Technology can help identify fraud only when the underlying data are accurate, complete, linked, current, and usable. If enrollment, exclusion, billing, licensure, ownership, or claims data are inaccurate, fragmented, stale, unverified, or not machine-readable, analytic tools will reproduce and may magnify those limitations. That creates two risks at once: sophisticated fraud may be missed, while legitimate providers may be flagged based on incomplete or misleading records. Technology can flag anomalies, compare records, and prioritize review, but it cannot correct poor data architecture or provide information that the system never collected. For that reason, better analytics must be paired with better data governance, clear evidentiary thresholds, and human review before a red flag becomes a payment denial, suspension, revocation, or referral.

Proportionality also governs what happens after a red flag is raised. Detection identifies a concern; acting on it is a separate decision, and the appropriate response depends on the risk's severity, immediacy, and the strength of the evidence. Notice and an opportunity to respond should be the baseline, except where immediate action is justified to protect program funds or beneficiaries, and a post-action process is provided. Payment suspension, claim denial, and enrollment revocation do not use identical procedures or timing, and some protections properly follow the action rather than precede it. The more severe and immediate the consequence for a provider or beneficiary, the stronger the case for prompt, meaningful review and a clear path to correction.

---

2. How can the federal government support state and federal agencies responsible for protecting Medicaid to better address fraud and abuse in the program?

One essential form of federal support is to protect the capacity, continuity, independence, and data infrastructure of the institutions that oversee Medicaid. Medicaid fraud enforcement depends on a shared federal-state architecture: state Medicaid Fraud Control Units (MFCUs)

[31] *See* U.S. Gov't Accountability Off., GAO-26-107799, Medicare: CMS's Use of Data Analytics to Identify and Prevent Fraud (2026), https://www.gao.gov/products/gao-26-107799.

investigate and prosecute provider fraud and patient abuse or neglect; state Medicaid agencies administer the program and operate internal program integrity controls; CMS sets federal requirements and supports state oversight; HHS-OIG funds, oversees, certifies, and supports the MFCU network; and DOJ brings federal civil and criminal enforcement where the facts warrant it. Federal support should strengthen that architecture in four practical ways: stable funding, protected oversight independence, routine data sharing, and state-facing technical capacity, especially as more Medicaid spending flows through managed care.[32]

Beginning with state enforcement, MFCUs operate across 53 jurisdictions, are usually housed in offices of state attorneys general, and must be separate and distinct from the state Medicaid agencies that run the program.[33] In FY 2025, MFCUs recovered nearly $2 billion, returned $4.64 for every dollar spent, obtained 1,185 convictions, and received 5,991 fraud referrals from managed care entities.[34] Federal support that strengthens this infrastructure is among the most direct ways to help states address Medicaid fraud and abuse.

That state infrastructure also depends on federal capacity. HHS-OIG annually recertifies MFCUs, assesses their compliance with federal requirements, and administers the federal grant funding that supports much of their work.[35] Yet HHS-OIG's FY 2027 Congressional Budget Justification warns that current funding is insufficient to provide the level of enforcement and oversight needed.[36] The office projects its lowest staffing level in two decades, even as health care fraud schemes become more complex and technologically sophisticated. It estimates that additional resources would allow it to address 400 to 450 viable fraud cases and more than 5,000 hotline complaints each year, and that without those resources, at least 1,200 viable fraud cases will go unpursued over the next three years. In that context, capacity is not a secondary management issue, but a constraint on Medicaid fraud enforcement itself.

Independence and continuity are also part of that capacity. In January 2025, at least 17 inspectors general were removed without the 30-day advance notice to Congress specified in the Inspector General Act, and the HHS Inspector General was among them.[37] HHS-OIG then operated under acting leadership for roughly eleven months, until the Senate confirmed a new Inspector General in December 2025. Federal support for Medicaid integrity, therefore, should include stable

---

[32] *See* Medicaid & CHIP Payment & Access Comm'n, Managed Care, https://www.macpac.gov/topic/managed-care/ ("More than half of federal and state Medicaid spending is on managed care. The proportion continues to grow each year.").
[33] *See* Medicaid Fraud Control Units, Office of Inspector Gen., U.S. Dep't of Health & Hum. Servs., https://oig.hhs.gov/fraud/medicaid-fraud-control-units-mfcu/.
[34] *See* Medicaid Fraud Control Units Fiscal Year 2025 Annual Report, Office of Inspector Gen., U.S. Dep't of Health & Hum. Servs. (2026), https://oig.hhs.gov/reports/all/2026/medicaid-fraud-control-units-annual-report-fiscal-year-2025/.
[35] *See* Medicaid Fraud Control Units, Office of Inspector Gen., U.S. Dep't of Health & Hum. Servs., https://oig.hhs.gov/fraud/medicaid-fraud-control-units-mfcu/.
[36] *See* Office of Inspector Gen., U.S. Dep't of Health & Hum. Servs., Fiscal Year 2027 Congressional Budget Justification (2026), https://oig.hhs.gov/about-oig/oig-budget/.
[37] *See* 5 U.S.C. §§ 401–424. *See also* Jack Goldsmith, *Trump Fired 17 Inspectors General—Was It Legal?,* Lawfare (Jan. 27, 2025), https://www.lawfaremedia.org/article/trump-fired-17-inspectors-general-was-it-legal.

funding for MFCUs and HHS-OIG, protection of inspector general independence, and continuity of leadership responsible for overseeing these programs.

The shared oversight infrastructure also experienced disruption. The Council of the Inspectors General on Integrity and Efficiency (CIGIE), the body that supports coordination across the inspector general community, reportedly faced a funding cutoff after the Office of Management and Budget (OMB) did not apportion certain funds, resulting in staff furloughs and disruptions to shared oversight functions, including public access to Oversight.gov—a critical transparency resource.[38] Funding was released only after senior Republicans, including the Republican chairs of the Senate Judiciary and Appropriations Committees, pressed the issue.[39] Fraud oversight depends not only on individual inspectors general but also on the shared systems that allow their work to be coordinated, searched, and made public. Those systems should not depend on ad hoc funding releases after congressional intervention.

Recent enforcement announcements should be understood against this backdrop. Additional resources and attention to fraud are welcome, and FY 2025 produced record False Claims Act recoveries and the largest health care fraud takedown in DOJ history.[40] But large recoveries and takedowns often reflect years of investigative work, referrals, and analysis developed well before the announcement, and they do not, by themselves, sustain the routine capacity that prevents losses. The same caution applies to new structures. A new National Fraud Enforcement Division[41] may help if it adds capacity, preserves expertise, and improves coordination with

---

[38] *See* Meryl Kornfield, *Trump Administration Moves to Defund Inspector General Watchdog Group*, WASH. POST (Sep. 30, 2025), https://www.washingtonpost.com/politics/2025/09/30/inspector-general-watchdog-cuts-trump/; Natalie Alms, *Judiciary Democrats Launch Watchdog Website Amid Withheld Funding from Inspector General Group*, NEXTGOV/FCW (Oct. 16, 2025), https://www.nextgov.com/digitalgovernment/2025/10/judiciary-democrats-launch-watchdog-website-amid-withheld-funding-inspector-general-group/408861/.

[39] *See* Sean Michael Newhouse & Natalie Alms, *Trump Administration Resumes Funding for Inspectors General Hub After Previously Blocking It*, GOV'T EXEC. (Nov. 18, 2025), https://www.govexec.com/oversight/2025/11/trump-administration-resumes-funding-inspectors-general-hub-after-previously-blocking-it/409615/; Meryl Kornfield & Hannah Natanson, *Trump Administration Revives Some Funding for IG Group*, WASH. POST (Nov. 18, 2025), https://www.washingtonpost.com/politics/2025/11/18/trump-administration-revives-some-funding-ig-group/; Press Release, U.S. S. Comm. Judiciary, Grassley, Collins Urge OMB to Release Appropriated Inspector General Funds (Sept. 30, 2025), https://www.judiciary.senate.gov/press/rep/releases/grassley-collins-urge-omb-to-release-appropriated-inspector-general-funds; Press Release, U.S. S. Comm. on Judiciary, OMB Releases Nearly $4.3 Million for CIGIE Following Push by Grassley, Collins (Nov. 18, 2025), https://www.judiciary.senate.gov/press/rep/releases/omb-releases-nearly-43-million-for-cigie-following-push-by-grassley-collins.

[40] *See* Press Release, U.S. Dep't of Just., Off. of Pub. Affs., *False Claims Act Settlements and Judgments Exceed $6.8B in Fiscal Year 2025* (Jan. 16, 2026), available at https://www.justice.gov/opa/pr/false-claims-act-settlements-and-judgments-exceed-68b-fiscal-year-2025 (reporting total FCA recoveries exceeding $6.8B for FY 2025; "over $5.7B" involving the health care industry).

[41] *See* Fact Sheet: President Donald J. Trump Establishes New Department of Justice Division for National Fraud Enforcement, White House (Jan. 8, 2026), https://www.whitehouse.gov/fact-sheets/2026/01/fact-sheet-president-donald-j-trump-establishes-new-department-of-justice-division-for-national-fraud-enforcement/.

HHS-OIG, MFCUs, and state Medicaid agencies, but it does not substitute for the other functions the system depends on. CMS program integrity offices, HHS-OIG, DOJ, state Medicaid agencies, and MFCUs perform related but distinct roles: some prevent improper payments, some audit and oversee operations, and some investigate or prosecute fraud. Many losses involve improper payments, weak controls, documentation failures, eligibility problems, or billing errors that do not warrant a criminal or False Claims Act referral but still require prevention, detection, correction, and recovery. Federal support should therefore strengthen the full system rather than any single piece of it.

Of course, preserving separate roles does not mean preserving silos. MFCUs, state Medicaid agencies, CMS, HHS-OIG, and DOJ each perform different functions, but Medicaid integrity depends on their ability to share timely, usable information. That is where federal support can make an immediate difference. A recent GAO report illustrates the problem.[42] Until December 2025, CMS generally did not notify supplemental payers, including state Medicaid agencies, when Medicare providers were under payment suspension for suspected fraud. As a result, some payers continued making beneficiary cost-sharing payments on claims that CMS had already flagged as potentially fraudulent. In the urinary-catheter scheme GAO reviewed, state Medicaid agencies paid at least $196,000 in combined state and federal cost-sharing funds in 2023 and 2024. Although the dollar amount was relatively small, GAO explained that this reflected a structural limitation: providers must be enrolled in a state Medicaid program to receive those payments, and providers engaged in Medicare fraud often do not enroll in Medicaid.

The finding remains relevant because it shows that fraud detected at the federal level may not reach state payment systems in time to prevent improper payments. CMS has begun closing that gap, but payment suspensions based on suspected fraud should trigger systematic information sharing rather than informal or ad hoc coordination. Whatever choices Congress and CMS make about Medicaid program design, federal support should focus on practical improvements that enhance capacity and oversight.

Congress should ensure adequate funding for HHS-OIG and MFCUs and protect the independence and continuity of inspectors general and shared infrastructure such as CIGIE. Congress and CMS should invest in interoperable data systems and reliable provider and beneficiary identifiers; make federal-state data sharing for fraud purposes systematic; expand training and technical assistance for state Medicaid agencies and MFCUs; and, given that much of Medicaid now runs through managed care, strengthen managed care fraud referral standards and metrics.

[42] *See* U.S. Gov't Accountability Off., GAO-26-107799, Medicare: CMS's Use of Data Analytics to Identify and Prevent Fraud (2026), https://www.gao.gov/products/gao-26-107799.