A SAYARI INTELLIGENCE BRIEF

The War on Fraud.

Protecting federal benefits programs through commercial intelligence.

EXECUTIVE SUMMARY

A federal escalation, a sophisticated threat, and the intelligence advantage your mission requires.

Federal benefits fraud is not just a financial problem. Spanning Medicare, Medicaid, housing assistance, food programs, and cash aid, it is an assault on vital programs that government agencies administer. Every dollar lost to Medicare fraud is a dollar that should have funded a patient's care. With a cumulative financial toll running into the hundreds of billions of dollars, it is an operational imperative with implications for your agency's mission, budget, and public accountability.

$100B+
Estimated annual Medicare and Medicaid fraud losses

$198M
Suspected hospice fraud identified by HHS OIG (2023)

75,000+
Providers on the OIG List of Excluded Individuals (LEIE)

This threat has evolved. Fraud networks operating against federal benefits programs now employ the same structural sophistication used by transnational organized crime: layered corporate ownership designed to defeat standard screening, "phoenix" companies that reconstitute under new identities following enforcement actions, and nominee operators who provide human cover for criminal enterprises with no legitimate business purpose.

The mandate is clear.

On March 16, 2026, President Trump signed an executive order establishing the Task Force to Eliminate Fraud. The order spans the Departments of Justice, HHS, Treasury, Agriculture, Labor, HUD, Education, Veterans Affairs, and Homeland Security. It mandates 30-day agency risk assessments, establishes a new DOJ Division for National Fraud Enforcement, and creates state-level accountability mechanisms that carry the threat of federal funding loss for jurisdictions that fail to meet anti-fraud standards.

This is the most consequential federal escalation in benefits program integrity enforcement in a generation. For agency leaders, it reframes anti-fraud capability as a core component of accountability.

Closing the intelligence gap.

Rules-based screening and single-source database checks were designed for a different threat environment. They identify known bad actors. They do not surface the networks those actors operate through, the shell companies they hide behind, or the associated entities they use to continue collecting payments after exclusion.

Sayari's Commercial World Model, a digital twin of global commerce that resolves more than 10 billion primary-source records worldwide, gives investigators and program managers the ability to:

→ **See through fraudulent ownership structures.** Sayari maps multi-layered beneficial ownership across domestic and international registries, surfacing the true controllers behind the entities billing your programs.

→ **Identify fraud indicators at scale.** Shared addresses, implausible business characteristics, nominee operators, and phoenix patterns are detectable across your entire provider or contractor ecosystem.

→ **Expose the full network, not just the initial target.** Known bad actors are connected to associates and enablers. Sayari maps those connections, enabling agencies to act on the whole scheme rather than just its visible edge.

→ **Screen across exclusion and sanctions databases.** Excluded providers, sanctioned individuals, and adverse corporate records are checked in parallel, not in isolation.

→ **Produce releasable intelligence products.** Publicly available commercial records create unclassified, releasable intelligence products that can be shared with state partners, prosecutors, or foreign liaison services without classification concerns.

WHAT THIS REPORT COVERS

Three case studies drawn directly from current federal enforcement priorities: (1) a Russia-linked transnational Medicare fraud scheme prosecuted under Operation Gold Rush; (2) the proliferation of hospice fraud concentrated in California but extending into multiple states; and (3) the documented failure of existing controls to prevent excluded providers from continuing to receive Medicaid payments through associated entities.

THE POLICY LANDSCAPE

The new national campaign to combat fraud.

On March 16, 2026, President Trump signed an executive order creating the Task Force to Eliminate Fraud within the Executive Office of the President. The Task Force coordinates representatives from eleven federal departments and agencies in a unified strategy to protect federal housing, food, medical, cash assistance, and other benefit programs from fraud, waste, and abuse.

The executive order explicitly identifies a range of threat actors exploiting the benefits system: domestic criminals, foreign gangs, ineligible providers, state and local officials, and non-governmental organizations. It acknowledges that lax controls, including self-certification of eligibility or inadequate verification mechanisms, have created systemic vulnerabilities that cost American taxpayers while denying benefits to legitimate recipients.

Key mandates of the March 2026 executive order.

→ **30-day risk assessments.** Each member agency must identify its highest-risk fraud transactions and processes within one month of the order's signing.

→ **60-day minimum anti-fraud requirements.** The Task Force must coordinate adoption of minimum controls including screening, identity verification, pre-payment integrity checks, and cross-program risk indicators.

→ **90-day implementation plans.** Each Task Force member must submit a measurable implementation plan.

→ **State accountability.** Federal funds may be withheld from jurisdictions failing to meet anti-fraud requirements.

→ **Enhanced enforcement.** The Attorney General is directed to promote qui tam (False Claims Act) actions and the DOJ's new Division for National Fraud Enforcement is activated.

→ **Provider revalidation.** Agencies are directed to develop processes for wide-scale provider reauthorizations and revalidations to deter fraudulent enrollment.

Broader fraud enforcement context.

The March 16 executive order caps a rapidly escalating enforcement environment. In January 2026, the White House announced the DOJ's Division for National Fraud Enforcement, the first dedicated division centralizing the federal government's approach to fraud prosecution across program types. That same month, Treasury-led initiatives — including FinCEN and IRS actions — signaled that financial institutions are viewed both as essential partners in combating fraud and as potential enforcement targets for failing to identify suspicious activity.

A companion executive order signed March 6 on combating cybercrime explicitly targeted transnational criminal organizations engaged in cyber-enabled fraud, directing the Attorney General to establish a Victims' Restoration Fund and instructing the Secretary of State to impose consequences on foreign governments tolerating cyber-enabled fraud.

The Centers for Medicare and Medicaid Services (CMS) has taken parallel action, implementing a nationwide temporary moratorium on enrollment of Durable Medical Equipment, Prosthetics, Orthotics, and Supplies (DMEPOS) companies, one of the highest-risk provider categories for Medicare fraud.

THE FRAUD LANDSCAPE

Scale, sophistication, and structure.

Financial dimensions.

While precise figures are difficult to establish given inherent detection gaps, estimates from federal oversight bodies and academic researchers point to annual losses in the range of $100 billion to more than $500 billion across Medicare, Medicaid, and other federal benefit programs from fraud. This is not a static problem. Fraud networks actively evolve their methods to stay ahead of enforcement, exploiting new provider categories, emerging program vulnerabilities, and cross-jurisdictional complexity.

$10.6B+
Fraudulent Medicare claims in a single Russia-linked scheme (Operation Gold Rush, 2025)

$50M+
In California hospice fraud charges in a single enforcement action (April 2026)

1,200
Medicaid Fraud Control Unit convictions, FY 2025 (HHS OIG)

Structural patterns.

Effective fraud detection requires understanding the structural signatures fraud networks leave in commercial records. Despite the diversity of fraud schemes, common architectural patterns recur with striking regularity:

→ **Beneficial owner concealment.**

Fraud networks use multi-layered corporate structures — shell companies, nominee operators, and international holding entities — to obscure true beneficial owners. Domestic LLCs with opaque ownership chains, registered agents who serve hundreds of unrelated entities, and international corporate vehicles in low-transparency jurisdictions are common tools. Traditional screening cannot penetrate these structures without tracing ownership through multiple layers.

→ **Phoenix companies.**

When enforcement shuts down a fraudulent operation, the underlying network frequently reconstitutes under a new entity name — often at the same address, with overlapping officers,

operating in the same program area. Identifying phoenix patterns requires connecting new registrations to prior enforcement targets through shared identifiers.

→ **Address clustering and shared infrastructure.**

High volumes of apparently independent businesses registered at a single address are a well-documented red flag. In the hospice context, investigators identified a single Los Angeles office building with 89 registered hospice entities. Similar patterns appear in DME fraud, personal care services fraud, and telehealth fraud schemes.

→ **Nominee operators.**

Sophisticated fraud schemes employ nominee individuals who appear in corporate records as owners, officers, or directors but exercise no actual control. Nominees frequently appear across multiple entities in the same network, creating a detectable pattern.

→ **Exclusion circumvention.**

Individuals and entities formally barred by HHS OIG continue receiving federal payments through new entities not yet linked to their exclusion, employment in roles that technically qualify, or operation through associated parties not yet on the exclusion list. The LEIE alone contains more than 75,000 records.

THE SAYARI APPROACH

Sayari for benefits program integrity.

Sayari is the risk orchestration and automation company providing government agencies and commercial institutions with immediate visibility into complex commercial relationships. Drawing on more than a decade of innovation, Sayari delivers the largest commercially available collection of corporate and trade data — more than 500 million entity profiles spanning public records from over 250 jurisdictions worldwide.

Cross-border beneficial ownership analysis.

Sayari's entity resolution engine automatically traces ownership and control through multi-layered corporate structures, crossing jurisdictional boundaries to identify ultimate beneficial owners.

AI-enabled network analysis.

Sayari's graph-based platform automatically resolves relationships between entities through shared officers, directors, addresses, registered agents, and other identifiers, compressing time to map a fraud network from months to hours.

Suspicious indicator detection.

Sayari flags shared addresses across multiple entities, nominee operator patterns, lack of web presence or verifiable business activity, implausible business characteristics, and recent formation combined with immediate high-volume billing.

Historical linkages and phoenix detection.

By maintaining historical records of corporate relationships, Sayari connects newly formed entities back to previously actioned or excluded individuals — enabling proactive intervention rather than waiting for the new entity to accumulate fraudulent claims.

Exclusions and adverse records integration.

Sayari integrates exclusion lists, sanction databases, debarment records, and adverse public records with corporate ownership data, enabling network-level screening rather than entity-by-entity checks.

Unclassified intelligence support.

Sayari's commercially available public records reconstruct network maps and support evidence packages using unclassified, releasable material — creating tear-line products shareable with state partners, prosecutors, or foreign liaison services without classification concerns.

APPLICATION FOR THE TASK FORCE MANDATE

The 30-day risk assessment requirement is precisely the kind of time-sensitive, data-intensive challenge where Sayari provides immediate value. Rather than reviewing individual provider records manually, agencies can leverage Sayari's automated screening to characterize entire provider populations against fraud indicators, surfacing the highest-risk segments for prioritized review. The 60-day minimum anti-fraud requirements can be operationalized through Sayari's API integration with agency payment and enrollment systems, enabling real-time screening of new enrollments before funds are disbursed.

CASE STUDY 1

Operation Gold Rush: Transnational healthcare fraud.

In June 2025, as part of "Operation Gold Rush," the U.S. Attorney's Office for the Eastern District of New York announced the indictment of eleven members of a Russia-based transnational healthcare fraud and money laundering scheme — the largest healthcare fraud case by loss amount ever recorded by the DOJ. The network purchased medical equipment companies using nominee owners to conceal involvement, submitted more than $10.6 billion in fraudulent Medicare claims using stolen patient data, and funneled proceeds through international shell companies.

$10.6B	11	16+
In fraudulent Medicare claims submitted in this single scheme	Defendants indicted — but the network extends far further	Florida-based healthcare entities Sayari linked to one indicted defendant

Sayari analysis: mapping the broader network.

The value of Sayari's platform extends beyond confirming known targets to identifying the wider network of associated entities that may be engaged in similar or related fraud activity. Sayari records from the Georgia Secretary of State identify Jason Onoufrienko, one of the indicted defendants, as an officer of Main Street DME Inc., a Georgia-based durable medical equipment company. This connection is immediately surfaced through Sayari's automated records ingestion from state corporate registries.

Extending the analysis from Main Street DME, Sayari network analysis identified further connections: records from the Alabama Secretary of State link a company named Express Healthcare Inc. to Onoufrienko, representing a potential additional vector for the fraud scheme across state lines.

Crucially, Sayari's graph analysis identified a link via Main Street DME between Onoufrienko and two individuals who, between 2020 and 2025, founded no fewer than sixteen Florida-based healthcare companies, including multiple DME providers. This network exhibits a concentrated suite of suspicious indicators:

→ All companies share one of two addresses corresponding to small Florida office buildings

→ Most maintain National Provider Identifier (NPI) numbers enabling Medicare and Medicaid billing

→ The companies lack maintained websites and verifiable operational footprints

→ Several have ostensible CEOs with no other presence in corporate records — consistent with nominee operator patterns

→ Consumer forums and independent watchdogs identified Main Street DME as a fraud concern as of late 2025

While these indicators do not conclusively confirm fraud, Sayari rapidly surfaced a broader pattern of incorporation consistent with the known fraud typology: newly formed healthcare entities registered at shared addresses with potential nominee operators, all maintaining active NPI numbers. This analysis — which might take investigators months through manual record review — was generated in hours, enabling investigators to prioritize these entities for follow-on review and potentially identify additional co-conspirators before additional fraudulent claims are processed.

CASE STUDY 2

Los Angeles hospice fraud: structural concentration at scale.

Hospice fraud has emerged as one of the most acute and rapidly escalating Medicare fraud threats in the United States, combining high per-patient billing rates, limited oversight of care delivery, and a proliferation of new providers that has outpaced regulatory capacity. A CBS News investigation of Los Angeles County — confirmed by a House Oversight Committee investigation, CMS enforcement actions, and DOJ prosecutions — documents a crisis of alarming scale.

1,800+
Hospice providers in LA County alone

700+
LA County hospices with multiple fraud red flags (CBS News analysis)

97%
Survival rate at one fraudulent LA hospice (vs ~20% national norm)

California, and Los Angeles County in particular, has become a focal point for hospice fraud, though the problem is national. A 2022 California State Auditor report found a 1,500% increase in hospice companies in LA County since 2010, six times more hospice providers than the national average relative to the elderly population. CMS data shows the typical LA County hospice billed Medicare roughly $29,000 per patient, more than double the national average of $13,200.

On April 2, 2026, federal authorities arrested eight individuals in connection with a $50 million hospice and healthcare fraud scheme in Southern California, in an operation directly tied to the administration's broader anti-fraud initiative. One of the charged individuals was already serving federal prison time for a prior hospice fraud conviction involving an illegal kickback scheme totaling $10.6 million. Her continued ability to operate fraudulent hospice entities through associated parties illustrates exactly the network-level persistence that evades entity-level screening.

What Sayari surfaced.

Sayari analysis of California Secretary of State records, Paycheck Protection Program loan recipient data, the SBA Dynamic Small Business database, and trademark applications from the US Patent and Trademark Office identified more than 270 hospice businesses registered within roughly eight blocks of a single street in the Van Nuys neighborhood of Los Angeles.

At least 250 of those have registered addresses at the same medium-sized office building on Friar Street. According to one real estate listing, the building has 62 suites; other listings describe the building as hosting over 300 tenants across suites, offices, and retail storefronts — a strong signal of virtual office arrangements rather than independent operating businesses. Even accounting for that, the collocation of such a large number of hospice-related businesses is a recognized red flag indicator for potential fraud, per the 2022 California State Auditor report.

Across the more than 270 hospice businesses in the Van Nuys area, many shared common officers or registering agents. The director of Van Nuys-based Caring Nurses Hospice Inc. is also director of at least eighteen other hospices spread between Los Angeles, Glendale, and Las Vegas. Among a sample of 371 unique names connected to Van Nuys hospices, the highest number of hospice companies associated with a single individual was 23 — a pattern of mass incorporation that is itself a recognized red flag for healthcare fraud.

> **WHY THIS MATTERS FOR YOUR AGENCY**
>
> A CMS moratorium on new California hospice licenses is a justified instrument given the scale of the problem. Sayari enables a more surgical complement: proactive screening of all existing enrolled hospice providers against fraud indicators, prioritizing entities exhibiting multiple red flags for enhanced review, pre-payment audits, or enrollment suspension. This transforms what is currently a reactive enforcement posture into a proactive, intelligence-driven operation.

CASE STUDY 3

Excluded providers, continuing payments.

The HHS OIG List of Excluded Individuals and Entities (LEIE) is one of the most consequential and underutilized tools in federal healthcare fraud prevention. The LEIE catalogs individuals and entities formally excluded from Medicare, Medicaid, and all other federal health care programs following convictions or other qualifying misconduct. No payment may be made for any items or services furnished, ordered, or prescribed by an excluded individual or entity, regardless of who submits the claim.

75,000+
Individuals and entities currently on the LEIE

2,228
Improper Medicaid payment records to excluded entities (Sayari analysis, 2018–2024)

$8.9M
Disbursed to a single Kansas provider for 10+ years post-exclusion

Despite this clear legal framework, excluded providers continue to receive federal healthcare payments through a series of circumvention strategies. The OIG's own enforcement statistics underscore the persistence of the problem. In FY 2025, Medicaid Fraud Control Unit convictions led to 900 new exclusions, each representing an individual or entity that had previously operated within the system.

Examples of circumvention techniques.

→ **New entity formation.** An excluded individual establishes or acquires a new entity not yet linked in CMS enrollment records to their exclusion status. The connection is not automatically surfaced in payment screening if the new entity has not yet been separately excluded.

→ **Employment by associated parties.** An excluded individual takes a formal employee, consultant, or contractor role with a non-excluded entity and continues to furnish, order, or prescribe services billed to federal programs.

→ **Nominee cover.** The excluded individual operates through a nominee owner who holds formal title while the excluded individual retains operational control and continues to direct fraudulent billing.

→ **Jurisdictional gaps.** Federal exclusion does not automatically trigger state-level exclusion in all jurisdictions. An individual excluded at the federal level may continue to be enrolled in state Medicaid programs in states without automatic cross-listing.

What Sayari's analysis surfaced.

Analysis comparing Sayari's SAM exclusions data and LEIE exclusions data with HHS Medicaid payments data illustrates one measure of the concern. Using National Provider Identifier (NPI) numbers, cross-checked with the public National Plan and Provider Enumeration System database, Sayari matched excluded entities with those receiving payments. When examining LEIE exclusions with Medicaid payments from 2018 through 2024, Sayari found 2,228 payment records involving excluded entities that occurred after those entities were added to the exclusion list.

One provider in particular continued to receive Medicaid payments for more than ten years after its exclusion, resulting in $8.9 million in disbursements. This provider also reported a P.O. box as a mailing address, with its physical address listed as a residential property in Kansas, not an evident business location.

> NETWORK-LEVEL EXCLUSION SCREENING
>
> Current exclusion screening typically operates at the entity level. A provider submitting a claim is checked against the LEIE to confirm it is not itself excluded. This misses excluded individuals operating through non-excluded entities and fails to detect the full scope of a network when only some members have been formally excluded. Sayari closes this gap by enabling network-level exclusion screening: starting from a known excluded entity or individual, Sayari's automated resolution identifies all associated entities through shared officers, addresses, agents, and ownership connections that may be controlled by or substantially connected to the excluded party.

CONCLUSION

Gaining the information advantage.

The federal government's war on fraud is a genuine inflection point in the integrity of the American benefits system. The Task Force to Eliminate Fraud, the DOJ's Division for National Fraud Enforcement, the CMS enrollment moratorium, and the accelerating pace of prosecutions collectively signal a sustained, high-priority enforcement campaign with real consequences for state agencies, providers, financial institutions, and criminal networks alike.

But reactive enforcement — even well-funded and politically prioritized reactive enforcement — cannot keep pace with fraud networks that evolve as quickly as vulnerabilities emerge. The Operation Gold Rush network extended to dozens of entities beyond the eleven indicted defendants. The hospice fraud ecosystem in Los Angeles County involves hundreds of potentially fraudulent operators even after targeted enforcement actions. Excluded providers continue to receive payments through associated entities that current screening misses. The gap between the fraud that enforcement has identified and the fraud that remains active is, by all available evidence, enormous.

Closing that gap requires proactive information advantage: the ability to map fraud networks ahead of enforcement action rather than in response to it, to screen entire populations of providers and beneficiaries against fraud indicators rather than reviewing individual records manually, and to connect newly formed entities back to known bad actors before they accumulate fraudulent claims. This is precisely the capability Sayari provides.

THE SAYARI VALUE PROPOSITION

Speed	Network maps generated in hours, not months — critical for the 30-day risk assessment manda
Scale	Screen entire provider or beneficiary populations against fraud indicators simultaneously.
Depth	Trace beneficial ownership through multi-layer structures across 250+ jurisdictions.
Persistence	Historical records surface phoenix companies and exclusion circumvention.

Integration	Cross-reference corporate networks against exclusion lists, sanctions, and adverse records in a
Defensibility	Publicly available commercial records create releasable, unclassified intelligence products for p

THE THREAT IS SOPHISTICATED. THE MANDATE IS URGENT. THE CAPABILITY EXISTS.

As federal oversight intensifies and the cost of compliance failure rises — for agencies, for financial institutions, and for states risking the loss of federal funding — Sayari's global intelligence infrastructure is indispensable for upholding national security and protecting the integrity of the American safety net. The information advantage is available. The question is who uses it first.

ABOUT SAYARI

The judgment infrastructure for trustworthy AI in economic security and commercial risk.

Sayari is the judgment infrastructure for trustworthy AI in economic security and commercial risk. The Sayari Commercial World Model resolves 10.6B+ primary-source records from 250+ jurisdictions forming the ground truth of global commerce. A Judgment Ontology, encoding over a decade of investigative tradecraft, and Superconductor, an agentic orchestration platform, deliver AI that reasons like an expert analyst, shows its work, and traces every finding to its source. Trusted by U.S. Customs and Border Protection, the U.S. Treasury, and Fortune 500 enterprises, Sayari is used by thousands of professionals across 35+ countries to secure supply chains and dismantle illicit networks. Headquartered in Washington, D.C.

To learn more, visit **sayari.com**.

TRUST PROOF

72%	of risk Sayari surfaces is absent from global watchlists
80%	reduction in workflow cycle time for typical investigations
60K+	partners screened for a top-3 telecom
100K+	merchants screened with sub-second latency