FINANCIAL CRIMES ENFORCEMENT NETWORK

Financial Trend Analysis

Health Care Fraud: Trends in Bank Secrecy Act Data

September 2026

Health Care Fraud: Trends in Bank Secrecy Act Data

This Financial Trend Analysis (FTA) focuses on patterns and trends identified in Bank Secrecy Act (BSA) reports linked to suspected health care fraud. This report is issued pursuant to Section 6206 of the Anti-Money Laundering Act of 2020, which requires the Financial Crimes Enforcement Network (FinCEN) to periodically publish BSA-derived threat pattern and trend information.[1] The information in this report is relevant to the public, including a wide range of consumers, businesses, and industries, and it highlights the value of BSA data filed by regulated financial institutions.

Executive Summary: Health care fraud imposes enormous costs on U.S. taxpayers, increases the overall cost of health care in the United States, and puts patients at risk.[2] [3] This Financial Trend Analysis provides threat pattern and trend information on potential health care fraud-related activity, based on Bank Secrecy Act (BSA) reports filed with FinCEN between 1 March 2025 and 28 February 2026 (the review period). In developing this FTA, FinCEN analyzed 5,702 BSA reports (the dataset) related to potential health care fraud that identified approximately $17.5 billion in suspicious activity, which includes both completed and attempted transactions.

- *Depository Institutions Filed the Majority of Potential Health Care Fraud-Related BSA Reports in the Dataset*: Depository institutions filed approximately 89 percent of reports in the dataset and accounted for nearly 87 percent of the reported suspicious activity amounts. Two depository institutions, the largest by asset size in the dataset, filed 29 percent of all health care fraud-related reports.
- *Suspected Health Care Fraud-Related Schemes Target a Mix of Medicare, Medicaid, and Private Insurance Programs*: Perpetrators of suspected health care fraud often target more than one program or insurance provider, receiving funds from a combination of federal and state programs, as well as private insurance companies. Medicare payments frequently originated from Medicare Administrative Contractors whereas Medicaid payments originated from state-level administrators.
- *Overwhelming Majority of Subjects Located in the United States*: Filers identified subjects located in all 50 U.S. states, as well as Puerto Rico, Guam, and the U.S. Virgin Islands. Of the approximately 13,000 subject addresses in the dataset, approximately 1.5 percent had a foreign address.

1. The Anti-Money Laundering Act of 2020 was enacted as Division F, §§ 6001-6511, of the William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021, Pub. L. 116-283 (2021).
2. *See* FinCEN, "Advisory on Health Care Fraud Schemes Targeting Medicare, Medicaid, and Other Federal and State Health Care Benefit Programs," FinCEN Advisory #HCF-2026-A001, 30 March 2026, https://www.fincen.gov/system/files/2026-03/FinCEN-Advisory-Health-Care-Fraud.pdf.
3. *See* "2026 National Money Laundering Risk Assessment," U.S. Department of the Treasury, March 2026, https://home.treasury.gov/system/files/246/2026-NMLRA.pdf.

- *Home Health Care Businesses Were the Most Frequently Identified Suspected Fraudulent Providers in BSA Reports*: Home health care businesses were identified as the suspected fraudulent providers in 20 percent of all suspected health care fraud-related BSA reports. Other frequently identified providers included hospice care companies, mental and/or behavioral health and addiction treatment providers and companies, medical equipment providers—including durable medical equipment—and adult or child daycares.
- *Suspected Fraudulent Funds Used for Personal Expenses and Luxury Goods, With Some International Transfers*: Suspected perpetrators employed a range of apparent money laundering techniques—from simple funds transfers to complex layering processes—before spending the obtained health care payments. In many cases, proceeds of suspected health care fraud that did not appear to go through a complex funds transfer process were used on personal expenses and luxury goods. Some funds were sent internationally.
- *Some Suspected Health Care Fraud Perpetrators May Be Involved in Criminal Networks*: A small percentage of filers reported suspected health care fraud activity potentially involving large fraud rings or criminal networks, as well as some potential connections with foreign entities. For the most part, filers did not specifically identify activity linked to known transnational criminal organizations (TCOs).

Scope and Methodology: FinCEN analyzed BSA reports that 1) included "health care fraud" as a suspicious activity type; and 2) included "suspicious receipt of government payments" as a suspicious activity type and included health care fraud-related key terms. FinCEN used a combination of automated and manual processes to remove any false positives and validate the dataset. Based on these parameters, FinCEN identified 5,702 filings filed between 1 March 2025 and 28 February 2026 that reported approximately $17.5 billion in suspicious activity, which includes both completed and attempted transactions. FinCEN identified these BSA reports based on the report's filing date, rather than the date of suspicious activity; as a result, the reports in the dataset sometimes also refer to incidents that occurred prior to the review period. In this report, FinCEN highlights prevalent trends and typologies used by suspected perpetrators of health care-related fraud as reflected in the dataset. FinCEN has based its analysis on the information provided in these BSA reports, as well as certain portions of transactional data underlying these BSA reports.

FinCEN issued an Advisory, "Health Care Fraud Schemes Targeting Medicare, Medicaid, and Other Federal and State Health Care Benefit Programs," on 30 March 2026, urging financial institutions to be vigilant about health care fraud schemes targeting government health care benefit programs.[4] Although BSA reports filed after the issuance of the Advisory were not included in the scope of this Financial Trend Analysis, the typologies and trends in the post-Advisory BSA filings are consistent with the findings of this report.

4. *See* FinCEN *supra* note 2.

A Note About Suspicious Activity Reporting

Suspicious activity reporting reflects only suspicious activity that has been identified and reported by financial institutions and, therefore, should not be considered a complete representation of the scope of any particular type of suspicious activity. Suspicious activity reporting may include additional transactions and information beyond a specific transaction that may be reportable as suspicious and, accordingly, the total reportable suspicious activity amount in any report may be overly inclusive. For example, suspicious activity reporting may reflect both completed and attempted transactions, both inbound and outbound transactions, and transfers between accounts. These suspicious activity amounts may also include typos and errors as submitted by filers. The reported suspicious activity in any individual suspicious activity filing may include both legal and illicit activities associated with a particular subject. Suspicious activity reporting may also describe continuing suspicious activity or amend earlier reporting, or reports that cover expanded networks involved in potential illicit activity and therefore may reflect cumulative transactions from a single filer involving the same subject.

What is Health Care Fraud?

Health care fraud is the act of knowingly and willfully executing, or attempting to execute, a scheme or artifice to defraud any health care benefit program; or to obtain by false or fraudulent means any of the money or property owned by, or under the custody or control of, any health care benefits program.[5] Health care fraud-related schemes frequently involve the abuse of health care benefits programs such as Medicare or Medicaid, in which a health care provider's practices are inconsistent with sound fiscal, business, or medical practices, and result in unnecessary cost to the program.[6] Commonly occurring health care fraud schemes include: the filing of false and fraudulent claims for reimbursement, including double billing, phantom billing, and upcoding; fraudulently inducing patient referrals or the use of items and services with kickbacks and bribes; stealing patients' health insurance identifiers, including via bogus marketing scams; impersonating health care professionals; and diverting legal prescriptions for illegal uses.[7] [8]

Health care spending in the United States totaled approximately $5.3 trillion in 2024, approximately $1.6 trillion of which was attributed to private health insurance spending and $1.9 trillion of which was attributed to Medicare and Medicaid spending, according to the U.S. Department of Health and Human Services' Centers for Medicare and Medicaid Services

5. *See* 18 U.S.C. § 1347.
6. *See* 42 C.F.R. § 455.2.
7. *See* "Healthcare Fraud," Federal Bureau of Investigation, https://www.fbi.gov/investigate/white-collar-crime/healthcare-fraud.
8. *See* FinCEN *supra* note 2.

(CMS).[9] The U.S. Department of the Treasury's 2026 *National Money Laundering Risk Assessment* notes that the amount of funding available for exploitation makes health care funding an attractive target for domestic and international criminals.[10]

Depository Institutions Were Key Filers of Suspected Health Care Fraud-Related BSA Reports

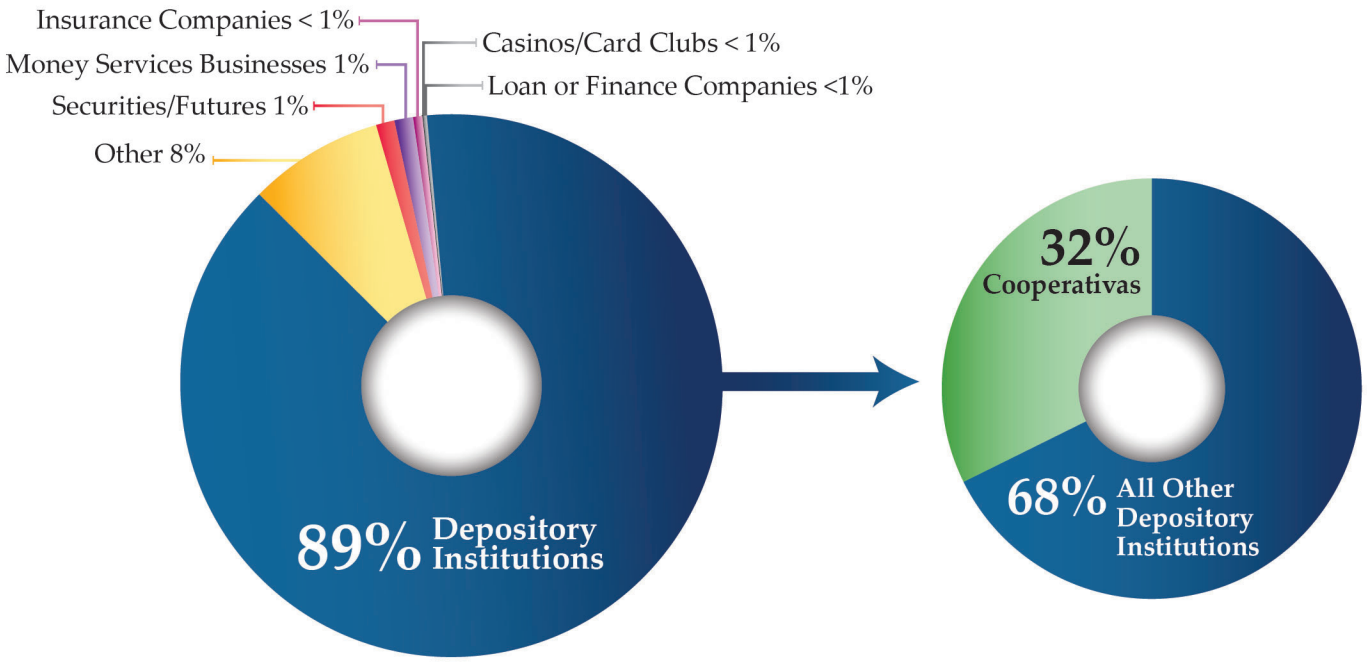
FinCEN analyzed 5,702 BSA reports filed by a total of 471 financial institutions, most of which were depository institutions. Overall, filers reported approximately $17.5 billion in suspicious activity, averaging approximately $3.3 million per filing and with a median amount of approximately $600,000. BSA reports were filed at a consistent rate, an average of 475 each month, with no notable spikes or dips in filings during the review period. Filers consisted of depository institutions, securities/futures firms, money services businesses (MSBs), insurance companies, casinos or card clubs, and loan or finance companies. Some filers within the dataset are categorized as "other," which includes certain corporate trustees of financial services companies.

Depository institutions filed the majority of BSA reports—408 depository institutions filed 5,080 BSA reports, or approximately 89 percent of the dataset—and reported the majority of the total suspicious activity amount, approximately $15.2 billion. Two depository institutions, which are also the largest banks in the dataset by asset size, filed 29 percent of all BSA reports in the dataset.[11] Moreover, one of those depository institutions filed double the number of BSA reports of any other filer (approximately 1,100 BSA reports).

Fifty-nine depository institutions in Puerto Rico, all of which were financial cooperatives (or *cooperativas*), filed 1,641 BSA reports, or approximately 29 percent of the dataset.[12] BSA reports filed by these financial cooperatives primarily identified suspicious activity related to eligibility for Puerto Rico's Medicaid program, approximately 67 percent of which reported suspicious activity below $15,000 (see box, "Possible Medicaid Eligibility Fraud in Puerto Rico" below).

9. *See* Centers for Medicare and Medicaid Services, "National Health Expenditures 2024 Highlights," U.S. Department of Health and Human Services, p. 1, 3, https://www.cms.gov/files/document/highlights.pdf.
10. *See* U.S. Department of the Treasury, "2026 National Money Laundering Risk Assessment," p. 8, *supra* note 3.
11. *See* "U.S. Domestically Chartered Commercial Banks, Ranked by Consolidated Assets as of December 31, 2025," United States Federal Reserve Board, Federal Reserve Statistical Release, https://www.federalreserve.gov/releases/lbr/current/.
12. Financial cooperatives in Puerto Rico, specifically *cooperativas de ahorro y crédito*, are similar to credit unions, providing loans, checking and savings accounts, and other financial services to businesses and individuals across Puerto Rico (*see* "COSSEC Fiscal Plan: A Road Map to Strengthen Financial Cooperatives," Financial Oversight and Management Board for Puerto Rico, 26 May 2023, https://oversightboard.pr.gov/cossec-fiscal-plan-a-road-map-to-strengthen-financial-cooperatives/).

Figure 1. Total Number of Suspected Health Care Fraud-Related BSA Reports by Filer Type (1 March 2025 – 28 February 2026)



Programs Potentially Targeted for Fraud Appear to Include a Mix of Medicare, Medicaid, and Private Insurance

Suspected health care fraud perpetrators most frequently received payments from Medicare and Medicaid providers at the federal and state levels—either directly or through intermediaries such as Medicare Administrative Contractors (MACs) or state-run programs—as well as private insurance, based on FinCEN's analysis of the dataset. Filers did not always definitively state the specific source of health care payments given the complexity of health care payment mechanisms (*e.g.*, some private companies operate as MACs and Medicaid payments may be disbursed through state-run programs or Managed Care Organizations). The median amount of funds received by potentially fraudulent health care providers was $611,667 per BSA report, based on FinCEN's analysis of the dataset.

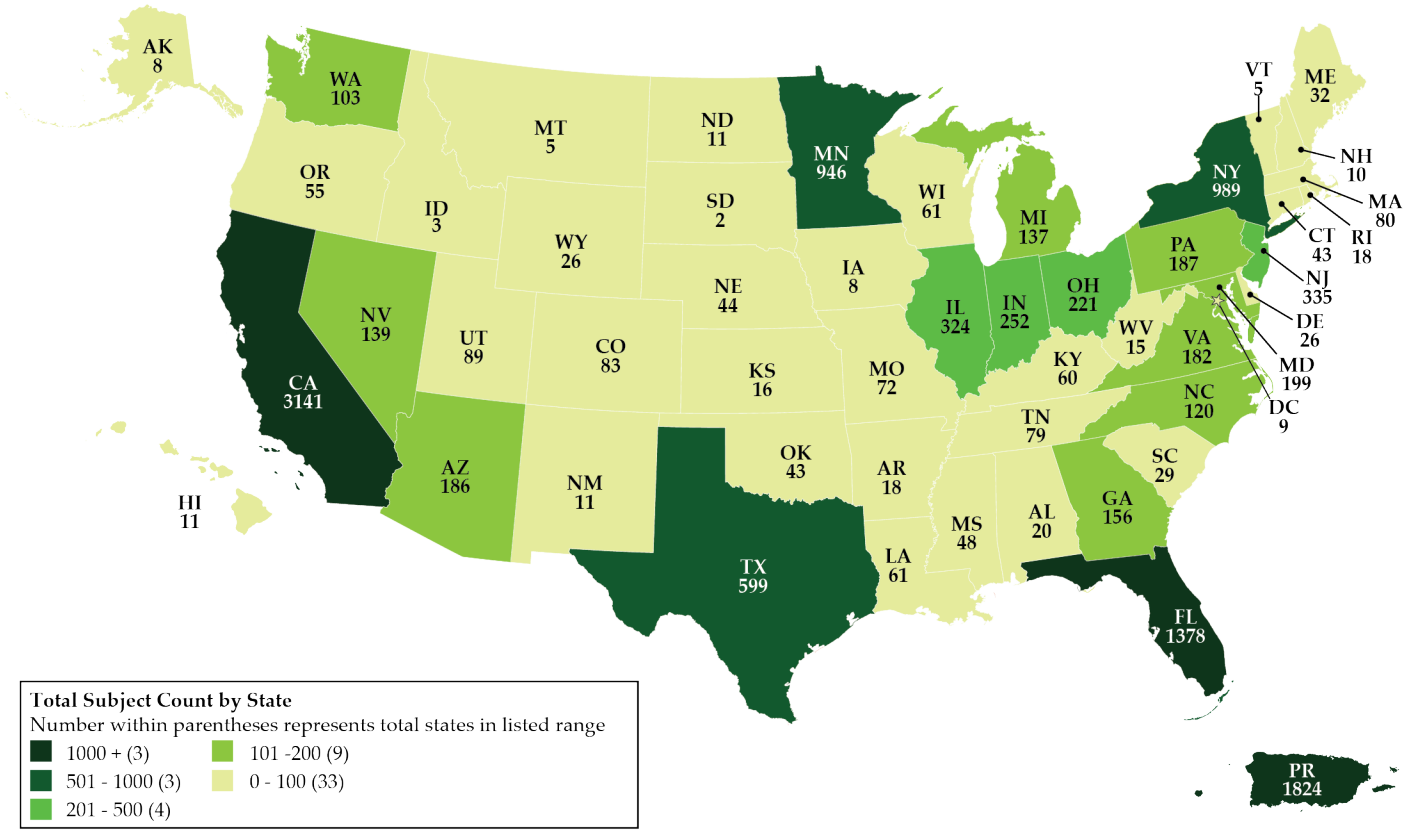
- Medicare and/or Medicaid were named in 2,190 BSA reports, or approximately 38 percent of the dataset; TRICARE was named in 70 BSA reports.
- MACs were identified in 1,247 BSA reports, or approximately 22 percent of the dataset. MACs are multi-state, regional private health care insurers that are responsible for administering certain Medicare claims.[13] MACs that cover Medicare Part A and Part B claims were the most frequently identified within the dataset (see Appendix A for additional information about MACs as well as Medicare Parts A and B).

13. *See* Centers for Medicare and Medicaid Services, "What's a MAC," U.S. Department of Health and Human Services, https://www.cms.gov/medicare/coding-billing/medicare-administrative-contractors-macs/whats-mac.

Overwhelming Majority of Subjects Located in the United States

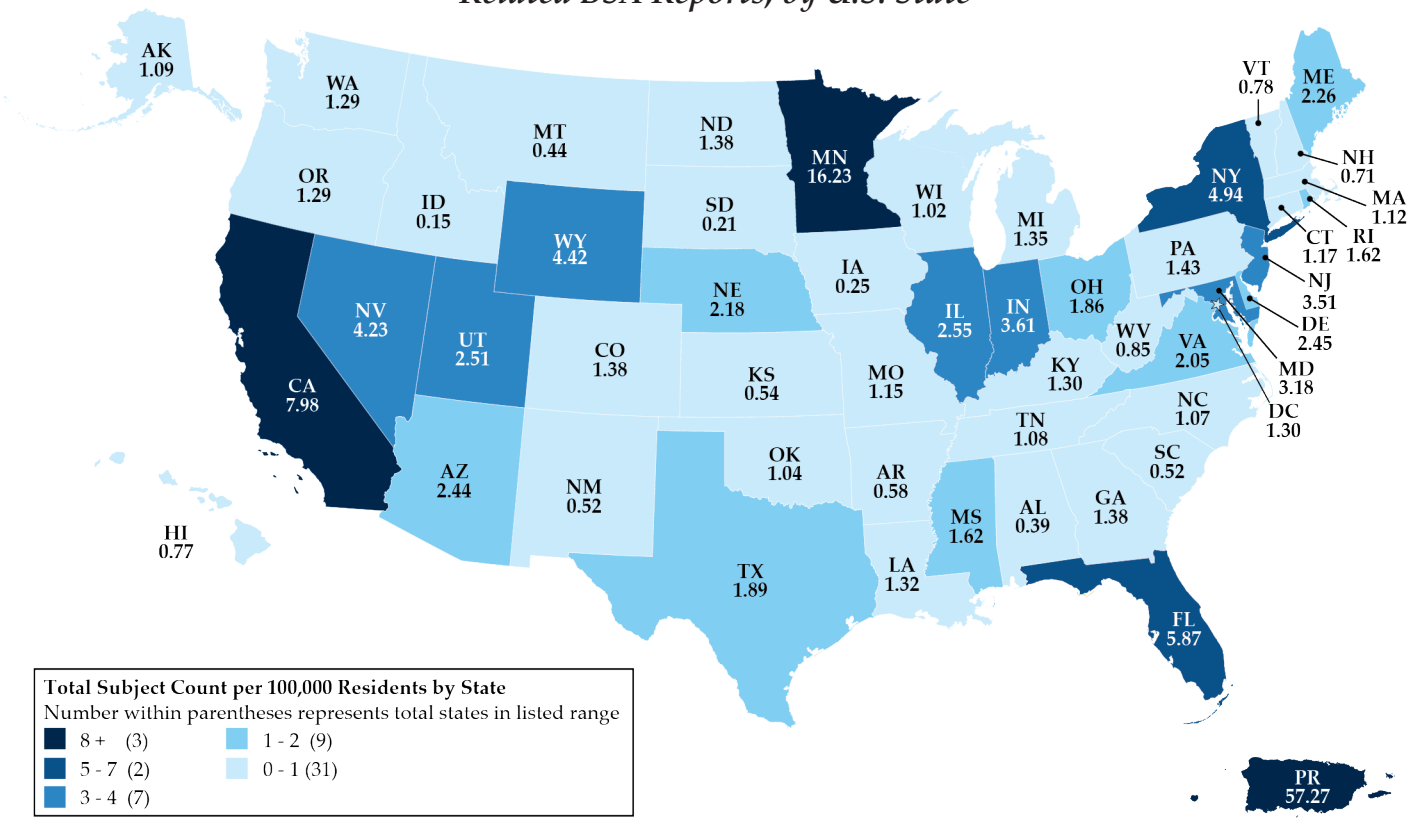
The health care fraud dataset overwhelmingly identified subjects with addresses in all 50 U.S. states and Washington, D.C., as well as multiple U.S. territories, including Guam, Puerto Rico, and the U.S. Virgin Islands, based on FinCEN's analysis of the dataset. Filers most frequently identified subjects with addresses in California, followed by Florida, New York, and Minnesota.[14] Of the 13,277 total subjects, only 187 subjects—identified in 116 BSA reports—had non-U.S. addresses, which were in approximately 50 other countries, including Armenia, Canada, Ghana, Hong Kong, Pakistan, the People's Republic of China, the Philippines, the United Arab Emirates, and the United Kingdom, among others.

Figure 2. Number of Subjects Identified in Suspected Health Care Fraud-Related BSA Reports, by U.S. State



14. The figures may also include subject addresses that appeared in multiple BSA reports. As such, the count of subject addresses for each state may be inflated. Additionally, at least 645 subject addresses in the dataset did not identify a state and were excluded from the count. Overall, an average of 2.3 addresses were identified in each BSA report.

Figure 3. Number of Subjects Per 100,000 Residents Identified in Suspected Health Care Fraud-Related BSA Reports, by U.S. State



Largely mirroring the overall count of subject addresses by state, 692 U.S. counties and 75 Puerto Rican localities were identified in the dataset, with California's Los Angeles County, Minnesota's Hennepin County, and Florida's Miami-Dade County, appearing the most frequently (see Appendix B for a full list of BSA report counts for the top counties).

Figure 4. Top 10 U.S. Counties with 120 or More Suspected Health Care Fraud-Related BSA Reports, 1 March 2025 – 28 February 2026[15]

County	Number of BSA Reports
Los Angeles, California	777
Hennepin, Minnesota	300
Miami-Dade, Florida	247
Kings, New York	174
Queens, New York	162
Cook, Illinois	137
Marion, Indiana	124
Orange, California	123
Palm Beach, Florida	122
Harris, Texas	120

15. This table does not include localities in Puerto Rico.

Home Health Care Businesses Most Frequently Identified Suspected Fraudulent Providers

The most frequently identified line of business for potentially fraudulent health care providers was home health care, which, based on FinCEN's analysis of the dataset, is typically either paid out of pocket or through Medicare Parts A and B.[16] The U.S. Department of Health and Human Services' Centers for Medicare and Medicaid Services (CMS) estimated an improper payment rate of approximately 9.5 percent in home health and hospice payments, totaling approximately $2.8 billion, in 2025.[17] CMS has also identified home health care as a field potentially vulnerable to fraud given that Medicare trusts physicians and nurses to provide accurate diagnoses and necessary services and does not verify claims or conditions before making payments.[18]

Figure 5. Top Five Provider Types Identified in Suspected Health Care Fraud Dataset

Provider Type	Percentage of BSA Reports*
Home Health Care	32
Hospice Care	8
Mental/Behavioral Health; Addiction Treatment	7
Medical Equipment (incl. DME)	5
Daycare (Adult and Child)	3

**Excludes BSA reports describing possible Medicaid eligibility fraud in Puerto Rico.*

- BSA reports referencing home health care accounted for more than 21 percent of the dataset—and nearly 32 percent of the dataset when BSA reports related to suspected Medicaid eligibility fraud in Puerto Rico are removed (see box, "Possible Medicaid Eligibility Fraud in Puerto Rico," below).
- The majority of home health care businesses were registered at residential homes.

Other frequently appearing health care provider types included hospice/palliative care companies, mental/behavioral health providers (including addiction treatment), durable medical equipment (DME) providers, adult daycares, pharmacies, physicians' offices, laboratory testing companies, and medical transportation companies. Some providers claimed to work in multiple fields, such as home health care and autism-related services or addiction treatment and adult daycare, among others.

16. *See* Medicare, "Home Health Services," U.S. Department of Health and Human Services, https://www.medicare.gov/coverage/home-health-services.
17. *See* Centers for Medicare and Medicaid Services, "2025 Medicare Fee-for-Service Supplemental Improper Payment Data," U.S. Department of Health and Human Services, p. 28, https://www.cms.gov/files/document/nov-2025-medicare-ffs-supplemental-improper-payment-data-2025922.pdf.
18. *See* Stephen Chahn Lee, "Law Enforcement Observations About Home Health Fraud," Centers for Medicare and Medicaid Services, U.S. Department of Health and Human Services, pp. 3-4, https://www.cms.gov/research-statistics-data-and-systems/monitoring-programs/medicare-ffs-compliance-programs/pre-claim-review-initiatives/downloads/special-open-door-forum-on-home-health-fraud.pdf.

Possible Medicaid Eligibility Fraud in Puerto Rico

Within the dataset, 59 Puerto Rican financial cooperatives (or *cooperativas*) filed 1,641 BSA reports, most of which described suspicious activity related to eligibility for Puerto Rico's Medicaid program. Financial cooperatives in Puerto Rico, specifically *cooperativas de ahorro y crédito*, are similar to credit unions and provide loans, checking and savings accounts, and other financial services.[19] [20]

Puerto Rico's Medicaid program operates as a component of the island's larger public health care system, referred to as Plan Vital (formerly known as "La Reforma" or "Mi Salud").[21] Nearly half of all Puerto Rican residents, approximately 1.3 million individuals, are enrolled in Medicaid and the Children's Health Insurance Program (CHIP) as of January 2026, according to Medicaid.gov.[22] To confirm or prove continued eligibility, Puerto Rican residents must submit a declaration certifying that the recipient's financial and household information is correct, as well as supporting documentation, which may include information about income or salary as well as about cash, savings, and deposits.[23] FinCEN's analysis of the dataset suggests that some Medicaid recipients confirm their financial information by seeking a balance certification letter from their financial institution.

Within the dataset, nearly all the filings by *cooperativas* identified suspicious activity in which customers reportedly sought to lower their account balances prior to eligibility or re-eligibility meetings with Plan Vital representatives, in order to remain below the eligibility threshold. To do this, customers reportedly withdrew enough money from their accounts—usually via cashier's check or cash withdrawal—to lower their account balances and then requested a "balance certification" letter to show that funds in their accounts were below the requisite amount. Either later that day or within a couple of days, customers then returned to the financial institution and re-deposited the funds.

Suspected Fraud Perpetrators' Level of Sophistication Varied Widely

Suspected health care fraud perpetrators' capabilities vary in terms of sophistication, ranging from individual perpetrators targeting a single health care program to networks of health care and non-health care-related entities—including likely shell companies—targeting multiple health care programs, based on FinCEN's analysis of the dataset. Some schemes are relatively straightforward, with health care payments sent to an account where the account signer is also the primary

19. *See* "COSSEC Fiscal Plan: A Road Map to Strengthen Financial Cooperatives," Financial Oversight and Management Board for Puerto Rico, 26 May 2023, https://oversightboard.pr.gov/cossec-fiscal-plan-a-road-map-to-strengthen-financial-cooperatives/.
20. *See* "Cooperativas de Ahorro y Crédito," Corporacion Publica Para la Supervision y Seguro de Cooperativas de Puerto Rico, https://www.cossec.pr.gov/coop-ahorro-y-credito.
21. *See* El Plan de Salud VITAL, "Sobre Vital," https://www.planvitalpr.com/plan-vital.
22. *See* Medicaid, "Medicaid & CHIP in Puerto Rico," U.S. Department of Health and Human Services, https://www.medicaid.gov/state-overviews/puerto-rico.html.
23. *See* Departemento de Salud, "Programa Medicaid," Gobierno de Puerto Rico, https://www.medicaid.pr.gov/CMS/34.

perpetrator of the fraud or where health care payments are spent on non-health care-related expenses directly from the receiving account. Other schemes involve the receipt of funding from multiple sources, including federal, state, and local health care programs and private insurance, and usually appear to involve complex money laundering processes, based on FinCEN's analysis of the dataset.

Perpetrators of the more straightforward schemes generally target only one program and/or insurance type, and the targeted program is often based in the perpetrator's home state. Additionally, the perpetrator generally expends little, if any, effort to obfuscate the source of funds, instead making non-health care-related purchases or other payments directly out of the receiving account. These schemes typically only involve one or two individuals and, while lucrative, tend to involve relatively smaller transaction amounts, based on FinCEN's analysis of the dataset.

- A BSA filer reported an adult daycare in Missouri received more than $680,000 in payments from Missouri Social Services. After receiving the funds, the daycare owner transferred them to another business account they own and then conducted cash withdrawals, issued checks related to real estate, made a payment for a luxury car, and sent funds to a family member.
- Another BSA filer identified a home health care agency registered at a residential home in Indiana that received funds from private insurance companies administering state-supported health plans. The home health care agency's owner reportedly spent more than $240,000 of the agency's funds on luxury apparel brands, as well as on gambling at a nearby casino.
- A BSA filer identified a genetic testing laboratory registered at a strip mall with no signage in Mississippi that received more than $190,000 in funds from a private insurance company and a MAC. Shortly after receiving the funds, the business account owner reportedly made cash withdrawals in multiple states and spent funds on seemingly non-health care-related items, including gambling and travel expenses.

By comparison, perpetrators of more sophisticated, larger-scale schemes target multiple funding mechanisms, fraudulently receiving funds from multiple sources, including federal, state, and local programs as well as private insurance, based on FinCEN's analysis of the dataset. Because legitimate providers are expected to receive funds from multiple sources—as their patients may have insurance coverage from a variety of insurers—these schemes can appear more legitimate than the simpler schemes described above. Additionally, sophisticated fraud schemes, some of which may be perpetrated by criminal organizations, may also involve complex money laundering processes and the incorporation of other crimes such as identity theft, forgery, and drug-related offenses, judging from the dataset and press releases from federal and state law enforcement agencies.[24]

24. *See* U.S. Attorney's Office Eastern District of New York, "11 Defendants Indicted in Multi-Billion Health Care Fraud Scheme, the Largest Case by Loss Amount Ever Charged by the Department of Justice," U.S. Department of Justice, 30 June 2025, https://www.justice.gov/usao-edny/pr/11-defendants-indicted-multi-billion-health-care-fraud-scheme-largest-case-loss-amount; "National Health Care Fraud Takedown Results in 455 Defendants Charged in Connection with Over $6.5 Billion in Alleged Fraud," U.S. Department of Justice, 23 June 2026, https://www.justice.gov/opa/pr/national-health-care-fraud-takedown-results-455-defendants-charged-connection-over-65; State of Arizona Attorney General, Health Care Fraud Takedown Case Filings, 2026, https://mcusercontent.com/cc1fad182b6d6f8b1e352e206/files/abd52a0a-0e46-1f3b-ab17-d6aa1671d015/Healthcare_Fraud_Takedown_2026_AGO_compressed.pdf.

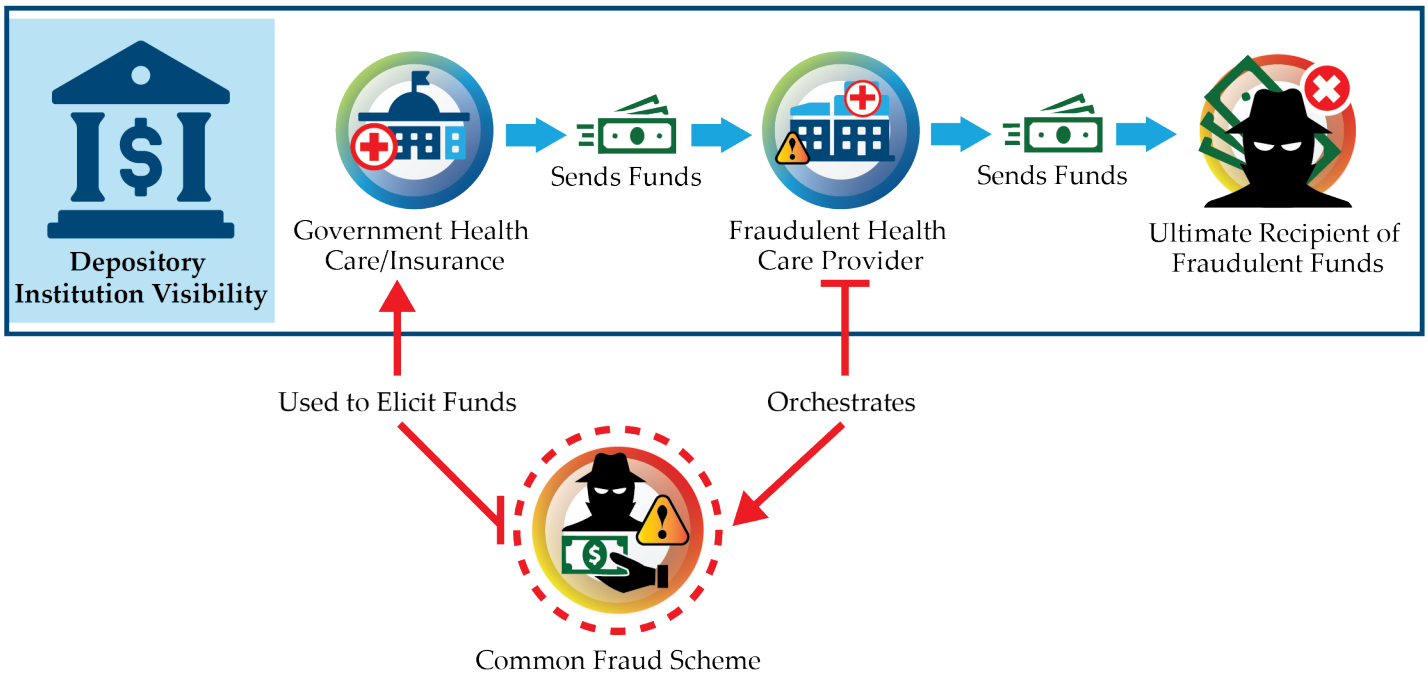
- A BSA filer identified payments totaling approximately $20 million from a MAC, state health agencies, and a pharmacy benefit management organization to a New York City-based pharmacy. The pharmacy then sent payments to numerous wholesale companies with registered addresses in Hong Kong. The filer suspected that the pharmacy is part of a larger fraud ring based in the New York City area.
- A BSA filer identified payments totaling approximately $2 million from companies in multiple health care fields, including home health care and hospice agencies, a medical transportation company, and a pharmacy, as well as non-health care companies, to multiple California-based individuals. These individuals then sent funds to potential shell companies and unrelated individuals, as well as a real estate company. One of the initial recipients was reportedly linked to organized crime and other specified unlawful activities.
- Another BSA filer identified nearly $870,000 sent from a state agency as well as private insurance companies that administer state health plans to a Minnesota-based adult daycare reportedly registered at a shuttered store front. The daycare then sent payments to numerous individuals under the guise of payroll, transferred funds to the business owner's personal accounts, and sent funds to a likely shell company. The business owner used some of the funds to issue checks payable to MSBs that specialize in international transfers.

The Federal Bureau of Investigation, U.S. Department of Health and Human Services Office of Inspector General, Centers for Medicare and Medicaid Services, and other federal, state, and local agencies have identified several health care fraud schemes frequently employed to illicitly obtain health care funds. These include double billing, billing for services not rendered (also known as phantom billing), unbundling, upcoding, and providing medically unnecessary services, among others (see Appendix C for additional information about commonly identified health care fraud schemes).[25] [26]

Based on FinCEN's analysis of the dataset, in most cases, financial institutions do not identify or describe the type of health care fraud schemes that health care providers have used to fraudulently obtain health care funds in BSA reports. Financial institutions see funds received from government health care agencies or private insurance but not the methods used to obtain those funds. FinCEN's analysis of the dataset indicates that financial institutions usually provide details of a health care fraud scheme after a customer has been publicly charged or indicted or when there is an ongoing investigation where a law enforcement authority has informed the financial institution of the methodology.

25. *See* "What We Investigate: Healthcare Fraud," Federal Bureau of Investigation, https://www.fbi.gov/investigate/white-collar-crime/healthcare-fraud.
26. *See* Centers for Medicare and Medicaid Services, "Common Types of Health Care Fraud Fact Sheet," U.S. Department of Health and Human Services, https://www.cms.gov/files/document/overviewfwacommonfraudtypesfactsheet072616pdf.

Figure 6. Depository Institution Visibility into Suspected Health Care Fraud Schemes



Schemes Perpetrated Mostly by Providers That Did Not Appear to Offer Any Medical Services

The majority of BSA filers described activity involving purported health care providers that did not appear to offer any medical services and used apparent shell companies to receive and move funds. However, a small number of BSA reports also appeared to describe activity involving legitimate medical providers engaged in potentially fraudulent practices.

In most cases, seemingly fraudulent providers were identified at addresses that appeared to be residential homes or non-medical buildings. At least 43 percent of the non-Puerto Rico Medicaid eligibility-related BSA reports identified potentially fraudulent activity by companies with addresses at residential homes.[27] However, potentially fraudulent medical providers were also located at addresses in non-medical buildings, including large office buildings that appeared to house numerous legitimate businesses, storefronts in strip malls, and standalone small offices, among others. In some cases, non-medical buildings reportedly had signage with the names of businesses, but the buildings themselves appeared to be abandoned or closed, sometimes with shuttered or boarded up windows and doors, and no indication of health care-related activity, according to BSA filers and open-source research of address information conducted by FinCEN. Filers also noted that there were no indications that these health care providers operated legitimate businesses elsewhere.

27. BSA reports may report activity linked to multiple companies registered at different types of locations. For example, a BSA report may identify activity by one business with a prominent storefront, another at an industrial building, and another at a residential home.

In the relatively few (less than five percent of the dataset) cases where filers described activity involving seemingly legitimate medical providers engaged in potentially fraudulent practices, these providers appeared to have engaged in fraudulent billing (e.g., double billing or phantom billing), accepted kickbacks, or provided medically unnecessary services, according to FinCEN's analysis of the dataset (see Appendix C for a list of known health care schemes). Some of the businesses, especially adult daycares, also appeared to commingle payments from other sources with payments received for providing medical care.

Unlike the suspected fraudulent providers, seemingly legitimate providers generally appeared to operate out of medical buildings with multiple other medical practices, or in standalone buildings with signage indicating the presence of the business, according to BSA filers and open-source research of address information conducted by FinCEN. These providers also appeared to offer medical services to patients. However, the reviewed dataset may underrepresent this segment of potential health care fraud, as these businesses have fewer obvious red flags for financial institutions to detect, especially without direct insight into billing practices or egregiously out of character financial activity.

- A BSA filer reported more than $25 million in Medicaid payments to an Alaska-based dentist's office. The dentist's office appeared to be active and providing dental services but had multiple owners who were not involved in dentistry. Additionally, the filer stated that the payments appeared to be used for cash withdrawals, personal expenses, and payments to the owners' other businesses.
- A BSA filer reported multiple insurance payments totaling more than $400,000 that used the same insurance claim numbers for multiple claimants with the same loss date to a Kentucky-based licensed health care professional. These deposits funded transfers to the health care professional's personal investment accounts. The health care professional previously had their operating license suspended but appears to have had the license reinstated and resumed business.
- A BSA filer reported payments totaling more than $330,000 from a MAC to a Pennsylvania-based hospice care business. While the business appeared to be active and providing services, the insurance payments funded payments to the owner's credit cards and transfers to personal accounts.

Suspected Fraudulently Obtained Funds Potentially Laundered, Also Used for Personal Expenses, Luxury Goods, or International Transfers

Suspected health care fraud perpetrators frequently sought to obfuscate the origin of funds received from health care programs via apparent money laundering techniques, including by sending funds via a series of circular transactions to other businesses and/or directly transferring funds to individuals linked to the provider. Others, typically those who were not part of a large network, often used the funds for personal expenses and sometimes for luxury purchases, travel, real estate, construction, or investments. While the funds were typically spent or transferred elsewhere domestically, there were multiple instances where funds were also sent overseas.

Flow of Funds Includes Circular Transactions with Other Businesses Linked to Health Care Providers

Some suspected fraudulently obtained funds, especially those linked to more sophisticated schemes, were sent via a series of circular transactions to other businesses linked to the owner and/or associates of the fraudulent provider; used for payments to various individuals under the guise of payroll; and/or used for other payments disguised as health care-related, according to FinCEN's analysis of the dataset. Additionally, potentially fraudulent providers often commingled health care payments with cash deposits, P2P transfers, wire transfers, and check deposits in business accounts, prior to spending the funds on non-health care-related expenses, making it difficult to determine which funds were used for these unrelated expenses. It was also not always clear if the other deposited funds were proceeds from other scams or were received for legitimate purposes, based on FinCEN's analysis of the dataset.

- A BSA filer reported that multiple insurance companies, including some MACs, sent approximately $4 million to a California-based home health care business registered at an address in an office building. In addition to health care funds, the business received check and wire credits from non-medical companies. These transactions funded transfers to other businesses—some medical and some non-medical—including lenders and a construction company.
- A second BSA filer reported that a New York-based adult daycare received approximately $2 million in payments from Medicare and Medicaid as well as transfers from other adult daycares and non-medical businesses. These transactions reportedly funded transfers to other adult daycares, various trade companies, and numerous individuals that the filer suggested may be part of a complex money laundering scheme.
- A third BSA filer reported that a MAC sent approximately $2 million to a California-based hospice care business registered at a small office building. These funds then exited the account in hundreds of small transactions to various individuals, consulting companies, advertising companies, marketing companies, and a real estate firm located in the United Arab Emirates. The filer noted that the business had no regular business activity (e.g., payroll, tax payments, or medical supplies purchases).

Suspected Health Care Fraud-Related Funds Used for Luxury Purchases, Personal Expenses, Real Estate

Proceeds of suspected health care fraud that did not appear to go through a complex funds transfer process were used for a variety of purposes, including personal expenses, luxury purchases, real estate purchases, and cash withdrawals. Direct use of the funds for personal use was often associated with lower amounts and smaller-scale fraud as opposed to the more complex schemes, which also typically implied greater organization and fraud on a larger scale.

- A BSA filer reported approximately $1.4 million in payments from a state health agency directly to a Maryland-based home health care business claiming to specialize in mental health and substance abuse recovery that was registered at a residential home. The funds were used for numerous personal expenses, including credit card payments, living expenses, payments to develop the owner's social media pages, and payments to a plastic surgeon.
- A second BSA filer identified approximately $580,000 in payments from a regional MAC to a California-based hospice care business that then sent a portion of the proceeds to a consulting firm. The consulting firm reportedly sent wire transfers to an MSB in the digital asset sector, likely for digital asset purchases.
- A third BSA filer reported approximately $80,000 sent from private insurance companies that administer state health plans to an Indiana-based home health care business registered at a residential home; the home health care business also received cash deposits and P2P transfers. The payments funded direct transfers to family members as well as likely personal purchases at various retailers.

Potentially Fraudulent Funds Primarily Sent Domestically, International Transactions Observed

Suspected health care fraud funds are primarily sent and spent within the United States, but approximately five percent of the dataset identified instances of funds either directly or indirectly funding international transfers, based on FinCEN's analysis. Suspected fraudulently received health care funds were sent to 32 countries—most frequently Hong Kong, but also Canada, Mexico, Nigeria, Pakistan, the People's Republic of China, the Philippines, Türkiye, and the United Arab Emirates, among others—based on FinCEN's analysis of the dataset. In most cases involving international transactions, the initial recipient of the suspected fraudulent health care funds sent money to at least one other party domiciled in the United States and that party then facilitated the international transfer, according to BSA filers. As a result of this layering, it is possible that a larger portion of the fraudulent proceeds were sent abroad, but financial institutions did not observe the activity since these transfers typically traverse multiple financial institutions, judging from FinCEN's analysis of the dataset.

- The transfers to Hong Kong appeared to primarily benefit possible shell companies and it was not clear what happened to the funds after they were transferred, judging from FinCEN's analysis of the dataset.
- FinCEN did not observe any instances of money being sent from a government health agency directly to a recipient outside of the United States. All initial recipients were domiciled domestically, based on FinCEN's analysis of the dataset.

Some counterparties that ultimately receive suspected fraudulently obtained funds may not be involved in laundering the proceeds or acting outside of their normal line of business. For example, while BSA filers suggested that some of the transactions sent to entities in Mexico may be for money laundering or illicit finance, others may be more straightforward expenses, such as personal vacations and travel. Several recipients of potentially fraudulent health care funds spent some of the money on travel, often to international destinations, judging from the dataset.

Some Suspected Health Care Fraud Perpetrators May Be Involved in Criminal Networks

Approximately four percent of the BSA reports, all of which were filed by depository institutions, identified some health care fraud-related suspicious activity potentially involving larger fraud rings or criminal networks in multiple locations throughout the United States, as well as some potential connections with foreign entities, based on FinCEN's analysis of the dataset. However, for the most part, filers did not specifically identify activity linked to TCOs.[28]

- Several filers reported potentially fraudulent hospice care providers in northern Los Angeles County that may be linked to organized crime. After receiving health care-related proceeds, these businesses rapidly sent the funds out to other businesses reportedly owned by the same network of individuals, most of which were not linked to the health care sector and included catering companies, bakeries, consultants, construction firms, and home contractors.
- Filers reported several home health care, adult daycare, and autism centers in Minnesota potentially tied to large fraud rings. These businesses would often send funds to other non-health care-related businesses, such as restaurants and real estate firms, as well as to MSBs for potential international transfers.
- Some filers reported activity involving potentially fraudulent adult daycares in the New York City area. Adult daycares in New York have previously been tied to sophisticated Chinese money laundering networks.[29]

28. Although the dataset did not include a significant number of BSA reports identifying TCO activity, FinCEN noted in its March 2026 Advisory that health care fraud is increasingly perpetrated by TCOs, according to information derived from open-source reporting and law enforcement information, in addition to BSA reporting (*see* FinCEN, *supra* note 2). For example, the U.S. Department of Justice has announced charges against numerous individuals that may be involved in larger TCOs, including as part of *Operation Gold Rush*, in which a Russia-based TCO allegedly orchestrated a multi-billion dollar health care fraud scheme that targeted Medicare and private health insurance companies (*see* "National Health Care Fraud Takedown Results in 324 Defendants Charged in Connection with Over $14.6 Billion in Alleged Fraud," U.S. Department of Justice, 30 June 2025, https://www.justice.gov/opa/pr/national-health-care-fraud-takedown-results-324-defendants-charged-connection-over-146).
29. For additional information about Chinese money laundering networks, *see* "Financial Trend Analysis: Chinese Money Laundering Networks: 2020-2024 Threat Pattern and Trend Information," FinCEN, August 2025, https://www.fincen.gov/system/files/2025-08/4000-10-INV-144549-S3F6L-FTA-CMLN-508.pdf.

- A few filers reported potentially fraudulently received Medicare funds sent to companies linked to La Cosa Nostra. The recipients commingled health care payments with funds from other sources and then sent transactions to non-health care-related businesses, such as restaurants, real estate, and asset management.

The information in this report is based on health care fraud-related information obtained from analysis of BSA data, and open-source publications, as well as insights from law enforcement and other partners. FinCEN welcomes feedback on this report, particularly from financial institutions. Please submit feedback to the FinCEN Regulatory Support Section by submitting an inquiry at www.fincen.gov/contact.

Appendix A: Glossary of Health Care-Related Terms and Programs

Children's Health Insurance Program (CHIP): CHIP provides low-cost health coverage to children and pregnant women in families that earn too much money to qualify for Medicaid, but too little to get private coverage.[30] Every state offers CHIP coverage and has its own rules about who qualifies for coverage, but programs are managed by states according to federal requirements.[31]

Durable Medical Equipment (DME): DME is medical equipment that can withstand repeated use and is used for a medical reason in a beneficiary's home.[32] DME is expected to last at least three years and is typically only useful for someone who is sick or injured.[33] Examples of DME include canes, walkers, wheelchairs, oxygen equipment, glucose monitors, infusion pumps, and hospital beds, among others.[34] Medicare covers DME in different ways, including plans where beneficiaries must buy the equipment, rent the equipment, or rent-to-own the equipment.[35]

Home Health Care: Home health care providers offer a wide range of health services that patients receive in their homes for an illness or injury to help improve their condition, maintain their current condition, or slow their rate of decline.[36] These services are provided to individuals who need intermittent skilled services and are homebound, meaning that leaving their home is not recommended due to their condition or individuals are unable to leave their homes.[37]

Hospice Care: Hospice care focuses on the care, comfort, and quality of life of a person with a serious illness or condition who is approaching the end of their life.[38] It is covered under Medicare Part A or through private insurance.[39]

Medicaid: Medicaid is a joint federal and state program that helps cover medical costs for people with limited income and resources.[40] Medicaid programs are administered by each state, but the federal government sets rules that all programs must follow.[41] Eligibility requirements and scope

30. *See* Medicaid, "Children's Health Insurance Program (CHIP)," U.S. Department of Health and Human Services, https://www.medicaid.gov/chip.
31. *See* "Medicaid & CHIP," U.S. Department of Health and Human Services, https://www.healthcare.gov/medicaid-chip/childrens-health-insurance-program/.
32. *See* Medicare, "Durable Medical Equipment (DME) Coverage," U.S. Department of Health and Human Services, https://www.medicare.gov/coverage/durable-medical-equipment-dme-coverage.
33. *See ibid.*
34. *See ibid.*
35. *See ibid.*
36. *See* Medicare, "Home Health Services," U.S. Department of Health and Human Services, https://www.medicare.gov/coverage/home-health-services.
37. *See ibid.*
38. *See* "What are Palliative Care and Hospice Care?" National Institute on Aging, https://www.nia.nih.gov/health/hospice-and-palliative-care/what-are-palliative-care-and-hospice-care.
39. *See ibid.*
40. *See* "What's the Difference Between Medicare and Medicaid?" U.S. Department of Health and Human Services, https://www.hhs.gov/answers/medicare-and-medicaid/what-is-the-difference-between-medicare-medicaid/index.html.
41. *See* Medicaid, "Medicaid State Plan Amendments," U.S. Department of Health and Human Services, https://www.medicaid.gov/medicaid/medicaid-state-plan-amendments.

of coverage can vary by state.[42] Medicaid may offer benefits that Medicare does not, including nursing home care and personal care services.[43]

Medicare: Medicare is a federal health insurance program for people aged 65 or over, people under 65 with certain disabilities, and people of all ages with End-Stage Renal Disease.[44] Medicare is divided into four parts (Parts A-D) that cover different aspects of health care.[45]

Medicare Administrative Contractors (MACs): MACs are private companies that have been awarded a geographic jurisdiction to process Medicare Part A and Part B medical claims or Durable Medical Equipment claims for Medicare Fee-For-Service (FFS) beneficiaries.[46] MACs serve as the primary operational contacts between the Medicare FFS program and the health care providers enrolled in the program.[47]

Medicare Advantage: Also known as "Part C," Medicare Advantage Plans are insurance coverage plans offered by a private insurance company approved by Medicare.[48] Medicare pays a fixed amount for beneficiaries' care every month to the companies offering the Medicare Advantage Plans; those companies must then follow rules set by Medicare, but each company can charge different out of pocket expenses and have different rules for how beneficiaries get services.[49] Medicare Advantage Plans provide Parts A and B coverage, most offer Part D coverage, and some may include additional coverage such as vision, hearing, or dental.[50]

Medicare Part A: Part A covers inpatient care in hospitals, critical access hospitals, and skilled nursing facilities, as well as hospice care and some home health care.[51] Beneficiaries must meet certain conditions for these benefits and typically do not pay a premium.[52] Informally, Part A is one part of "original Medicare," which uses a model where the government pays health care providers directly for each individual service.[53]

42. *See* Medicaid, "Medicaid, Children's Health Insurance Program, & Basic Health Program Eligibility," U.S. Department of Health and Human Services, https://www.medicaid.gov/medicaid/national-medicaid-chip-program-information/medicaid-childrens-health-insurance-program-basic-health-program-eligibility-levels.
43. *See* "What's the Difference Between Medicare and Medicaid?" U.S. Department of Health and Human Services, https://www.hhs.gov/answers/medicare-and-medicaid/what-is-the-difference-between-medicare-medicaid/index.html.
44. *See* Centers for Medicare and Medicaid Services, "Medicare Program – General Information," U.S. Department of Health and Human Services, https://www.cms.gov/about-cms/what-we-do/medicare.
45. *See ibid.*
46. *See* Centers for Medicare and Medicaid Services, "What's a MAC?" *supra* note 13.
47. *See ibid.*
48. See "What is Medicare Part C?" U.S. Department of Health and Human Services, https://www.hhs.gov/answers/medicare-and-medicaid/what-is-medicare-part-c/index.html.
49. *See ibid.*
50. *See ibid.*
51. *See* Medicare, "What Part A Covers," U.S. Department of Health and Human Services, https://www.medicare.gov/providers-services/original-medicare/part-a.
52. *See ibid.*
53. *See* Medicare, "What Original Medicare Covers," U.S. Department of Health and Human Services, https://www.medicare.gov/providers-services/original-medicare.

Medicare Part B: Part B covers medically necessary services and preventative services.[54] Medically necessary services are services or supplies to diagnose and treat a medical condition; preventative services are services or supplies to prevent illness or detect it at an early stage when treatment is likely to work best.[55] Examples of what Part B covers include ambulance services, clinical research, DME, limited outpatient prescription drugs, mental health and substance abuse disorders, and oxygen equipment and accessories.[56] Informally, Part B is one part of "original Medicare."[57]

Medicare Part D: Part D, the most recent addition to Medicare, is drug coverage that helps pay for brand-name and generic prescription drugs.[58] Part D is optional and offered to everyone enrolled in Medicare by insurance companies and private companies approved by Medicare.[59]

Medicare Supplemental Insurance: Also known as "Medigap," this is supplemental insurance that beneficiaries can purchase from a private health insurance company to help pay for out-of-pocket costs in Medicare Parts A and B, such as copayments, coinsurance, and deductibles.[60] Generally, beneficiaries must have a Medicare plan to purchase supplemental insurance.[61]

Plan Vital: Formerly known as La Reforma and Mi Salud, Plan Vital is the public health care system in Puerto Rico. It partners with Medicaid to provide coverage to low-income individuals.[62]

TRICARE: TRICARE is the uniformed services health care program for active duty service members, active duty family members, National Guard and reserve members and their families, military retirees and their family members, survivors, and certain former military spouses.[63] TRICARE offers a variety of plans that have different ranges of coverage, bringing together resources of the military health care system with civilian providers and allowing beneficiaries to get medical care at either military hospitals and clinics or with non-military providers.[64]

54. *See* Medicare, "What Part B Covers," U.S. Department of Health and Human Services, https://www.medicare.gov/providers-services/original-medicare/part-b.
55. *See ibid.*
56. *See ibid.*
57. *See ibid.*
58. *See* Medicare, "What's Medicare Drug Coverage (Part D)?" U.S. Department of Health and Human Services, https://www.medicare.gov/health-drug-plans/part-d.
59. *See ibid.*
60. *See* Medicare, "What's Medicare Supplement Insurance (Medigap)?" U.S. Department of Health and Human Services, https://www.medicare.gov/health-drug-plans/medigap.
61. *See ibid.*
62. *See* Medicaid, "Medicaid & CHIP in Puerto Rico," U.S. Department of Health and Human Services, https://www.medicaid.gov/state-overviews/puerto-rico.html.
63. *See* "TRICARE 101," Defense Health Agency, https://tricare.mil/Plans/New.
64. *See ibid.*

Appendix B: Top Five Cities in Counties with the Largest Number of Suspected Health Care Fraud-Related BSA Reports, March 2025 Through February 2026[65]

County	City	Number of BSA Reports
Los Angeles, California	Glendale	295
	Los Angeles	186
	Van Nuys	181
	Burbank	174
	North Hollywood	139
Hennepin, Minnesota	Minneapolis	229
	Brooklyn Park	39
	Maple Grove	23
	Bloomington	22
	Eden Prairie	17
Miami-Dade, Florida	Miami	183
	Hialeah	80
	Doral	26
	Miami Lakes	21
	Homestead	16
Kings, New York	Brooklyn	174
Queens, New York	Flushing	60
	Jamaica	37
	Forest Hills	23
	Fresh Meadows	17
	Rego Park	13
Cook, Illinois	Chicago	89
	Lincolnwood	14
	Skokie	11
Marion, Indiana	Indianapolis	124
Orange, California	Anaheim	36
	Irvine	21
	Huntington Beach	16
	Santa Ana	15
	Garden Grove	11

65. Count of suspected health care fraud-related BSA reports with at least one subject from the listed city. Only cities with 10 or more BSA reports were included.

County	City	Number of BSA Reports
Palm Beach, Florida	Boca Raton	64
	West Palm Beach	21
	Delray Beach	19
	Lake Worth	16
	Palm Beach Gardens	11
Harris, Texas	Houston	92
	Katy	12
	Spring	11

Appendix C: Common Health Care Fraud-Related Schemes

Billing for Services Not Rendered (also known as phantom billing): Occurs when providers bill for services not rendered. This may include instances where no medical care was provided, some medical care was provided but not the services included in the claim, or billing for claims that have already been paid out. This also may occur when providers bill for patients that may not exist and whose identifying information comprises synthetic identity theft.[66]

Bogus Free Services: Occurs when patients are convinced to provide their personal information in order to receive free, non-existent treatment for their condition or to enroll in a fake benefit plan. These scams often result in stolen identities and fraudulent charges to various health programs.[67]

Charging for Personal Expenses: Occurs when providers include personal expenses in claims and costs charged to a federal health program. This is most often seen with nursing homes billing Medicaid, as nursing homes are reimbursed based upon the annual submission of a cost report that may surreptitiously include personal expenses.[68]

Doctor Shopping: Occurs when patients visit multiple providers to get multiple prescriptions for controlled substances. In these cases, each prescriber is not aware that the patient has already received prescriptions for a controlled substance. Doctor shopping is often linked to drug diversion.[69]

Double Billing: Also referred to as duplicate claims, occurs when a provider bills two times for one service in an attempt to be paid twice. Often, providers may change a portion or small details of the second claim in order to not submit an exact duplicate of a previously submitted claim.[70]

Drug Diversion: Occurs when prescription drugs are deflected from their lawful purpose (*i.e.*, to recipients who need the drugs for medical reasons) into the illegal market. Examples of this include individuals selling their prescription drugs to third parties, health care providers selling or transferring prescription drugs to third parties, and drug manufacturing companies diverting drugs from their intended source.[71]

66. *See* "Financial Crimes Report to the Public," Federal Bureau of Investigation, 27 February 2012, https://www.fbi.gov/file-repository/reports-and-publications/stats-services-publications-financial-crimes-report-2010-2011-financial-crimes-report-2010-2011.pdf/view.
67. *See ibid.*
68. *See* "Common Health Care Fraud Schemes," Commonwealth of Virginia's Office of the Attorney General, https://www.oag.state.va.us/index.php/programs-outreach/medicaid-fraud?id=511.
69. *See* "What We Investigate: Healthcare Fraud," Federal Bureau of Investigation, https://www.fbi.gov/investigate/white-collar-crime/healthcare-fraud.
70. *See ibid.*
71. *See* Centers for Medicare and Medicaid Services, "Do you Know About Drug Diversion?" U.S. Department of Health and Human Services, https://www.cms.gov/medicare-medicaid-coordination/fraud-prevention/medicaid-integrity-education/downloads/infograph-do-you-know-about-drug-diversion-%5Bapril-2016%5D.pdf.

Excessive Services: Occurs when medical services or equipment are provided that, although medically necessary for the patient, are in excess of the patient's needs.[72]

Kickbacks: Occurs when individuals who refer patients to a particular hospital or doctor are paid for those referrals.[73]

Medical Identity Theft: Involves the misuse of a person's identity to wrongfully obtain health care goods, services, or funds. Different schemes may involve stolen identities for beneficiaries or physicians, may involve synthetic identities, and/or may involve persons both living and deceased.[74]

Medically Unnecessary Services: Occurs when medical services or items that are not medically necessary and not justified by a patient's condition or diagnosis are provided.[75]

Unbundling: Occurs when providers submit individual claims in order to maximize the reimbursement for tests or procedures that are required to be billed together at a reduced cost.[76]

Upcoding: Occurs when a provider submits a bill using a procedure code that yields higher payments than the code for the service actually rendered (may apply to services or items).[77]

72. *See ibid.*
73. *See* Commonwealth of Virginia's Office of the Attorney General, "Common Health Care Fraud Schemes," *supra* note 68.
74. *See* Centers for Medicare and Medicaid Services, "Common Types of Health Care Fraud Fact Sheet," U.S. Department of Health and Human Services, https://www.cms.gov/files/document/overviewfwacommonfraudtypesfactsheet072616pdf.
75. *See* Centers for Medicare and Medicaid Services, "Items & Services Not Covered Under Medicare," U.S. Department of Health and Human Services, https://www.cms.gov/files/document/mln906765-items-services-not-covered-under-medicare.pdf.
76. *See* Centers for Medicare and Medicaid Services, "Common Types of Health Care Fraud Fact Sheet," *supra* note 74.
77. *See ibid.*