

BENEFITS LAW JOURNAL

Treasury and FinCEN Announce Heightened Focus on Healthcare Fraud

By Tom Schulte and Mark S. Hedberg

In this article, the authors review a healthcare fraud advisory issued by FinCEN urging financial institutions to be vigilant in detecting, preventing, and reporting fraudulent activity targeting governmental healthcare benefits programs, such as Medicare and Medicaid.

The U.S. Department of the Treasury's Financial Crimes Enforcement Network (FinCEN) has joined other federal law enforcement agencies in placing a "whole-of-government" focus on combatting benefits fraud against the federal and state governments. In a March 30, 2026, Healthcare Fraud Advisory (Advisory),¹ FinCEN urged financial institutions to be vigilant in detecting, preventing, and reporting fraudulent activity targeting governmental healthcare benefits programs, such as Medicare and Medicaid. FinCEN also identified 24 new, healthcare-focused "red flags." Although the Advisory is directed to financial institutions, non-bank clients in the healthcare sector can derive important guidance from the Advisory's analysis.

The authors, attorneys with Hunton Andrews Kurth LLP, may be contacted at tschulte@hunton.com and mhedberg@hunton.com, respectively.

BACKGROUND

While certainly not a new federal priority, the Trump Administration has recently upped federal efforts to prevent and punish healthcare and other benefits fraud. The Administration recently announced a new DOJ National Fraud Division specifically created to enforce criminal and civil law against those who commit fraud at the expense of government benefits programs. The National Fraud Division will work hand-in-hand with a larger White House Task Force to Eliminate Fraud. Through its Advisory, FinCEN and Treasury have signaled their alignment with government-wide, anti-fraud efforts.

THE ADVISORY

The Advisory begins by discussing three main healthcare-related fraud concerns: (1) use of shell companies to falsely register as legitimate healthcare companies; (2) filing claims for reimbursement arising from unnecessary, substandard, or non-existent care; and (3) laundering ill-gotten reimbursements through U.S. and international financial systems. The Advisory then delineates 24 “red flags” that financial institutions should watch for in preventing healthcare fraud (the 24 flags are reproduced in full below). According to the Advisory, legitimate healthcare reimbursement activity generally follows a standardized and predictable pattern, such that sudden changes in a healthcare customer’s account activity in conjunction with other red flags could be indicative of fraudulent activity.

The Advisory concludes with a reference to FinCEN’s whistleblower program, which incentivizes individuals to report violations of the Bank Secrecy Act (BSA) by offering them a share in the penalties that result from their whistleblowing activity. Under the Trump Administration, FinCEN has worked to develop and roll out a whistleblower program that has otherwise been non-existent compared to other whistleblower programs, like the *qui tam* provisions of the False Claims Act.²

THE BIGGER PICTURE

Preventing fraud against the government remains a top enforcement priority, and that focus is only intensifying. Indeed, DOJ has increasingly relied on the False Claims Act to address suspected fraud by healthcare entities, recovering a record \$5.7 billion in healthcare-related FCA cases.³ In light of FinCEN’s Advisory, healthcare clients should expect increased scrutiny from their financial institutions, particularly in the realm of customer due diligence and transaction verification.

Financial institutions in turn will face increased pressure to file Suspicious Activity Reports (SARs) with respect to questionable health-care-related activity. To prepare for investigations resulting from such SAR filings, clients should maintain detailed and descriptive records of costs and services for which reimbursement is sought. Clients are also encouraged to review the Advisory's list of red flags and assess whether their current financial activity could trigger one or more of the flags. Finally, given the Advisory's focus on whistleblowing, clients should evaluate their internal reporting channels to ensure they are robust, effective, and easily accessible to employees.

RED FLAGS

- A customer with neither legal permanent residence in the United States nor significant experience in the health care industry (e.g., based on the customer's stated occupation) tries to open a bank account as the owner or employee of a recently established or purchased health care provider or supplier registered with a Health Care Benefit Program.
- A customer is a health care provider or supplier registered with a Health Care Benefit Program that has beneficial owners with prior health care or government benefits fraud convictions.
- A customer is the nominal or beneficial owner of a health care provider or supplier registered with a Health Care Benefit Program and has familial or business affiliations with individuals with health care or government benefits fraud convictions.
- A customer is a health care provider or supplier registered with a Health Care Benefit Program, and the account is accessed through an Internet Protocol (IP) address or Device ID that is linked to multiple accounts at the financial institution or other financial institutions or connected to foreign jurisdictions.
- A customer is a health care provider or supplier registered with a Health Care Benefit Program and has nominal and beneficial owners listed on the account who also appear on bank accounts for other separate and distinct health care providers or suppliers.

- A customer is a recently established or purchased health care provider or supplier registered with a Health Care Benefit Program, and there are changes in the individuals listed as beneficiaries of the corporate account without a change to the name or Tax Identification Number on the account.
- A customer that is a recently established or purchased health care provider or supplier receives a significant amount of reimbursements from a Health Care Benefit Program or commercial insurers and then immediately transfers those funds to other recently established companies with the same nominal or beneficial owners, little to no online presence, and other indicators of illicit shell company activity.
- A customer is a recently established health care provider or supplier that receives a significant number of reimbursements from a Health Care Benefit Program or commercial insurers soon after starting operations.
- A customer is a health care provider or supplier registered with a Health Care Benefit Program that is receiving a significant increase in reimbursements soon after a change in beneficial ownership.
- A customer is a health care provider or supplier that suddenly has a significant increase in reimbursements from Health Care Benefit Programs or commercial insurers.
- A customer is a recently established or purchased health care provider or supplier registered with Health Care Benefit Programs or commercial insurers that receives a significant amount of reimbursements inconsistent with the customer's profile (e.g., receiving a significant amount of payments from Medicare Part A and Part B MACs for reimbursements beyond the expected activity of other similar health care providers or suppliers).
- A customer is a health care provider or supplier that receives significant volumes of reimbursements from a Health Care Benefit Program or commercial insurers but has little to no legitimate business expenses associated with the provision of health care goods and services (e.g., receiving reimbursements from DME MACs but little to no purchases of DME).

- A customer is a health care provider or supplier that receives a significant volume of reimbursements from a single Health Care Benefit Program as opposed to other customers that receive reimbursements from multiple Health Care Benefit Programs (e.g., a customer is receiving a significant amount of reimbursements from one MAC for only one type of health care good or service such as DME).
- A customer is a health care provider or supplier with a significant amount of transactional activity consisting of “consulting fees,” “marketing fees,” and other nondescriptive, repetitive invoices.
- A customer is a health care provider or supplier that receives a significant volume of reimbursements from a Health Care Benefit Program and transfers the funds to another company registered to a residential address.
- A customer is a health care provider or supplier that has outgoing transactions to, or expenditures related to, companies that have no apparent related nexus to the health care industry. This could include residential real estate and luxury goods such as art or jewelry.
- A customer is a health care provider or supplier with consistently low to moderate billing for a year or more and then suddenly begins to file a large number of claims (i.e., spike billing).
- A customer is a health care provider or supplier with a pattern of making significant cash withdrawals for no readily apparent business reason.
- A customer is a health care provider or supplier with a significant increase in cash withdrawals correlating to a significant increase in billings (i.e., customer is potentially paying kickbacks).
- A customer is a health care provider or supplier that is transferring a significant volume of funds to individuals via high-value checks.
- Without credible explanation, a customer routinely cashes high-value checks drawn from accounts associated with a health care provider or supplier.

- A customer that is a health care provider or supplier, or the customer's employee, engages in behavior suggesting efforts to evade the Currency Transaction Report (CTR) reporting requirement (e.g., alters or cancels a transaction when advised a CTR would be filed or engages in structuring with multiple cash transactions for under \$10,000), as well as avoid recordkeeping requirements.
- A customer is a recently established or purchased health care provider or supplier registered with a Health Care Benefit Program that sends a significant amount of wire transfers to individuals and companies located in foreign jurisdictions.
- A customer is a health care provider or supplier registered with a Health Care Benefit Program that sends money transfers to VASPs, brokerage accounts, and online betting platforms for no seemingly legitimate business reason.

NOTES

1. <https://www.fincen.gov/system/files/2026-03/FinCEN-Advisory-Health-Care-Fraud.pdf>.
2. Several litigants have recently challenged the constitutionality of the False Claims Act's qui tam provisions, some of which have been successful.
3. <https://www.justice.gov/opa/pr/false-claims-act-settlements-and-judgments-exceed-68b-fiscal-year-2025>.

Copyright © 2026 CCH Incorporated. All Rights Reserved.
Reprinted from *Benefits Law Journal*, Autumn 2026,
Volume 39, Number 3, pages 17–22, with permission from
Wolters Kluwer, New York, NY, 1-800-638-8437,
www.WoltersKluwerLR.com



Wolters Kluwer