FinCEN ADVISORY

FIN-2026-A001 **March 30, 2026**

FinCEN Advisory on Health Care Fraud Schemes Targeting Medicare, Medicaid, and Other Federal and State Health Care Benefit Programs

Suspicious Activity Report (SAR) Filing Request:
FinCEN requests that financial institutions reference this Advisory in SAR field 2 (Filing Institution Note to FinCEN) and the narrative by including the key term "**HCF-2026-A001**" and select, as applicable, SAR field 34(g) (Healthcare/Public or Private Health Insurance) and any other applicable check box.

The U.S. Department of the Treasury's (Treasury) Financial Crimes Enforcement Network (FinCEN) is issuing this Advisory in close coordination with the Federal Bureau of Investigation (FBI) and the U.S. Department of Health and Human Services Office of Inspector General (HHS-OIG) to urge financial institutions[1] to be vigilant in identifying and reporting suspicious transactions potentially related to health care fraud schemes targeting Medicare, Medicaid, and other Federal and state health care benefit programs (hereafter "Health Care Benefit Programs"). This Advisory builds on Treasury's work to combat the potentially billions of dollars in rampant health care and government benefits fraud in Minnesota and across the country.[2]

Every year, fraudsters (including unscrupulous medical professionals), domestic organized crime groups, and, increasingly, transnational criminal organizations (TCOs) submit false and fraudulent claims to Health Care Benefit Programs. These schemes threaten the integrity of both the U.S. health care and financial systems, impose enormous costs on taxpayers, waste critical resources for beneficiaries of these programs, and increase the cost of health care in the United States.

Recognizing that financial fraud threatens the integrity of Federal programs and undermines trust in government, on March 25, 2025, President Trump issued Executive Order (E.O.) 14249, *Protecting America's Bank Account Against Fraud, Waste, and Abuse*. Among other things, E.O. 14249 declared that it is the policy of the United States to defend against financial fraud and improper payments.[3]

1. *See* 31 U.S.C. § 5312(a)(2); 31 C.F.R. § 1010.100(t).
2. *See* Treasury, Press Release, "U.S. Treasury Secretary Scott Bessent Takes Decisive Action Against Somali Fraud in Minneapolis" (Jan. 13, 2026).
3. *See* The White House, Executive Order on Protecting America's Bank Account Against Fraud, Waste, and Abuse, 90 Fed. Reg. 14011 (Mar. 28, 2025); The White House, "Fact Sheet: President Donald J. Trump Protects America's Bank Account Against Waste, Fraud, and Abuse" (Mar. 25, 2025).

Fraud is one of FinCEN's Anti-Money Laundering and Countering the Financing of Terrorism (AML/CFT) National Priorities.[4] Fraud, including health care fraud and government benefits fraud, also continues to be one of the largest sources of illicit proceeds in the United States according to Treasury's 2026 National Money Laundering Risk Assessment.[5] Bank Secrecy Act (BSA) reporting indicates that health care fraud has increased significantly since the COVID-19 pandemic.[6] From 2020 through 2025, FinCEN observed a 330 percent increase in BSA reporting on health care fraud. This significant increase in BSA reporting peaked in 2025 with financial institutions filing a record of over 3,800 initial SARs that checked SAR field 34(g) (Healthcare/Public or Private Health Insurance).[7] This BSA reporting, however, likely represents only a small fraction of the amount of illicit activity connected to health care fraud in the United States.

FinCEN, in its capacity as administrator of the BSA and financial intelligence unit of the United States, and in partnership with FBI and HHS-OIG, is deploying its tools, authorities, and resources to support the Trump Administration's whole-of-government effort to combat fraud, waste, and abuse involving Federal payments.[8] This Advisory provides financial institutions with an overview of health care fraud schemes targeting Health Care Benefit Programs. It also highlights the associated money laundering typologies and red flag indicators to identify and report suspicious activity to FinCEN and reminds financial institutions of their reporting requirements under the BSA. FinCEN strongly encourages financial institutions to voluntarily report suspicious activity related to fraud and also strongly encourages immediate notification to law enforcement regarding fraud schemes targeting Health Care Benefit Programs.

The information contained in this Advisory is derived from FinCEN's analysis of BSA data, open-source reporting, and information provided by law enforcement partners.

Reporting Fraud, Waste, and Abuse

FinCEN encourages financial institutions and the public to report any tips or complaints about potential fraud, waste, abuse, and mismanagement involving HHS programs to HHS-OIG (Submit a Hotline Complaint).

Victims of cyber-enabled health care fraud schemes should file a complaint with the FBI's Internet Crime Complaint Center (IC3) or file a report with their nearest FBI field office.[9]

4. *See* FinCEN, "Anti-Money Laundering and Countering the Financing of Terrorism National Priorities" (June 30, 2021).
5. *See* Treasury, "2026 National Money Laundering Risk Assessment" (Mar. 2026), at p. 1.
6. *See* FinCEN, FIN-2021-A001, "Advisory on COVID-19 Health Insurance- and Health Care-Related Fraud" (Feb. 2, 2021).
7. *See* FinCEN, SAR Stats.
8. *See* FinCEN, FIN-2026-Alert001, "FinCEN Alert on Fraud Rings and Their Exploitation of Federal Child Nutrition Programs in Minnesota" (Jan. 9, 2026).
9. According to FBI IC3, "[c]yber-enabled crime includes any illegal activity that is assisted using cyber-related means. Cyber-enabled crime involves the use of internet technology to communicate false or fraudulent representations to consumers. In addition to websites, emails, and chat rooms, almost all telephone calls utilize internet technology. These crimes may include, but are not limited to, advance-fee schemes, non-delivery of goods or services, computer hacking, or employment/business opportunity schemes, and intrusion-based crimes such as ransomware and data breaches." *See* FBI IC3, Frequently Asked Questions.

Fraud Schemes Targeting Health Care Benefit Programs and Associated Money Laundering Typologies

HHS, in partnership with state governments and commercial insurers, administers Health Care Benefit Programs through the Centers for Medicare and Medicaid Services (CMS).[10] These programs provide health care benefits for adults over 65, the disabled, lower-income individuals, and other eligible beneficiaries.[11] Health care providers and suppliers, including medical professionals, medical supply companies, and home and hospice care companies, must enroll and obtain provider or supplier numbers to submit claims for reimbursement for goods or services provided to program beneficiaries.

Submitting a claim involves providing the name and identification number of the beneficiary and associated medical professional to the Health Care Benefit Program for reimbursement. The issuer of reimbursements can depend on the specific Health Care Benefit Program. For example, for Medicare Part A[12] and Part B[13] medical claims or durable medical equipment (DME) claims for Medicare Fee-For Service (FFS) beneficiaries, reimbursements are issued to health care providers and suppliers by Medicare Administrative Contractors (MACs)[14] on behalf of CMS. In the case of Medicaid, a joint Federal and state program, state-level agencies each administer their own state Medicaid programs and issue reimbursements to the health care providers and suppliers.[15]

Use of Straw Owners and Shell Companies to Register as Health Care Providers and Suppliers

According to Federal law enforcement, illicit actors are increasingly exploiting Health Care Benefit Programs by filing false and fraudulent claims for reimbursement, including for nonexistent, exploitative, substandard, or unnecessary medical care. As part of these schemes, illicit actors often use straw owners (including non-resident aliens and stolen identities of retired physicians) to establish shell companies to obfuscate their ultimate beneficial ownership and register the entities as health care providers and suppliers with Health Care Benefit Programs. Those straw owners and their recently established shell companies then use fraudulent beneficial ownership information, false store fronts, and stolen or fictious documentation to open bank accounts as

10. *See* CMS, "Fact Sheet: Medicare & Medicaid Basics" (June 2024). Some health care benefit programs such as Medicare Part C are offered by private companies. *See* HHS, What is Medicare Part C.
11. *See generally* HHS, Health Insurance.
12. Medicare Part A helps beneficiaries cover inpatient care in hospitals, critical access hospitals, and skilled nursing facilities (not custodial or long-term care). It also helps cover hospice care and some home health care. *See* HHS, What is Medicare Part A.
13. Medicare Part B helps beneficiaries cover medical services like doctors' services, outpatient care, and other medical services that are not covered under Medicare Part A. *See* HHS, What is Medicare Part B.
14. MACs are private health care insurers that have been awarded a geographic jurisdiction to process Medicare Part A and Part B medical claims or DME claims for Medicare FFS beneficiaries. CMS relies on a network of MACs to serve as the primary operational contact between the Medicare FFS program and the health care providers enrolled in the program. MACs are multi-state, regional contractors responsible for administering both Medicare Part A and Medicare Part B claims. *See* CMS, What's a MAC.
15. *See generally* HHS, What's the Difference Between Medicare and Medicaid.

supposedly legitimate health care providers and suppliers.[16] Illicit actors may also purchase companies already registered with Health Care Benefit Programs, fail to notify CMS and/or the state-level agencies of the change in ownership as required, and use that pre-existing company for fraudulent purposes.[17] In both cases, these companies can purport to be involved in various sectors of the health care industry, especially medical supply companies for DME, home and hospice care companies, pharmacies, telemedicine companies, laboratories, and adult day care centers.

Filing False and Fraudulent Claims for Non-Existent, Exploitative, Substandard, or Unnecessary Medical Care

After registering with Health Care Benefit Programs, illicit actors obtain the names and identification numbers of beneficiaries enrolled in these programs, and use that information to file false and fraudulent claims for reimbursement, including nonexistent, exploitative, substandard, or unnecessary medical care in violation of Federal law, including criminal law and the False Claims Act.[18] This is often facilitated by paying kickbacks and bribes through recruiters and marketers to complicit doctors, nurses, pharmacists, and other medical professionals for fraudulent, non-existent, exploitative, or unnecessary medical care in violation of the Anti-Kickback Statute and other Federal laws.[19] This practice can include kickbacks and bribes for patient referrals, prescriptions, and doctors' orders – in some cases authorized when a doctor has not even evaluated a patient.[20] Illicit actors may also target beneficiaries directly through telemarketers and in-person recruiters that employ deceptive or fraudulent tactics to enlist witting or unwitting patients into, for example, ordering unnecessary DME or genetic testing.[21] In other cases, illicit actors may target both physicians and beneficiaries and steal their identification numbers through health care-related scams and other identity theft schemes.[22]

Illicit actors can submit the false claims to Health Care Benefit Programs through multiple methods, including:

16. In some cases, the illicit actors may physically accompany their straw owners to open the bank accounts. FinCEN encourages financial institutions to include surveillance footage as supporting documentation in health care fraud SAR filings to assist law enforcement investigations.
17. *See, e.g.*, U.S. Department of Justice (DOJ), U.S. Attorney's Office, Eastern District of New York, Press Release, "11 Defendants Indicted in Multi-Billion Health Care Fraud Scheme, the Largest Case by Loss Amount Ever Charged by the Department of Justice" ("Operation Gold Rush") (June 30, 2025); Indictment, Doc. No. 4, *United States v. Imam Nakhmatullaev, et al.*, No. 1:25-cr-203 (E.D.N.Y. June 18, 2025) ("Indictment"). *See also* DOJ, Press Release, "Durable Medical Equipment Owner Sentenced to 12 Years for $61 Million Medicare Fraud Scheme" (July 1, 2025); DOJ, Press Release, "Four California Residents Sentenced to Prison in Connection with $16M Hospice Fraud and Money Laundering Scheme" (Nov. 18, 2025).
18. *See, e.g.*, DOJ, Press Release, "Foreign National Sentenced for $3.2 Million Medicare Fraud Scheme" (May 20, 2025).
19. *See, e.g.*, DOJ, Press Release, "Two Individuals Plead Guilty to $68M Adult Day Care Fraud Scheme" (Jan. 15, 2026); DOJ, Press Release, "Doctor Sentenced to Seven Years in Prison for $24M Medicare Fraud" (Dec. 12, 2025); DOJ, Press Release, "Georgia Man Sentenced for $24M Kickback and Medicare Fraud Conspiracy" (Dec. 2, 2025).
20. *See id.*
21. *See, e.g.*, DOJ, Press Release, "Two Healthcare Executives Convicted for Exploiting Elderly Medicare Advantage Beneficiaries in $34 Million Fraud Scheme" (Jan. 7, 2026); DOJ, Press Release, "Michigan Doctor Sentenced to Four Years for $6.3M Medicare Fraud Scheme" (June 26, 2025); DOJ, Press Release, "Missouri Man Sentenced to 10 Years in Prison for $147M Health Care Fraud Conspiracy" (Dec. 12, 2025); DOJ Press Release, "Marketer Sentenced for $11.5M Genetic Testing Fraud and Kickback Scheme" (Sept. 19, 2025).
22. *See* Federal Communications Commission (FCC), Older Americans and Medicare Call Scams; Federal Trade Commission (FTC), Spot Health Insurance Scams; *see, e.g.*, DOJ, Press Release "Foreign National Sentenced for $3.2 Million Medicare Fraud Scheme" (May 20, 2025).

- *Billing for Exploitative, Substandard, or Unnecessary Goods or Services:* Filing claims for the provision of goods or services that are exploitative, substandard, or medically unnecessary;[23]
- *Double Billing:* Filing multiple claims for the same good or service;[24]
- *Phantom Billing:* Filing a claim for a good or service that was never provided to the patient;[25]
- *Unbundling:* Filing multiple claims for goods or services that are bundled together;[26] and
- *Upcoding:* Filing a claim for a more expensive good or service than the patient received.[27]

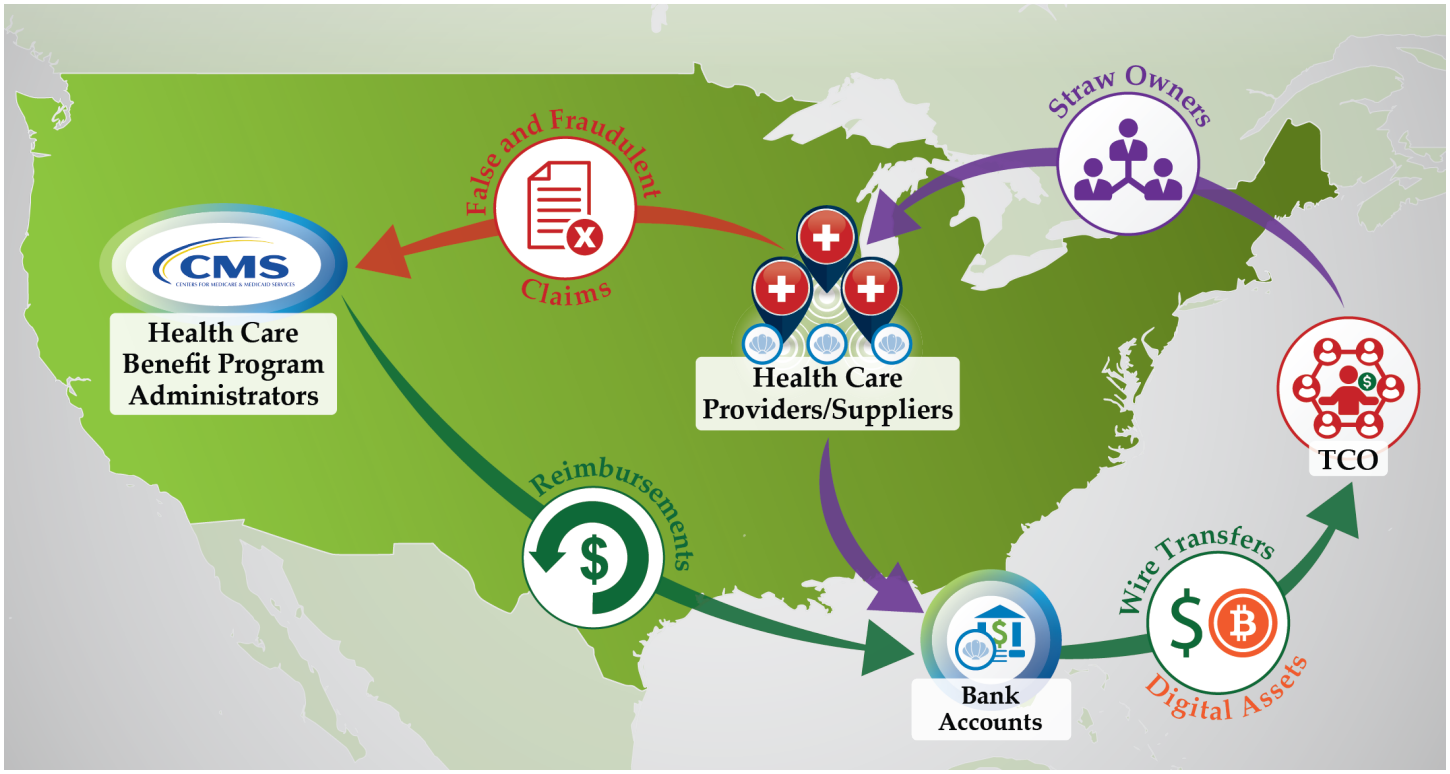
Obfuscation of Fraudulent Reimbursements through the U.S. and International Financial Systems

Once a claim is paid by an Automated Clearing House (ACH) deposit or, in limited cases, via paper check,[28] the illicit actor then immediately launders the fraudulently obtained reimbursement through the U.S. and international financial systems. In some cases, the illicit actor may also recruit complicit insiders within financial institutions to circumvent AML controls and facilitate the money laundering operation.[29] The laundering process can involve one or more of the following typologies:

- Wire transfers to bank accounts owned by individuals and shell companies under the illicit actor's direct or indirect control, located inside or outside the United States;
- Wire transfers to U.S. virtual asset service providers (VASPs) for purchase of digital assets, which are then sent to unhosted wallets or to wallets held at foreign-located VASPs in jurisdictions with weak or non-existent AML/CFT frameworks;
- Wire transfers to U.S. broker-dealers;[30]
- Wire transfers to online betting platforms;
- Check deposits to money mule accounts at banks;
- Cash withdrawals through banks and money services businesses (MSBs), including check cashers;[31] and
- Purchases of real estate, luxury goods, and high-value property in the United States or abroad.

23. *See, e.g.*, DOJ, Press Release, "Wound Graft Company Owners Sentenced for $1.2B Health Care Fraud and Agree to Pay $309M to Resolve Civil Liabilities Under the False Claims Act" (Dec. 12, 2025).
24. *See, e.g.*, DOJ, U.S. Attorney's Office, Western District of Washington, Press Release, "DOJ and Evergreen Treatment Services Settle Allegations Regarding Double Billing of Government Health Programs" (June 13, 2024).
25. *See, e.g.*, DOJ, Press Release, "Pharmacist Sentenced to Over Six Years in Prison for $6M Health Care Fraud Scheme" (Dec. 12, 2025).
26. *See, e.g.*, DOJ, Press Release, "Skyline Urology to pay $1.85 Million to Settle False Claims Act Allegations of Medicare Overbilling" (Feb. 25, 2019); DOJ, U.S. Attorney's Office, Eastern District of Pennsylvania, Press Release, "Coordinated Health and CEO Pay $12.5 Million to Resolve False Claims Act Liability for Fraudulent Billing" (Dec. 11, 2018).
27. *See, e.g.*, DOJ, U.S. Attorney's Office, Eastern District of Michigan, Press Release, "Hospitalist Companies Agree to Pay Nearly $4.4 Million to Settle False Claims Act Allegations" (Oct. 17, 2023).
28. As of September 30, 2025, Treasury has ceased issuing paper checks for most Federal payments. *See* The White House, Executive Order on Modernizing Payments To and From America's Bank Account, 90 Fed. Reg. 14001 (Mar. 28, 2025); The White House, "Fact Sheet: President Donald J. Trump Modernizes Payments to and from America's Bank Account" (Mar. 25, 2025).
29. *See, e.g.*, DOJ, Press Release, "Brooklyn Banker Pleads Guilty to Laundering Proceeds of Medicare Fraud for Transnational Criminal Organization" (Feb. 3, 2026).
30. *See* 31 C.F.R. § 1010.100(h).
31. *See* 31 C.F.R. § 1010.100(ff)(2) (defining check cashers).

Figure 1: Example of a TCO-Orchestrated Health Care Fraud Scheme



Case Study

11 Defendants Indicted in Multi-Billion Health Care Fraud Scheme, the Largest Case by Loss Amount Ever Charged by the U.S. Department of Justice (DOJ)

On June 30, 2025, the DOJ announced the results of its largest National Health Care Fraud Takedown in history with criminal charges against 324 defendants for alleged participation in various health care fraud schemes involving over $14.6 billion in intended loss.[32]

In one case that was part of the Takedown, dubbed by Federal law enforcement as "Operation Gold Rush," 11 defendants were indicted in the largest health care fraud case by loss amount ever charged by the DOJ for orchestrating a multi-billion dollar health care fraud and money laundering scheme to target, exploit, and steal from Medicare and Medicare Supplemental Insurers.[33] As alleged in the indictment, the defendants were members of a TCO based in Russia and elsewhere (hereafter, the "Organization") that submitted over $10.6 billion in fraudulent Medicare claims for DME. To do so, the Organization purchased dozens of DME

32. *See* DOJ, "National Health Care Fraud Takedown Results in 324 Defendants Charged in Connection with Over $14.6 Billion in Alleged Fraud" (June 30, 2025).
33. *See* Operation Gold Rush and Indictment, *supra* note 17. Medicare Supplement Insurance (Medigap) is supplemental insurance administered by private health insurance companies that Medicare beneficiaries can purchase to pay for out-of-pocket costs. *See* Medicare, What's Medicare Supplement Insurance. Fraud schemes targeting Medicare may also generate improper payments from Medigap insurers through similar billing patterns and beneficiary exploitation methods. CMS visibility into such activity is generally indirect, reinforcing the importance of financial institutions' awareness of related risks.

companies (hereafter "Scheme DME Companies") that had the ability to submit claims to Medicare and Medicare Supplemental Insurers. The Organization paid foreign nationals and others to serve as nominee owners of the Scheme DME Companies. The Organization then created fictitious corporate records that falsely indicated that the nominee owners controlled the Scheme DME Companies when, in fact, they were controlled by the Organization's foreign-based leadership. The Organization then used the Scheme DME Companies to rapidly submit false and fraudulent health care claims to Medicare. To submit the claims, the Organization stole the identities and personally identifiable information of more than one million Americans, including older adults and disabled Americans.

As further alleged, the Organization exploited the U.S. financial system by depositing checks into accounts at U.S. financial institutions and transferring funds out of accounts. The Organization used a range of tactics to circumvent AML controls at multiple financial institutions. Nominee owners, many of whom were unlawfully present in the United States, used false documentation to open accounts and disguise the true beneficial ownership and control of the Scheme DME Companies. Using the Scheme DME Companies to open accounts allowed the Organization to benefit from the illusion of legitimate commercial activity. Upon opening the accounts, the Organization funneled fraud proceeds from Medicare and Medicare Supplemental Insurers into the accounts as seemingly "clean" money. From there, the Organization siphoned off the funds to shell companies and various banks overseas, including banks in China, Singapore, Pakistan, Israel, and Türkiye. To further conceal the money trail, the Organization leveraged digital assets to launder the stolen funds.

Four defendants were arrested June 25, 2025 in Estonia on these charges, and the United States is seeking their extradition. The remaining seven defendants are at large.

HHS-OIG and CMS prevented the Organization from receiving the vast majority of the money that it conspired to steal from Medicare. The fraudulent scheme nonetheless resulted in nearly $900 million in payments to Scheme DME Companies from Medicare Supplemental Insurers and approximately $41 million in Medicare payments to the Scheme DME Companies.[34]

Soon after, DOJ, FBI, HHS-OIG, and other agencies established a Health Care Fraud Data Fusion Center to detect, investigate, and prosecute emerging health care fraud schemes, and implement E.O. 14243 by reducing duplicative data teams, increasing operational efficiency through a whole-of-government approach, and leveraging cloud computing, artificial intelligence, and other agency resources.[35]

34. *See* Operation Gold Rush and Indictment, *supra* note 17.
35. *See* DOJ, Press Release, "National Health Care Fraud Takedown Results in 324 Defendants Charged in Connection with Over $14.6 Billion in Alleged Fraud" (June 30, 2025); DOJ, Speech, "Head of Criminal Division Matthew R. Galeotti Announces Results of Health Care Fraud Takedown" (June 30, 2025); The White House, Executive Order on Stopping Waste, Fraud, and Abuse by Eliminating Information Silos, 90 Fed. Reg. 13681 (Mar. 20, 2025); *see also* DOJ, Health Care Fraud Unit; CMS, "Fraud Defense Operations Center" (Jan. 2026).

Red Flag Indicators of Fraud Schemes Targeting Health Care Benefit Programs

FinCEN has identified the following red flags to help financial institutions detect, prevent, and report suspicious activity connected to health care fraud schemes targeting Health Care Benefit Programs. Payments for reimbursements of health care benefits generally follow standardized and predictable payments patterns, which may make unusual changes in reimbursement activity (*e.g.*, deviations in payment volumes, timing, and credit and debit transactions) after enrollment or changes in ownership particularly indicative of health care fraud when assessed alongside other red flags. These payments can also include in the payment field the name of the MACs or state-level agencies issuing the reimbursements to the health care providers or suppliers. FinCEN encourages financial institutions to review whether their customers are receiving payments from MACs or state-level agencies for health care benefit reimbursements and use a risk-based approach to assess if such payments are consistent with their customer profile.[36] As no single red flag is determinative of illicit or suspicious activity, financial institutions should consider the surrounding facts and circumstances, such as a customer's historical financial activity, whether the transactions are in line with prevailing business practices, and whether the customer exhibits multiple red flags, before determining if a behavior or transaction is suspicious or otherwise indicative of a connection to health care fraud.

1. 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.

2. 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.

3. 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.

4. 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.

5. 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.

36. *See* **Appendix: MAC Jurisdictions** on pp. 11-13 for maps and a list of all MACs that have been awarded a geographic jurisdiction to process claims for Medicare Part A and Part B, home health and hospice care, and DME. *See also* CMS, A/B MAC Jurisdictions; CMS, Home Health & Hospice MAC Jurisdictions; CMS, DME MAC Jurisdictions; CMS, Medicare Administrative Contractors.

6. 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.

7. 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.

8. 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.

9. 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.

10. 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.

11. 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).

12. 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).

13. 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).

14. 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.

15. 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.

16 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.

17 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).

18 A customer is a health care provider or supplier with a pattern of making significant cash withdrawals for no readily apparent business reason.

19 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).

20 A customer is a health care provider or supplier that is transferring a significant volume of funds to individuals via high-value checks.

21 Without credible explanation, a customer routinely cashes high-value checks drawn from accounts associated with a health care provider or supplier.

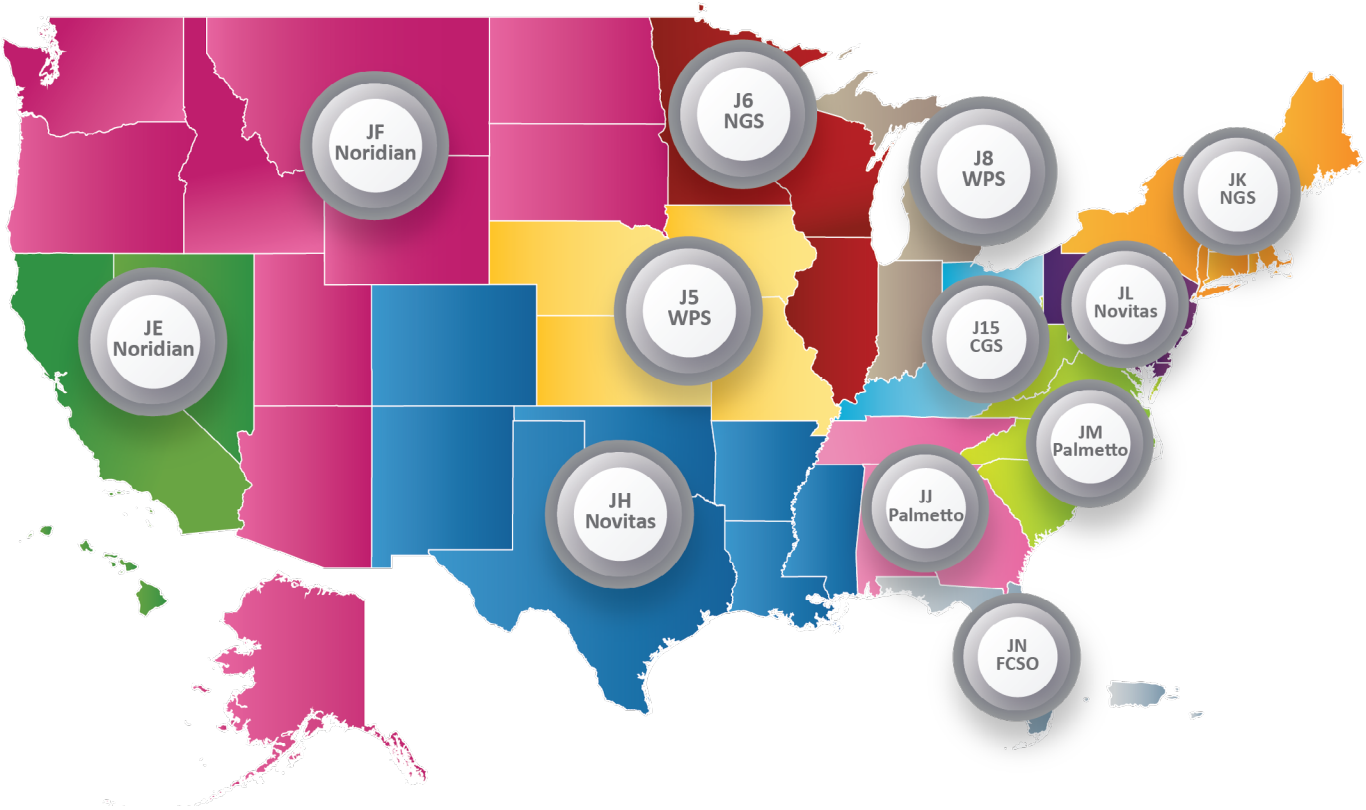
22 A customer that is a health care provider or supplier, or the customer's employee, engages in behavior suggesting efforts to evade the Currency Transaction Report (CTR) reporting requirement (*e.g.*, alters or cancels a transaction when advised a CTR would be filed or engages in structuring with multiple cash transactions for under $10,000), as well as avoid recordkeeping requirements.[37]

23 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.

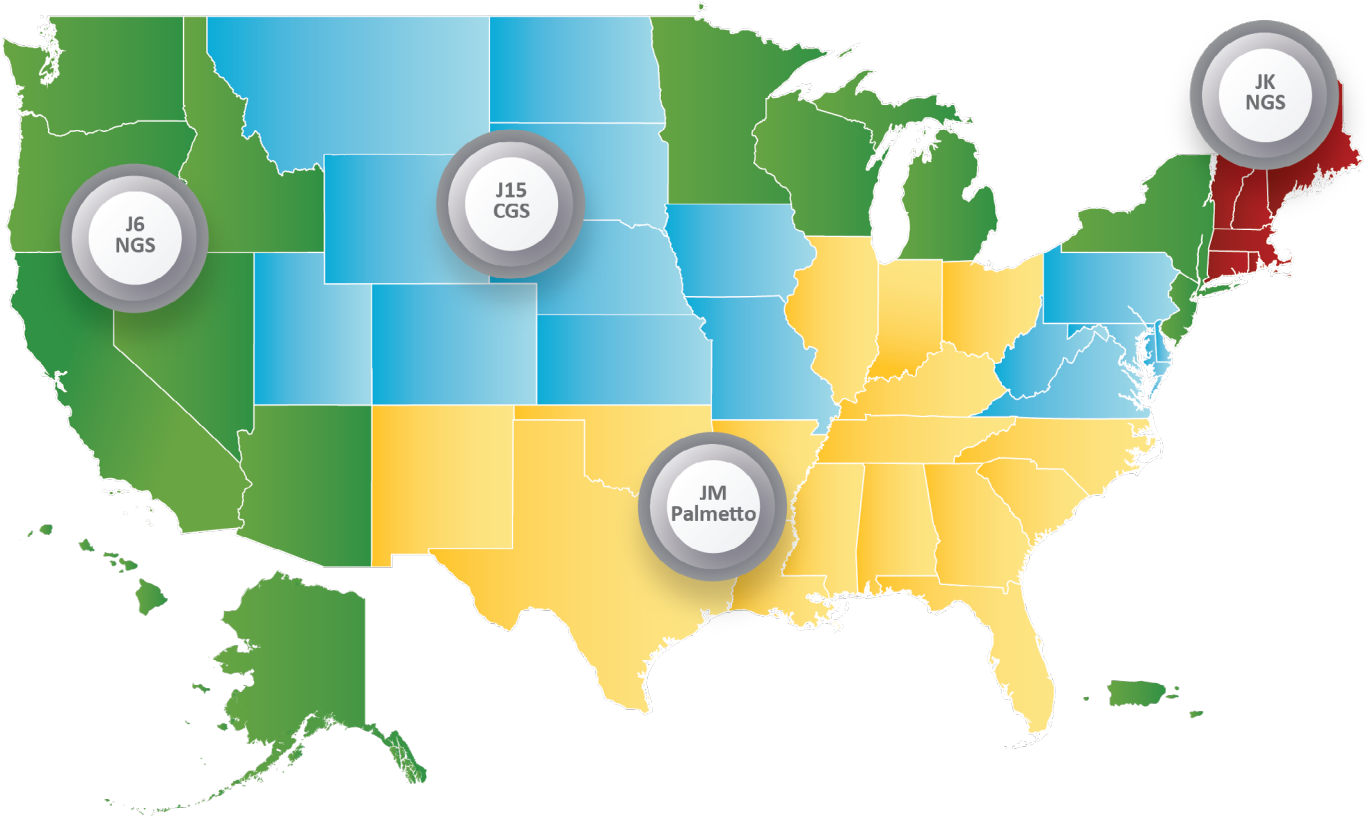
24 A customer is a health care provider or supplier registered with a Health Care Benefit Program that sends money transfers to VASPs, brokerage accounts, and online betting platforms for no seemingly legitimate business reason.

Appendix: MAC Jurisdictions

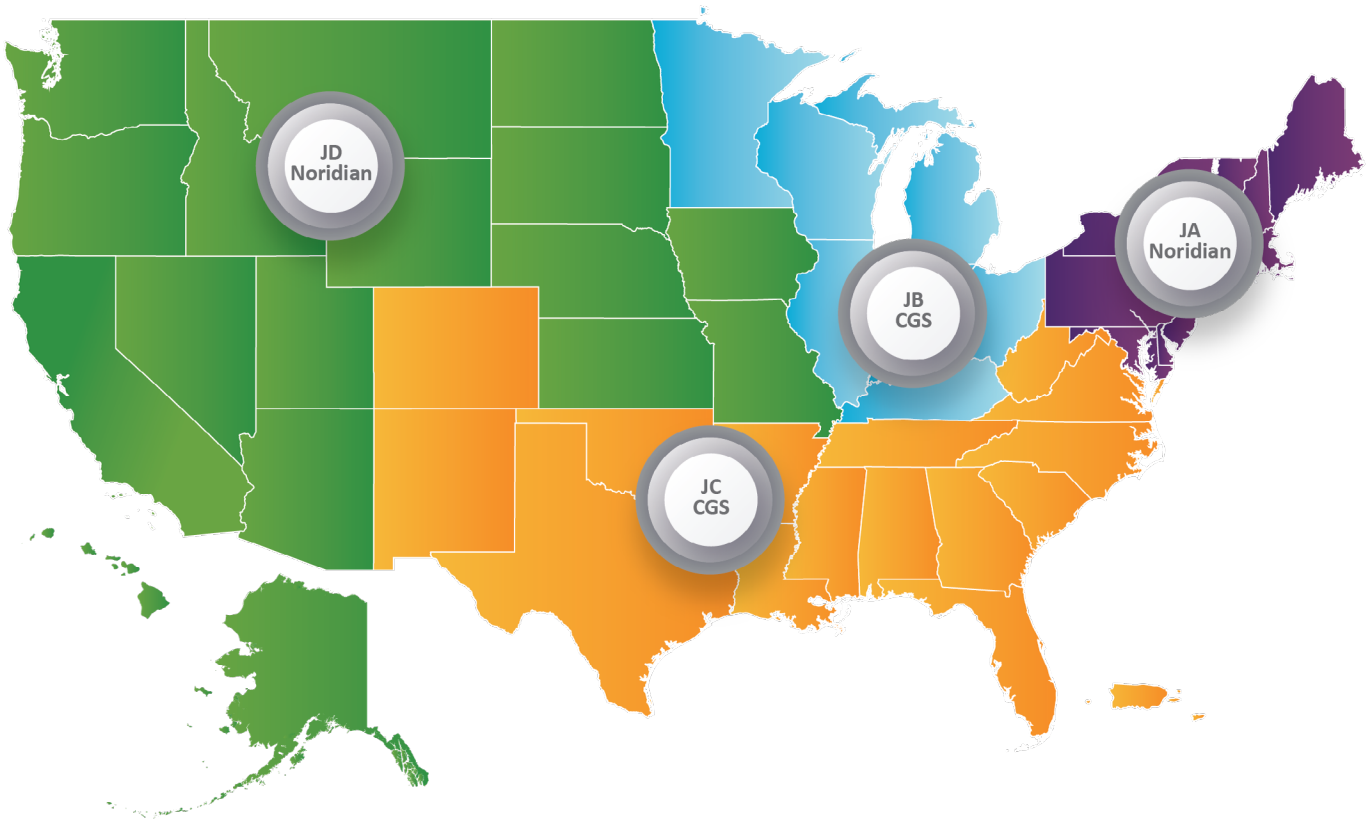
A/B MAC Jurisdictions



Home Health & Hospice MAC Jurisdictions



DME MAC Jurisdictions



MACs

MAC Jurisdiction	Processes Part A & Part B Claims for the following states/territories:	MAC
DME A	Connecticut, Delaware, District of Columbia, Maine, Maryland, Massachusetts, New Hampshire, New Jersey, New York, Pennsylvania, Rhode Island, Vermont	Noridian Healthcare Solutions, LLC
DME B	Illinois, Indiana, Kentucky, Michigan, Minnesota, Ohio, Wisconsin	CGS Administrators, LLC
DME C	Alabama, Arkansas, Colorado, Florida, Georgia, Louisiana, Mississippi, New Mexico, North Carolina, Oklahoma, South Carolina, Tennessee, Texas, Virginia, West Virginia, Puerto Rico, U.S. Virgin Islands	CGS Administrators, LLC
DME D	Alaska, Arizona, California, Hawaii, Idaho, Iowa, Kansas, Missouri, Montana, Nebraska, Nevada, North Dakota, Oregon, South Dakota, Utah, Washington, Wyoming, American Samoa, Guam, Northern Mariana Islands	Noridian Healthcare Solutions, LLC
5	Iowa, Kansas, Missouri, Nebraska	Wisconsin Physicians Service Government Health Administrators
6	Illinois, Minnesota, Wisconsin ****HH + H for the following states**: Alaska, American Samoa, Arizona, California, Guam, Hawaii, Idaho, Michigan, Minnesota, Nevada, New Jersey, New York, Northern Mariana Islands, Oregon, Puerto Rico, US Virgin Islands, Wisconsin and Washington	National Government Services, Inc.
8	Indiana, Michigan	Wisconsin Physicians Service Government Health Administrators

MAC Jurisdiction	Processes Part A & Part B Claims for the following states/territories:	MAC
15	Kentucky, Ohio **HH + H for the following states**: Delaware, District of Columbia, Colorado, Iowa, Kansas, Maryland, Missouri, Montana, Nebraska, North Dakota, Pennsylvania, South Dakota, Utah, Virginia, West Virginia, and Wyoming	CGS Administrators, LLC
E	California, Hawaii, Nevada, American Samoa, Guam, Northern Mariana Islands	Noridian Healthcare Solutions, LLC
F	Alaska, Arizona, Idaho, Montana, North Dakota, Oregon, South Dakota, Utah, Washington, Wyoming	Noridian Healthcare Solutions, LLC
H	Arkansas, Colorado, New Mexico, Oklahoma, Texas, Louisiana, Mississippi	Novitas Solutions, Inc.
J	Alabama, Georgia, Tennessee	Palmetto GBA, LLC
K	Connecticut, New York, Maine, Massachusetts, New Hampshire, Rhode Island, Vermont **HH + H for the following states**: Connecticut, Maine, Massachusetts, New Hampshire, Rhode Island, and Vermont	National Government Services, Inc.
L	Delaware, District of Columbia, Maryland, New Jersey, Pennsylvania (includes Part B for counties of Arlington and Fairfax in Virginia and the city of Alexandria in Virginia)	Novitas Solutions, Inc.
M	North Carolina, South Carolina, Virginia, West Virginia (excludes Part B for the counties of Arlington and Fairfax in Virginia and the city of Alexandria in Virginia) **HH + H for the following states**: Alabama, Arkansas, Florida, Georgia, Illinois, Indiana, Kentucky, Louisiana, Mississippi, New Mexico, North Carolina, Ohio, Oklahoma, South Carolina, Tennessee, and Texas	Palmetto GBA, LLC
N	Florida, Puerto Rico, U.S. Virgin Islands	First Coast Service Options, Inc.

** Also Processes Home Health and Hospice claims

Reminder of Relevant BSA Obligations and Tools for U.S. Financial Institutions

Suspicious Activity Reporting

A financial institution is required to file a SAR if it knows, suspects, or has reason to suspect a transaction conducted or attempted by, at, or through the financial institution involves funds derived from illegal activity; is intended or conducted to disguise funds derived from illegal activity; is designed to evade regulations promulgated under the BSA; lacks a business or apparent lawful purpose; or involves the use of the financial institution to facilitate criminal activity.[38] All statutorily defined financial institutions may voluntarily report suspicious transactions under the existing suspicious activity reporting safe harbor.[39]

38. *See* 31 U.S.C. § 5318(g)(1); *see also* 31 C.F.R. §§ 1020.320, 1021.320, 1022.320, 1023.320, 1024.320, 1025.320, 1026.320, 1029.320, 1030.320.
39. *See* 31 U.S.C. § 5318(g)(3). Financial institutions may report suspicious transactions regardless of amount involved and still take advantage of the safe harbor.

When a financial institution files a SAR, it is required to maintain a copy of the SAR and the original or business record equivalent of any supporting documentation for a period of five years from the date of filing the SAR.[40] Financial institutions must provide any requested documentation supporting the filing of a SAR upon request by FinCEN or an appropriate law enforcement or supervisory agency.[41] When requested to provide supporting documentation, financial institutions should take special care to verify that a requestor of information is, in fact, a representative of FinCEN or an appropriate law enforcement or supervisory agency. A financial institution should incorporate procedures for such verification into its BSA compliance or AML program. These procedures may include, for example, independent employment verification with the requestor's field office or face-to-face review of the requestor's credentials.

SAR Filing Instructions

SARs, and compliance with other BSA requirements, are crucial to identifying and stopping health care fraud. FinCEN requests that financial institutions indicate a connection between the suspicious activity being reported and the activities highlighted in this Advisory by including the key term "**HCF-2026-A001**" in SAR field 2 (Filing Institution Note to FinCEN), as well as in the narrative. Financial institutions may highlight additional Advisory, Alert, or Notice keywords in the narrative, if applicable.

Financial institutions should select SAR field 34(g) (Healthcare/Public or Private Health Insurance) and any other applicable check box. Financial institutions also should select all other relevant suspicious activity fields, such as those in SAR fields 36 (Money Laundering) and 38 (Other Suspicious Activities), if applicable.

Financial institutions should include all available information relating to the account and locations involved in the reported activity, identifying information related to other entities and persons involved in the activity and the status of their accounts with the institution. Financial institutions also should provide all available information regarding other domestic and foreign financial institutions involved in the activity; where appropriate, financial institutions should consider filing a SAR jointly on shared suspicious activity.[42]

Financial institutions are required to file complete and accurate reports that incorporate all relevant information available. In situations involving violations requiring immediate attention, such as ongoing money laundering schemes, a financial institution should also immediately notify, by telephone, an appropriate law enforcement authority, in addition to filing a timely SAR.[43] Immediate notification to law enforcement is especially important in situations involving suspected terrorist activity, as terrorists and terrorist organizations often rely on the

40. *See* 31 C.F.R. §§ 1020.320(d), 1021.320(d), 1022.320(c), 1023.320(d), 1024.320(c), 1025.320(d), 1026.320(d), 1029.320(d), 1030.320(d).
41. *See id.*; *see also* FinCEN, FIN-2007-G003, "Suspicious Activity Report Supporting Documentation" (June 13, 2007).
42. *See* 31 C.F.R. §§ 1020.320(e)(1)(ii)(A)(2))(i), 1021.320(e)(1)(ii)(A)(2)), 1022.320(d)(1)(ii)(A)(2), 1023.320(e)(1)(ii)(A)(2)(i), 1024.320(d)(1)(ii)(A)(2), 1025.320(e)(1)(ii)(A)(2), 1026.320(e)(1)(ii)(A)(2)(i), 1029.320(d)(1)(ii)(A)(2), 1030.320(d)(1)(ii)(A)(2).
43. *See, e.g.*, 31 C.F.R. §§ 1020.320(b)(3), 1022.320(b)(3), 1023.320(b)(3).

international financial system to acquire funding to sustain and finance their operations and engage in acts of terrorism. Additionally, FinCEN emphasizes that any financial institution and any director, officer, employee, or agent of such institution who makes, or requires another to make any voluntary disclosure of any possible violation of law or regulation to a government agency under the BSA or its implementing regulations is protected from liability for any such disclosure.[44]

Financial institutions wanting to report suspicious transactions that may potentially relate to terrorist activity should call the Financial Institutions Toll-Free Hotline at (866) 556-3974 (7 days a week, 24 hours a day).[45]

Other Relevant BSA Reporting Requirements

Financial institutions and other entities or persons may also have other relevant BSA reporting requirements to provide information in connection with the subject of this Advisory. These include obligations related to the CTR,[46] Report of Cash Payments Over $10,000 Received in a Trade or Business (Form 8300),[47] Report of Foreign Bank and Financial Accounts (FBAR),[48] Report of International Transportation of Currency or Monetary Instruments (CMIR),[49] Registration of Money Services Business (RMSB),[50] and Designation of Exempt Person (DOEP).[51]

Due Diligence

Banks, brokers or dealers in securities, mutual funds, and futures commission merchants and introducing brokers in commodities (FCM/IBs) are required to have appropriate risk-based procedures for conducting ongoing customer due diligence that include, but are not limited to: (i) understanding the nature and purpose of customer relationships for the purpose of developing a customer risk profile; and (ii) conducting ongoing monitoring to identify

44. 31 U.S.C. § 5318(g)(3); *see, e.g.*, 31 C.F.R. 1020.320(f).
45. The purpose of the hotline is to expedite the delivery of this information to law enforcement. Financial institutions should immediately report any imminent threat to local-area law enforcement officials.
46. A report of each deposit, withdrawal, exchange of currency, or other payment or transfer, by, through, or to a financial institution that involves a transaction in currency of more than $10,000. Multiple transactions may be aggregated when determining whether the reporting threshold has been met. *See* 31 C.F.R. §§ 1010.310-313, 1020.310-313, 1021.310-313, 1022.310-313, 1023.310-313, 1024.310-313, and 1026.310-313.
47. A report filed by a trade or business that receives currency in excess of $10,000 in one transaction or two or more related transactions. The transactions are required to be reported on a joint FinCEN/Internal Revenue Service form when not otherwise required to be reported on a CTR. *See* 31 C.F.R. §§ 1010.330-331. A Form 8300 also may be filed voluntarily for any suspicious transaction, even if the total amount does not exceed $10,000.
48. A report filed by a U.S. person that has a financial interest in, or signature or other authority over, foreign financial accounts with an aggregate value exceeding $10,000 at any time during the calendar year. *See* 31 C.F.R. § 1010.350; FinCEN Form 114.
49. A form filed to report the transportation of more than $10,000 in currency or other monetary instruments into or out of the United States. *See* 31 C.F.R. § 1010.340.
50. A form filed to register an MSB with FinCEN, or to renew such a registration. *See* 31 C.F.R. § 1022.380.
51. A report filed by banks to exempt certain customers from currency transaction reporting requirements. *See* 31 C.F.R. § 1010.311.

and report suspicious transactions and, on a risk basis, to maintain and update customer information.[52] Covered financial institutions are required to identify and verify the identity of beneficial owners of legal entity customers, subject to certain exclusions and exemptions.[53] Among other things, this facilitates the identification of legal entities that may be owned or controlled by foreign politically exposed persons (PEPs).

Senior foreign political figures and due diligence obligations for private banking accounts

In addition to these due diligence obligations, under section 312 of the USA PATRIOT Act (31 U.S.C. § 5318(i)) and its implementing regulations, covered financial institutions must implement due diligence programs for private banking accounts held for non-U.S. persons that are designed to detect and report any known or suspected money laundering or suspicious activity conducted through or involving such accounts.[54] Covered financial institutions must establish risk-based controls and procedures for ascertaining the identities of nominal and beneficial owners of such accounts and ascertaining whether any of these owners are senior foreign political figures, and for conducting enhanced scrutiny on accounts held by senior foreign political figures that is reasonably designed to detect and report transactions that may involve the proceeds of foreign corruption.[55]

AML/CFT program and correspondent account due diligence requirements

Financial institutions are reminded of AML/CFT program requirements,[56] and covered financial institutions are reminded of correspondent account due diligence requirements under Section 312 of the USA PATRIOT Act (31 U.S.C. § 5318(i)) and implementing regulations.[57] As described in FinCEN Interpretive Release 2004-1, the AML/CFT program of an MSB must include risk-based policies, procedures, and controls designed to identify and minimize risks associated with foreign agents and counterparties.[58]

52. *See* 31 C.F.R. §§ 1020.210(a)(2)(v), 1023.210(b)(5), 1024.210(b)(6), 1026.210(b)(5).
53. *See* 31 C.F.R. §§ 1010.230, 1010.650(e)(1) (defining "covered financial institution").
54. *See* 31 C.F.R. § 1010.620. The definition of "covered financial institution" is found in 31 C.F.R. § 1010.605(e)(1). The definition of "private banking account" is found in 31 C.F.R. § 1010.605(m). The definition of "non-U.S. person" is found in 31 C.F.R. § 1010.605(h).
55. *See* 31 C.F.R. § 1010.620(c).
56. *See* 31 C.F.R. §§ 1010.210, 1020.210, 1021.210, 1022.210, 1023.210, 1024.210, 1025.210, 1026.210, 1027.210, 1028.210, 1029.210, 1030.210.
57. *See* 31 C.F.R. § 1010.610.
58. *See* FinCEN, Anti-Money Laundering Program Requirements for Money Services Businesses with Respect to Foreign Agents or Foreign Counterparties, Interpretive Release 2004-1, 69 Fed. Reg. 74,439 (Dec. 14, 2004); *see also* FinCEN, FIN-2016-G001, "Guidance on Existing AML Program Rule Compliance Obligations for MSB Principals with Respect to Agent Monitoring" (Mar. 11, 2016).

Information Sharing

Information sharing among financial institutions is critical to identifying, reporting, and preventing health care fraud, government benefits fraud, and other illicit financial activity. Financial institutions and associations of financial institutions sharing information under the safe harbor authorized by section 314(b) of the USA PATRIOT Act are reminded that they may share information with one another regarding individuals, entities, organizations, and countries suspected of possible terrorist financing or money laundering, including laundering of the proceeds of fraud.[59] In accordance with the requirements of section 314(b) and its implementing regulations, FinCEN strongly encourages such voluntary information sharing as it relates to money laundering or possible terrorist financing in connection with Foreign Terrorist Organizations (FTOs)[60] and Specially Designated Global Terrorists (SDGTs).[61] Given the transnational nature of illicit activity related to fraud, FinCEN also encourages U.S. financial institutions to continue to use, and potentially expand, their existing processes to collect and share information with foreign financial institutions in furtherance of investigations that involve cross-border activity.[62]

FinCEN's Whistleblower Program

FinCEN maintains a whistleblower incentive program for violations of the BSA and certain national security laws such as the International Emergency Economic Powers Act (IEEPA). Individuals located in the United States or abroad who provide information may be eligible for awards if the information they provide leads to a successful enforcement action that results in monetary penalties exceeding $1,000,000 and the statutory requirements in 31 U.S.C. § 5323 are otherwise met. Under 31 U.S.C. § 5323, there are certain confidentiality protections to individuals submitting information as well as certain protections from retaliation by employers. Individuals may also choose to submit information anonymously to FinCEN, including through an attorney. FinCEN is currently accepting whistleblower tips and encourages those with knowledge of potential violations to contact FinCEN. To learn more about FinCEN's Whistleblower Program, visit https://www.fincen.gov/whistleblower-program.

The Financial Crimes Enforcement Network's Advisory Program communicates priority money laundering, terrorist financing, and other illicit finance threats and vulnerabilities to the U.S. financial system. Financial institutions may use this information to support effective, risk-based, and reasonably designed anti-money laundering and countering the financing of terrorism (AML/CFT) programs and suspicious activity monitoring systems to help generate highly useful information for law enforcement and national security agencies.

59. *See* 31 C.F.R. § 1010.540; *see also* FinCEN, "Section 314(b) Fact Sheet" (Dec. 2020).
60. *See* U.S. Department of State, "Foreign Terrorist Organizations."
61. The White House, Blocking Property and Prohibiting Transactions with Persons Who Commit, Threat to Commit, or Support Terrorism, 66 Fed. Reg. 49079 (Sept. 23, 2001).
62. *See* FinCEN, FIN-2025-G001, "Cross-Border Information Sharing By Financial Institutions and SAR Confidentiality" (Sept. 5, 2025).

For Further Information

FinCEN's website (www.fincen.gov) contains information on how to register for FinCEN Updates emails which are sent when new content is added to the site. Questions or comments regarding the contents of this Advisory should be addressed to the FinCEN Regulatory Support Section by submitting an inquiry at www.fincen.gov/contact.

The mission of the Financial Crimes Enforcement Network is to safeguard the financial system from illicit use, combat money laundering and its related crimes including terrorism, and promote national security through the strategic use of financial authorities and the collection, analysis, and dissemination of financial intelligence.