



FinCEN ADVISORY

FIN-2021-A001

February 2, 2021

Advisory on COVID-19 Health Insurance- and Health Care-Related Fraud

While FinCEN has observed a wide range of COVID-19 related fraud, this advisory primarily focuses on COVID-19-related fraud involving the health care industry.

This Advisory should be shared with:

- Chief Executive Officers
- Chief Operating Officers
- Chief Compliance Officers
- Chief Risk Officers
- AML/BSA Departments
- Legal Departments
- Cyber and Security Departments
- Customer Service Agents
- Bank Tellers

SAR Filing Request:

FinCEN requests financial institutions reference this advisory in SAR field 2 (Filing Institution Note to FinCEN) and the narrative by including the following key term: “**FIN-2021-A001**” and select SAR field 34g (health care – public or private health insurance). Additional guidance for filing SARs appears near the end of this advisory.

enforcement partners. Additional COVID-19-related information is located on FinCEN’s website at <https://www.fincen.gov/coronavirus>, which also contains information on how to register for [FinCEN Updates](#).

Introduction

The Financial Crimes Enforcement Network (FinCEN) is issuing this advisory to alert financial institutions to health insurance and health care frauds related to the COVID-19 pandemic. These frauds target Medicare, Medicaid/Children’s Health Insurance Program (CHIP), and TRICARE as well as health care programs provided through the Departments of Labor and Veterans Affairs (collectively, “health care benefit programs”) and private health insurance companies. In addition, the United States government has observed frauds in connection with COVID-19 relief funds for health care providers, such as those provided under the Paycheck Protection Program and Health Care Enhancement Act (PPP-HCEA).¹ This advisory contains descriptions of COVID-19-related fraud involving health care benefit programs and health insurance, associated financial red flag indicators, select case studies, and information on reporting suspicious activity.

This advisory is based on FinCEN’s analysis of COVID-19-related information obtained from Bank Secrecy Act (BSA) data, public reporting, and law

1. See Pub. L. No. 116-139.

Financial Red Flag Indicators of COVID-19 Health Insurance- and Health Care-Related Fraud Activity

Law enforcement and financial institutions have detected numerous instances of potential frauds related to health care benefit programs, health insurance, and COVID-19 health care relief funds.² Criminals are adapting known health insurance and health care fraud to take advantage of the pandemic. The following are representative types of this illicit activity:

- *Unnecessary services:* Ordering or submitting claims for expensive tests or services that do not test for COVID-19, oftentimes in conjunction with COVID-19 testing, such as medically unnecessary and expensive respiratory testing, allergy testing, genetic testing, narcotics screening, or whole-body health assessments,³ or providing testing for services not usually rendered by the company.
- *Billing schemes:* Billing for services not provided, or overbilling (e.g., upcoding or unbundling), when administering or processing COVID-19 testing and treatments.⁴
- *Kickbacks:* Paying service providers or purported marketing organizations an illegal kickback or bribe in exchange for ordering, or arranging for the ordering of, services and testing.
- *Health care technology schemes:* False and fraudulent representations about COVID-19 testing, treatments, or cures are used to defraud insurance carriers and to perpetrate fraud on the financial markets by defrauding investors.⁵
- *Telefraud and telehealth schemes:* Collecting beneficiaries' personally identifiable information (PII), including Medicare information. Solicitations will often link their requests for information to COVID-19 treatment and prevention, such as testing or protective equipment. Fraudsters then submit fraudulent claims for payment from health care benefit programs. Fraudsters have also used the stolen PII to submit fraudulent telehealth services claims.⁶

2. For information concerning frauds related to the COVID-19 vaccine, *see* FinCEN Notice, [FIN-2020-NTC4](#), “FinCEN Asks Financial Institutions to Stay Alert to COVID-19 Vaccine-Related Scams and Cyberattacks,” (December 28, 2020).
3. *See* Department of Justice (DOJ) Press Releases, “[United States Attorney’s Office Announces Charges in Fraud Cases Related to COVID-19](#),” (May 27, 2020) and “[Georgia Woman Arrested for Role in Scheme to Defraud Health Care Benefit Programs Related to Cancer Genetic Testing and COVID-19 Testing](#),” (May 15, 2020).
4. *See* DOJ Press Releases, “[Two Owners of New York Pharmacies Charged in a \\$30 Million COVID-19 Health Care Fraud and Money Laundering Case](#),” (December 21, 2020); and “[United States Attorney’s Office Announces Charges in Fraud Cases Related to COVID-19](#),” (May 27, 2020). Upcoding occurs when a provider bills the insurance company for higher and more expensive levels of medical service than were actually performed. Unbundling fraud occurs when a provider bills for multiple codes for a group of procedures that are covered in a single global billing code.
5. *See* DOJ Press Release, “[Medical Technology Company President Charged in Scheme to Defraud Investors and Health Care Benefit Programs in Connection with COVID-19 Testing](#),” (June 9, 2020). For additional information, including red flags for fraudulent COVID-19 testing, treatments, and cures, *see* FinCEN Advisory, [FIN-2020-A002](#), “Advisory on Medical Scams Related to the Coronavirus Disease 2019 (COVID-19),” (May 18, 2020).
6. *See* HHS-OIG Fraud Alert, “[COVID-19 Fraud is Rapidly Evolving](#),” (Last update, December 21, 2020) and “[National Telefraud Takedown Scheme](#)” (Current as of September 2020).

- *Fraudulently obtaining COVID-19 health care relief funds:* Filing false claims and applications for Federal relief funds,⁷ such as those provided under the Coronavirus Aid, Relief, and Economic Security (CARES) Act's Provider Relief Fund,⁸ the PPP-HCEA,⁹ or the Economic Impact Disaster Loan (EIDL) program, and the claim or application has a nexus to health care benefit programs.¹⁰
- *Identity theft leading to additional fraud:* Targeting beneficiaries for their PII and then using the stolen PII to commit COVID-19-related fraud against health care benefit programs.¹¹

To discern whether a health insurance fraud is COVID-19-related, financial institutions should assess whether the activity occurred around or after the Secretary of Health and Human Services' public health emergency declaration of January 31, 2020,¹² and whether the underlying purported service relates to COVID-19.

As no single financial red flag indicator is necessarily indicative of illicit or suspicious activity, financial institutions should consider all surrounding facts and circumstances before determining if a transaction is suspicious or otherwise indicative of potentially fraudulent activities related to COVID-19. In line with a risk-based approach to compliance with the BSA, financial institutions also are encouraged to perform additional inquiries and investigations where appropriate.

FinCEN identified the financial red flag indicators described below to alert financial institutions to fraud related to health insurance and health care, and to assist financial institutions in detecting, preventing, and reporting suspicious transactions related to such COVID-19-related fraud.

Such financial red flag indicators may include:

Additional, medically unnecessary services or billing schemes

- 1 After the COVID-19 public health emergency declaration, a health care service provider's account receives or continues to receive: (1) health care benefit program or health insurance payments well above the provider's estimated business transactions; or (2) payments at

7. See DOJ Press Releases, "[Florida Man Charged with COVID Relief Fraud, Health Care Fraud and Money Laundering](#)," (July 29, 2020); "[Florida Man Charged with COVID Relief Fraud and Health Care Fraud](#)," (July 10, 2020); and "[Ophthalmologist Previously Charged with Health Care Fraud Indicted For Defrauding SBA Program Intended To Help Small Businesses During COVID-19 Pandemic](#)" (June 24, 2020).
8. See U.S. Department of Health and Human Services (HHS), "[CARES Act Provider Relief Fund](#)," (Last reviewed on January 21, 2021).
9. See Pub. L. No. 116-139. For more information about unemployment insurance fraud, not necessarily connected to the health care industry, see FinCEN Advisory, [FIN-2020-A007](#), "Advisory on Unemployment Insurance Fraud During the Coronavirus Disease 2019 (COVID-19) Pandemic," (October 13, 2020).
10. See Pub. L. No. 116-123 and U.S. Small Business Administration, Information Notice [5000-20037](#), "Guidance Regarding Identification and Reporting of Suspicious Activity in the COVID-19 EIDL Loan Program," (July 22, 2020).
11. See HHS-Office of Inspector General (OIG) Fraud Alert, "[COVID-19 Fraud is Rapidly Evolving](#)," (Last update, December 21, 2020). For more information about identity theft related to COVID-19 relief efforts, including red flags, see FinCEN Advisory, [FIN-2020-A005](#), "Advisory on Cybercrime and Cyber-Enabled Crime Exploiting the Coronavirus Disease 2019 (COVID-19) Pandemic," (July 30, 2020); and FinCEN Advisory, [FIN-2020-A003](#), "Advisory on Imposter Scams and Money Mule Schemes Related to Coronavirus Disease 2019 (COVID-19)," (July 7, 2020).
12. See HHS, "[Determination that a Public Health Emergency Exists](#)," (January 31, 2020).

the same volume despite an expected diminished activity level during the public health emergency (e.g., a non-emergency medical transport company receiving higher than expected payments during stay-at-home orders).

- 2 A health care service provider's account receives health care benefit program or health insurance payments beyond the expected type or volume of service, based on staffing and other characteristics of the business (e.g., processing COVID-19 tests when the medical facility does not typically offer diagnostic services, or the facility is processing a high volume of tests despite only employing a few medical personnel).
- 3 A COVID-19-related health care service provider's business account has unusual transaction activities, such as payments for personal or medically irrelevant expenses (e.g., payments to automobile dealers, travel agents, or retailers of luxury goods).

Potential fraudulent businesses

- 4 Following the COVID-19 public health emergency declaration, personal or business accounts, especially ones that did not previously receive health care-related payments, begin receiving steep increases in health care benefit program or health insurance payments.
- 5 A purported health care service provider's account receives health care benefit program or health insurance payments related to COVID-19 services, and then individuals immediately withdraw the funds in a manner that is not typical for health care businesses (e.g., cashier's checks, cash withdrawals, certain types of Automated Clearing House (ACH) transfers, or domestic and international wire transfers).
- 6 After the COVID-19 public health emergency determination, a purported health care provider's account does not receive small-dollar check deposits, payments from merchant fee servicers, or cash payments from patients that would indicate patient copayments. This may indicate the absence of actual business activity.
- 7 A newly formed health care business account has a volume or type of payment that seems inconsistent with expected levels of activity for such an account.
- 8 The physical location of a purported medical facility receiving reimbursements for COVID-19-related health care services or relief funds is non-existent, a residential address, a commercial mail receiving agency address (e.g., a UPS Store address), or another non-office building address (e.g., a purported medical facility is listed as a laboratory, but the physical address is a vacant lot, car dealership, restaurant, or retail store).
- 9 The purported laboratory, health care service provider, or medical service personnel or their counterparties appear to have a minimal web presence, or one that begins around the time of the COVID-19 public health emergency declaration.

- 10 Following the public health emergency declaration, the physical location of a purported medical facility receiving payments for health care services or relief funds is far from the physical location of the majority of its patients or the providers purported to be practicing there, unless the facility is providing appropriate telehealth services (e.g., a purported medical facility located in a western state receives payments related to patients residing on the East Coast).

Kickbacks and money laundering

- 11 After the COVID-19 public health emergency declaration, a health care service provider's or other business account begins having overly complex, medical-related transactions involving multiple counterparties indicative of possible structuring, layering, kickbacks, or fraudulent medical claims.
- 12 A health care service provider's account makes frequent or unusually large payments recorded as advertising or marketing expenses, or makes recurring round-dollar payments to one or multiple individuals in a manner inconsistent with its payroll-related withdrawals. The payments may reference "director fees," "consulting fees," "marketing," or "business process outsourcing."
- 13 A health care service provider starts receiving payments from laboratories and health care services companies, but there is no financial documentation (e.g., operating expense payments) that the provider rendered legitimate services. When questioned, the provider indicates that he or she invested in the company and the payments are dividends or payments for services (e.g., a laboratory pays a physician for services related to a COVID-19 laboratory test). The tests, however, are not related to the physician's specialization or do not normally require a physician's involvement.

Fraudulently obtaining COVID-19-relief funds¹³

- 14 An account with no previous known association with providing health care services, receives an unexpected or excessive COVID-19-related payment that appears to be the CARES Act's Provider Relief Fund or the PPP-HCEA payments. Shortly after the account receives the deposit, an individual(s) withdraws the funds via large cash withdrawals, cashier's checks, wires to an overseas account, transfers to personal accounts, or payments for non-business expenses.
- 15 An account previously associated with providing health care services but that has not been recently active or appears to be defunct, receives an unexpected or excessive COVID-19-related payment that appears to be the CARES Act's Provider Relief Fund or the PPP-HCEA payments.
- 16 An account holder receives a substantial amount of reimbursements from health care benefit programs or health insurance companies for services rendered at the same time that the account holder receives COVID-19-related unemployment insurance payments.¹⁴

-
13. These red flag indicators pertain only to suspicious activity with a nexus to the health care industry and COVID-19. For non-health care industry suspicious activities related to COVID-19, please review FinCEN's prior COVID-19 related advisories and notices located on FinCEN's website at <https://www.fincen.gov/coronavirus>.
14. For more information about COVID-19-related unemployment insurance fraud, see FinCEN Advisory, [FIN-2020-A007](#), "Advisory on Unemployment Insurance Fraud during the Coronavirus Disease 2019 (COVID-19) Pandemic," (October 13, 2020).

Case Studies

Two Owners of New York Pharmacies Charged in a \$30 Million COVID-19 Health Care Fraud and Money Laundering Case¹⁵

Federal authorities indicted two owners of several New York-area pharmacies for their alleged roles in a \$30 million health care fraud and money laundering scheme. The indictment alleges that the defendants acquired control over dozens of New York pharmacies by paying others to pose as the owners of the pharmacies and hiring pharmacists to pretend to be supervising pharmacists at the pharmacies, for the purpose of obtaining pharmacy licenses and insurance plan credentialing. According to the indictment, the defendants used COVID-19 emergency override billing codes to submit fraudulent claims to Medicare, for which they were allegedly paid over \$30 million for medications that never were purchased by the pharmacies, prescribed by physicians, or dispensed to patients. The defendants frequently filed such claims during periods when pharmacies were non-operational, and used doctors' names on prescriptions without their permission.

The indictment also alleges that, with the proceeds of the fraud, the defendants engaged in a complex, money laundering conspiracy where they created sham pharmacy wholesale companies and fabricated invoices to legitimate pharmaceutical drug purchases. In a first phase, the defendants conspired with an international money launderer who arranged for funds to be wired from the sham pharmacy wholesale companies to companies in China for distribution to individuals in Uzbekistan. The defendants received cash in exchange, provided for by members of the Uzbekistani immigrant community to an unlicensed money transfer business for remittance to their relatives in Uzbekistan, minus a commission that was deducted by the money launderer. In a second phase, when the amount of fraudulent proceeds exceeded the amount of cash available in the Uzbekistani immigrant community, the defendants directed the international money launderer to transfer funds back from the sham wholesale companies to the defendants, their relatives, or their designees, in the form of certified cashier's checks and bags of cash. The defendants used the proceeds of the scheme to purchase real estate and other luxury items.

15. See DOJ Press Release, "[Two Owners of New York Pharmacies Charged in a \\$30 Million COVID-19 Health Care Fraud and Money Laundering Case](#)," (December 21, 2020).

Medical Technology Company President Charged in Scheme to
Defraud Investors and Health Care Benefit Programs in Connection
with COVID-19 Testing¹⁶

The president of a California-based medical technology company allegedly paid kickbacks and bribes to marketers and doctors to run an allergy screening test for 120 allergens on every patient regardless of medical necessity. As the COVID-19 pandemic progressed and many patients in the United States faced difficulty obtaining access to COVID-19 testing, the company president sought to expand the pre-existing allergy test scheme and capitalize on a national emergency for financial gain by combining the COVID-19 test with the more expensive allergy testing which did not identify or detect COVID-19. In addition, the company president allegedly made false claims to investors concerning the company's ability to provide accurate, fast, reliable, and cheap COVID-19 tests. The Fraud Section of the Criminal Division of the Department of Justice and the U.S. Attorney's Office for the Northern District of California charged the individual in connection with his alleged participation in schemes to mislead investors, to manipulate the company's stock price, and to conspire to commit health care fraud in connection with the submission of over \$69 million in false and fraudulent claims for allergy and COVID-19 testing. HHS-OIG, the U.S. Postal Inspection Service, the Federal Bureau of Investigation, the Veterans Affairs Office of Inspector General, and the Defense Criminal Investigative Service investigated the case.

Information on Reporting Suspicious Activity

Suspicious Activity Report (SAR) Filing Instructions

SAR reporting, in conjunction with effective implementation of BSA compliance requirements by financial institutions, is crucial to identifying and stopping health insurance and health care frauds, including those related to the COVID-19 pandemic. Financial institutions should provide all pertinent information in the SAR. Following these filing instructions will make it easier for FinCEN, law enforcement, supervisors, and other relevant government agencies to identify and utilize the information submitted in the SAR.¹⁷

- FinCEN requests that financial institutions reference this advisory by including the key term “FIN-2021-A001” in SAR field 2 (Filing Institution Note to FinCEN) and the narrative portion of the SAR to indicate a connection between the suspicious activity being reported and the activities highlighted in this advisory.

16. See DOJ Press Release, “[Medical Technology Company President Charged in Scheme to Defraud Investors and Health Care Benefit Programs in Connection with COVID-19 Testing](#),” (June 9, 2020).
17. FinCEN requests that financial institutions only reference this advisory if the suspicious activity relates to the health care industry and COVID-19. For non-health care industry suspicious activities related to COVID-19, please review FinCEN’s prior COVID-19 related advisories and notices located on FinCEN’s website at <https://www.fincen.gov/coronavirus>.

- Financial institutions also should select SAR field 34(g) (health care – public or private health insurance) as the associated suspicious activity type to indicate a connection between the suspicious activity being reported and COVID-19. Financial institutions should include additional detail about the type of health care fraud (e.g., Medicare – services not provided) in the narrative.
- FinCEN requests that financial institutions wishing to report potential health care fraud unrelated to COVID-19 should not include this advisory's key term in SAR field 2 or the SAR's narrative portion. Instead, please select field 34(g) and detail the activity in the narrative (e.g. addiction treatment – services not provided; or pain clinic – "marketing" fees).
- Please refer to FinCEN's [May 2020 Notice Related to the Coronavirus Disease 2019 \(COVID-19\)](#) which contain information regarding reporting COVID-19-related crime, and remind financial institutions of certain BSA obligations.

For Further Information

Financial institutions should send questions or comments regarding the contents of this advisory to the FinCEN Regulatory Support Section at frc@fincen.gov.

To report suspected heath care fraud, waste, or abuse within Medicare, Medicaid, CHIP, or the Marketplaces, please go to the following website to determine the best resource to notify:
<https://www.cms.gov/About-CMS/Components/CPI/CPIReportingFraud>.

For the general public to report suspected fraud, waste, or abuse in Medicare or Medicaid call the HHS OIG at 1-800-HHS-TIPS (1-800-447-8477).

The mission of FinCEN 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.