FinCEN ADVISORY

FIN-2020-A002

May 18, 2020

Advisory on Medical Scams Related to the Coronavirus Disease 2019 (COVID-19)

Detecting, preventing, and reporting COVID-19-related scams and illicit activity is critical to our national security, safeguarding legitimate relief efforts, and protecting innocent people from harm.

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: "**COVID19 FIN-2020-A002**" and select SAR field 34(z) (Fraud-other). Additional guidance for filing SARs appears near the end of this advisory.

The Financial Crimes Enforcement Network (FinCEN) is issuing this advisory to alert financial institutions to rising medical scams related to the COVID-19 pandemic. This advisory contains descriptions of COVID-19-related medical scams, case studies, red flags, and information on reporting suspicious activity.[1]

This is the first of several advisories FinCEN intends to issue concerning financial crimes related to the COVID-19 pandemic. These advisories are based on FinCEN's analysis of COVID-19-related information obtained through public reports, Bank Secrecy Act (BSA) data, and law enforcement partners. FinCEN will issue financial analyses and intelligence, as appropriate, to financial institutions to help them detect, prevent, and report suspected illicit activity.[2] Additionally, FinCEN has temporarily expanded its Rapid Response Program, which supports law enforcement and financial institutions in the recovery of funds stolen via fraud, theft, and other financial crimes related to COVID-19.

1. While this advisory focuses on medical-related scams, financial institutions should note that criminal actors may use similar fraudulent methods involving non-medical-related goods or services. Many COVID-19-related scams are similar to those observed before the pandemic, and illicit actors have modified their schemes to take advantage of, and profit from, the pandemic by victimizing innocent people and businesses.
2. For up-to-date information on FinCEN COVID-19-related releases, please visit FinCEN Coronavirus Updates at https://www.fincen.gov/coronavirus.

Financial Red Flag Indicators of COVID-19 Fraudulent Activity

BSA data, as well as information from other federal agencies, foreign government partners, and public sources indicate possible illicit activities related to the COVID-19 pandemic regarding (1) fraudulent cures, tests, vaccines, and services; (2) non-delivery scams; and (3) price gouging and hoarding of medical-related items, such as face masks and hand sanitizer. FinCEN identified the following red flag indicators to help financial institutions identify COVID-19-related medical scams, and to assist financial institutions in detecting, preventing, and reporting suspicious transactions associated with the COVID-19 pandemic.

As no single red flag is necessarily indicative of illicit or suspicious activity, financial institutions should consider additional contextual information and 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 indicators, before determining if a transaction is suspicious or otherwise indicative of fraudulent COVID-19-related activities. In line with their risk-based approach to compliance with the BSA, financial institutions also are encouraged to perform additional inquiries and investigations where appropriate. Some of these red flags are common indicators of fraudulent merchant activity committed by shell or fraudulent retail or wholesale business operators. Additionally, some of the red flag indicators outlined below may apply to multiple COVID-19-related fraudulent activities.

Medical-Related Frauds, Including Fraudulent Cures, Tests, Vaccines, and Services

Several federal agencies have detected fraudulent COVID-19-related cures, tests, vaccines, and associated services being offered to the public.[3] Examples of fraudulent medical services include claims related to purported vaccines or cures for COVID-19, claims related to products that purportedly disinfect homes or buildings, and the distribution of fraudulent or unauthorized at-home COVID-19 tests. Some of these scams may be perpetrated by illicit actors who recently formed unregistered or unlicensed medical supply companies. Financial indicators of these scams may include:

3. *See* Department of Justice (DOJ) Press Release, "Georgia resident arrested for selling illegal products claiming to protect against viruses," (April 9, 2020); U.S. Department of Homeland Security News Release, "ICE HSI arrests Georgia resident for selling illegal pesticide, claiming it protects against coronavirus," (April 14, 2020); U.S. Customs and Border Protection (CBP) National Media Release, "CBP Officers Seize Fake COVID-19 Test Kits at LAX," (March 14, 2020); FTC Press Release, "FTC, FDA Send Warning Letters to Seven Companies about Unsupported Claims that Products Can Treat or Prevent Coronavirus," (March 9, 2020); and Federal Bureau of Investigation (FBI) Press Releases, "FBI Warns of Emerging Health Care Fraud Schemes Related to COVID-19 Pandemic," (April 13, 2020); and "FBI Warns Health Care Professionals of Increased Potential for Fraudulent Sales of COVID-19-Related Medical Equipment," (March 27, 2020).

1. U.S. authorities, such as the Federal Trade Commission (FTC), the Food and Drug Administration (FDA), or the DOJ, have identified the company, merchant, or business owners as selling fraudulent products.[4]

2. A web-based search or review of advertisements indicates that a merchant is selling at-home COVID-19 tests,[5] vaccines, treatments, or cures.

3. The customer engages in transactions to or through personal accounts related to the sale of medical supplies, which could indicate that the selling merchant is an unregistered or unlicensed business or is conducting fraudulent medical-related transactions.

4. The financial institution's customer has a website with one or more indicia of suspicion, including a name/web address similar to real and well-known companies, a limited internet presence, a location outside of the United States, and/or the ability to purchase pharmaceuticals without a prescription when one is usually required.

5. The product's branding images found in an online marketplace appear to be slightly different from the legitimate product's images, which may indicate a counterfeit product.

6. The merchant is advertising the sale of highly sought-after goods related to the COVID-19 pandemic and response at either deeply discounted or highly inflated prices.

7. The merchant is requesting payments that are unusual for the type of transaction or unusual for the industry's pattern of behavior. For example, instead of a credit card payment, the merchant requires a pre-paid card, the use of a money services business, convertible virtual currency, or that the buyer send funds via an electronic funds transfer to a high-risk jurisdiction.

8. Financial institutions might detect patterns of high chargebacks and return rates in their customer's accounts. These patterns can be indicative of merchant fraud in general.

Case Study: U.S. Authorities Take Action Against Fraudulent COVID-19 Tests and Treatments

4. For current lists of COVID-19-related warning letters and fraudulent products, visit FDA: "Fraudulent Coronavirus Disease 2019 (COVID-19) Products" and FTC: "FTC Coronavirus Warning Letters to Companies." For information pertaining to COVID-19-related DOJ actions, visit: "Coronavirus Fraud News."

5. At the time of this publication, the FDA has authorized three at-home tests: the "LabCorp COVID-19 RT-PCR," the Rutgers Clinical Genomics Laboratory's molecular Laboratory Developed Test, and the Everlywell COVID-19 Test Home Collection Kit. *See* FDA News Release, "Coronavirus (COVID-19) Update: FDA Authorizes First Test for Patient At-Home Sample Collection," (April 21, 2020); FDA News Release, "Coronavirus (COVID-19) Update: FDA Authorizes First Diagnostic Test Using At-Home Collection of Saliva Specimens," (May 8, 2020); and FDA News Release, "FDA Authorizes First Standalone At-Home Sample Collection Kit that can be used with Certain Authorized Tests," (May 16, 2020).

Non-Delivery Fraud of Medical-Related Goods Scams

The COVID-19 pandemic has disrupted global shipping and created sudden and substantial demand for certain goods, especially medical-related goods. This demand creates a situation where criminals may defraud consumers and companies through non-delivery of merchandise. In these non-delivery scams, a customer pays a company for goods the customer will never receive. These bogus companies advertise test kits, masks, drugs, and other goods they never intend to deliver, and sometimes never possess at all. Victims can include unsuspecting companies, hospitals, governments, and consumers. These fraudulent transactions occur through websites, robocalls, or on the Darknet. Some schemes involve shell companies[6] to facilitate transactions. In its March 27, 2020 warning to the health care industry, the FBI asked the medical community to exercise due diligence and appropriate caution when dealing with unfamiliar vendors and when relying on unidentified third-party brokers in the supply chain.[7] Financial indicators of these scams may include:

9. The merchant does not appear to have a lengthy corporate history (e.g., the business was established within the last few months), lacks physical presence or address, or lacks an Employer Identification Number. Additionally, if the merchant has an address, there are noticeable discrepancies between the address and a public record search for the company or the street address, multiple businesses at the same address, or the merchant is located in a high-risk jurisdiction or a region that is not usually associated with the merchandise they are selling.

10. Searches in corporate databases reveal that the merchant's listing contains a vague or inappropriate company name, multiple unrelated names, a suspicious number of name variations, multiple "doing business as" (DBA) names, or does not align with its business model.

11. Merchants are reluctant to provide the customer or the financial institution that is processing the transactions with invoices or other documentation supporting the stated purpose of trade-related payments.

12. The financial institution does not understand the merchant's business model, and has difficulty determining the true nature of the company and its operations.

13. The merchant cannot provide shipment-tracking numbers to the customer or proof of shipment to a financial institution so it may process related financial transactions.

6. Shell companies are defined as non-publicly traded corporations or limited liability companies (LLCs) that have no physical presence beyond a mailing address and generate little to no independent economic value. *See* FinCEN Guidance, FIN-2006-G014 "Potential Money Laundering Risks Related to Shell Companies," (November 2006); and Suspicious Activity Reports (SAR) Activity Review: Issue 1 (October 2000), Issue 2 (June 2001), and Issue 7 (August 2004).

7. *See* FBI Press Release, "FBI Warns Health Care Professionals of Increased Potential for Fraudulent Sales of COVID-19-Related Medical Equipment," (March 27, 2020).

14 The merchant claims several last minute and suspicious delays in shipment or receipt of goods. For example, the merchant claims that the equipment was seized at port or by authorities, that customs has not released the shipment, or that the shipment is delayed on a vessel and cannot provide any additional information about the vessel to the customer or their financial institution.

15 The merchant cannot explain the source of the goods or how the merchant acquired bulk supplies of highly sought-after goods related to the COVID-19 pandemic.

16 Domestic or foreign governments have identified the merchant or its owners/incorporators as being associated with fraudulent and criminal activities.

17 A newly-opened account receives a large wire transaction that the accountholder failed to mention during the account opening process.

Case Study: A Virginia Financial Institution Alerted the U.S. Secret Service (USSS) and Successfully Helped Prevent a $317 Million Non-Delivery Scam

Price Gouging and Hoarding of Medical-Related Items

FinCEN and DOJ have received numerous reports of suspected hoarding and price gouging related to the COVID-19 pandemic. DOJ established the Hoarding and Price Gouging Task Force on March 24, 2020, to address COVID-19-related market manipulation, hoarding, and price gouging. According to DOJ, hoarding and price gouging are defined as the act by any person or company of accumulating an unreasonable amount of any of these materials for their personal use, or accumulating any of these materials for purposes of selling them far above prevailing market prices.[8] In many cases, individuals have been selling surplus items or newly acquired bulk shipments of goods, such as masks, disposable gloves, isopropyl alcohol, disinfectants, hand sanitizers, toilet paper, and other paper products at inflated prices because of the COVID-19 pandemic. Payment methods vary by scheme and can include the use of pre-paid cards, money services businesses, credit card transactions, wire transactions, or electronic fund transfers. On March 23, 2020, President Trump issued Executive Order (E.O.) 13910, pursuant to section 102 of the Defense Production Act, which prohibits hoarding of designated items.[9] Financial indicators of these scams may include:

8. *See* DOJ, "Department of Justice COVID-19 Hoarding and Price Gouging Task Force," (March 24, 2020).

9. *See* E.O. 13910, "Executive Order on Preventing Hoarding of Health and Medical Resources to Respond to the Spread of COVID-19," (March 23, 2020). The E.O. does not define hoarding. The E.O delegates the authority to prevent hoarding to the Secretary of Health and Human Services and to designate materials "the supply of which would be threatened by persons accumulating the material either in excess of reasonable demands of business, personal, or home consumption, or for the purpose of resale at prices in excess of prevailing market prices." Furthermore, the Attorney General of the United States stated that the "Department will investigate and prosecute those who acquire vital medical supplies in excess of what they would reasonably use or for the purpose of charging exorbitant prices to the healthcare workers and hospitals who need them." *See* DOJ, "Department of Justice COVID-19 Hoarding and Price Gouging Task Force," (March 24, 2020).

18 In addition to the use of personal accounts for business purposes (*see* indicator number 3 above), a customer begins using their personal accounts for business-related transactions after January 2020, and sets up a medical supply company or is selling highly sought-after COVID-19-related goods online, such as hand sanitizer, toilet paper, masks, and anti-viral or disinfectant cleaning supplies.

19 The customer begins using their money services or bank account differently. For example, prior to January 2020, the customer never linked their account to the sale of goods on the internet. Since the COVID-19 pandemic began, however, the customer is receiving deposits with payment messages indicating that they are for the sale of medical goods, disinfectants, sanitizers, and paper products sold on the internet.

20 The customer's accounts are receiving or sending electronic fund transfers (EFT) to/from a newly established company that has no known physical or internet presence.

21 The customer's account is used in transactions for COVID-19-related goods, such as masks and gloves, with a company that is not a medical supply distributor, is involved in other non-medical-related industries, or is not known to have repurposed its manufacturing to create medical-related goods. For example, the company is currently selling medical and sanitary supplies, and prior to January 2020, the company was listed as an automotive shop, a lumberyard, or a restaurant.

22 The customer makes unusually large deposits that are inconsistent with the customer's profile or account history. Upon further investigation, the customer states, or open-source research indicates, that the customer was selling COVID-19-related goods not usually sold by the customer.

Case Study: FBI Arrests Brooklyn Man for Possession and Sale of Scarce Medical Equipment

Case Studies[10]

Medical-Related Frauds, Including Fraudulent Cures, Tests, Vaccines, and Services[11]

U.S. Authorities Take Action Against Fraudulent COVID-19 Tests and Treatments

On March 12, 2020, CBP officers at Los Angeles International Airport (LAX) intercepted a package containing suspected counterfeit or fraudulent COVID-19 test kits arriving from the United Kingdom (U.K.). The officers found six plastic bags containing various vials manifested as "Purified Water Vials," and filled with a white liquid labeled as "Corona Virus 2019nconv (COVID-19)" and "Virus1 Test Kit."[12] The seizure triggered a joint U.S.-U.K. investigation and additional seizures.[13]

In a separate case, DOJ charged and arrested a U.K. national for shipping from the U.K. to California and Utah mislabeled drugs purported to be a COVID-19 treatment. In the scheme, the fraudster created packages labeled "Trinity COVID-19 SARS Antipathogenic Treatment" kits, even though the kits had not been approved by the FDA to treat COVID-19 or for any other use. This matter was investigated jointly by the FDA's Office of Criminal Investigation and Homeland Security Investigations, with assistance from CBP and the United States Postal Inspection Service.[14]

10. *See* Financial Action Tasks (FATF) publication, "COVID-19-related Money Laundering and Terrorist Financing Risks and Policy Responses," (May 2020), which identifies FATF countries' challenges, good practices, and policy responses to money laundering and terrorist financing threats and vulnerabilities arising from the COVID-19 pandemic.
11. Other U.S. law enforcement actions include COVID-19-related arrests made by the law enforcement partners of the National Intellectual Property Rights Coordination Center (IPR Center). These arrests related to shipping mislabeled and unapproved "treatments" for patients suffering from COVID-19. *See* IPR Center Newsroom, DOJ Press Release, "U.K. National Charged with Shipping Mislabeled and Unapproved 'Treatments' for Patients Suffering from COVID-19," (April 1, 2020), and FDA, "Coronavirus Disease 2019 (COVID-19)." During a weeklong operation held March 3-10, 2020, INTERPOL, the World Customs Organization (WCO), and Europol, in collaboration with United States and partners, seized more than 37,000 counterfeit medical devices, counterfeit surgical masks, and illicit pharmaceuticals, and they identified more than 2,000 websites with false advertisements and online marketplaces selling counterfeit goods. *See* INTERPOL News, "Global operation sees a rise in fake medical products related to COVID-19," (March 19, 2020), and WCO Newsroom, "COVID-19 Urgent Notice: counterfeit medical supplies and introduction of export controls on personal protective equipment," (March 23, 2020).
12. *See* CBP National Media Release, "CBP Officers Seize Fake COVID-19 Test Kits at LAX," (March 14, 2020).
13. *See* WCO Newsroom, "COVID-19 Urgent Notice: counterfeit medical supplies and introduction of export controls on personal protective equipment," (March 23, 2020).
14. *See* DOJ Press Release, "U.K. National Charged with Shipping Mislabeled and Unapproved 'Treatments' for Patients Suffering from COVID-19," (April 1, 2020).

Non-Delivery Fraud Scams

A Virginia Financial Institution Alerted the U.S. Secret Service (USSS) and Successfully Helped Prevent a $317 Million Non-Delivery Scam

A foreign government contacted a reliable New York-based law firm for help procuring 30-50 million N95 masks for the foreign country's national police department. The New York firm reached out to a healthcare/telemedicine telemarketing company (Company A), which in turn reached out to Company B, purportedly representing "a conglomerate of doctors" that had purchased millions of masks. Company B supplied Company A with contracts falsely claiming that Company B had 50 million masks stored in a warehouse in Houston, Texas, and requiring a payment of $317 million into an escrow account.

To execute the transactions, the foreign government sent $317 million to New York for further transfer to Company A's account held at a Virginia financial institution. The Virginia financial institution became suspicious that Company A's account had only been opened the previous day, and the account owner never mentioned to the financial institution that the owner was expecting a $317 million wire transaction. The Virginia financial institution contacted the USSS.

The USSS reviewed BSA data and interviewed the accountholder for Company A. The investigation revealed that, although Company A had suspicions about Company B, Company A appeared to be a victim, hired as a "broker" for the $317 million non-delivery scam. USSS interviewed the Chief Executive Officer (CEO) of Company B who admitted that there were no masks and that he never had possession of 50 million masks.

Price Gouging and Hoarding of Medical-Related Items

FBI Arrests Brooklyn Man for Possession and Sale of Scarce Medical Equipment

On March 30, 2020, FBI agents arrested a resident of Brooklyn, New York, for lying to them about his hoarding and sale of surgical masks, medical gowns, and other medical supplies.[15]

The individual allegedly sold certain designated materials, including N95 respirators, to doctors and nurses at inflated prices. In one instance, a doctor in New Jersey contacted the individual via a WhatsApp chat group labeled "Virus2020!" The individual agreed to sell to the doctor approximately 1,000 N95 masks and other assorted materials for $12,000, an approximately 700 percent markup from the normal price charged for those materials. The individual directed the doctor to an auto repair shop in Irvington, New Jersey, to pick up the order. According to the doctor, the repair shop contained enough materials, including hand sanitizers, disinfecting products, chemical cleaning supply agents, and surgical supplies, to outfit an entire hospital. In another instance, the individual allegedly offered to sell surgical gowns to a nurse and directed the nurse to his residence in Brooklyn.

15. *See* DOJ Press Release, "Brooklyn Man Arrested for Assaulting FBI Agents and Making False Statements About His Possession and Sale of Scarce Medical Equipment," (March 30, 2020).

Information on Reporting Suspicious Activity

Suspicious Activity Report (SAR) Filing Instructions

SAR reporting, in conjunction with effective implementation of due diligence requirements by financial institutions, is crucial to identifying possible financial crimes related to the COVID-19 pandemic, as well as unrelated frauds and financial crimes associated with foreign and domestic political corruption, money laundering, terrorist financing, and other illicit finance. Financial institutions should provide all pertinent available information in the SAR form and narrative. Adherence to the filing instructions below will improve FinCEN and law enforcement's ability to effectively identify and pull actionable SARs and information from the FinCEN Query systems to support COVID-19-related cases.

- FinCEN requests that financial institutions reference this advisory by including the key term "COVID19 FIN-2020-A002" in SAR field 2 (Filing Institution Note to FinCEN) and the narrative to indicate a connection between the suspicious activity being reported and the activities highlighted in this advisory.
- Financial institutions should also select SAR field 34(z) (Fraud - other) as the associated suspicious activity type to indicate a connection between the suspicious activity being reported and COVID-19. Financial institutions should include the type of fraud and/or name of the scam or product (e.g., Product Fraud – non delivery scam) in SAR field 34(z).
- Please refer to FinCEN's Notice Related to the Coronavirus Disease 2019 (COVID-19) May 18 Notice Related to COVID-19, which contains information regarding reporting COVID-19-related crime, and reminds financial institutions of certain BSA obligations.

For Further Information

Questions or comments regarding the contents of this advisory should be addressed to the FinCEN Regulatory Support Section at frc@fincen.gov.

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.