EXHIBIT 92

The Financial Crimes Enforcement Network (FinCEN) Encourages Financial Institutions to Communicate Concerns Related to the Coronavirus Disease 2019 (COVID-19) and to Remain Alert to Related Illicit Financial Activity

Immediate Release: March 16, 2020

On March 13, 2020, President Trump declared a National Emergency in response to COVID-19.[1] FinCEN requests financial institutions affected by the COVID-19 pandemic to contact FinCEN and their functional regulator as soon as practicable if a COVID-19-affected financial institution has concern about any potential delays in its ability to file required Bank Secrecy Act (BSA) reports. Financial institutions seeking to contact FinCEN should call FinCEN's Regulatory Support Section (RSS) at 1-800-949-2732 and select option 6 or e-mail at FRC@fincen.gov (mailto:FRC@fincen.gov). FinCEN's RSS will continue to be available to support financial institutions for the duration of the COVID-19 pandemic.

Financial institutions are encouraged to keep FinCEN and their functional regulators informed as their circumstances change.

FinCEN also advises financial institutions to remain alert about malicious or fraudulent transactions similar to those that occur in the wake of natural disasters. FinCEN is monitoring public reports and BSA reports of potential illicit behavior connected to COVID-19 and notes the following emerging trends:

1. Imposter Scams – Bad actors attempt to solicit donations, steal personal information, or distribute malware by impersonating government agencies (e.g., Centers for Disease Control and Prevention), international organizations (e.g., World Health Organization (WHO)[2]), or healthcare organizations.
2. Investment Scams – The U.S. Securities and Exchange Commission (SEC) urged investors to be wary of COVID-19-related investment scams, such as promotions that falsely claim that the products or services of publicly traded companies can prevent, detect, or cure coronavirus.[3]
3. Product Scams – The U.S. Federal Trade Commission (FTC) and U.S. Food and Drug Administration (FDA) have issued public statements and warning letters to companies selling unapproved or misbranded products that make false health claims pertaining to COVID-19.[4] Additionally, FinCEN has received reports regarding fraudulent marketing of COVID-19-related supplies, such as certain facemasks.
4. Insider Trading – FinCEN has received reports regarding suspected COVID-19-related insider trading.

In addition, please see FinCEN's advisory, FIN-2017-A007 "Advisory to Financial Institutions Regarding Disaster-Related Fraud" (October 31, 2017) for descriptions of other relevant typologies, such as benefits fraud, charities fraud, and cyber-related fraud.[5] For suspected suspicious transactions linked to COVID-19, along with checking the appropriate suspicious activity report-template (SAR-template) box(es) for certain typologies, FinCEN also encourages financial institutions to enter "COVID19" in Field 2 of the SAR-template.

Financial institutions are encouraged to review information from other relevant functional regulators as updates are available. FinCEN will continue to monitor this situation and will release updated information for financial institutions as appropriate.

---

[1] Remarks by President Trump, Vice President Pence, and Members of the Coronavirus Task Force in Press Conference: https://trumpwhitehouse.archives.gov/briefings-statements/remarks-president-trump-vice-president-pence-members-coronavirus-task-force-press-briefing-3/ (https://trumpwhitehouse.archives.gov/briefings-statements/remarks-president-trump-vice-president-pence-members-coronavirus-task-force-press-briefing-3/)

[2] WHO statement concerning imposter scams: https://www.who.int/about/communications/cyber-security (https://www.who.int/about/communications/cyber-security).

[3] SEC Notice on COVID-19 related investment scams: https://www.sec.gov/oiea/investor-alerts-and-bulletins/ia_coronavirus (https://www.sec.gov/oiea/investor-alerts-and-bulletins/ia_coronavirus).

[4] FTC and FDA joint updated statement concerning product scams: https://www.consumer.ftc.gov/blog/2020/03/ftc-fda-warnings-sent-sellers-scam-coronavirus-treatments (https://www.consumer.ftc.gov/blog/2020/03/ftc-fda-warnings-sent-sellers-scam-coronavirus-treatments).

FDA statement concerning product scams: https://www.fda.gov/consumers/health-fraud-scams/fraudulent-coronavirus-disease-2019-covid-19-products (https://www.fda.gov/consumers/health-fraud-scams/fraudulent-coronavirus-disease-2019-covid-19-products).

[5] FIN-2017-A007- Advisory to Financial Institutions Regarding Disaster-Related Fraud (October 31, 2017): https://www.fincen.gov/sites/default/files/advisory/2017-10-31/FinCEN%20Advisory%20FIN-2017-A007-508%20Compliant.pdf (https://www.fincen.gov/sites/default/files/advisory/2017-10-31/FinCEN%20Advisory%20FIN-2017-A007-508%20Compliant.pdf).

The Financial Crimes Enforcement Network Provides Further Information to Financial Institutions in Response to the Coronavirus Disease 2019 (COVID-19) Pandemic

Immediate Release: April 03, 2020

This notice updates the Financial Crimes Enforcement Network's (FinCEN's) March 16, 2020 COVID-19 Notice,[1] provides additional information to assist financial institutions in complying with their Bank Secrecy Act (BSA) obligations during the COVID-19 pandemic, and announces a direct contact mechanism for urgent COVID-19-related issues. FinCEN recognizes financial institutions face challenges related to the COVID-19 pandemic. In addition, FinCEN is committed to promoting the success of the Coronavirus Aid, Relief, and Economic Security Act (CARES Act), including the need to facilitate expeditious disbursal of CARES Act funds. Accordingly, FinCEN will issue further information, as appropriate, as the CARES Act is implemented and questions arise.

Compliance with BSA Obligations

Compliance with the Bank Secrecy Act (BSA) remains crucial to protecting our national security by combating money laundering and related crimes, including terrorism and its financing. FinCEN expects financial institutions to continue following a risk-based approach, and to diligently adhere to their BSA obligations. FinCEN also appreciates that financial institutions are taking actions to protect employees, their families, and others in response to the COVID-19 pandemic, which has created challenges in meeting certain BSA obligations, including the timing requirements for certain BSA report filings. FinCEN will continue outreach to regulatory partners and financial institutions to ensure risk-based compliance with the BSA, and FinCEN will issue additional new information as appropriate.

Beneficial Ownership Information Collection Requirements for Existing Customers

One of the primary components of the CARES Act is the Paycheck Protection Program (PPP). For eligible federally insured depository institutions and federally insured credit unions, PPP loans for existing customers will not require re-verification under applicable BSA requirements, unless otherwise indicated by the institution's risk-based approach to BSA compliance.

For non-PPP loans, FinCEN reminds financial institutions of FinCEN's September 7, 2018 ruling (FIN-2018-R004) offering certain exceptive relief to beneficial ownership requirements. To the extent that renewal, modification, restructuring, or extension for existing legal entity customers falls outside of the scope of that ruling, FinCEN recognizes that a risk-based approach taken by financial institutions may result in reasonable delays in compliance.

FinCEN will continue to assess reasonable risk-based approaches to BSA obligations and will issue further information, as appropriate, particularly as the CARES Act is implemented.

BSA Reporting Obligations & Updates to Currency Transaction Report (CTR) Filing Obligations

FinCEN has heard from certain financial institutions and trade associations for financial institutions about difficulties in meeting certain BSA obligations, including the timing requirements for certain BSA report filings. In response to concerns regarding certain timing requirements of BSA filings, FinCEN recognizes that certain regulatory timing requirements with regard to BSA filings may be challenging during the COVID-19 pandemic and that there may be some reasonable delays in compliance.

FinCEN hereby suspends implementation of the February 6, 2020 ruling (FIN-2020-R001) on CTR filing obligations when reporting transactions involving sole proprietorships and entities operating under a "doing business as" (DBA) name (the "2020 Ruling") until further notice. FinCEN will issue further information on these types of CTR filings at an appropriate time with reasonable implementation periods. Until such issuance, financial institutions should continue to report transactions involving sole proprietorships and DBAs under prior practice. Those financial institutions that have already made the necessary changes to comply with the 2020 Ruling need not revert to prior practice, and may report CTRs in accordance with the now-suspended ruling.

New FinCEN COVID-19 Online Contact Mechanism

FinCEN has created a COVID-19-specific online contact mechanism, via a specific drop-down category, for financial institutions to communicate to FinCEN COVID-19-related concerns while adhering to their BSA obligations. Financial institutions that wish to communicate such COVID-19-related concerns to FinCEN must go to www.FinCEN.gov (http://www.FinCEN.gov), click on "Need Assistance," and select "COVID19" in the subject drop-down list.[2] Such COVID-19-related communications are strongly encouraged but not required. FinCEN will review COVID-19-related communications. Depending on the volume of such communications, however, FinCEN may only respond via an automated message confirming receipt to communications regarding delays in filing of BSA reports due to COVID-19. FinCEN also encourages financial institutions to

contact their functional regulator(s) or other BSA examining authority as soon as practicable if a financial institution has BSA compliance concerns because of the COVID-19 pandemic.[3] Financial institutions are encouraged to keep FinCEN and their functional regulator(s) or other BSA examining authority informed as their circumstances change.

Encouragement of Innovative Efforts and Other Reminders

FinCEN encourages financial institutions to consider, evaluate, and, where appropriate, responsibly implement innovative approaches to meet their BSA/anti-money laundering compliance obligations, in order to further strengthen the financial system against illicit financial activity and other related fraud. Furthermore, FinCEN reminds financial institutions of the December 3, 2018 Joint Statement on Innovative Efforts to Combat Money Laundering and Terrorist Financing issued by the Board of Governors of the Federal Reserve System, the Federal Deposit Insurance Corporation, FinCEN, the National Credit Union Administration, and the Office of the Comptroller of the Currency.[4]

As noted in its March 16 COVID-19 Notice, FinCEN reminds financial institutions to review information from other relevant functional regulators as updates become available. FinCEN's March 16 COVID-19 Notice alerted financial institutions to imposter scams, investment scams, product scams, and insider trading. FinCEN also advised financial institutions to remain alert for malicious or fraudulent transactions similar to those that occur in the wake of natural disasters, such as those described in FinCEN's advisory, FIN-2017-A007, "Advisory to Financial Institutions Regarding Disaster-Related Fraud" (October 31, 2017), including benefits fraud, charities fraud, and cyber-related fraud.[5] FinCEN will continue to monitor the COVID-19 National Emergency and will release updated information for financial institutions as appropriate.

---

[1] FinCEN's March 16 COVID-19 Notice: https://www.fincen.gov/news/news-releases/financial-crimes-enforcement-network-fincen-encourages-financial-institutions (https://www.fincen.gov/news/news-releases/financial-crimes-enforcement-network-fincen-encourages-financial-institutions).

[2] FinCEN's Regulatory Support Section will continue to be available to support financial institutions for the duration of the COVID-19 pandemic.

[3] COVID-19 communications to FinCEN are in addition to, and do not supersede, any methods suggested for financial institutions to communicate COVID19-related concerns to their functional regulator or BSA examining authority.

[4] Joint Statement on Innovation Efforts: https://www.fincen.gov/sites/default/files/2018-12/Joint%20Statement%20on%20Innovation%20Statement%20%28Final%2011-30-18%29_508.pdf (https://www.fincen.gov/sites/default/files/2018-12/Joint%20Statement%20on%20Innovation%20Statement%20%28Final%2011-30-18%29_508.pdf).

[5] FIN-2017-A007 - Advisory to Financial Institutions Regarding Disaster-Related Fraud (October 31, 2017): https://www.fincen.gov/sites/default/files/advisory/2017-10-31/FinCEN%20Advisory%20FIN-2017-A007-508%20Compliant.pdf (https://www.fincen.gov/sites/default/files/advisory/2017-10-31/FinCEN%20Advisory%20FIN-2017-A007-508%20Compliant.pdf).

(https://www.facebook.com/fincentreasury)(https://www.linkedin.com/company/fincen)(https://twitter.com/FinCENnews)(https://www.youtube.com/@fincentreasury)

USA.gov (https://www.USA.gov) | Regulations.gov (https://www.Regulations.gov) | Treasury.gov (https://www.treasury.gov) | IRS.gov (https://www.IRS.gov) | Freedom of Information Act (FOIA) (/freedom-information-act-foia-and-guide-accessing-fincen-information) | NO FEAR Act (https://home.treasury.gov/footer/no-fear-act) | Vote.gov (https://vote.gov/) | Accessibility (/accessibility) | EEO & Diversity Policy (/equal-employment-opportunity-and-diversity-policy) | Privacy Policy (/privacy-security) | Public Posting Notice of Finding of Discrimination (https://home.treasury.gov/footer/no-fear-act) | Security and Vulnerability Disclosure Policies (VDP) (/security-and-vulnerability-disclosure-policies) | Office of Inspector General (https://oig.treasury.gov/)

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.

FinCEN NOTICE

May 18, 2020

FinCEN updated its USA PATRIOT Act Section 314(b) Fact Sheet in December 2020. The Fact Sheet, which addresses safe harbor protections in connection with certain private-sector information sharing, supersedes the material concerning information sharing provided below.

Notice Related to the Coronavirus Disease 2019 (COVID-19)

The Financial Crimes Enforcement Network (FinCEN) is issuing this Notice as part of FinCEN's COVID-19-related response. This Notice contains pertinent information regarding reporting COVID-19-related criminal and suspicious activity and reminds financial institutions of certain Bank Secrecy Act (BSA) obligations. FinCEN intends to issue multiple COVID-19-related advisories. Each advisory will refer financial institutions to this Notice.

COVID-19-Related Updates to Financial Institutions

FinCEN has published notices on its website that provide information to assist financial institutions in complying with their BSA obligations during the COVID-19 pandemic, which include a direct contact mechanism for urgent COVID-19-related issues. FinCEN encourages financial institutions to monitor FinCEN's website and the Department of the Treasury's website on The Coronavirus Aid, Relief, and Economic Security (CARES) Act for up-to-date information concerning compliance with BSA obligations.[1]

BSA Reporting Obligations

Compliance with the BSA remains crucial to protecting our national security by combating money laundering and related crimes, including terrorism and its financing. FinCEN expects financial institutions to continue following a risk-based approach and to diligently adhere to their BSA obligations. FinCEN also appreciates that financial institutions are taking actions to protect employees, their families, and others in response to the COVID-19 pandemic. FinCEN recognizes that current circumstances may create challenges with respect to certain BSA obligations, including the timing requirements for certain BSA report filings. FinCEN will continue outreach to regulatory partners and financial institutions to ensure risk-based compliance with the BSA, and FinCEN will issue additional information as appropriate.[2]

1. For up-to-date information on FinCEN's COVID-19-related releases, please visit FinCEN's Coronavirus Updates at https://www.fincen.gov/coronavirus. Those interested in receiving notifications from FinCEN may sign up for FinCEN Updates, at no charge, to receive updates with links to new information when content is added to FinCEN's website for any of the enrolled user's selected categories. For up-to-date information concerning the Department of the Treasury's CARES Act information, please visit https://home.treasury.gov/policy-issues/cares.
2. *See* FinCEN Notice, "The Financial Crimes Enforcement Network Provides Further Information to Financial Institutions in Response to the Coronavirus Disease 2019 (COVID-19) Pandemic," (April 3, 2020).

Financial institutions that wish to communicate their organizational COVID-19-related concerns, such as issues with the timely filing of BSA reports, should go to www.fincen.gov, click on "Need Assistance," and select "COVID19" in the subject drop-down list.

SAR Filing Instructions

In light of the COVID-19 pandemic, some financial institutions have added COVID-19 statements to their disclaimers or are using SAR narratives to address COVID-19's impact on their SAR filing abilities. Financial institutions should not include in the SAR narrative their challenges during the pandemic; the SAR narrative should include COVID-19 when it is tied to suspicious activity only. However, filers who have already included references to COVID-19 in matters not related to the pandemic do not need to file corrected reports.

Provision of SAR Supporting Documentation to Law Enforcement and FinCEN

In order to effectively respond to and combat fraud schemes, (e.g. those exploiting the COVID-19 pandemic), law enforcement and FinCEN require full details related to SAR filings, including supporting documentation, as quickly as possible.

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.[3] Financial institutions must provide any requested SAR and all documentation supporting the filing of a SAR upon request by FinCEN or an appropriate law enforcement or supervisory agency.[4] When requested to provide supporting documentation, financial institutions should verify that a requestor of information is, in fact, a representative of FinCEN or an appropriate law enforcement or supervisory agency.

Disclosure of SARs and supporting documentation to appropriate law enforcement and supervisory agencies is protected by the safe harbor provisions applicable to both voluntary and mandatory suspicious activity reporting by financial institutions.[5]

Information Sharing

Information sharing among financial institutions is critical to identifying, reporting, and preventing evolving fraud schemes, including those related to COVID-19. 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 relating to transactions that the institution suspects may

3. *See* 31 C.F.R. §§ 1020.320(d), 1021.320(d), 1022.320(c), 1023.320(d), 1024.320(c), 1025.320(d), and 1026.320(d).
4. *Id*. *See also* FinCEN Guidance, FIN-2007-G003, "Suspicious Activity Report Supporting Documentation," (June 13, 2007).
5. *See* 31 U.S.C. § 5318(g)(3).

involve the proceeds of one or more specified unlawful activities ("SUAs") and such an institution will still remain protected from civil liability under the section 314(b) safe harbor. The SUAs listed in 18 U.S.C. §§ 1956 and 1957 include an array of fraudulent and other criminal activities, including fraud against individuals or the government. FinCEN strongly encourages information sharing via section 314(b) where financial institutions suspect that a transaction may involve terrorist financing or money laundering, including one or more SUAs.[6]

Reporting COVID-19-Related Criminal Activity

There are a variety of U.S. government agencies positioned to assist in investigating and combating COVID-19-related criminal activity. Financial institutions and their customers should consider reporting COVID-19 crimes to the following agencies:

COVID-19-Related Fraud Schemes: Department of Justice (DOJ) urges the public to report suspected fraud schemes related to COVID-19 by calling the National Center for Disaster Fraud (NCDF) hotline (1-866-720-5721).[7] The NCDF can receive and enter complaints into a centralized system that can be accessed by all U.S. Attorney Offices, as well as DOJ law enforcement components, to identify, investigate, and prosecute fraud schemes. The NCDF coordinates complaints with 16 additional federal law enforcement agencies, as well as state Attorneys General and local authorities. The public may also report CARES Act-related fraud or other COVID-19-related financial crime to the U.S. Secret Service (USSS) by contacting their local USSS field office. Additionally, Department of Homeland Security (DHS) (including Homeland Security Investigations (HSI) and Immigration and Customs Enforcement) encourages the reporting of COVID-19 financial, cyber, and import/export fraud via the Operation Stolen Promise website / intake email address.

Cyber- and Internet-related Crime: Federal Bureau of Investigation's (FBI) Crime Complaint Center (IC3);[8] the DHS's CISA National Cybersecurity Communications and Integration Center (NCCIC); and HSI's Operation Stolen Promise fraud intake.[9]

Identity Theft and Fraud: The Federal Trade Commission and the Social Security Administration fraud hotline (1-800-269-0271).

Federal Tax Fraud: Fraud involving payment of federal taxes should be reported to the Treasury Inspector General for Tax Administration.

6. For further guidance related to the 314(b) Program, see FinCEN Fact Sheet, "Section 314(b)" (November 2016) and FinCEN Guidance, FIN-2009-G002, "Guidance on the Scope of Permissible Information Sharing Covered by Section 314(b) Safe Harbor of the USA PATRIOT Act," (June 16, 2009).
7. *See* DOJ Press Release, "Attorney General William P. Barr Urges American Public to Report COVID-19 Fraud," (March 20, 2020).
8. *See* the FBI's IC3 website, https://www.ic3.gov/.
9. *See* HSI "Operation Stolen Promise" website, HSI COVID-19 Fraud website, https://www.ice.gov/topics/operation-stolen-promise.

Response and Recovery of Funds

To better assist the public during the COVID-19 pandemic, FinCEN has temporarily expanded its Rapid Response Program to support law enforcement and financial institutions in the recovery of funds stolen via fraud, theft, and other financial crimes related to COVID-19. FinCEN has already been involved in multiple Rapid Response matters involving allegations of COVID-19 fraud, to include assisting in the recovery of $300 million in one case. To request immediate assistance in recovering cybercrime- and COVID-19-related stolen funds, financial institutions should file a complaint with the FBI's IC3, contact their local FBI field office, or contact the nearest USSS field office. Contacting law enforcement for fund recovery assistance does not relieve a financial institution from its SAR filing obligations.

FinCEN, in partnership with the FBI, the USSS, HSI, and the U.S. Postal Inspection Service, as well as counterpart Financial Intelligence Units abroad, can help financial institutions recover funds stolen as the result of business email compromise (BEC) and cybercrime schemes through its Rapid Response Program. Through these partnerships, FinCEN has successfully assisted in the recovery of approximately $900 million with the assistance of 64 countries. While FinCEN does not ensure recovery of BEC stolen funds, FinCEN has achieved greater success in recovering funds when victims or financial institutions report BEC-unauthorized and fraudulently induced wire transfers to law enforcement within 24 hours.

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.

FinCEN ADVISORY

FIN-2020-A003 July 7, 2020

Advisory on Imposter Scams and Money Mule Schemes Related to Coronavirus Disease 2019 (COVID-19)

Detecting, preventing, and reporting consumer fraud and other illicit activity related to COVID-19 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 MM FIN-2020-A003**" and select SAR field 34(z) (Fraud - other). Additional guidance for filing SARs appears near the end of this advisory.

Introduction

The Financial Crimes Enforcement Network (FinCEN) is issuing this advisory to alert financial institutions to potential indicators of imposter scams and money mule schemes, which are two forms of consumer fraud observed during the COVID-19 pandemic. Many illicit actors are engaged in fraudulent schemes that exploit vulnerabilities created by the pandemic. This advisory contains descriptions of imposter scams and money mule schemes, financial red flag indicators for both, and information on reporting suspicious activity.

This advisory is intended to aid financial institutions in detecting, preventing, and reporting potential COVID-19-related criminal activity. This advisory is based on FinCEN's analysis of COVID-19-related information obtained from Bank Secrecy Act (BSA) data, open source reporting, and law enforcement partners. FinCEN will issue COVID-19-related information to financial institutions to help enhance their efforts to detect, prevent, and report suspected illicit activity on its website at https://www.fincen.gov/coronavirus, which also contains information on registering to receive FinCEN Updates.

Financial Red Flag Indicators of COVID-19 Imposter Scams and Money Mule Schemes

Consumer frauds include imposter scams and money mule schemes, where actors deceive victims by impersonating federal government agencies, international organizations, or charities. FinCEN identified the financial red flag indicators described below to alert financial institutions to these frauds and to assist financial institutions in detecting, preventing, and reporting suspicious transactions associated with the COVID-19 pandemic.

As no single financial red flag indicator 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 potentially fraudulent COVID-19-related activities. In line with their risk-based approach to compliance with the BSA, financial institutions are also encouraged to perform additional inquiries and investigations where appropriate. Additionally, some of the financial red flag indicators outlined below may apply to multiple COVID-19-related fraudulent activities.

Imposter Scams

In imposter scams, criminals impersonate organizations such as government agencies, non-profit groups, universities, or charities to offer fraudulent services or otherwise defraud victims. While imposter scams can take multiple forms, the basic methodology involves an actor (1) contacting a target under the false pretense of representing an official organization, and (2) coercing or convincing the target to provide funds or valuable information, engage in behavior that causes the target's computer to be infected with malware, or spread disinformation.[1] In the case of schemes connected to COVID-19, imposters may pose as officials or representatives from the Internal Revenue Service (IRS),[2] the Centers for Disease Control and Prevention (CDC),[3] the World Health Organization (WHO), other healthcare or non-profit groups, and academic institutions.[4]

1. *See* Federal Trade Commission (FTC) Business Blog, "Seven Coronavirus Scams Targeting Your Business," (March 25, 2020).
2. For information on IRS imposter scams in general, *see* FTC's "IRS Imposter Scams Infographic," (January 2020).
3. *See* Federal Bureau of Investigation (FBI) Internet Crime Complaint Center (IC3) Public Service Announcement "FBI Sees Rise in Fraud Schemes Related to the Coronavirus (COVID-19) Pandemic," (March 20, 2020).
4. FTC maintains links to resources concerning scams and the current trends it has observed. *See* FTC's "Coronavirus Advice for Consumers."

Illicit actors can use imposter scams to defraud and deceive the vulnerable, including the elderly and unemployed, through the solicitation of payments (such as digital payments and virtual currency), donations, or personal information via email, robocalls, text messages,[5] or other communication methods. For example, an imposter may contact potential victims by phone, email, or text to imply that the victim must verify personal information or send payments to scammers in return for COVID-19-related stimulus payments or benefits, including Economic Impact Payments (EIP)[6] under the Coronavirus Aid, Relief, and Economic Security (CARES) Act.[7] Another instance includes imposters contacting victims and posing as government or health care representatives engaged in COVID-19 contact tracing activities, implying that a victim must share personal or financial information as part of contact tracing efforts.[8] Multiple examples include phishing schemes, where imposters send communications appearing to come from legitimate sources, to collect victims' personal and financial data and potentially infect their devices by convincing the target to download a malicious attachment or click malicious links.[9]

Scammers may also impersonate legitimate charities or create sham charities, taking advantage of the generosity of the public and embezzling donations intended for COVID-19 response efforts.[10]

5. For information about COVID-19-related imposter scams conducted by text messages and phone calls, see the Federal Communications Commission (FCC), "COVID-19 Consumer Warnings and Safety Tips," (May 20, 2020). The FTC and the FCC have sent warning letters to multiple Voice over Internet Protocol (VoIP) service providers for allegedly routing illegal pandemic-related scam telemarketing or robocalls. *See* FTC Press Release, "FTC and FCC Send Joint Letters to Additional VoIP Providers Warning against 'Routing and Transmitting' Illegal Coronavirus-related Robocalls," (May 20, 2020).
6. EIP may take the form of Automated Clearing House (ACH) deposits, U.S. Treasury checks, or prepaid debit cards. *See* U.S. Department of the Treasury (Treasury) Press Release "Treasury is Delivering Millions of Economic Impact Payments by Prepaid Debit Card," (May 18, 2020).
7. The FTC, the IRS, and the Treasury Inspector General for Tax Administration (TIGTA) each published information about imposter scams, particularly as they relate to EIP. *See* FTC Blog, "Want to Get Your Coronavirus Relief Check? Scammers do too," (April 1, 2020) and "Coronavirus Checks: Flattening the Scam Curve," (April 8, 2020); IRS News Release, "IRS Issues Warning About Coronavirus-related Scams; Watch Out For Schemes Tied To Economic Impact Payments," (April 2, 2020) and the IRS's Economic Impact Payment Information Center, (April 8, 2020); and TIGTA Press Release, "TIGTA Urges Taxpayers to "Be On High Alert" For Coronavirus Relief Payment Scams," (April 7, 2020).
8. *See* Department of Justice (DOJ) Press Release "U.S. Attorney Warns Public of COVID-19 Contact Tracing Frauds," (May 28, 2020).
9. *See* Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA) and the United Kingdom's (U.K.) National Cyber Security Centre (NCSC) Alert, "COVID-19 Exploited by Malicious Cyber Actors" (April 8, 2020); and DHS, "Common Scams: Know How to Spot a Fake." Additionally, *see* WHO Cybersecurity, "Beware of Criminals Pretending to be WHO," (April 2020). *See also* FTC Blog, "COVID-19 Scams Targeting College Students," (May 27, 2020); and DOJ Press Release, "Federal Law Enforcement Encourages the Public to Remain Vigilant to Covid-19 Scams," (April 22, 2020).
10. Multiple U.S. Attorneys' Offices (USAOs) warn of criminals who may seek to exploit legitimate relief efforts for their own illicit gain by soliciting donations to sham charities or crowdfunding sites. *See* USAO for the Southern District of Georgia, "U.S. Attorney Warns of Coronavirus Scams Targeting Vulnerable Victims," (March 25, 2020); USAO for the Eastern District of Oklahoma, "Department of Justice Requests Citizens be Aware of And Report COVID-19 Fraud," (March 24, 2020); and USAO for the Middle District of Tennessee, "U.S. Attorney and FBI Urge the Public to Report Suspected Fraud Related to Tornado Destruction and COVID-19," (March 23, 2020). Additionally, the U.S. Securities and Exchange Commission (SEC) noted the potential for charity investment frauds, where actors falsely claim that investments will provide financial support or medical treatment to people in need, with the money instead stolen. *See* SEC Investor Alerts and Bulletins, "Frauds Targeting Main Street Investors -- Investor Alert," (April 10, 2020). *See also* FTC's information to avoid charity scams, "Make Your Coronavirus Donations Count," (May 5, 2020).

Criminals often use social media accounts, door-to-door collections, flyers, mailings, telephone and robocalls, text messages, websites, and emails mimicking legitimate charities and non-profits to defraud the public. These operations may include words like "relief," "fund," "donation," and "foundation" in their titles to give the illusion that they are a legitimate organization.[11]

Given that many scammers may be targeting customers as opposed to financial institutions directly, financial institutions, when interacting with their customers, should remain on the alert for potential suspicious activities. Financial red flag indicators of imposter scams may include:

1. A customer indicating that a person claiming to represent a government agency contacted him or her by phone, email, text message, or social media asking for personal or bank account information to verify, process, or expedite EIPs, unemployment insurance, or other benefits.[12] In particular, be alert to communications emphasizing "stimulus check" or "stimulus payment" in solicitations to the public, sometimes claiming that the fraudulent entity can expedite the "stimulus check" or other government payment on behalf of the beneficiary for a fee paid by gift card or prepaid card.

2. Receipt of a document that appears to be a check or a prepaid debit card from the U.S. Treasury, often in an amount less than the expected EIP, with instructions to contact the fraudulent government agency, via a phone number or online, to verify personal information in order to receive the entire benefit.

3. Unsolicited communications from purported trusted sources or government programs related to COVID-19, instructing readers to open embedded links or files or to provide personal or financial information, including account credentials (e.g., usernames and passwords).

4. Email addresses in COVID-19 correspondence that do not match the name of the sender, contain misspellings, or do not end in the corresponding domain of the organization from which the message allegedly was sent. For example, government agencies will use ".gov" or ".mil." Many legitimate charities will use ".org." WHO emails will contain "@who.int." Fraudsters, however, may use ".com" or ".biz" in place of the expected domain.

5. Email correspondence that contains subject lines that government or industry have identified as being associated with phishing campaigns, or that contains embedded links or webpage addresses for purported COVID-19 resources that have irregular URLs (e.g., slight variations in domain extensions like ".com," ".org," and ".us"). Examples of U.S. government-identified COVID-19 phishing email subject lines include "2020 Coronavirus Updates," "Coronavirus Updates," "2019-nCov: New confirmed cases in your City," and "2019-nCov: Coronavirus outbreak in your city (Emergency)."[13]

11. *See* FTC, "How to Donate Wisely and Avoid Charity Scams."
12. For more information on EIPs, visit IRS, "Economic Impact Payment Information Center," (June 30, 2020).
13. *See* DHS CISA and U.K. NCSC Alert, "COVID-19 Exploited by Malicious Cyber Actors," (April 8, 2020).

6 Solicitations where the person, email, or social media advertisement seeks donations on behalf of a reputable organization, but is not affiliated with the reputable organization (e.g., the solicitor is not recognized or endorsed as an employee or volunteer by the organization, the email address is misspelled or not connected to the organization, or the social media advertisement directs individuals to an unaffiliated website).

7 A charitable organization soliciting donations that (1) does not have an in-depth history, financial reports, IRS annual returns, documentation of their tax-exempt status, or (2) cannot be verified by using various internet-based resources that may assist in confirming the group's existence and its nonprofit status.

Money Mule Schemes

A money mule is "a person who transfers illegally acquired money on behalf of or at the direction of another."[14] Money mule schemes, including those related to the COVID-19 pandemic, span the spectrum of using unwitting, witting, or complicit money mules.[15] An **unwitting** or **unknowing** money mule is an individual who is "unaware that he or she is part of a larger criminal scheme." The individual is motivated by his/her trust in the actual romance, job position or proposition.[16] A **witting** money mule is an individual who "chooses to ignore obvious red flags or acts willfully blind to his/her money movement activity." The individual is motivated by financial gain or an unwillingness to acknowledge his/her role.[17] A **complicit** money mule is an individual who is "aware of his/her role as a money mule and is complicit in the larger criminal scheme." The individual is motivated by financial gain or loyalty to a criminal group.[18] During the COVID-19 pandemic, U.S. authorities

14. *See* FBI, "Money Mule Awareness" (July 2019). For more information on money mules in general, *see* FinCEN, "Updated Advisory on Email Compromise Fraud Schemes Targeting Vulnerable Business Processes," (July 16, 2019); "FinCEN Analysis: Bank Secrecy Act Reports Filed by Financial Institutions Help Protect Elders from Fraud and Theft of Their Assets," (December 4, 2019); and DOJ, "Justice Department Announces Landmark Money Mule Initiative," (December 4, 2019).
15. For more information about unwitting, witting, and complicit individuals involved in money mule scams, *see* FBI, "Money Mule Awareness" (July 2019).
16. For examples of how an unwitting money mule is recruited and used, *see id*., p. 4.
17. For examples of how a witting money mule is recruited and used, *see id*., p. 5.
18. For examples of how a complicit money mule is recruited and used, *see id*.

have detected recruiters using money mule schemes, such as good-Samaritan, romance, and work-from-home schemes.[19] U.S. authorities also have identified criminals using money mules to exploit unemployment insurance programs during the COVID-19 pandemic.[20]

Financial red flag indicators of COVID-19 money mule schemes may include:

8 The customer's personal bank account starts to receive transactions that do not fit his or her transactional history profile, including overseas transactions, the purchase of large sums of convertible virtual currency, or transactions in large fiat amounts, or the account generally had a low balance until the customer became involved in a money mule scheme. When asked about the changes in transactions, the customer declines requests for "know your customer" documents or inquiries regarding sources of funds, and may mention COVID-19, relief work, or a "work-from-home" opportunity as the source of the income.

9 The customer opens a new bank account in the name of a business and, shortly thereafter, someone transfers the funds out of the account. The person transferring the funds could be the registered accountholder or someone else, and may keep a portion of the money he or she transferred (per instruction of the scammer). While this activity, in and of itself, may not be suspicious, it may become so if the individual provides unsatisfactory answers to the financial institution's inquiries, declines to provide essential "know your customer" documents, or mentions COVID-19, relief work, or "work from home" opportunities as the source of the funds.

10 The customer opens accounts in his or her name at multiple banks so he or she may receive money from various individuals or businesses, then moves the money to other accounts at the direction of the customer's purported employer.

11 The customer receives multiple state unemployment insurance payments to his or her account, or to multiple accounts held at the same financial institution, within the same disbursement timeframe (e.g., weekly or biweekly payments) issued from one or multiple states.

12 The customer's account(s) receives an unemployment deposit from a different state in which he or she reportedly resides or has previously worked.

19. The FBI has released information on how criminals are taking advantage of the COVID-19 pandemic to steal money, access personal and financial information, and use individuals as money mules. *See* FBI Press Release, "FBI Warns of Money Mule Schemes Exploiting the COVID-19 Pandemic," (April 6, 2020). In work-from-home schemes, for example, COVID-19 money mule recruiters, under a false charity or company label, may approach targets with a seemingly legitimate offer of employment under the pretense of work-from-home jobs, often through internet or social media advertisements, emails, or text messages. Once the target accepts the "employment," he or she receives instructions to move funds through accounts or to set up a new account in the target's name for the "business." The target (i.e., the money mule) earns money by taking a percentage of the funds that he or she helps to transfer per the instructions of the "employer." For more information on fraudulent job offers, *see* FTC Blog, "Looking for work after Coronavirus layoffs?," (April 13, 2020).

20. *See* Washington State Employment Security Department, "Statement from Commissioner Suzi LeVine on the rise in unemployment imposter fraud attempts," (May 14, 2020) and "Update on imposter fraud from Commissioner Suzi LeVine," (May 18, 2020).

13. The customer's account receives unemployment insurance payments for numerous employees or the accountholder name and ACH payment "remit to" name do not match.

14. Deposited funds are quickly diverted via wire transaction to foreign accounts located within countries known for having poor anti-money laundering controls.

15. The customer makes one or more atypical transactions involving an overseas account, especially through unusual payment methods for the customer. When asked about the transaction, the customer indicates it is for a person located overseas who is in need of financial assistance because of the COVID-19 pandemic.

16. Documentation from the customer shows that the purported employer or recruiter uses a common web-based, free email service instead of a company-specific email. For example, instead of a company- or organization-specific email address, such as first.lastname@ABCcompany.com or lastname@XYZ_NGO.org, the email address is from a common and free email address provider.

17. The customer provides information that his or her purported employer asked the customer to receive funds into his or her personal bank account, so that the employer can then process or transfer funds via wire transfer, ACH, mail, or money services businesses out of the customer's personal account.

18. The customer states, or information shows, that an individual, whom the customer may not have known previously, requested financial assistance to send/receive funds through the customer's personal account, including requests by individuals claiming to be a:

    a. U.S. Service member who is reportedly stationed abroad;

    b. U.S. citizen working or traveling abroad; or

    c. U.S. citizen quarantined abroad.

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 and stopping financial crimes, including those related to the COVID-19 pandemic. Financial institutions should provide all pertinent and available information in the SAR and narrative. Adherence to the filing instructions below will improve FinCEN's and law enforcement's abilities to effectively identify actionable SARs using the FinCEN Query system and pull information to support COVID-19- related investigations.

- FinCEN requests that financial institutions reference this advisory by including the key term "COVID19 MM FIN-2020-A003" 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., imposter scam or money mule scheme) in SAR field 34(z). In addition, FinCEN encourages financial institutions to report certain types of imposter scams and money mule schemes using fields such as SAR field 34(l) (Fraud- Mass-marketing), or SAR field 38(d) (Other Suspicious Activities- Elder Financial Exploitation), as appropriate with the circumstances of the suspected activity.
- Please refer to FinCEN's Notice Related to the Coronavirus Disease 2019 (COVID-19), which contains information regarding reporting COVID-19-related crime, and reminds 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.

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.

FinCEN ADVISORY

FIN-2020-A005 July 30, 2020

Advisory on Cybercrime and Cyber-Enabled Crime Exploiting the Coronavirus Disease 2019 (COVID-19) Pandemic

Detecting, preventing, and reporting illicit transactions and cyber activity will help protect legitimate relief efforts for the COVID-19 pandemic and help protect financial institutions and their customers against malicious cybercriminals and nation-state actors.

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-CYBER FIN-2020-A005**" and select SAR field 42 (Cyber Event). Additional guidance on filing SARs appears near the end of this advisory.

Introduction

The Financial Crimes Enforcement Network (FinCEN) is issuing this advisory to alert financial institutions to potential indicators of cybercrime and cyber-enabled crime observed during the COVID-19 pandemic. Many illicit actors are engaged in fraudulent schemes that exploit vulnerabilities created by the pandemic. This advisory contains descriptions of COVID-19-related malicious cyber activity and scams, associated financial red flag indicators, and information on reporting suspicious activity.

This advisory is intended to aid financial institutions in detecting, preventing, and reporting potential COVID-19-related criminal activity. This advisory is based on FinCEN's analysis of COVID-19-related information obtained from Bank Secrecy Act (BSA) data, open source reporting, and law enforcement partners. FinCEN will continue issuing COVID-19-related information to financial institutions to help enhance their efforts to detect, prevent, and report suspected illicit activity on its website at https://www.fincen.gov/coronavirus, which also contains information on how to register to receive FinCEN Updates.

Financial Red Flag Indicators of Cybercrime and Cyber-Enabled Crime Exploiting COVID-19

This advisory addresses the primary means by which cybercriminals and malicious state actors are increasingly exploiting the COVID-19 pandemic in cyber-enabled crime through malware and phishing schemes, extortion, business email compromise (BEC) fraud, and exploitation of remote applications, especially against financial and healthcare systems.[1]

FinCEN has identified the following red flag indicators of COVID-19 cyber-enabled crimes[2] to assist financial institutions in detecting, preventing, and reporting suspicious transactions associated with the COVID-19 pandemic. As no single financial red flag indicator 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 potential fraudulent COVID-19-related activities. In line with their risk-based approach to compliance with the BSA, financial institutions are also encouraged to perform additional inquiries and investigations where appropriate. Additionally, some of the financial red flag indicators outlined below may apply to multiple COVID-19-related fraudulent activities. Given that many scammers may be directly targeting customers, financial institutions should remain on the alert for potential suspicious activities involving their customers.

Targeting and Exploitation of Remote Platforms and Processes

The significant migration toward remote access in the pandemic environment presents opportunities for criminals to exploit financial institutions' remote systems and customer-facing processes. Cybercriminals and malicious state actors are targeting vulnerabilities in remote

1. *See* Department of Justice (DOJ) Press Release, "Department of Justice Announces Disruption of Hundreds of Online COVID-19 Related Scams," (April 22, 2020); the United Kingdom (U.K.) National Cyber Security Centre (NCSC) Press Release, "Public Urged to Flag Coronavirus Related Email Scams as Online Security Campaign Launches," (April 21, 2020); Department of Homeland Security's (DHS) Cybersecurity and Infrastructure Security Agency (CISA) Notification, "Defending Against COVID-19 Cyber Scams," (March 6, 2020); Europol Report, "Pandemic Profiteering: How Criminals Exploit the COVID-19 Crisis," (March 27, 2020); DHS CISA and Federal Bureau of Investigation (FBI) Public Service Announcement, "People's Republic of China (PRC) Targeting of COVID-19 Research Organizations," (May 13, 2020); FBI's Internet Crime Complaint Center (IC3) Public Service Announcement, "Increased Use of Mobile Banking Apps Could Lead to Exploitation," (June 10, 2020); and DHS CISA, National Security Agency, NCSC, and Canada Communications Security Establishment Joint Advisory, "APT29 Targets COVID-19 Vaccine Development," (July 16, 2020).
2. For the purpose of this advisory, cyber-enabled crime refers to illegal activities (e.g., fraud, identity theft, etc.) carried out or facilitated by electronic systems and devices, such as networks and computers. *See* FinCEN Advisory, FIN-2016-A005, "Advisory to Financial Institutions on Cyber-Events and Cyber-Enabled Crime," (October 25, 2016).

applications and virtual environments to steal sensitive information, compromise financial activity, and disrupt business operations.[3] Remote identity processes[4] also face significant risks, which may include:

- *Digital Manipulation of Identity Documentation*: Criminals often seek to undermine online identity verification processes through the use of fraudulent identity documents, which can be created by manipulating digital images of legitimate government-issued identity documents to alter the information and/or photos displayed.[5]
- *Leveraging Compromised Credentials Across Accounts*: Cybercriminals commonly undermine weak authentication processes in attempted account takeovers via methods such as credential stuffing attacks. In these attacks, cybercriminals generally use lists of stolen account credentials (typically usernames or email addresses, and associated passwords) to conduct automated login attempts to gain unauthorized access to victim accounts.

Financial red flag indicators of this sort of activity may include:[6]

1. The spelling of names in account information does not match the government-issued identity documentation provided for online onboarding.
2. Pictures in identity documentation, especially areas around faces, are blurry or low resolution, or have aberrations. Pictures in identity documentation or other images of persons in remote identity verification[7] show visual signs indicating possible image manipulation (e.g., incongruences in coloration near the edge of the face, or double edges or lines on delineated facial features).
3. Images of identity documentation have visual irregularities that indicate digital manipulation of the images, especially around information fields likely to have been changed to conduct synthetic identity fraud (e.g., name, address, and other identifiers).

3. For information related to publicly disclosed cybersecurity vulnerabilities and exposures, *see* U.S. Department of Commerce, National Institute for Standards and Technology (NIST), "National Vulnerability Database;" MITRE, "Common Vulnerabilities and Exposures: CVE List Home;" and FBI IC3 Public Service Announcements, "Cyber Actors Take Advantage of COVID-19 Pandemic to Exploit Increased Use of Virtual Environments," (April 1, 2020) and "Increased Use of Mobile Banking Apps Could Lead to Exploitation," (June 10, 2020). *See also* FinCEN Director Kenneth A. Blanco's, prepared remarks delivered at the Consensus Blockchain Conference, "Consensus Blockchain Conference (Virtual)," (May 13, 2020).
4. For the purposes of this advisory, "remote identity processes" include remote processes for customer onboarding and identity verification, as well as authentication of customers for account access purposes. For more information on digital identity standards, *see* NIST, "Digital Identity Guidelines," (December 1, 2017), and the Financial Action Task Force (FATF), "Guidance on Digital Identity," (March 6, 2020).
5. Criminals exploiting identity verification processes will typically use either information associated with a real individual's identity (i.e., identity theft) or create a new fabricated identity that usually consists of a real identifier, such as a social security number or driver's license number, with other fake information (i.e., synthetic identity fraud). For more information on example typologies and financial red flag indicators involving identity theft and identity fraud, *see* FinCEN Report, "Identity Theft: Trends, Patterns, and Typologies Reported in Suspicious Activity Reports," (October 2010).
6. *Id*. *See also* Interagency Guidelines on Identity Theft Detection, Prevention, and Mitigation, 16 CFR Part 681, app. A.
7. Images in identity verification other than identity documentation may include pictures or video of the customer (e.g., "selfie" images) taken as part of the financial institution's onboarding process.

4. A customer's physical description on identity documentation does not match other images of the customer.

5. A customer refuses to provide supplemental identity documentation or delays producing supplemental documentation.

6. Customer logins occur from a single device or Internet Protocol (IP) address across multiple seemingly unrelated accounts, often within a short period of time.

7. The IP address associated with logins does not match the stated address in identity documentation.

8. Customer logins occur within a pattern of high network traffic with decreased login success rates and increased password reset rates.

9. A customer calls a financial institution to change account communication methods and authentication information, then quickly attempts to conduct transactions to an account that never previously received payments from the customer.

Phishing, Malware, and Extortion

FinCEN and U.S. law enforcement have observed significant increases in broad-based and targeted phishing campaigns that are attempting to lure companies, especially healthcare and pharmaceutical providers, with offers of COVID-19 information and supplies.[8] Phishing scams target individuals with communications appearing to come from legitimate sources to collect victims' personal and financial data and potentially infect their devices by convincing the target to download malicious programs.[9] Cybercriminals usually send these phishing communications by email but may also use phone calls or text messages.

In these new schemes, phishing scammers will often reference COVID-19 themes, such as payments related to the Coronavirus Aid, Relief, and Economic Security (CARES) Act,[10] in the subjects and bodies of emails. Some phishing emails lure victims by advertising ways to make money, such as through investing in convertible virtual currencies (CVCs) or via domain names that mimic names of organizations, including those that provide or enable teleworking capabilities.[11] Cybercriminals

8. The U.S. Secret Service (USSS) and DHS CISA have noted an increase in malware, phishing, and extortion campaigns related to COVID-19. *See* USSS Press Release, "Secret Service Issues COVID-19 (Coronavirus) Phishing Alert," (March 9, 2020).

9. *See* DHS CISA and U.K. NCSC Joint Alert (AA20-099A), "COVID-19 Exploited by Malicious Cyber Actors," (April 8, 2020); and DHS, "Common Scams: Know How to Spot a Fake."

10. Pub. L. 116–136, 116th Congress (2020).

11. Since January 2020, tens of thousands of new domains have been registered with terms related to COVID-19 and/or disaster and healthcare response efforts (e.g., "quarantine," "vaccine," and "CDC"), many including or mimicking names of companies that provide or enable teleworking capabilities. U.S. law enforcement agencies have disrupted hundreds of malicious domains used to exploit the pandemic. *See* FinCEN Advisory, FIN-2020-A003, "Advisory on Imposter Scams and Money Mule Schemes Related to Coronavirus Disease 2019 (COVID-19)," (July 7, 2020). *See also*, FBI Press Release, "FBI Expects a Rise in Scams Involving Cryptocurrency Related to the COVID-19 Pandemic," (April 13, 2020).

are also distributing malware,[12] including ransomware, through phishing emails, malicious websites and downloads, domain name system (DNS) hijacking or spoofing attacks, and fraudulent mobile applications. These techniques can be applied in broader campaigns involving social media, such as the recent exploit targeting Twitter and prominent users of the platform.[13] Financial institutions dealing in CVC should be especially alert to the potential use of their institutions to launder proceeds affiliated with cybercrime, illicit darknet marketplace activity, and other CVC-related schemes and take appropriate risk mitigating steps consistent with their BSA obligations.

FinCEN assesses that instances of extortion will also continue to grow in the wake of the COVID-19 pandemic. So far in 2020, FinCEN has received numerous suspicious activity reports (SARs) involving ransomware[14] targeting medical centers and municipalities. Much of this ransomware was delivered by exploiting the COVID-19 lures described above. We expect criminals to continue targeting entities that are vulnerable due to their involvement in pandemic response, such as researchers working on medical treatments or manufacturers of personal protective equipment. In other instances of extortion, criminals are threatening to expose victims and their families to COVID-19 if they do not pay the extortion fee. In almost all cases, criminals require ransomware-related extortion payments to be made in CVC.[15]

Financial red flag indicators of this sort of activity may include the following:

10 Information technology enterprise activity related to transaction processes or information is connected to cyber indicators that have been associated with possible illicit activity. Malicious cyber activity may be evident in system log files, network traffic, or file information.[16]

11 Email addresses purportedly related to COVID-19 do not match the name of the sender or the corresponding domain of the company allegedly sending the message.

12. Malware can enable criminals to access compromised computers and computer systems to steal credentials, exfiltrate sensitive information through mechanisms like screenshots or keylogging, alter account information, and conduct fraudulent transactions.

13. *See* FinCEN Alert, FIN-2020-Alert001, "FinCEN Alerts Financial Institutions to Convertible Virtual Currency Scam Involving Twitter," (July 16, 2020).

14. Ransomware, a specific type of malware, typically encrypts data on systems in the interest of extorting ransom payment from victims in exchange for decrypting the information and giving victims access to their systems again.

15. Financial institutions dealing in CVC should be especially alert to the laundering of proceeds affiliated with cybercrime, illicit darknet marketplace activity, and other CVC-related schemes. *See* FinCEN Advisory, FIN-2019-003, "Advisory on Illicit Activity Involving Convertible Virtual Currency," (May 9, 2019).

16. Because cyber indicators are helpful red flag indicators that financial institutions can use to identify related suspicious financial activity, FinCEN, DHS CISA, and the U.S. Department of the Treasury's Office of Cybersecurity and Critical Infrastructure Protection (OCCIP) offer a broad range of helpful cyber indicator resources, including, but not limited to: FinCEN's Cyber Indicator Lists (CILs), shared through the FinCEN Secure Information Sharing System; OCCIP's CILs and circulars, available upon request; and DHS CISA's cyber analytic products and services, including a comprehensive list of COVID-19-related indicators of compromise in CSV or STIX-formatted XML formats, the Cyber Information Sharing and Collaboration Program (CISCP), and the Automated Indicator Sharing (AIS) program. Public-private and industry partnerships, such as the Financial Services Information Sharing and Analysis Center, and open source and commercial cyber threat feeds can also be useful resources.

12 Unsolicited emails related to COVID-19 from untrusted sources encourage readers to open embedded links/files or to provide personal or financial information, such as usernames and passwords or other account credentials.

13 Emails from untrusted sources or addresses similar to legitimate telework vendor accounts offer remote application software, often advertised at no or reduced cost.

14 Emails contain subject lines identified by government or industry as associated with phishing campaigns (e.g., "Coronavirus Updates," "2019-nCov: New confirmed cases in your City," and "2019-nCov: Coronavirus outbreak in your city (Emergency)").

15 Text messages have embedded links purporting to be from or associated with government relief programs and payments.

16 Embedded links or webpage addresses for purported COVID-19 resources have irregular uniform resource locators (URLs) that do not match that of the expected destination site or are similar to legitimate sites but with slight variations in the domain (e.g., variations in domain extensions like ".com," ".org," and ".us") or web address spelling.

Business Email Compromise (BEC) Schemes

Cybercriminals have increasingly exploited the COVID-19 pandemic by using BEC schemes, particularly targeting municipalities and the healthcare industry supply chain. A common BEC scheme involves criminals convincing companies to redirect payments to new accounts, while claiming the modification is due to pandemic-related changes in business operations. BEC criminals often use spoofed or compromised email accounts to communicate these urgent, last-minute payment changes. In the COVID-19 environment, criminals insert themselves into communications by impersonating a critical player in a business relationship or transaction, typically posing as providers of healthcare supplies, to intercept or fraudulently induce a payment for critically needed supplies.[17]

Financial red flag indicators of this sort of activity may include the following:[18]

17 A customer's transaction instructions contain different language, timing, and amounts in comparison to prior transaction instructions, especially regarding transactions involving healthcare providers or supplies purchases.

17. *See* FBI Press Release, "FBI Anticipates Rise in Business Email Compromise Schemes Related to the COVID-19 Pandemic," (April 6, 2020). *See also* Europol Press Release, "Corona Crimes: Suspect Behind €6 Million Face Masks and Hand Sanitisers Scam Arrested Thanks to International Police Cooperation," (April 6, 2020).

18. For general BEC-scheme financial red flag indicators, *see* FinCEN Advisories, FIN-2016-A003, "Advisory to Financial Institutions on E-mail Compromise Fraud Schemes," (September 6, 2016), and FIN-2019-A005, "Updated Advisory on Email Compromise Fraud Schemes Targeting Vulnerable Business Processes," (July 16, 2019).

18 Transaction instructions, typically involving a healthcare-sector counterparty or referencing purchase of healthcare or emergency response supplies, originate from an email account closely resembling, but not identical to, a known customer's email account.

19 Emailed transaction instructions direct payment to a different account for a known beneficiary. The transmitter may claim a need to change the destination account as part of a COVID-19 pandemic response, such as moving the account to a financial institution in a jurisdiction less affected by the disease, and assert urgency to conduct the transaction.

20 Emailed transaction instructions request to move payment methods from checks to ACH transfers as a response to the pandemic.

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 and stopping financial crimes, including those related to the COVID-19 pandemic. Financial institutions should provide all pertinent available information in the SAR 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 system to support COVID-19-related cases.

- FinCEN requests that financial institutions reference this advisory by including the key term "**COVID19-CYBER FIN-2020-A005**" 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 that suspect fraudulent COVID-19-related activity should mark all appropriate check boxes on the SAR form to indicate a connection between COVID-19 and the suspicious activity being reported. For example, if the activity includes a COVID-19-related account takeover involving an ACH transfer, financial institutions can select SAR field 38a and 38z, and note in the "other" box, "COVID-19 account takeover fraud – ACH."[19]
- Financial institutions should also include any relevant technical cyber indicators related to cyber events and associated transactions reported in a SAR within the available structured cyber event indicator fields. For example, for a COVID-19-related cyber event against a financial institution, financial institutions can select SAR fields 42a and 42z (noting in the

19. For additional guidance on identifying account takeover activity and related SAR filing instructions, *see* FinCEN Advisory, FIN-2011-A016, "Account Takeover Activity," (December 19, 2011).

"other" box the COVID-19-related cyber event), and SAR fields 44(a)-(j), (z), including email or CVC wallet addresses, malicious domains or URLs, and any other known cyber event indicators.

- For cyber-enabled crime involving fraud driven by COVID-19, financial institutions should select SAR field 34z (Fraud – other) as the associated suspicious activity type. Additionally, financial institutions should include the type of cybercrime or scheme as a keyword (e.g., "COVID 19 BEC Fraud," "EAC fraud," or "BEC data theft") in SAR field 34(z).
- Please refer to FinCEN's May 18, 2020 Notice Related to the Coronavirus Disease 2019, which contains information regarding reporting COVID-19-related crime and FinCEN's Rapid Response Program, and reminds 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.

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.

FinCEN ADVISORY

FIN-2020-A007 October 13, 2020

Advisory on Unemployment Insurance Fraud During the Coronavirus Disease 2019 (COVID-19) Pandemic

Detecting and preventing unemployment insurance fraud and other illicit activity related to COVID-19 are critical to safeguarding the integrity of government relief efforts.

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 UNEMPLOYMENT INSURANCE FRAUD FIN-2020-A007**" and select SAR field 34(z) (Fraud - other). Additional guidance for filing SARs appears near the end of this advisory.

Introduction

The Financial Crimes Enforcement Network (FinCEN) is issuing this advisory to alert financial institutions to unemployment insurance (UI) fraud observed during the COVID-19 pandemic. Many illicit actors are engaged in fraudulent schemes that exploit vulnerabilities created by the pandemic. This advisory contains descriptions of COVID-19-related UI fraud, associated financial red flag indicators, 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, open source reporting, and law enforcement partners.

Financial Red Flag Indicators of Unemployment Insurance Fraud Related to COVID-19 Relief

As unemployment claims in the United States have surged due to the pandemic, U.S. law enforcement and financial institutions have detected numerous instances of COVID-19-related UI fraud. The following are representative types of this illicit activity:

- *Fictitious employer-employee fraud:* filers falsely claim they work for a legitimate company, or create a fictitious company and supply fictitious employee and wage records to apply for UI payments;

- *Employer-employee collusion fraud:* the employee receives UI payments while the employer continues to pay the employee reduced, unreported wages;
- *Misrepresentation of income fraud:* an individual returns to work and fails to report the income in order to continue receiving UI payments, or in an effort to receive higher UI payments, an applicant claims higher wages than he/she previously earned;
- *Insider fraud:* state employees use credentials to inappropriately access or change UI claims, resulting in the approval of unqualified applications, improper payment amounts, or movement of UI funds to accounts that are not on the application; or
- *Identity-related fraud:* filers submit applications for UI payments using stolen or fake identification information to perpetrate an account takeover.[1]

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 schemes targeting UI programs, and to assist financial institutions in detecting, preventing, and reporting suspicious transactions related to such fraud.

Financial red flag indicators of UI fraud may include:

1 Account(s) held at the financial institution receive(s):

a. UI payments from a state other than the state in which the customer reportedly resides or has previously worked;

b. Multiple state UI payments within the same disbursement timeframe;

c. UI payments in the name of a person other than the accountholder, or in the names of multiple unemployment payments recipients;

d. UI payments and regular work-related earnings, via direct deposit or paper checks;

e. Numerous deposits or electronic funds transfers (EFTs) that indicate they are UI payments from one or more states to persons other than the accountholder(s);

f. A higher amount of UI payments in the same timeframe than similarly situated customers received.

1. *See*, FinCEN Advisory, FIN-2020-A005, "Advisory on Cybercrime and Cyber-Enabled Crime Exploiting the Coronavirus Disease 2019 (COVID-19) Pandemic," (July 30, 2020). In some situations, fraudsters use the stolen identification information to perpetrate an account takeover. For additional information on identifying account takeover activity, *see* FinCEN Advisory, FIN-2011-A016, "Account Takeover Activity," (December 19, 2011).

2. The customer withdraws the disbursed UI funds in a lump sum by cashier's checks, by purchasing a prepaid debit card, or by transferring the funds to out-of-state accounts.

3. The customer's UI payments are quickly diverted via wire transfer to foreign accounts, particularly to accounts in countries with weak anti-money laundering controls.

4. The customer receives or sends UI payments to a peer-to-peer (P2P) application or app. The funds are then wired to an overseas account, or withdrawn using a debit card, in a manner that is inconsistent with the spending patterns of similarly situated customers.

5. Individuals quickly withdraw disbursed UI funds via online bill payments addressed to an individual(s), as opposed to businesses, as payee(s), with some individual payees receiving multiple online bill paychecks over a short time period.

6. The IP address associated with logins for an account conducting suspected UI-fraud activities does not map to the general location of stated address in identity documentation for the customer or where the UI payment originated.

7. Individuals direct UI-related EFTs, or deposit UI checks into suspected shell/front company accounts, which may be indicative of money mules transferring these funds in and out of the accounts.

8. Multiple accounts receiving UI payments at one or more financial institutions are associated with the same free, web-based email account that may appear in more than one UI application.

9. A newly opened account, or an account that has been inactive for more than thirty days, starts to receive numerous UI deposits. After a financial institution suspects UI fraud and requests additional identification documentation to verify the identity(ies) of the customer(s), queried individuals provide documents that are incorrect or forged, which may be an indicator of an account takeover or identity theft.

10. After a financial institution suspects UI fraud and conducts due diligence, it determines that the customer does not have a history of living at, or being associated with, the address to which the UI check or UI debit card is sent, or within the geographical area in which the registered debit card is being used.

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 and stopping unemployment insurance fraud related to the COVID-19 pandemic. Financial institutions should provide all pertinent and available information in the SAR and narrative.

- FinCEN requests that financial institutions reference this advisory by including the key term "**COVID19 UNEMPLOYMENT INSURANCE FRAUD FIN-2020-A007**" 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 also should 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. When addressing unemployment fraud in a SAR, financial institutions should include the keywords "unemployment fraud" in SAR field 34(z).
- When filing a SAR, in addition to standard transaction data, providing the following information is highly valuable to law enforcement: relevant email addresses, IP addresses with their respective timestamps, login information with location and timestamps, cyber-related information and technical indicators, virtual currency wallet addresses, mobile device information (such as device International Mobile Equipment Identity (IMEI)), phone numbers, monikers, and description and timing of suspicious electronic communications.
- Please refer to FinCEN's Notice Related to the Coronavirus Disease 2019 (COVID-19), which contains information regarding reporting COVID-19-related crime, and reminds 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 illicit activity please visit our website at https://www.fincen.gov/coronavirus, which also contains information on registering to receive FinCEN Updates.

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.

FinCEN ADVISORY

FIN-2021-A002 **February 24, 2021**

Advisory on Financial Crimes Targeting COVID-19 Economic Impact Payments

Detecting, preventing, and reporting financial crimes related to Economic Impact Payments is vital to the United States' economic recovery, and critical to 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: "**FIN-2021-A002**" and select SAR field 34(z) (Fraud - other). Additional guidance for filing SARs appears near the end of this advisory.

Introduction

The Financial Crimes Enforcement Network (FinCEN) is issuing this advisory to alert financial institutions to fraud and other financial crimes related to the Economic Impact Payments (EIPs),[1] authorized by the Coronavirus Aid, Relief, and Economic Security (CARES) Act,[2] and the Coronavirus Response and Relief Supplemental Appropriations Act of 2021.[3]

This advisory contains descriptions of EIP fraud, associated red flag indicators, and information on reporting suspicious activity. This Advisory is part of a series published by FinCEN on COVID-19-related frauds and criminal activity.[4]

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

1. For more information about EIPs, *see* Treasury Press Release, "Treasury and IRS Begin Delivering the Second Round of Economic Impact Payments to Millions of Americans," (December 29, 2020); and Internal Revenue Service (IRS) Economic Impact Payment Information Center, (Last updated February 17, 2021) and Coronavirus and Economic Impact Payments: Resources and Guidance, (Last updated February 17, 2021). If Congress authorizes any future payments, please monitor these resources for information related to any additional payments.
2. Public Law 116–136.
3. Public Law 116-260.
4. For a complete listing of FinCEN's COVID-19-related publications, please visit FinCEN's Coronavirus webpage.

EIP-Related Fraud and Theft

U.S. authorities have detected a wide range of EIP-related fraud and theft involving a variety of criminal actors. The following examples are a non-exhaustive list of this type of criminal activity.

- *Fraudulent checks*: Fraudsters send potential victims fraudulent checks, instructing the recipients to call a number or verify information online in order to cash the fraudulent EIP checks. Victims are asked for personal or banking information under the guise that the information is needed to receive or speed up their EIP. Fraudsters then use the information obtained to commit various crimes, such as identity theft and the unauthorized access of bank accounts.[5]
- *Altered checks*: Fraudsters deposit altered EIP checks, often via automated teller machine (ATM) or mobile device. These altered checks may modify the name of the payee, or leave the name blank, and the amount may be altered prior to deposit. There is reporting of checks being chemically altered so the original payee is removed.
- *Counterfeit checks*: Fraudsters deposit counterfeit EIP checks, often via ATM or mobile device. Fraudsters have various methods to create a counterfeit check, including checks reproduced from digital images of checks issued by the U.S. Department of the Treasury. However, such counterfeit checks will often have irregularities involving the check number, paper, coloring, and/or font.
- *Theft of EIP*: Such thefts can include individuals stealing an EIP from the U.S. mail; requesting an EIP disbursal for an ineligible person; seeking another person's EIP without the payee's knowledge and/or approval, or through coercive means; or using stolen Personally Identifiable Information (PII), including providing false bank account information to the IRS to claim an EIP.
- *Phishing schemes using EIP as a lure*: Fraudsters perpetrate phishing schemes using emails, letters, phone calls, and text messages containing keywords such as "Corona Virus," "COVID-19," and "Stimulus," with the purpose of obtaining PII and financial account information, such as account numbers and passwords.[6]
- *Inappropriate seizure of EIP*: A private company that may have control over a person's finances or serves as his or her representative payee seizes a person's EIP, for wage garnishments or debt collection, and does not return the inappropriately seized payments.[7]

5. *See* IRS News Release, "IRS Issues Warning about Coronavirus-related Scams; Watch Out for Schemes Tied to Economic Impact Payments," (April 2, 2020).
6. *See* IRS News Release, "IRS Warns Against COVID-19 Fraud; Other Financial Schemes," (June 8, 2020). For more information about phishing schemes and 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).
7. *See* Social Security Administration, Second Economic Impact Payment (Last updated January 15, 2021) and Economic Impact Payments Paid by the CARES Act (Last updated November 23, 2020); and IRS Press Release, "Economic Impact Payments Belong to Recipient, not Nursing Homes or Care Facilities," (June 16, 2020).

Red Flag Indicators of Financial Crimes Related to EIPs

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 has identified the financial red flag indicators described below to alert financial institutions to potential fraud and thefts related to EIPs as well as to assist financial institutions in detecting, preventing, and reporting suspicious transactions related to such activities. Such financial red flag indicators may include:

Fraudulent, altered, counterfeit, or stolen EIP checks, Automated Clearing House (ACH) deposits, and prepaid debit cards

1. An account holder attempts to deposit one or more checks that appear to be issued by the U.S. Treasury, but are fraudulent or counterfeit checks.[8] When questioned, the customer may disclose that he or she:

   (i) was sent a partial payment, and needed to verify his or her PII or financial information before receiving the full EIP; or

   (ii) received the check purportedly from a current or former employer with instructions that the check was the customer's "stimulus payment" and that he or she was to buy prepaid cards and send them to another individual.

2. An existing account receives, or an account holder makes, multiple EIP-related deposits for individuals other than the account holder(s), and the individuals named on the checks reside outside the geographic region of the account holder, or do not have a history at the account holder's purported address. This may be indicative of funnel account activities in which multiple EIPs are deposited or transferred throughout the United States into one account, which may be held by a fraudster or a money mule working for the fraudster.

3. An existing account receives an excessive number of EIPs via U.S. Treasury check or deposits related to a prepaid debit card linked to the same address (e.g., an account receiving more checks than expected relative to the customer's profile and financial institution's customer due diligence).

8. The U.S. Secret Service (USSS) and the Department of the Treasury announced several security features in official U.S. Treasury checks. *See* USSS Press Release, "U.S. Secret Service in Partnership with the U.S. Department of the Treasury Launch – Know Your U.S. Treasury Check Campaign," (April 20, 2020). For a description of the official U.S. Treasury check, *see* U.S. Treasury Check Security Features, (April 2020). The status of EIP and other Treasury checks can be determined by using Treasury's Bureau of Fiscal Services' Treasury Check Verification System (TCVS).

4 A customer opens a new account with an EIP check or debit card, and the name of the potential account holder is different from that of the depositor or the payee of EIP.

5 The EIP check is deposited, or the debit card's funds are transferred, into dormant accounts with little or no prior activity.

Theft of multiple EIPs

6 Individual accounts opened after the U.S. government announced the EIP program, receive U.S. Treasury checks or direct deposits from the U.S. Treasury that could indicate multiple EIPs, and for individuals other than the account holder.

7 The account holder is a child under age 17 at the end of the taxable year, but the account received numerous EIPs.

8 Rapid transfers of multiple EIPs into one account could indicate that bad actors are consolidating the payments. After the funds are consolidated, the funds may be quickly (a) withdrawn via large cash withdrawals or serial ATM withdrawals; (b) used to purchase convertible virtual currencies (CVC); (c) transferred out of the account via a money services business such as cryptocurrency exchangers and peer-to-peer mobile payment systems, or wire transfers to other accounts; (d) used for large purchases at merchants that offer cash back as an option, in amounts not typical of this type of merchant; or (e) transferred onto prepaid debit or gift cards.

9 An account receives several EIP-related deposits and almost immediately thereafter (a) disburses funds for large purchases at merchants that offer cash back as an option, in amounts not typical of this type of merchant, or (b) has funds transferred onto prepaid debit or gift cards.

10 Deposits of one or more EIP U.S. Treasury checks or electronic deposits made into an account held by (a) a retail business, or (b) a personal account of a business owner or employee and the account holder is not the payee/endorser. This may indicate that the business is using identifiers of its employees or customers to apply for their EIP benefits for the purpose of inappropriately collecting the payments.

11 The same Internet Protocol (IP) address is used to transfer funds from several EIP debit cards to a bank account, especially if that IP address is located outside of the United States or associated with a business.

Other frauds and thefts occurring in an account receiving EIPs

12 An account receives (a) numerous deposits or electronic funds transfers (EFTs) that indicate the payments are linked to EIPs, and (b) unemployment insurance payments[9] from one or more states in names that do not match the account holder(s).

9. FinCEN Advisory, FIN-2020-A007, "Advisory on Unemployment Insurance Fraud During the Coronavirus Disease 2019 (COVID-19) Pandemic," (October 13, 2020).

13 An account with several EIP deposits also receives numerous tax refunds from federal and state governments for individuals other than the account holder(s). The names indicated on the EIPs and tax returns may be the same but are not those of the account holder(s).

14 Deposits of one or more EIP checks or electronic deposits are made into a nursing home or assisted living facility's business account and those payments have not been returned to the resident. This may be an indication that the business is inappropriately withholding residents' EIP funds.

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 EIP-related fraud and theft. Financial institutions should provide all pertinent information in the SAR.

- FinCEN requests that financial institutions reference this advisory by including the key term "**FIN-2021-A002**" 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.
- FinCEN also requests that filers mention "**economic impact payment**" in the SAR narrative along with any other relevant behavior, such as counterfeit checks, money mule activity, or identity theft, to indicate a connection between those activities and EIP frauds and thefts. Additionally, FinCEN requests that filers use this program-specific term and avoid relying on generalized key terms, such as "stimulus check."
- 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., economic impact payment) in SAR field 34(z).
- FinCEN requests filers not report the potential victim of an EIP fraud scheme as the subject of the SAR. Rather, all available information on the victim should be included in the narrative portion of the SAR.
- Please refer to FinCEN's May 2020 Notice Related to the Coronavirus Disease 2019 (COVID-19) and February 2021 Consolidated COVID-19 Suspicious Activity Report Key Terms and Filing Instructions, which contain 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.

For more information about TCVS, please visit Treasury's Bureau of Fiscal Services website, Treasury Check Verification System, or contact Fiscal Service at (855) 868-0151, option 1 or paymentintegrity@fiscal.treasury.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.

FinCEN NOTICE

FIN-2021-NTC1 **February 24, 2021**

Consolidated COVID-19 Suspicious Activity Report Key Terms and Filing Instructions

The Financial Crimes Enforcement Network (FinCEN) is issuing this Notice to consolidate filing instructions and key terms for fraudulent activities, crimes, and cyber and ransomware attacks related to Coronavirus Disease 2019 (COVID-19), and to remind financial institutions of recent updates to FinCEN guidance concerning Section 314(b). FinCEN has published a series of advisories and notices on COVID-19-related threats to assist financial institutions with the filing of suspicious activity reports (SARs) involving such threats. In this Notice, FinCEN further requests that financial institutions consult the tables below when filing SARs for COVID-19-related activity.

Table 1 contains key terms and instructions related to government programs. Table 2 contains a summary of the key terms and instructions for COVID-19-related activities that are not tied to specific government programs. Table 3 provides a list of additional FinCEN's COVID-19-related publications. Financial institutions that follow the instructions set forth below will assist FinCEN, law enforcement, financial regulators, and other relevant government agencies in identifying and utilizing the information submitted in COVID-19-related SARs.

Financial institutions should consult previously published advisories and notices for additional SAR filing instructions related to the advisories and notices included below. If financial institutions wish to cite more than one advisory, then they should use only the FinCEN identification numbers (FINs) listed in the tables below in Field 2, and provide the full references in the SAR narrative. FinCEN requests that filers be as specific as possible in their SAR filings. For instance, if the SAR addresses a government program, FinCEN requests that filers use program-specific keywords, as detailed in the keyword columns in Table 1 below, and avoid relying on generalized key terms, such as "stimulus," "CARES Act," or "benefit." Doing so will expedite identification of relevant SARs for appropriate investigative, analytical, supervisory, and other authorized purposes.

Table 1: COVID-19 Government Programs

Government Program	Keyword(s) for Suspicious Activity and narrative	Field 2 (Note to FinCEN)	Suspicious Activity Field(s) 32-42
Economic Injury Disaster Loan (EIDL) Program[1]	Economic injury disaster	COVID19 EIDL FUNDS FRAUD[2]	34(z) (Fraud - other)
Economic Impact Payments (EIP)[3]	Economic impact payment	FIN-2021-A002	34(z) (Fraud - other)
Paycheck Protection Program (PPP)[4]	Paycheck protection	FIN-2021-NTC1	34(z) (Fraud - other)
State Unemployment Insurance[5]	Unemployment	COVID19 UNEMPLOYMENT INSURANCE FRAUD FIN-2020-A007[6]	34(z) (Fraud - other)
Pandemic Unemployment Assistance	Unemployment	COVID19 UNEMPLOYMENT INSURANCE FRAUD FIN-2020-A007[7]	34(z) (Fraud - other)
Main Street Lending[8]	FED MSL	FIN-2021-NTC1	34(z) (Fraud - other)

1. For more information regarding this loan program, please visit U.S. Small Business Administration (SBA), Economic Injury Disaster Loans.
2. FinCEN News, "Prepared Remarks of FinCEN Director Kenneth A. Blanco, delivered virtually at the ACAMS AML Conference," (September 29, 2020).
3. For more information about EIPs, please visit Internal Revenue Service (IRS), Economic Impact Payment Information Center.
4. For more information regarding the PPP, please visit SBA, Paycheck Protection Program.
5. For more information about COVID-19-related unemployment insurance programs and relief, please visit the U.S. Department of Labor, Unemployment Insurance Relief During COVID-19 Outbreak.
6. FinCEN Advisory, FIN-2020-A007, "Advisory on Unemployment Insurance Fraud During the Coronavirus Disease 2019 (COVID-19) Pandemic," (October 13, 2020).
7. *Id.*
8. For more information regarding the Main Street Lending Program, please visit Board of Governors of the Federal Reserve System, Main Street Lending Program.

Table 2: Other COVID-19-related Crimes and Frauds

Potential Fraud or Crime	Keyword(s) for Suspicious Activity and narrative	Field 2 (Note to FinCEN)	Suspicious Activity Field(s) 32-42
Cyber crime	BEC fraud, EAC fraud, and others as warranted	COVID19-CYBER FIN-2020-A005[9]	34 (z) (Fraud –other) for BEC, EAC; 38 (a) account takeover; 42 (a), (b), and/or (z), as appropriate (noting the (z) "other" box the COVID-19 cyber event); 44 (a) through (j) cyber event indicators, as relevant and available
Health insurance and health care	Kickbacks, services not provided, billing schemes, and others as warranted	FIN-2021-A001[10]	34(g) (Health care – public or private health insurance)
Medical products	Fraudulent products, non-delivery scam, price gouging, hoarding	COVID19 FIN-2020-A002[11]	34(z) (Fraud - other)
Vaccine-related scams and cyber crimes	Vaccine scam or vaccine ransomware	FIN-2020-NTC4[12]	34(z) (Fraud - other)
Money mule and imposter scams	Imposter, money mule scams	COVID19 MM FIN-2020-A003[13]	34(z) (Fraud - other)

9. FinCEN Advisory, FIN-2020-A005, "Advisory on Cybercrime and Cyber-Enabled Crime Exploiting the Coronavirus Disease 2019 (COVID-19) Pandemic," (July 30, 2020).
10. FinCEN Advisory, FIN-2021-A001, "Advisory on COVID-19 Health Insurance- and Health Care-Related Fraud," (February 2, 2021).
11. FinCEN Advisory, FIN-2020-A002, "Advisory on Medical Scams Related to the Coronavirus Disease 2019 (COVID-19)," (May 18, 2020).
12. FinCEN Notice, FIN-2020-NTC4, "FinCEN Asks Financial Institutions to Stay Alert to COVID-19 Vaccine-Related Scams and Cyberattacks," (December 28, 2020).
13. FinCEN Advisory, FIN-2020-A003, "Advisory on Imposter Scams and Money Mule Schemes Related to Coronavirus Disease 2019 (COVID-19)," (July 7, 2020).

Table 3: Additional FinCEN COVID-19-related Publications

Field 2 (Note to FinCEN)	Title
February 1, 2021 FAQs	Paycheck Protection Program Frequently Asked Questions (FAQs)
FIN-2020-NTC3	Notice Related to the Coronavirus Disease 2019 (COVID-19)
FIN-2020-NTC2	The Financial Crimes Enforcement Network Provides Further Information to Financial Institutions in Response to the Coronavirus Disease 2019 (COVID-19) Pandemic
FIN-2020-NTC1	The Financial Crimes Enforcement Network (FinCEN) Encourages Financial Institutions to Communicate Concerns Related to the Coronavirus Disease 2019 (COVID-19) and to Remain Alert to Related Illicit Financial Activity

Updates to Section 314(b) Fact Sheet and Information Sharing Documents

FinCEN updated its USA PATRIOT Act Section 314(b) Fact Sheet in December 2020. The Fact Sheet, which addresses safe harbor protections in connection with certain private-sector information sharing, supersedes the material concerning information sharing provided in FinCEN's May 2020 Notice Related to the Coronavirus Disease 2019 (COVID-19).

For Further Information

Additional COVID-19-related information, including COVID-19-related advisories and notices, is located on FinCEN's website at https://www.fincen.gov/coronavirus, which also contains information on how to register for FinCEN Updates.

Questions or comments regarding the contents of this notice 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.