FinCEN NOTICE

FIN-2020-NTC4 **December 28, 2020**

FinCEN Asks Financial Institutions to Stay Alert to COVID-19 Vaccine-Related Scams and Cyberattacks

The Financial Crimes Enforcement Network (FinCEN) is issuing this Notice to alert financial institutions about the potential for fraud, ransomware attacks, or similar types of criminal activity related to COVID-19 vaccines and their distribution.[1] As of December 28, 2020, the U.S. Food and Drug Administration (FDA) has issued two emergency use authorizations for COVID-19 vaccines in the United States.[2] This Notice also provides specific instructions for filing Suspicious Activity Reports (SARs) regarding such suspicious activity related to COVID-19 vaccines and their distribution.

COVID-19 vaccine fraud may include the sale of unapproved and illegally marketed vaccines, the sale of counterfeit versions of approved vaccines, and illegal diversion of legitimate vaccines.[3] Already, fraudsters have offered, for a fee, to provide potential victims with the vaccine sooner than permitted under the applicable vaccine distribution plan.[4]

In addition, cybercriminals, including ransomware operators, will continue to exploit the COVID-19 pandemic alongside legitimate efforts to develop, distribute, and administer vaccines. FinCEN is aware of ransomware directly targeting vaccine research, and FinCEN asks financial institutions to stay alert to ransomware targeting vaccine delivery operations as well as the supply chains required to manufacture the vaccines. Financial institutions and their customers should also be alert to phishing schemes luring victims with fraudulent information about COVID-19 vaccines.

---

1. For additional information, *see* FinCEN Advisory, FIN-2020-A002, "Advisory on Medical Scams Related to the Coronavirus Disease 2019 (COVID-19)," (May 18, 2020); FinCEN Advisory, FIN-2020-A006, "Advisory on Ransomware and the Use of the Financial System to Facilitate Ransom Payments," (October 1, 2020); and FinCEN Advisory, FIN-2020-A005, "Advisory on Cybercrime and Cyber-Enabled Crime Exploiting the Coronavirus Disease 2019 (COVID-19) Pandemic," (July 30, 2020).
2. For current information on COVID-19-related vaccines, *see* FDA "COVID-19 Vaccines."
3. *See* Federal Bureau of Investigation (FBI) Press Release, "Federal Agencies Warn of Emerging Fraud Schemes Related to COVID-19 Vaccines" (December 21, 2020); FDA, "Beware of Fraudulent Coronavirus Tests, Vaccines and Treatments," (Last update, December 15, 2020); U.S. Department of Homeland Security (DHS), Immigration and Customs Enforcement (ICE) News Release, "ICE Pivots to Combat COVID-19 Vaccine Fraud with Launch of Operation Stolen Promise 2.0," (November 30, 2020); INTERPOL News Release, "INTERPOL Warns of Organized Crime Threat to COVID-19 Vaccines," (December 2, 2020); and Europol Early Warning Notification, "Vaccine-related Crime During the COVID-19 Pandemic," (December 4, 2020).
4. For more information about fraudsters targeting vaccine distribution in the United States, *see* FBI Press Release, "Federal Agencies Warn of Emerging Fraud Schemes Related to COVID-19 Vaccines" (December 21, 2020); and Federal Trade Commission, "COVID-19 Vaccines are in the Pipeline. Scammers Won't be Far Behind," (December 8, 2020).

Suspicious Activity Report (SAR) Filing Instructions

SAR reporting, in conjunction with effective implementation of Bank Secrecy Act (BSA) compliance requirements by financial institutions, is crucial to identifying and stopping fraud, cybercrime, and cyber-enabled crime, including those related to the COVID-19 vaccine. Financial institutions should provide all pertinent information in the SAR.

- FinCEN requests that financial institutions reference "**FIN-2020-NTC4**" in SAR field 2 (Filing Institution Note to FinCEN) and the narrative portion of the SAR to indicate a connection between the suspicious activity being reported and the activities highlighted in this notice.
- 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., vaccine scam or vaccine ransomware) in SAR field 34(z).
- FinCEN requests that filers further detail the reported activity in the narrative portion of the SAR. If the activity is suspected of being a scam, filers should provide known details about how the scammers contacted the victim, how the victim provided or attempted to provide payment related to the scam, and any other available details including data related to the financial transactions or method of contact, such as Internet Protocol (IP) addresses and phone numbers. For guidance on ransomware attacks, see FinCEN Advisory, FIN-2020-A006, "Advisory on Ransomware and the Use of the Financial System to Facilitate Ransom Payments," (October 1, 2020).
- Please refer to FinCEN's May 2020 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

Additional COVID-19-related information, including advisories and notices, can be found 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.