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.