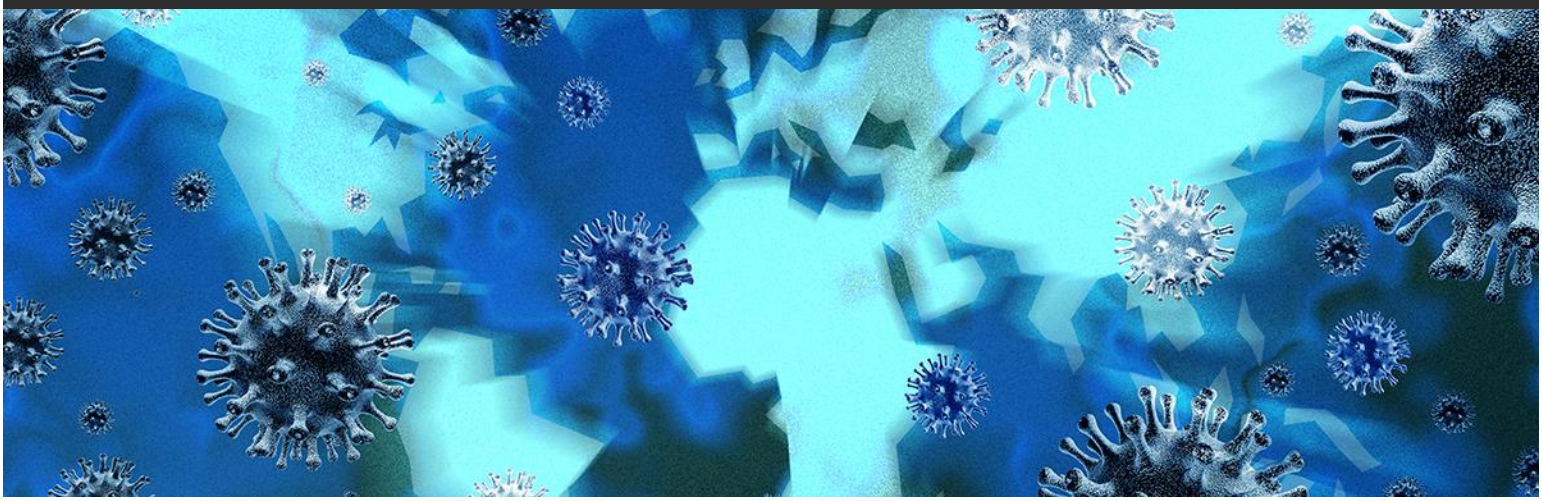
GT GreenbergTraurig

Alert | Health Emergency Preparedness Task Force: Coronavirus Disease 2019



July 2020

FinCEN Alerts Financial Institutions to COVID-19-Related Imposter Scams and Money Mule Schemes

On July 7, 2020, the U.S. Department of the Treasury's Financial Crimes Enforcement Network (FinCEN) published an Advisory to alert financial institutions to potential indicators of imposter scams and money mule schemes that have become prevalent during the Coronavirus Disease 2019 (COVID-19) pandemic. FinCEN issued a similar Advisory on May 18, 2020, discussing medical scams related to COVID-19 and a Notice with instructions for reporting COVID-19-related suspicious activity. We discussed FinCEN's May 18 Advisory and Notice in a prior GT Alert.

Imposter Scams

Imposter scams involve the impersonation of organizations such as government agencies, nonprofit groups, universities, or charities to offer fraudulent services or otherwise defraud victims. FinCEN explains that imposter scams involve 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. Examples of imposter scams include tricking consumers into giving money or personal information in return for Economic Impact Payments (EIPs) under the Coronavirus Aid, Relief, and Economic Security (CARES) Act, posing as government or health care contact tracers to elicit

personal information, and impersonating charities or creating sham charities claiming to take donations for pandemic-relief efforts.

Although imposter scams generally target customers rather than financial institutions directly, financial institutions should be on alert for red-flag indicators of COVID-19-related imposter scams when interacting with customers. Such red flag indicators include:

- Customers indicating that a government agency contacted them requesting personal or bank account information to verify, process, or expedite EIPs, unemployment insurance, or other benefits (special attention should be placed on communications emphasizing "stimulus checks" or "stimulus payments").
- 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 expected for an EIP, with instructions to contact the fraudulent government agency to verify personal information to receive the full EIP benefit.
- Solicitations for donations to charitable organizations that do not have an in-depth history, financial reports or documentation of tax-exempt status, or that cannot be verified through internet-based resources.

Money Mule Schemes

FinCEN defines "money mules" as persons who transfer illegally acquired money on behalf of or at the direction of another. During the COVID-19 pandemic, money mules have included unwitting, witting, and complicit participants. Money mule schemes have included good-Samaritan, romance, and work-from-home schemes. Financial red-flag indicators of money mule schemes include:

- Customers who receive multiple state unemployment-insurance payments to their account or to multiple accounts at the same financial institution within the same disbursement timeframe (e.g., weekly or biweekly payments) issued from one or multiple states.
- Customers making atypical transactions involving overseas accounts that the customer indicates is for a person located overseas who is in need of financial assistance in light of the COVID-19 pandemic.
- Customers who state, or where 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 U.S. Service members who are reportedly stationed abroad, U.S. citizens working or traveling abroad, or U.S. citizens quarantined abroad.

Suspicious Activity Report (SAR) Filing Instructions

The July 7 Advisory reminds financial institutions to provide all pertinent available information in the SAR form and narrative, and to adhere to the following filing instructions to assist FinCEN and law enforcement in effectively identifying actionable SARs and information to support COVID-19-related investigations:

- Include a reference to the Advisory in SAR field 2 by adding the term "COVID19 MM FIN-2020-A003" and indicating in the SAR narrative a connection between the suspicious activity being reported and activities highlighted in the Advisory.

- Select SAR field 34(z) (Fraud-other) as the associated suspicious activity type to indicate a connection between the suspicious activity 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).

FinCEN also encourages financial institutions to report certain types of imposter scams and money mule schemes using SAR field 34(l) (Fraud-Mass-marketing) or SAR field 38(d) (Other Suspicious Activities-Elder Financial Exploitation), as appropriate.

Financial institutions should be continuously enhancing their anti-money laundering monitoring systems to incorporate COVID-19-related schemes and red flags identified by regulators and law enforcement. Continuous updating of anti-money laundering monitoring systems is critical to ensuring ongoing compliance with BSA requirements and regulatory expectations.

For more information and updates on the developing COVID-19 situation, visit GT's Health Emergency Preparedness Task Force: Coronavirus Disease 2019.

Authors

This GT Alert was prepared by:

- Carl A. Fornaris | +1 305.579.0626 | fornarisc@gtlaw.com
- Marina Olman-Pal | +1 305.579.0779 | olmanm@gtlaw.com
- Kyle R. Freeny ‡ | +1 202.331.3118 | freenyk@gtlaw.com
- Emily M. Wassermann | +1 305.579.0799 | wassermanne@gtlaw.com

‡ Admitted in California. Practice in the District of Columbia limited to matters and proceedings before Federal courts and Agencies.