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.