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.