Coronavirus relief funds mistakenly being direct deposited to cybercriminals

James J. Giszczak, Dominic A. Paluzzi, Joelle H. Dvir, Hussein Jaward, CIPP/US | Tuesday, April 21, 2020

The Internal Revenue Service has started direct depositing coronavirus relief funds into millions of bank accounts, but some of these funds are not arriving to the intended recipients.

The IRS is depositing the funds into the most recent bank accounts that it has on file from recipients' income tax filings. However, these accounts are not always legitimate. As we approach April each year, there is an influx of fraudulent tax return incidents that we assist our tax preparer clients through. These incidents typically involve a cybercriminal e-filing a fraudulent tax return on an individual's behalf seeking a tax refund and changing the direct deposit account on file to the cybercriminal's in order to receive the refund. For individuals impacted by tax return fraud this year, the stakes are even higher. While the IRS has implemented a number of initiatives to help prevent tax return fraud, coronavirus relief funds are being deposited to the cybercriminals' bank accounts that are still tied to the fraudulent 2019 tax return (or 2018 if no return has been filed for 2019 yet).

There are a number of steps tax professionals can take to help their clients prevent this. First, tax professionals should immediately inform the IRS of information security incidents and cooperate with the IRS' investigation thereafter. Doing so allows the IRS to mark consumer files and bank accounts as being potentially compromised and to determine safer ways to provide relief funds to consumers. Second, tax professionals should advise their clients to monitor the status of their stimulus relief funds at https://www.irs.gov/coronavirus/get-my-payment. This website also allows recipients to modify their

bank account information if their relief fund disbursement has not been scheduled yet. If the funds were disbursed to the wrong bank account, tax professionals should advise impacted clients to contact the IRS through the agency's website and report the problem. Third, tax professionals should ensure that data security incidents are properly analyzed under the applicable data breach notification laws and that their clients are timely notified of such incidents, if required. This will allow clients to take steps to safeguard themselves against identity theft before it happens. And fourth, tax professionals should proactively engage data privacy and cybersecurity professionals and computer forensic experts to assist in mitigating cyber risks and responding to security incidents. Proactive risk mitigation can prevent information security incidents--and protect client data from being compromised. And prompt incident response can prevent cybercriminals from misusing client data.

Attorneys from McDonald Hopkins' Data Privacy and Cybersecurity Team are available to guide tax professionals through incidents relating to tax return fraud and misdirected coronavirus relief fund disbursements.

James J. Giszczak

Team member bio

Dominic A. Paluzzi

Team member bio

Joelle H. Dvir

Team member bio

Hussein Jaward, CIPP/US

Team member bio