Legal Intelligencer
https://www.law.com/thelegalintelligencer/2020/05/07/fraud-in-the-time-of-covid-19-stay-informed-to-stay-safe/

Fraud in the Time of COVID-19: Stay Informed to Stay Safe

COVID-19 related fraud has been a topic in nearly all of the newsletters that are hitting my inbox and many of the news stories I have been reading. Some are a twist on the old scams, and some are new, based on the fears and vulnerabilities the pandemic has exposed.

By **Nicole McNeil Donecker** | May 07, 2020 at 01:56 PM


Nicole McNeil Donecker of Marcum.

When I first volunteered to write this article at the end of 2019, I had a completely different topic in mind. Then our world changed practically overnight. A virus started spreading across the world with so many unknowns attached to it, later being classified as and quickly escalated to pandemic status. COVID-19 forced the closure of business offices, creating a remote workforce. Even though businesses have been shuttered, the businesses of fraud and scam have not.

COVID-19 related fraud has been a topic in nearly all of the newsletters that are hitting my inbox and many of the news stories I have been reading. Some are a twist on the old scams, and some are new, based on the fears and vulnerabilities the pandemic has exposed.

For example, in Louisville, Kentucy, a COVD-19 “testing site” was charging people $240 per test in cash. The individual receiving the test could also provide his Medicare or Social Security card to confirm identity. The “testing site” claimed any government medical plan would be billed directly. This was one of multiple “testing sites” run out of Louisville by the council president.

Economic Impact Payments

As businesses closed and millions of American households are lost their income, Congress passed the CARES Act to provide funds to those who meet certain income criteria. While most economic impact payments have already been distributed by direct deposit, more payments will be distributed by paper check. These paper checks open the door for fraud.

The Secret Service, in conjunction with the Department of the Treasury, issued a press release on April 20 to help the public identify the **security features of the U. S. Treasury checks**. These security features include:

- A new Treasury seal that reads “Bureau of Fiscal Service” to the right of the Statue of Liberty;
- The seal is printed with “bleeding ink” that will run and turn red when moisture is applied;
- The checks are printed with a watermark that reads “U.S. TREASURY” when held up to the light;
- The check includes ultraviolet overprinting pattern that is naked to the eye;
- Microprinting on the back of the check with the words “USAUSAUSA;” and
- Printing of “Economic Impact Payment President Donald J. Trump” to the lower right of the Statue of Liberty.

As with the warnings from the Secret Service and Treasury Department, the IRS continues to remind everyone that the service will not contact taxpayers by email, phone or text for information. IRS Commissioner Chuck Rettig stated, “The IRS isn’t going to call you asking to verify or provide your financial information so you can get an economic impact payment or refund faster. That also applies to surprise emails that appear to be coming from the IRS.” The IRS’s website provides several reminders to taxpayers of what “scammers” may do or say:

- The official name is “economic impact payment.” Scammers will emphasize words like “Stimulus Check” or “Stimulus Payment.”
- Ask taxpayers to sign over their economic impact check to the scammer.
- Request personal or financial information verification by phone, email, text or social media to receive or speed up receipt of the economic impact payment.
- Suggest that they can get the economic payment faster by working on the taxpayer’s behalf.
- Send taxpayers a bogus check in the mail. The check could be in an odd amount, and the scammer will request the taxpayer to call a number or verify information online in order to cash it.

Additionally, the IRS is warning tax professionals about the use of Virtual Private Networks (VPNs) and recommends using only an encrypted VPN for transmitting sensitive client data, as preparers are working remotely. Social distancing has prevented tax professionals from having face-to-face meetings with clients, which prevents building in-person relationships with new and potential clients. Scammers can take advantage of this anonymity to pose as a “new client” and send phishing emails with attachments that contain viruses and malware. It is recommended that tax professionals call “new clients” to confirm the emails and attachments and not take the bait.

Department of Justice and Law Enforcement

On March 16, Attorney General William Barr issued a memorandum to all U.S. Attorneys regarding the Department of Justice’s priorities as they relate to COVID-19, protecting the justice system and detecting, deterring, and punishing wrongdoing. The memorandum states, “Every U.S. Attorney’s Office is thus hereby directed to prioritize the detection, investigation, and prosecution of all criminal conduct related to the current pandemic.”

U.S. Department of Justice **issued a fraud alert** for COVID-19 fraud. The fraud alert provides examples of fraudulent and criminal behavior currently being reported by businesses and individuals in addition to the fraud and scams surrounding the economic impact payments. The **FBI website includes multiple alerts** related to COVID-19 frauds. Many of the new frauds and scams seem to fit into familiar categories or are variations on common frauds designed to prey upon new fears surrounding COVID-19 including:

- Unlawful hoarding and price-gouging
- Testing scams
- Treatment scams
- Supply scams
- Provider scams
- Charity scams
- Phishing scams and cyber intrusions

- App scams
- Investment scams
- “$1,000 check” scams
- Other scams include individuals claiming to work for the government, banks / credit cards offering assistance with financial needs related to student loans, foreclosure and eviction, unemployment, and debt relief.

Barr established the COVID-19 Hoarding and Price Gauging Task Force to “aggressively pursue bad actors who amass critical supplies far beyond what they could use or for the purpose of profiteering. Scarce medical supplies need to be going to hospitals for immediate use in care, not to warehouses for later overcharging.”

On March 25, the Department of Health and Human Services (HHS) issued a notice under Executive Order 13910 and section 102 of the Defense Production Act of 1950 designating certain materials as “scarce materials or threatened materials.” Among the materials identified are the N95 filtering facepiece respirators, more commonly known as “N95” masks.

A press release from the U.S. Attorney’s Office for the District of New Jersey announced a criminal complaint against Baruch Feldheim of Brooklyn, New York. Although Feldheim is charged with assault of a federal officer and false statement in the amended criminal complaint, he is alleged to have hoarded almost 200,000 N95 masks, 600,000 medical gloves, 130,000 surgical masks and other medical equipment. According to the criminal complaint, certain individuals agreed to purchase specific PPE items for $12,000 or a markup of approximately 700%.

On April 24, the Eastern District of New York charged Amardeep Singh under the Defense Production Act with hoarding and price gouging of scarce PPE. Singh is considered the first person charged under the Defense Production Act with hoarding and price gouging during the COVID-19 pandemic. Beginning in mid-March, Singh received 67 shipments of disposable face masks, disposable surgical gowns, hand sanitizer and digital thermometers weighing over 5.5 tons. The press release from the U. S. Attorney’s Office states that Singh was selling disposable face masks at $1, a 1,328% markup from the purchase price of $0.07 each. If convicted, Singh could face one year in prison.

In a twist on the hoarding theme, some other unscrupulous actors were attempting to sell nonexistent goods. A news headline appeared at the end of March stating, “Union Locates Massive Supply of N95 Masks.” The SEUI-United Healthcare Workers in California thought it had located a warehouse containing 39 million N95 masks. A Pittsburgh businessman became the middleman between the health care professionals in the United States and an Australian broker and Kuwaiti manufacturer. U.S. Attorney for the Western District of Pennsylvania Scott Brady has stated that the Justice Department has begun an investigation of these two foreign entities attempting to defraud health care companies in the United States. Brady also stated that other groups have allegedly attempted to sell masks with 40% of the cost due up front for expedited delivery of masks that do not exist.

The FBI is also battling fraud related to COVID-19. A cooperative effort between internet domain providers and registrars shut down hundreds of domains being used to commit frauds related to COVID-19. In the press release dated April 22, the FBI Internet Crime Complaint Center (IC3) stated it had received over 3,600 complaints related to suspicious websites and domains as of that date.

The Federal Trade Commission is also spreading awareness of potential scams by creating “FTC Scam Bingo” with bingo card blocks that read “COVID-19 cure” and “hung up on robocall,” for example (since most people are now working from home, more scam calls are being answered). The card can be shared on social media using the hashtag #FTCScamBingo. By sharing and playing “bingo,” you can help in recognizing and avoiding potential scams. The “bingo card” can be found here: **https://www.consumer.ftc.gov/blog/2020/03/now-more-ever-spot-scams-ftcscambingo**.

During this “new normal,” we must continue to be vigilant about the multitude of frauds and scams that are out there. Staying informed is essential to staying safe from those trying to exploit people during this pandemic. The IRS encourages taxpayers to report unsolicited emails, text messages and social media attempts to solicit information to **phishing@irs.org**. If you suspect COVID-19 fraud, call the National Disaster Fraud Hotline at 866-720-5721 or email **disaster@leo.gov**. Cyber scams should be reported to **https://www.ic3.gov/default.aspx**.

Nicole McNeil Donecker *is an advisory services manager in Marcum's Philadelphia office. She focuses her practice on forensic accounting and litigation support services. Contact her at* ***Nicole.donecker@marcumllp.com****.*