Department of Justice

STATEMENT OF THE
U.S. DEPARTMENT OF JUSTICE

CALVIN A. SHIVERS
ASSISTANT DIRECTOR
FEDERAL BUREAU OF INVESTIGATIONS

BEFORE THE

COMMITTEE ON THE JUDICIARY
UNITED STATES SENATE

FOR A HEARING ENTITLED

"COVID-19 FRAUD: LAW ENFORCEMENT'S RESPONSE TO THOSE EXPLOITING THE PANDEMIC"

PRESENTED

JUNE 9, 2020

CALVIN A. SHIVERS
ASSISTANT DIRECTOR
FEDERAL BUREAU OF INVESTIGATIONS
U.S DEPARTMENT OF JUSTICE

STATEMENT FOR THE RECORD

BEFORE

THE UNITED STATES SENATE COMMITTEE ON THE JUDICIARY
WASHINGTON, D.C.
FOR A HEARING ENTITLED
"COVID-19 FRAUD: LAW ENFORCEMENT'S RESPONSE TO THOSE EXPLOITING THE PANDEMIC."

JUNE 9, 2020

Chairman, Ranking Member, and Members of the Committee, thank you for the opportunity to appear before you today to discuss the rapidly evolving threats to the United States homeland posed by the myriad of fraud schemes which seek to exploit the global COVID-19 pandemic. The FBI has worked to counter the threats posed by fraud schemes and illicit finance activities since its inception—these threats are pervasive and have become more frequent and sophisticated over time. Moreover, they adversely affect the United States by destabilizing our financial system and institutions and harming people at higher risk (including older adults and people with underlying medical conditions).

On March 16, 2020, the Attorney General issued a memorandum on fraud in connection with COVID-19. Within days, the FBI established a COVID-19 Working Group comprised of representatives from all 56 FBI field offices and 500 total participants from the Department of Justice (Department) and FBI to combat the criminals undermining our nation during this crisis. The COVID-19 pandemic has only served to increase the number of stimulus, healthcare, bank, elder, and government fraud schemes. As of May 28, 2020, the Internet Crime Complaint Center (IC3) received nearly the same amount of complaints in 2020 (~320,000) as they had for the entirety of 2019 (~400,000). Approximately 75% of these complaints are frauds and swindles, presenting a challenge for the FBI's criminal program given the sheer volume of submissions.

We have also seen the sale of counterfeit personal protective equipment (PPE), fraudulent unemployment insurance claims, and even criminals who are engaging in online predatory behavior targeting children who are continuing their education from home. Keeping pace with these threats and their volume is a significant challenge for the Federal Bureau of Investigation (FBI), but one we are tackling head on in conjunction with our many federal, state, local, private sector, non-profit, and community partners.

INCREASED RISK OF CHILD EXPLOITATION

Online sexual exploitation comes in many forms. Individuals may coerce children into providing sexually explicit images or videos of themselves and/or younger family members.

With the threat of posting the images publicly or sending them to the child's friends and family if the child does not continue sending the material, they are forced into an abusive cycle of exploitation. Other offenders may make casual contact with children online, gain their trust, and introduce sexual conversation that increases in egregiousness over time. This activity may ultimately result in an online relationship that includes sexual conversation, the exchange of illicit images, and physically meeting the child in-person for the purpose of engaging in illegal sexual activities.

School closures as a result of COVID-19 have increased the presence of children online, desensitizing them to being online and putting them in a position of increased risk. To proactively counter these risks, we have worked to warn parents, educators, caregivers, and children about the dangers of online sexual exploitation and signs of child abuse through public service announcements (PSAs), billboards, and meetings with our private sector partners hosting video communications platforms. In particular, we have emphasized parents' and other caregivers' need to be mindful about children's use of apps and platforms that feature end-to-end encryption, direct messaging, video chats, file uploads, and user anonymity, which predators often use to contact children directly and evade law enforcement.

During the last few months, the FBI has received more than 315 reports of incidents throughout the United States and in other countries in which a Zoom participant was able to broadcast a video depicting child sexual abuse material (CSAM). The FBI considers this activity to be a violent crime. Every time child sexual abuse material is viewed, the depicted child is re-victimized. Furthermore, anyone who is exposed to child sexual abuse material during a virtual event may be traumatized by the experience. In the last 75 days, we have identified over 400 victims due to this activity.

PAYCHECK PROTECTION PROGRAM

With the passage of the CARES Act, the FBI has seen fraudsters shift their efforts towards exploiting the various programs aimed at relieving the detrimental economic effects of COVID-19. Of particular interest are criminals fraudulently applying for Paycheck Protection Program (PPP) loans or targeting PPP funds once they have been disbursed.

The FBI's IC3 has received numerous complaints from business owners unable to legitimately apply for a PPP loan because their Employer Identification Numbers (EINs) were already used for fraudulent loan applications. There have also been reports of fraudulent websites claiming to facilitate PPP loans, which gather all the personally identifiable information necessary to apply for a PPP loan, only to not follow through with the assistance, but likely use the information for their own nefarious purposes.

In order to effectively target this growing threat, the FBI has formed a PPP Fraud Working Group in coordination with the Department's Fraud Section and the Small Business Administration Office of Inspector General. Through the efforts of our field offices and the PPP Working Group, nearly 100 investigations have been initiated since the inception of the program, with over $42 million in potential fraud identified and over $900,000 recovered. These

investigations involve bank insiders, previously convicted felons, the use of dormant or cash businesses, and identity theft.

ADVANCE FEE AND BUSINESS EMAIL COMPROMISE SCHEMES

In the current environment, demand for PPE and other goods far exceeds supply, and businesses have had to alter standard practices to continue operations. Such an environment is ripe for exploitation by fraudulent actors perpetrating advance fee and business email compromise (BEC) schemes. In the advance fee schemes related to procurement: a victim pre-pays a purported seller or a broker for goods such as ventilators, masks, sanitizer or other in-demand products, and then receives little or nothing in return. BEC schemes often involve fraudsters spoofing a legitimate email address known to the recipient or the use of an email address that is nearly identical to one known and trusted by the victim to instruct them to redirect legitimate payments to bank accounts controlled by the fraudsters.

Recent examples of COVID-19-related BEC attempts include a financial institution that received an email, allegedly from the CEO of a company, who had previously scheduled a transfer of $1 million, requesting that the transfer date be moved up and the recipient account be changed "due to the Coronavirus outbreak and quarantine processes and precautions." The email address used by the fraudsters was almost identical to the CEO's actual email address, with only one letter altered.

In another instance, a fraudster spoofed the email address of a CEO who had been approved for a PPP loan, contacted the financial institution facilitating the loan and requested that the PPP funds be transferred to a new account at a different institution. The FBI is also aware of multiple incidents in which state government agencies, attempting to procure ventilators or PPE, wire transferred funds to fraudulent brokers and sellers in advance of receiving the items. The brokers and sellers included both domestic and foreign entities. In one case, an individual claimed to represent an entity with which the purchasing agency had an existing business relationship. By the time the purchasing agencies became suspicious of the transactions, much of the funds had been transferred outside the reach of U.S. law enforcement and were unrecoverable.

MONEY MULES

With the U.S. unemployment rate soaring and large numbers of people being secluded at home, fraudsters are increasingly targeting individuals through "work from home" opportunities or dating websites to use as money mules. Criminals who obtain money illegally need to find a way to move and hide the illicit funds. They frequently scam other people, known as money mules, into moving this illicit money for them. These money mules are asked to receive funds in their personal bank account and then "process" or "transfer" funds via wire transfer, ACH, mail, or money service businesses, such as Western Union or MoneyGram.

Acting as a money mule—allowing others to use one's bank account or conducting financial transactions on behalf of others—not only jeopardizes the mule's financial security and compromises their personally identifiable information but is also a crime. Over the last several

years, the FBI has dedicated significant resources to educating the public on common red flags that they may be acting as a money mule and has continued to reinforce this messaging to address the rise of COVID-19-related money mule schemes. The FBI encourages individuals to protect themselves by refusing to send or receive money on behalf of individuals and businesses for which they are not personally or professionally responsible, and to watch out for online job postings and emails from individuals promising easy money for little to no effort.

VIRTUAL ASSETS

With the rise in the use of virtual assets and encrypted devices and applications, the interconnectivity of communication platforms, and the ever-changing landscape of emerging payment systems, the world is more connected today than ever. This also means it has becoming increasingly difficult to track illicit finance flows and identify the criminal actors behind them.

Fraudsters are leveraging increased fear and uncertainty during the COVID-19 pandemic to steal Americans' money and launder it through the complex virtual asset ecosystem. Some criminals use virtual assets to conduct illicit transactions because these currencies offer potential anonymity. Furthermore, these transactions are often not tied to a real-world identity and enable criminals to quickly move criminal proceeds among countries.

People of all ages, including older adults, are being victimized by criminals through virtual asset-related fraud schemes. Developments in virtual asset technology and an increasing number of businesses accepting virtual assets as payment have driven their growing popularity and accessibility. There are not only numerous virtual asset service providers online, but also thousands of virtual asset kiosks located throughout the world which are vulnerable to exploitation by criminals to facilitate their schemes. Many traditional fraud and money laundering schemes are now orchestrated via virtual assets. The FBI has published a PSA about an increase in virtual asset fraud schemes related to COVID-19, including blackmail attempts, work from home scams, paying for non-existent treatments/equipment, and investment scams. It should be stressed that there are legitimate charities, investment platforms, and e-commerce sites that accept payment in virtual assets. However, unsolicited requests for donations via virtual assets or pressure to use virtual currency should be approached with caution.

PERSONAL PROTECTIVE EQUIPMENT

Scammers are taking advantage of the COVID-19 pandemic to steal money through a variety of means. The FBI is working to educate the health care industry, financial institutions, other private sector partners, and the American public of an increased potential for fraudulent activity dealing with the purchase of COVID-19-related medical equipment. Furthermore, we have worked through the Department to coordinate with the Federal Emergency Management Agency (FEMA) and the U.S. Department of Health and Human Services (HHS) to allocate for purchase by the government at fair market value certain designated supplies that have been stockpiled in excess of an individual's need and/or for the purpose of selling it in excess of prevailing market prices. This is all being done in alignment with the Defense Production Act (DPA).

In price gouging and hoarding investigations in Jackson, Los Angeles, Newark, and New York, the FBI seized the PPE in an effort to stop criminal violations of the DPA and get the PPE to first responders and medical professionals. To date we have acquired millions of units of PPE from the aforementioned jurisdictions, to include surgical masks, gloves, respirators, shoe covers, protective gowns, lab coats/overall, and face shields/goggles. We are working closely with the Department to determine the next steps for the redistribution, purchase, and/or sale of these items.

HEALTH CARE FRAUD SCHEMES

Legitimate medical professionals and scientists throughout the U.S. are working hard to find a cure, approved treatment, and vaccine for COVID-19. Unfortunately, bad actors are selling fraudulent COVID-19 test kits and unapproved treatments through telemarketing calls, social media platforms, and door-to-door visits at the same time. Many scammers are promising free care and free COVID-19 testing to patients in order to gain access to their personal and health insurance information, including their dates of birth, Social Security numbers, and financial data.

While the methods are ones we have seen before, the current atmosphere of fear and urgency aids criminals in taking advantage of the American public, particularly at-risk populations like older adults and people with underlying health conditions. Prior health care fraud investigations have shown that once scammers obtain an individual's personal information, they use it to bill federal health care programs and/or private health insurance plans for tests and procedures the individual did not receive and pocket the proceeds. Some bad actors are selling fraudulent at-home test kits while others are even going door-to-door and performing fake tests for money.

ACTIVE RESPONSE AND LOOKING FORWARD

While these frauds prove difficult to address, they are not impossible, and the FBI is making every effort to investigate them. First, we have relied heavily on public education and awareness—only when the general public knows about schemes like BEC and counterfeit goods can it report them. The FBI needs solid leads that we can aggregate in databases and systems like IC3 for analysis. From there, we can identify the perpetrators and follow illicit money to its source.

The repercussions of the COVID-19 pandemic have not and will not end any time soon. While we reflect on our actions thus far to counter specific threats to U.S. national security, we must also anticipate and prepare to address emerging criminal schemes of an even larger scale. Initially, PPE-related hoarding/gauging schemes, investment and consumer fraud schemes promoting fake COVID-19 cures/treatments/tests, BEC schemes, and advance fee schemes were the most prevalent fraud schemes related to COVID-19. While these continue, the FBI has seen the fraud landscape shifting over the past month as criminals continue to attempt to fraudulently obtain funds made available through the CARES Act stimulus. In response, the FBI is working with DOJ and relevant federal agency inspectors general to actively address substantial numbers of fraudulent PPP loans and Economic Injury Disaster Loan Emergency Advances.

As a result of the COVID-19 pandemic, the FBI has also identified an increase in health care fraud. As the number of people seeking treatment for the virus has increased, so too have the number of criminal actors seeking to profit from the crisis by exploiting vulnerabilities in the delivery of medical services. The FBI, together with our law enforcement and regulatory partners, as well as our partners in the private sector, has identified a variety of fraudulent schemes targeting both government sponsored health care programs, particularly Medicare and Medicaid, and private health insurance plans, including overbilling for services, billing for services not rendered, and billing for medically unnecessary services. We have seen many of these schemes before, and we are aggressively working to stop them.

The FBI is also pursuing criminals who file fraudulent claims for unemployment insurance payments, often using stolen identities, and routing the funds to themselves. We continue to engage heavily with private sector partners, particularly financial institutions and health insurance companies, to communicate the fraud trends we are seeing, gain valuable insights from the institutions on what they have seen, and share intelligence related to investigations. We have received countless valuable referrals from financial institutions in the form of Financial Crimes Enforcement Network (FinCEN) Suspicious Activity Reports that relate to already open investigations or have led to the initiation of new investigations. These relationships with the private sector have allowed us to more efficiently and effectively address many of the fraud schemes that have emerged since the beginning of the COVID-19 pandemic, and we continue to rely on these relationships as schemes change and evolve.

The FBI is engaged in myriad efforts to combat COVID-19 threats, from improving threat identification and information sharing inside and outside of the government to examining the way we operate to disrupt and defeat these threats. All facets of the FBI are working to counter these threats and head off those that are just emerging. We are proud to work alongside our federal law enforcement and private sector partners to protect the American public from COVID-19 related scams during these difficult times. These collaborative efforts are the key to quickly reducing the threat from COVID-19 related criminal activity, so the American public can focus on protecting themselves and their families during these trying times.

Thank you, Chairman Graham and Ranking Member Feinstein, for bringing attention to these issues. I would be happy to answer any questions you might have.