

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

HEARING BEFORE THE COMMITTEE ON THE JUDICIARY UNITED STATES SENATE ONE HUNDRED SIXTEENTH CONGRESS

SECOND SESSION

JUNE 9, 2020

Serial No. J-116-54

Printed for the use of the Committee on the Judiciary



www.judiciary.senate.gov
www.govinfo.gov

U.S. GOVERNMENT PUBLISHING OFFICE

WASHINGTON : 2026

COMMITTEE ON THE JUDICIARY

LINDSEY O. GRAHAM, South Carolina, *Chairman*

| | |
|-----------------------------|----------------------------------|
| CHARLES E. GRASSLEY, Iowa, | DIANNE FEINSTEIN, California, |
| JOHN CORNYN, Texas | <i>Ranking Member</i> |
| MICHAEL S. LEE, Utah | PATRICK J. LEAHY, Vermont |
| TED CRUZ, Texas | RICHARD J. DURBIN, Illinois |
| BEN SASSE, Nebraska | SHELDON WHITEHOUSE, Rhode Island |
| JOSH HAWLEY, Missouri | AMY KLOBUCHAR, Minnesota |
| THOM TILLIS, North Carolina | CHRISTOPHER A. COONS, Delaware |
| JONI ERNST, Iowa | RICHARD BLUMENTHAL, Connecticut |
| MIKE CRAPO, Idaho | MAZIE K. HIRONO, Hawaii |
| JOHN KENNEDY, Louisiana | CORY A. BOOKER, New Jersey |
| MARSHA BLACKBURN, Tennessee | KAMALA D. HARRIS, California |

LEE HOLMES, *Republican Chief Counsel and Staff Director*

PHILLIP A. BREST, *Democratic Chief Counsel and Acting Staff Director*

CONTENTS

OPENING STATEMENTS

| | Page |
|------------------------------|------|
| Graham, Hon. Lindsey O. | 1 |
| Feinstein, Hon. Dianne | 2 |
| Prepared statement | 35 |

WITNESSES

| | |
|-----------------------------------------------------|-----|
| Carpenito, Craig | 3 |
| Prepared statement | 38 |
| Questions submitted with no response returned | 63 |
| D'Ambrosio, Michael | 7 |
| Prepared statement | 51 |
| Responses to written questions | 75 |
| Hughes, William | 2 |
| Prepared statement | 38 |
| Questions submitted with no response returned | 105 |
| Shivers, Calvin A. | 5 |
| Prepared statement | 56 |
| Questions submitted with no response returned | 124 |

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

TUESDAY, JUNE 9, 2020

UNITED STATES SENATE,
COMMITTEE ON THE JUDICIARY,
Washington, DC.

The Committee met, pursuant to notice, at 10:08 a.m., in Room SD-106, Dirksen Senate Office Building, Hon. Lindsey O. Graham, Chairman of the Committee, presiding.

Present: Senators Graham [presiding], Grassley, Hawley, Tillis, Ernst, Blackburn, Feinstein, Durbin, Whitehouse, Klobuchar, Blumenthal, Hirono, and Booker.

**OPENING STATEMENT OF HON. LINDSEY O. GRAHAM,
A U.S. SENATOR FROM THE STATE OF SOUTH CAROLINA**

Chairman GRAHAM. Good morning, everybody. Thank you very much for attending the hearing, and I am sure we will have more come in throughout the morning.

We have got four witnesses: Mr. Craig Carpenito, is that right? U.S. Attorney for the District of New Jersey; Bill Hughes, Associate Deputy Attorney General; Calvin Shivers, Assistant Director of the Criminal Investigative Division, FBI; Michael D'Ambrosio, Assistant Director of the Office of Investigations, United States Secret Service.

So we talked about this before, fraud related to the CARES Act, scams out there against seniors selling masks that don't work, trying to play on people's fears. Unfortunately, when you try to do some good in the country, people take advantage of it, and we are going to hear from our folks today about what's going on out there and some ideas about how to make sure it stops, if we can.

Phase 4 will be coming. There's a need, in my view, for a Phase 4, so I would like to learn as much as we can about the Paycheck Protection Program, the economic impact for individuals, and supplemental unemployment benefits, how those programs are sometimes being abused, and generally about what people are doing out there to scam Americans, particularly our seniors, and that's the purpose of the hearing.

And, with that, I will turn it over to Senator Feinstein.

**OPENING STATEMENT OF HON. DIANNE FEINSTEIN,
A U.S. SENATOR FROM THE STATE OF CALIFORNIA**

Senator FEINSTEIN. Thank you, Mr. Chairman. I will put my statement in the record so you can proceed. Thank you.

[The prepared statement of Ranking Member Feinstein appears as a submission for the record.]

Chairman GRAHAM. Thank you.

Anything from anybody?

[No response.]

Chairman GRAHAM. Okay. Let us start with Mr. Hughes.

STATEMENT OF WILLIAM HUGHES, ASSOCIATE DEPUTY ATTORNEY GENERAL, U.S. DEPARTMENT OF JUSTICE, WASHINGTON, DC

Mr. HUGHES. Good morning, Mr. Chairman, Ranking Member Feinstein, and Members of the Committee. Thank you for inviting me to appear before you today with several of my colleagues to discuss Federal law enforcement efforts to deter, detect, and prosecute those who violate Federal law by exploiting the COVID-19 pandemic and the economic dislocation it has caused.

Before I focus on the topic of the day, I want to take a moment to address the tragic killing of George Floyd. As Attorney General Barr and Deputy Attorney General Rosen have previously said, the video images of the police conduct in this instance are incredibly disturbing. As the Attorney General previously announced, the Department is conducting a parallel and independent investigation into this incident in collaboration with the FBI to determine whether Federal civil rights laws were violated. We intend to conduct that investigation as swiftly as possible and are not sparing any resources.

We know that George Floyd's death was not the first of its kind, and it exposes concerns that reach far beyond this specific incident. The outrage that Mr. Floyd's death has triggered is real, legitimate, and deeply rooted. While the vast majority of police officers do their job honorably and in accordance with the law, we see instances like this one that erode confidence in the American criminal justice system. America takes great pride in the rule of law being a bedrock principle, and as the Nation's leading Federal law enforcement agency, the Department of Justice is committed to doing its part to seek justice for Mr. Floyd and his loved ones and to secure the confidence of all Americans and law enforcement.

I know these issues are important to you. They are important to us. We welcome the opportunity to have discussions on this subject in the days ahead. But for today, for this hearing, our subject is the pandemic, the related economic disruption, and those that wish to exploit others for their own gain during tremendously challenging times. The Attorney General has made clear that, notwithstanding the operational challenges the pandemic presents, it is critical that the Department is vigilant in detecting, investigating, and prosecuting wrongdoing relating to the crisis. It has become a high priority for us.

Since the early days of the pandemic, we have been receiving reports of individuals and businesses using the crisis as an opportunity to exploit both Americans and Government programs de-

signed to assist Americans that have been hard hit. Leveraging the public's concern about the pandemic, fraudsters utilize many schemes to separate Americans from the money in their bank accounts, from their Government benefits, and from their personally identifiable information.

Other fraudsters and unscrupulous opportunists have gotten into the personal protective equipment trade, looking to defraud and price gouge health providers, first responders, and other essential workers who have no choice but to pay astronomical prices for protective equipment that their health depends on.

We are also seeing schemes that target taxpayer-backed relief programs that provide Americans and American businesses financial help as they weather a disrupted economy. In particular, fraudsters are targeting the Payroll Protection Program, the Economic Impact Payment Program, and State unemployment benefit programs.

The pandemic has also changed the cyber threat landscape. Child predators on the internet see widespread closing of schools, stay-at-home orders, and reliance on internet platforms as the primary means of communication as an opportunity to prey on children. Cyber criminals also see the widespread work-from-home posture of many American businesses as an opportunity to attack and infiltrate business computer networks, to disable systems or steal or hold hostage valuable data.

As I am sure you will agree, it is reprehensible that anyone would use this crisis as an opportunity to profit at another person's expense or otherwise prey on the public. The Department of Justice will not tolerate it, and our resolve is demonstrated by our efforts to coordinate across Department offices and components, to collaborate with other Government agencies, and to engage with industry and the public.

We are already bringing cases to hold fraudsters accountable and to disrupt their schemes, and we will be doing so for the foreseeable future.

I thank you again for the invitation, and I look forward to your questions.

[The prepared statement of Mr. Hughes and Mr. Carpenito appears as a submission for the record.]

STATEMENT OF HON. CRAIG CARPENITO, UNITED STATES ATTORNEY, DISTRICT OF NEW JERSEY, U.S. DEPARTMENT OF JUSTICE, NEWARK, NJ

Mr. CARPENITO. Good morning, Chairman Graham, Ranking Member Feinstein, and Members of the Committee. I am Craig Carpenito, the United States Attorney for the District of New Jersey. I was appointed by Attorney General Barr to lead the Department's Hoarding and Price Gouging Task Force. We are grateful for the privilege of appearing before you today to discuss the Department's efforts to detect and prosecute those who, for their personal financial gain, seek to exploit the COVID-19 pandemic and the economic dislocation it has caused.

The Attorney General and the Deputy Attorney General are leading those efforts, and we are honored to help them in that vital task. We want to thank the Committee for its attention to these

issues and for the good work of the Department of Justice to protect the safety and security of our Nation during this unprecedented crisis.

Before I answer your questions today about price gouging, hoarding, and COVID-19 fraud, however, I would like to take a moment to acknowledge the senseless and tragic death of George Floyd at the hands of the Minneapolis police. I am proud of the people of New Jersey who have raised their voices in peaceful protest, seeking justice and reform in the name of Mr. Floyd and the other victims like him. I hear and appreciate their call for change. In New Jersey, we have witnessed productive community and law enforcement partnerships in cities like Newark and Camden. These partnerships have lowered crime and restored trust. While we in New Jersey are proud of these efforts, we recognize that we must and we will do more.

Now let me turn to the reason I am here today. We've seen a broad range of illegal conduct throughout the country in these past few months. Our strategies and responses have evolved to meet new challenges as they arise, but our core philosophy has not. The Department will investigate and prosecute those who seek to treat COVID-19 as an opportunity to defraud the public and the Government.

The Department has received many reports of individuals and businesses using the crisis to seek windfall profits at the expense of public safety and the health and welfare of the American people. These reports range from the sale of fake cures of COVID-19 online to hoarding and price gouging of critical medical supplies, to defrauding the CARES Act economic programs. The Department is aggressively investigating those reports and has already commenced prosecutions.

The Department's attorneys work side by side with our partners at the Federal Bureau of Investigation and the United States Secret Service, as well as other Federal, State, and local agency partners.

Make no mistake. The fight against COVID-19 is a fight to save precious lives every day. Our medical professionals and first responders put their own lives at risk to stand between the virus and each of us. The personal protective equipment that they wear is the only shield they have to protect themselves as they bravely go face to face with the virus each day. It helps ensure our heroes do not fall victim to the disease. It also helps ensure that they do not bring it home to their families and their broader communities.

Hoarding and price gouging in particular have inhibited front-line health care professionals, essential workers, and the public from acquiring the supplies they need to protect themselves from contracting the virus. Hospitals, first responders, and retail consumers have been targeted by individuals who view the scarcity of critical medical materials as a path to get rich quick. This conduct has disrupted our supply chains and markets and jeopardized the safety of our communities.

In response, Attorney General Barr and Deputy Attorney General Rosen assembled the Department's Hoarding and Price Gouging Task Force to combat and prevent hoarding and price gouging. The task force is comprised of over 100 experienced Fed-

eral prosecutors throughout the Nation's 93 U.S. Attorney's Offices and Department components here in Washington. The task force's primary mission is to identify, investigate, and prosecute illegal hoarding and price gouging of crucial medical supplies, including personal protective equipment such as face masks that are essential to preventing the spread of the virus. We do so in the larger context of the current public health crisis. The decisions the Department makes to open investigations or to bring charges are intended to help the public health response. Accordingly, the task force is focusing on profiteering, especially by market participants who sell scarce materials for excessive prices that far exceed their reasonable cost.

The task force also is investigating counterfeit, misbranded, and defective medical supplies imported into the U.S. from abroad. These flawed products are entering our stream of commerce and creating safety hazards. We will use all of our tools at our disposal to identify these products and those who transact in them here and abroad and hold them accountable.

The Department's efforts are ongoing, but they have already yielded substantial results. We have brought several Federal criminal cases across the country alleging price gouging fraud, misbranding, and other charges. Just last week, the task force commenced the Department's first criminal prosecution against a foreign manufacturer for sending defective and misbranded N95 respirator masks into the United States during the pandemic. Instead of protecting our medical professionals, these materials would've silently put them in harm's way. We have also seized hoarded materials and worked with agency partners to distribute them to those on the front lines to fight COVID-19.

Thank you again for inviting us to address these important topics, and I look forward to answering your answers.

[The prepared statement of Mr. Carpenito and Mr. Hughes appears as a submission for the record.]

Chairman GRAHAM. Mr. Shivers.

**STATEMENT OF CALVIN A. SHIVERS, ASSISTANT DIRECTOR,
CRIMINAL INVESTIGATIVE DIVISION, FEDERAL BUREAU OF
INVESTIGATION, WASHINGTON, DC**

Mr. SHIVERS. Good morning, Chairman Graham, Ranking Member Feinstein, and Members of the Committee. My name is Calvin Shivers, and I am the Assistant Director of the FBI's Criminal Investigative Division. Thank you for the opportunity to appear before you today to discuss the FBI's response to COVID-19-related fraud.

As head of the FBI's Criminal Investigative Division, I oversee the FBI's financial crimes and fraud against the Government programs. In my role as the Assistant Director of the Criminal Division, I also oversee civil rights, color of law, and hate crime investigations. I believe it's important that I take a moment to address the recent events which have grabbed our Nation's attention before I focus on the issues surrounding today's hearing.

I along with my colleagues at the FBI offer our sincerest condolences to the family and friends of George Floyd. The FBI's Civil Rights Program has a long and proud history of protecting the

rights of the American people. As the primary Federal agency responsible for civil rights investigations, we at the FBI are committed to utilizing our full set of investigative and intelligence capabilities to address violations of Federal civil rights laws. In pursuit of justice, we are conducting a thorough investigation into the actions that led to George Floyd's death.

The FBI recognizes the rights of citizens to exercise their First Amendment rights, and we will continue to work to protect our citizens and their ability to exercise those rights free of violence.

Now I will shift back to the topic at hand.

These are unprecedented times for most Americans. Due to COVID-19, people are understandably worried about their health and their livelihood. Although we are coming together in various communities and throughout the country, unfortunately there are individuals who seek to exploit our anxieties and fears by selling fake COVID-19 cures or vaccines. They are also peddling fraudulent investment opportunities in companies purportedly working to develop cures or vaccines for COVID-19. These were some of the earliest COVID-19 fraud schemes that the FBI identified.

When the Attorney General issued a memorandum on March 16 of this year directing U.S. Attorneys to prioritize COVID-19-related fraud investigations and prosecutions, the FBI was ready. Within days, all 56 FBI field offices began working a wide range of investigations related to COVID-19 fraud schemes.

As we began our investigations, we saw a number of different criminal schemes. We saw subjects hoarding personal protective equipment, or PPE, and attempting to sell it at exorbitant prices. We also saw people selling counterfeit or substandard PPE. The FBI worked closely with the Department of Justice and other law enforcement partners to conduct price-gouging investigations or seize counterfeit PPE.

The CARES Act was designed to provide fast and direct economic assistance to families, American workers, and small businesses. However, there are individuals who seek to steal money from the people the CARES Act was designed to help. With the passage of the CARES Act, we began to see fraudsters shift their efforts toward exploiting the various programs created to relieve the severe economic effects of COVID-19. To effectively target this growing threat, the FBI formed a Payroll Protection Program Fraud Working Group in coordination with the Department of Justice's Fraud Section and the Small Business Administration's Office of Inspector General. Through this effort, 116 investigations have been initiated, and over \$126 million in potential fraud has been identified.

We're also beginning to see health care fraud. We are seeing fraudulent billing for services not received, charges for unnecessary procedures, and fraud related to telemedicine.

In addition to fraud schemes, we are seeing crimes targeting our children. School closures have increased the presence of children online. In addition, social distancing restrictions and the isolation of children at home may afford criminal actors with an opportunity to sexually exploit vulnerable children. We are proactively countering this threat through active investigations. We're also working to educate the public regarding the warning signs and the danger of online sexual exploitation.

Although these threats are numerous and evolving rapidly, the FBI has and will continue to be vigilant in addressing these crimes and holding the individuals who commit these crimes accountable. We rely heavily on public education and awareness. When the general public is made aware of fraudulent schemes and criminal activity, they are better situated to report them. For that reason, I am incredibly appreciative of the opportunity to speak with you today.

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

[The prepared statement of Mr. Shivers appears as a submission for the record.]

Chairman GRAHAM. Mr. D'Ambrosio.

STATEMENT OF MICHAEL D'AMBROSIO, ASSISTANT DIRECTOR, U.S. SECRET SERVICE, DEPARTMENT OF HOMELAND SECURITY, WASHINGTON, DC

Mr. D'AMBROSIO. Thank you, Chairman Graham, Ranking Member Feinstein, and distinguished Members of this Committee. Before I begin, like my colleagues, I'd like to express my deep sadness and frustration with the tragic events of recent weeks. Having served in Government for nearly 29 years, nothing troubles me more than police misconduct. It severely erodes the essential trust necessary for law enforcement to effectively protect and serve our communities. Law enforcement must be held to the highest standard. Racism and discrimination in any form is totally unacceptable. The Secret Service is committed and, indeed, oath-bound to ensuring that all Americans are afforded their constitutional rights to equal treatment under the law and to freedom of speech and assembly. Those rights are inalienable, and no duty is higher for a law enforcement officer than to protect them.

Returning to the subject of this hearing, thank you all for inviting me to speak about the current wave of COVID-19-related crime and the work of the United States Secret Service to counter it.

As early as February of this year, the Secret Service identified individuals and groups seeking to exploit the pandemic for illicit profit. We quickly took action to build the capacity and strategy necessary to combat what we anticipated would be a surge of criminal activity.

Major disasters have long invited fraud. From the terrorist attacks on 9/11 to Hurricanes Katrina and Maria and, indeed, well before, criminals throughout history have viewed public emergencies as opportunities to defraud the public. However, the fraud associated with the current COVID-19 pandemic presents a scale and scope of risks we have not seen before. Enabled by the internet, criminals all over the world are defrauding anxious citizens, distressed businesses, and Government stimulus programs alike.

Since we released our first alert on March 4, we have observed a significant proliferation of criminal schemes. In particular, we have seen a surge in crimes targeting various economic relief programs such as those provided by the CARES Act. Countering this fraud has become a core focus of our investigative work, and I expect our investigative efforts will continue for years.

The Secret Service, in addition to our protective mission, is responsible for the investigation of criminal violations of U.S. law pertaining to the U.S. financial system. As the Assistant Director of the Office of Investigations, I lead the over 160 field offices of the Secret Service, which includes our network of Electronic and Financial Crimes Task Forces, which conduct specialized investigations of cyber and financial crimes.

The immediate investigative focus of the Secret Service is to disrupt and deter criminal activity that could hinder an effective response to the pandemic by assisting organizations at risk of fraud and by working to recover any funds stolen from Americans. Longer term, we will ensure that those who have criminally exploited this crisis are arrested and successfully prosecuted.

I am pleased to report that the Secret Service has already seen tremendous success emerge from our investigative efforts to date. We have initiated over 100 criminal investigations and prevented approximately \$1 billion in fraud losses. Among other law enforcement actions, the Secret Service has successfully disrupted hundreds of online COVID-19-related scams, halted the illicit sale of stolen COVID-19 test kits online, and is leading a nationwide effort to counter a vast international scheme to defraud U.S. State unemployment systems. We have also released regular threat intelligence and alerts to provide industry, consumers, and our law enforcement partners with best practices to defend themselves from the latest criminal threats.

However, we are not achieving these results by ourselves. We can credit much of our success to the close partnerships we have built with a range of Government and industry partners. In particular, we are working closely with the various agencies of the Department of Treasury, with the Cybersecurity and Infrastructure Security Agency and Homeland Security Investigations, as well as various offices of the Inspector General, particularly from the Department of Labor and Small Business Administration. And, of course, my colleagues to the right within the Department of Justice, their COVID-19 Task Force, and the Federal Bureau of Investigation have all been essential partners.

I am committed to ensuring the Secret Service is doing our part on behalf of the American people to counter criminal activity exploiting this pandemic. I look forward to answering your questions on how we can work together to address this threat.

Thank you.

[The prepared statement of Mr. D'Ambrosio appears as a submission for the record.]

Chairman GRAHAM. Thank you all.

I will start with the Secret Service. Can you give me some examples of how people are taking advantage of the Paycheck Protection Program?

Mr. D'AMBROSIO. We primarily right now are focused on the unemployment insurance.

Chairman GRAHAM. Okay. I am sorry. Tell me about unemployment.

Mr. D'AMBROSIO. So right now it is a mainly stolen identity theft investigation in which criminals are utilizing stolen PII, things that they have acquired on whether it be the dark web, whether

it be network intrusions, and they are using that stolen information to apply for Social Security benefits, and probably across right now about 29 States across the country that we have seen. It's not a very complex fraud. It's the availability of PII out in public—

Chairman GRAHAM. Got you.

Mr. D'AMBROSIO [continuing]. That allows for this to occur.

Chairman GRAHAM. Is there anything this Committee can do to help you in this endeavor? Do you have all the tools you need in current law?

Mr. D'AMBROSIO. We have the tools right now that we need for this particular—

Chairman GRAHAM. Do you have the resources?

Mr. D'AMBROSIO [continuing]. We have the resources with the partnerships that we've created, whether it be the—

Chairman GRAHAM. Okay.

Mr. D'AMBROSIO. The Department of Labor as well as the—

Chairman GRAHAM. The answer is yes, right? Okay.

Mr. D'AMBROSIO [continuing.] The answer is yes.

Chairman GRAHAM. Mr. Shivers, I appreciate what you all are doing at the FBI. When it comes to consumer fraud, what are you seeing most of?

Mr. SHIVERS. Sir, on the consumer fraud—

Chairman GRAHAM. Your mic, please. Thank you.

Mr. SHIVERS [continuing]. All right. So as I mentioned in my opening, on the consumer fraud, initially private citizens were targeted through a number of schemes. Many of those schemes included offers to sell counterfeit COVID-19 cures or vaccines and, as I mentioned in the opening, also investment opportunities. And so what we see is a wide range of citizens being targeted through a number of means—

Chairman GRAHAM. Is that problem getting better or worse, or is it about the same?

Mr. SHIVERS [continuing]. I think COVID-19 obviously has shined a light on an opportunity for criminals to take advantage of a specific type of scheme, and so what we see is a number of ways that they are reaching individuals, through unsolicited phone calls or through unsolicited emails. So there's a wide range. And what we ask the public to do is to make reports to ic3.gov, and that gives us greater visibility on the nature of threats and the number—

Chairman GRAHAM. Is there anything the Committee can do to—do you have the tools you need to deal with the problem?

Mr. SHIVERS [continuing.] We do, sir.

Chairman GRAHAM. Okay. Thank you.

Mr. Carpenetti—is that right?

Mr. CARPENITO. Carpenito, sir.

Chairman GRAHAM. Carpenito. I am sorry. Tell us about the fraudulent sales going on out there. What's going on in terms of overseas activity?

Mr. CARPENITO. So what we have been seeing, sir, with regards to hoarding and price gouging is the trends have indicated to us that initially what we had was fraud relating to a spike in the prices of the materials. In this country we essentially had a supply chain that consisted of six major suppliers of these masks, the N95

masks, three-ply masks just like these, that were a commoditized product that were sold at relatively cheap prices, pennies, to our first responders and our medical professionals. They were easy to obtain, and they were something that I think were taken for granted as part of our system.

What happened was, just like any scenario we've seen in our country's history, where we have a national crisis, there is always going to be that dark underbelly that rises to the top and tries to profit illicitly from the fears of folks that are most impacted by the pandemic. And what happened here was a bunch of interlopers in the market came in, obtained mass quantities of these materials, and held onto them, raised the prices, and price gouged. These masks went from being 50, 60 cents apiece to selling for \$7, \$8, as high as \$25 in some cases.

What we've done is we've gotten the word out about the invocation of the Defense Production Act, the fact that it makes it illegal to do that, to price gouge, and we've opened up a series of investigations. So we've been getting out there to try and find any stockpiles if they exist and get that material back into the supply chain.

Chairman GRAHAM. Do you have the tools you need to continue down this path?

Mr. CARPENITO. We do, sir. The Defense Production Act gives us the ability to bring this conduct to light and to remedy it.

Chairman GRAHAM. Mr. Shivers, very quickly, can you tell us a little bit about the Paycheck Protection Program? What kind of problems have you seen there?

Mr. SHIVERS. Yes, what we've seen are fraudulent filings from individuals who are either exaggerating the number of employees that they may have within their business or perhaps they don't have any employees. And so what they are doing is taking advantage of—

Chairman GRAHAM. How do you find out about these cases?

Mr. SHIVERS [continuing.] It's a wide range. Part of it is outreach that the FBI conducts with the banking sector and with the private sector. And one of the things that we do is we've formed relationships with financial institutions and provided them with training, having an idea of what to look for, some of the fraud indicators. So part of it's a relationship.

The other part of that relationship is with the Small Business Administration's Office of Inspector General, and so through coordination with SBA's OIG, we are also receiving information that helps us open cases.

Chairman GRAHAM. Okay. Mr. Hughes, finally—and I am sorry to go over here—we are looking at a Phase 4, and I'm sure we will do one. If you could get back to the Committee—you don't have to do it now in 30 seconds, but if there is anything you don't have in terms of being able to deal with this, let us know. If you need more resources, let us know. But, generally speaking, how do we stand? Do you have the resources and tools necessary to oversee these programs at this point in time?

Mr. HUGHES. I think the answer is yes, and, Chairman Graham, we really appreciate the Committee's support. There are a number of legislative proposals that have been in discussion, one of which is increasing deterrence by increasing sentencing guidelines for

fraud committed during national emergencies. We look forward to continuing to discuss that——

Chairman GRAHAM. Well, you give us a list of things you think would help.

Chairman GRAHAM. Senator Feinstein.

Senator FEINSTEIN. In my 26 years on this Committee, Mr. Chairman, I've never seen anything quite like this. If I understand it, the Federal Trade Commission has reported that, as of June 7, consumers have lost nearly \$48 million due to coronavirus-related fraud. And this includes scam offers for vaccines, test kits, cures, air filters that were falsely advertised. That there's been unacceptable price gouging on basic items like hand sanitizer, sophisticated schemes targeting State governments.

I understand in Washington State, for example, criminals used stolen personal information to file fraudulent unemployment claims. And it goes on and on.

And then you have the Nigerian fraud ring known as Scattered Canary that's used personal information likely obtained through prior consumer data breaches to fraudulently obtain millions of dollars. And it's bizarre.

Why is this so unique to have all of this? What is there in this program that attracts this kind of fraud effort?

Mr. HUGHES. Thank you, Senator, for your question. I think there are two things going on here. One, you have a pandemic which is rightfully a major concern and basically every American's life—there is a lot unknown still about COVID-19. And you also have an economic disruption which rightfully sparked serious response from the Federal Government in the way of economic relief. And so those two events simultaneously created a situation where you have many consumers out there who are anxious about their own health——

Senator FEINSTEIN. But you're so broad-based in your comments. Nothing is specific. Let me ask you a specific. Apparently, Washington State was able to recover the \$300 million that it had paid for fraudulent claims related to one scheme. What other big fraud cases are out there? And what is being done to stop it?

Mr. HUGHES [continuing.] We are doing several things. First is that we have hundreds of investigations open all over the Department of Justice. We're working with every single law enforcement agency in the executive branch. We are pursuing separate courses, investigations, monitoring trends about the criminal conduct regarding each one of these programs. And some of the cases——

Senator FEINSTEIN. Well, talk to me for a minute about Scattered Canary, this Nigerian fraud ring.

Mr. HUGHES [continuing.] So, Senator, I am unable to discuss the specifics of any particular matter or any particular potential target. What I will say is that, especially with respect to unemployment benefits fraud, there is strong indication that some of the perpetrators are overseas entities or organizations and that they're using money mules and other standard mechanisms to transfer money outside of the country.

Senator FEINSTEIN. Is this a Nigerian fraud ring? Is Scattered Canary a Nigerian fraud ring?

Mr. HUGHES. So, Senator, I am not personally knowledgeable as to that organization. I am happy to take that——

Chairman GRAHAM. Does anybody know about this?

Mr. D'AMBROSIO. Yes, Senator.

Chairman GRAHAM. Well, tell us about it.

Senator FEINSTEIN. Thank you.

Mr. D'AMBROSIO. There has been some reporting on Scattered Canary being Nigerian, but I have no specific information to confirm those particular activities.

Senator FEINSTEIN. Could you tell us what you know?

Mr. D'AMBROSIO. What I do know is that the fraud, again, as you stated, Senator, is essentially stolen PII that is out already in public or whether it's particularly bought off the dark web for these particular crimes, and then they're utilized to file fraudulent unemployment insurance claims. And that money has been seen transiting through money mules, as has already been said.

Senator FEINSTEIN. Well, have these consumer data breaches fraudulently obtained hundreds of millions of dollars in unemployment benefits from State governments? Could you gentlemen answer the question yes or no?

Mr. D'AMBROSIO. I can't answer the exact amount, Senator, that has been obtained. I can tell you that the Secret Service, based on an alert that we published in late May, the information that we received back from working with over 100 financial institutions, that it mitigated the loss of about \$500 million in payments. And so that's anecdotal information that we've received from the financial institutions.

Senator FEINSTEIN. So how did Washington State recover the \$300 million that it had paid in fraudulent claims related to one of these schemes? Can anybody answer that question?

Mr. HUGHES. Senator, I don't think we have that information at our fingertips. We can take it back and discuss with our colleagues.

Senator FEINSTEIN. Because, you know, I've been here for a while, and, Mr. Chairman, I've never seen anything like it. It's a program riddled with fraud.

Chairman GRAHAM. Well, here's what I believe. If you put \$3 trillion out there, people will take advantage of it. And we had to do it. And I'll share your frustration. It's been a lot of generalities here. We would like to know what can we do, what's going on, who's doing it, and how widespread is it.

Senator FEINSTEIN. That's right.

And could any of you gentlemen summarize what is going on and what it's going to take to stop it?

Mr. HUGHES. Senator, that's an incredibly broad question. If you are talking just about CARES Act fraud, there is targeting of the Payroll Protection Program by fraudsters misrepresenting their small business or the characteristics of their small business or misrepresenting that there is a small business at all. There are fraudsters who are using PII that they've accumulated or bought on the internet to apply for unemployment benefit programs that are State-sponsored. And there are a number of schemes relating to economic impact payments, again, relying on PII to apply for these payments or to defraud recipients of those payments, to hand those over to the fraudsters.

Senator FEINSTEIN. Well, let me ask you this. The FTC reported that as of June 7 consumers have lost nearly \$48 million due to coronavirus-related fraud, and that includes scams for vaccines, test kits, miracle cures, air filters that were falsely advertised as capable of removing COVID-19 from the air in people's homes.

So there're all these fraudulent business practices out there, apparently. What is being done to stop them, to arrest and convict?

Mr. HUGHES. I think we're vigorously investigating and using the tools that we have, both criminal and civil. When you bring a prosecution, you have forfeiture powers should there be a guilty plea and or a verdict at trial of guilty. On the civil side, you have a number of different statutes which allow you to to make the fraudster forfeit his ill-gotten gains. In order to disrupt, we have a statute that allows us to seek a TRO, a preliminary injunction, and ultimately an injunction. That is a quicker solution to stopping some of these schemes, many of which involve an online website which is the major marketing mechanism of some of these fraudsters.

Senator FEINSTEIN. The information I have before me I've never had before me in any program in 26 years, and I wonder if it's worth continuing. How do you stop this fraud?

Mr. CARPENITO. So, Senator, maybe I can help respond by what the Department of Justice has done to try and police these programs.

First, I can tell you——

Senator FEINSTEIN. Could you indicate to us how many cases have been brought, convictions sought, and convictions obtained?

Mr. CARPENITO [continuing.] What I can tell you is we've received thousands of referrals through the network of task forces that have been put up. Right away, right when the pandemic came to be, Attorney General Barr I think showed very swift leadership in forming two task forces specific to COVID-19—one relating to general fraud related to COVID-19; the other, my task force, relating to the hoarding and price gouging, which was meant to stand up very quickly to try and get the valuable PPE to the individuals who needed it as quickly as possible.

Those programs each have approximately 100 prosecutors in each of them that are focusing on the COVID-related crime. It takes some time to work a white-collar case, and it has to be done covertly because we don't want to do anything to disrupt the network of criminals before we can get a hold of where the money is, we can trace everything, especially for overseas cases. So we're working them expeditiously.

I can tell you there are hundreds of investigations in my task force alone and thousands nationally related to COVID fraud in general. We've also formed partnerships with our State Attorney Generals to share information. Sharing information in white-collar cases like this is critical to being able to get to the money, because at the end of the day that's what this is about. We want to prevent individuals from sending payments or from having their bank accounts pillaged. We want to prevent Government programs from the same. And where it's already happened, we need to cooperate with law enforcement to work with financial institutions to trace those transactions.

And I know it can be frustrating at times that we can't get into specifics, but one of the reasons we can't is, you know, our network operates through the ability to stay covert and find these resources, this money. Before we pounce and we go into court and go public on it, we have to have everything locked down if we are going to be successful.

Chairman GRAHAM. Senator Feinstein, we will have a Round 2, but I think, Senator Grassley, you are next, sir.

Senator GRASSLEY. Thank you.

I've heard thus far that you've got the resources you need and you've got the tools that you need. I hope that that is right. Time will tell. If that's true, that's very nice.

I want to start out with a compliment to the Justice Department in some things that are related to the pandemic and some things that might not be related. But I want to compliment the people that have filed price-fixing suits against Pilgrim's Pride and Claxton Poultry, because I've always felt there is not enough competition in the agriculture industry. And also last week, the Department of Justice announced that it had issued what they refer to as "civil investigative demands" to the Nation's four largest meatpackers, and those four largest ones have about 80 percent of all the packing industry and slaughter industry in the country as a whole. And there's plenty of reason to believe that there might not be things right there. When a month ago the price of beef to the farmer went down about 60 percent, the price to the consumer went up about 25 percent.

I sent a letter on March 31 to the secretary or to General Barr, and I've done that over a period of 20 years under both Republican and Democrat administrations, hardly getting any results whatsoever. So you can imagine how surprised I am but thankful for this Administration taking those moves to make sure that the marketplace is working in that industry, because farmers are very depressed by some of the things that are happening in that industry.

So let me go to questions. On April the 7, Senator Klobuchar and I sent a letter to the Attorney General Barr expressing our serious concern about price gouging and hoarding of essential medical supplies. We asked for information from the Department's implementation and enforcement of the President's Executive order. We've not received a response from the Justice Department, so I hope we'll get it soon. It's important that Congress have this data as we figure out how to best address the problems we face.

We appreciate when agencies are quick to share information with us on our requests for that information. For example, the Secret Service has been very good about giving us periodic updates on the COVID-19-related fraud efforts. I encourage the Justice Department and the FBI to follow that example.

So to any one of the three from the Justice Department that can respond, can you tell me when Senator Klobuchar and I will get a response to our April 7 letter?

Mr. HUGHES. Senator, thank you for your question. I do not know the answer to that question. All I can assure you is that when we receive letters, they're reviewed, and work starts on replies promptly. Replies have to go through a rigorous process, so sometimes it can take longer than we would all like.

I defer to Mr. Carpenito on any substance that that letter was seeking to elicit. But we have your letter, and I understand it is being worked on, and I can check with OLA after this hearing as to the status.

Senator GRASSLEY. Also, to anybody from the Justice Department and/or the FBI witnesses, I am interested in what difficulties or obstacles have you encountered when investigating and prosecuting these cases.

Mr. CARPENITO. Thank you, Senator. As I said previously, thankfully, because of the invocation of the Defense Production Act, it has given us the tools that we need to investigate and prosecute price gouging. As you know, the act is what made the act of hoarding with the intent to sell materials that were designated as scarce by the Department of Health and Human Services at exponentially higher prices than pre-pandemic prices criminal. Without that act, we would not be able to operate.

The challenges that we have are the same challenges that you have in any sort of a disaster relief-related fraud situation. We faced it in New Jersey after Hurricane Sandy.

As Senator Graham correctly stated, when you put this kind of money out into the ether, because you have to take care of society and, you know, take care of those who are desperately in need of it, the cockroaches are going to come out of the dark and into the light. There is always some underbelly that is going to try and defraud these programs.

We are using our traditional tools and our traditional partners to root out those frauds. It takes a little bit of time, because what you see there is there is a delay in the exposure, right? We have to follow trends, follow the money, to be able to root it out.

With regards to hoarding and price gouging, I think that we showed a very aggressive stance. We brought our first prosecution within a week of the invocation of the Defense Production Act. The President put it into play on March 23. On March 25, HHS designated scarce materials. On April 1, we had arrested the first person for selling exponentially higher priced PPE. The charges we filed there were for making false statements to the FBI, because he was trying to hide his conduct, and assaulting a Federal officer, because the individual coughed in the face of the FBI agents who were looking to interview him and told them he had COVID-19 to back them away from him. But we were able to recover close to a million pieces of PPE and distribute them within 48 hours to front-line medical professionals.

Senator GRASSLEY. Could I ask one more question?

Chairman GRAHAM. Go ahead.

Senator GRASSLEY. I do not know which one of you can answer this, but I believe that China's decision to halt exports allowed criminals to sell fake and faulty goods to our hospitals, putting the health and safety of our workers at serious risk. Is it reasonable to believe that the increase in fake and faulty medical supplies were a direct result of China's decision to stop exports to the medical—of medical supplies? And if not, why not? Whichever one of you can answer that.

Mr. CARPENITO. Sure. I will take that question, Senator. So, Senator, we can't talk about any of our investigations that are non-

public. What I can tell you is if you—I do not know if you noticed, but on Friday we filed a criminal complaint against a Chinese company for the importation of fraudulent N95 respirators. In that case, what we allege is that a Chinese company sent to the United States knowingly false materials. How were they false? They purported to be N95 respirators that were licensed by the FDA and by NIOSH, which is the licensing body for these materials that make them the most attractive to medical professionals.

The N95 respirator has been so important here because what medical professionals say is that you need that 95 percent filtration to protect our doctors, our nurses, our first responders from interacting directly with the virus. These materials were imported into the U.S. with the intent to sell them to medical professionals, and when we seized them, they did not look to us as though they were authentic materials. We worked with the FBI, the FDA, and Customs and Border Patrol. We had the materials tested. They failed that filtration test. And we do intend to continue to investigate any importation of fraudulent materials, and I think you can plan to see additional cases coming in the future.

Chairman GRAHAM. Senator Durbin.

Senator DURBIN. Thanks, Mr. Chairman.

Mr. Carpenito, you talked about putting \$3 trillion on the table and watching the cockroaches come in. In your testimony you've identified six six prosecutions under the PPP Act so far. Four and a half million loans have been issued so far.

So let me ask you, are you just getting started? Or is that it for cockroaches? It strikes me that unless you have a pretty powerful statement pretty early on, some of the adolescent efforts being made to qualify for PPP loans are just going to continue apace.

Mr. HUGHES. Senator, if you do not mind, I will address the PPP. So with that program, there are number of ways that we get referrals of cases to investigate and potentially prosecute. One is just walk-ins. As the FBI will tell you, they have field offices around the country, and complainants will walk in saying that they're aware of some wrongful conduct with respect to the program.

A second source is data that we share among Federal agencies. I can't get into more specifics on that.

Senator DURBIN. I have a limited amount of time. How you collect it and get your leads is important, but not critical to answering my question. Is this pace of six prosecutions after several months and 4.5 million loans indicating you are just getting started, or this is the pace that you think will warn America not to try to cheat the Government?

Mr. HUGHES. I think we're just getting started, and for the foreseeable future we will be bringing these cases. The limitation periods on this conduct are anywhere between 5 and 10 years. And we are engaging extensively to ensure that the public understands the serious consequences of exploiting this program.

Senator DURBIN. I certainly hope whatever you do, you continue this effort, but do it more publicly with more volume, calling attention to it. This exploitation that is spelled out in your testimony of six is almost laughable.

Mr. HUGHES. I can assure you, Senator, there are plenty of investigations currently going on.

Senator DURBIN. These are not thoughtful, conniving individuals. They're just silly efforts to exploit the Government in the belief that it is an easy thing to do. I mean, to invent companies, invent payrolls—I mean that seems to me to be fairly traceable.

So let me go to another aspect. The Chairman just stepped back in. I am glad he is here because I wanted him to hear this. When I got briefed a few years ago by major corporations in the United States, they told me that retail theft was so massive in this country that products that were made exclusively by one company were being sold in volume on the internet by sellers that went unidentified and they had to be stolen. They were only made by one company. They had to be stolen from a warehouse or in the chain of commerce somewhere. They were being sold by the hundreds. It wasn't just a casual sale. And when these companies went after this theft ring, they were stopped cold by Amazon, Facebook, and eBay, who said, "We have no obligation to disclose the names of our sellers. Even if they are fencing stolen goods, no obligation to disclose the names of our sellers."

You made a reference, Mr. Carpenito, to profiteering online with marketplace platforms like Amazon and Facebook. On March 25, a group of 34 State attorneys generals wrote to those three companies and other online marketplaces to urge them to do more to crack down on price gouging on their platforms, including urging the companies to create mechanisms to allow consumers to report suspected price gouging.

The question is simple. What kind of cooperation are you getting from Amazon, Facebook, and eBay when it comes to those who are using the internet to sell products that are misrepresenting their health qualities or their application in COVID-19?

Mr. CARPENITO. Thank you, Senator. I can tell you that from day one in the formation of the task force, we engaged with private corporations, including online retailers, to talk to them about what their policies were with regards to price gouging, how they identified those instances, and sought to create a referral relationship with those retailers.

Senator DURBIN. How are you doing?

Mr. CARPENITO. Without getting into specifics because there's nothing public, I can tell you that we have been cooperating and that we have received referrals from those platforms.

Senator DURBIN. So now they are disclosing sellers when you believe that they have violated the law?

Mr. CARPENITO. Again, I feel constrained by Department policy on talking about nonpublic investigations, but what I can tell you is that we have had contact with them, we have engaged, and we are working cooperatively with them on referrals.

Senator DURBIN. They stonewalled us for years on retail theft, saying—eBay in particular—it's none of your damned business who's selling what, even if it's clearly stolen goods. And if you are telling me we have got a breakthrough here when it comes to this pandemic and national emergency of those who are trying to sell—misrepresent products on the internet, that you now have the cooperation of these sales places, these marketplaces, I think we need to know one way or the other whether you do or don't.

Mr. CARPENITO. What I can tell you, sir, is—I don't know if I would use the term "breakthrough." What I can tell you is that we have had contact with these companies, we have sought their cooperation and asked them to make any referrals of anyone who is hoarding or price gouging the designated materials underneath the HHS order, and we have active relationships with at least some of the companies that you mentioned.

Senator DURBIN. Mr. Chairman, I am going to quit here. I went a little longer than I should've. But let me tell you, Senator Cassidy and I have introduced a bill called the "INFORM Consumers Act," and it gets to the bottom line here, that Amazon, Facebook, eBay have to disclose to law enforcement when there is the obvious sale in their marketplace of goods that are either stolen or being misrepresented to the consumers of America, for example, NIOSH-cleared products and it turns out it's a big old lie. Some of these places in the past would not even tell you who the sellers were. They claimed it is confidential and private.

Chairman GRAHAM. Well, I think it is a good question, so, Mr. Carpenito?

Mr. CARPENITO. Senator, what I can tell you—

Chairman GRAHAM. Would the bill help that he is talking about? Is it a problem?

Mr. CARPENITO [continuing.] In my experience the Department of Justice can use process, we can send subpoenas; we have mechanisms to obtain that information, when justified, where we see indications of fraud or any indications that there has been wrongful conduct.

Senator DURBIN. This is a new development if you do, and I will tell you, Home Depot came to me, no small company, and said, "Stolen goods with our brand, made only by us, sold on eBay in volume, and they won't tell us who is selling it." If that's changed, this is a breakthrough, and I—

Chairman GRAHAM. Yes, I agree. So see if you can followup.

Mr. CARPENITO [continuing.] Will do, sir. Thank you.

Chairman GRAHAM. Senator Tillis.

Senator TILLIS. Thank you, Mr. Chairman. Thank you, gentlemen, for being here and for the work you are doing.

I was actually pleased to hear you all bring up, and a number of the Members, focusing on counterfeit, the threat of counterfeit goods. That's something I have focused a lot on as Chair of the Intellectual Property Subcommittee. This is not something new to the COVID response. I literally saw a biking helmet that was marketed as one of the most protective if you bought it from Specialized, it did the job. I saw somebody just put their foot on this helmet and it crushed before a Senate Committee. There are a lot of counterfeit products coming from China that are clearly a threat to our public health, and now it's only on steroids in response to the COVID pandemic.

One question or a couple of questions I have. You've talked about the PPEs and the N95 masks. Other personal protective equipment is something that we have got to focus on, but I am also worried about counterfeit medications potential when we have breakthroughs on therapeutics, counterfeit versions of those. They may

actually fit the bill, but not being distributed according to licenses. In other cases, they may just be inadequate or ineffective.

I think the same thing, the same risk, could hold true in terms of test kits and some of the other materials that we're putting together for the COVID response.

Can you tell me a little bit about how we're specifically focusing on that and whether—my suspicion is China is the greatest threat, but any other jurisdictions that we should be looking at?

Mr. HUGHES. Let me just address briefly pharmaceuticals and testing, and I'll allow Mr. Carpenito or the rest of the panel to address PPE.

We're working very closely with the FDA. They've taken a more flexible regulatory approach to help spur innovation in the medical device and the pharmaceutical space. The types of crimes in that area that we are focusing on are the obvious scams, the clearly fraudulent products or medications. We are trying to disrupt those quickly, and largely by bringing an injunction while a criminal investigation is still going. Some of the cases that we have brought so far stopped a scam selling ozone gas as a treatment, unregistered pesticides, colloidal silver, and other treatments that were sold and marketed as either cures for or effective prevention measures for COVID-19.

Senator TILLIS. If others of you want to chime in, is this a China problem, or do we have other jurisdictions that we have a similar threat in terms of counterfeit products?

Mr. HUGHES. The cases I was referring to are domestic cases, but I will defer to Mr. Carpenito on PPE.

Mr. CARPENITO. Once again, I can tell you what we see trend-wise, and what we see trend-wise is we have numerous investigations, and we have seen trends that there is the importation of materials that are either counterfeit, misbranded, or just completely fraudulent. Those were the three buckets that—

Senator TILLIS. Primarily from China?

Mr. CARPENITO [continuing.] What I can tell you is that we have one publicly available prosecution that I can talk about where we have filed a criminal case in the Eastern District of New York against a Chinese company that we believe intentionally sent fraudulent materials.

Senator TILLIS. And the Chinese company is a government-owned enterprise?

Mr. CARPENITO. I believe that is the case in China, sir.

Senator TILLIS. I want to move on to something else. I want to keep to my time. I have a Committee markup I have to run to. But, Mr. Shivers—right? I want to make sure I got that right. I butcher names repeatedly here.

Mr. SHIVERS. That is correct.

Senator TILLIS. First off, I want to thank you for the work, and I did get to listen to your testimony in my office. But can you tell me about other things? I was talking about some of the test kits and other things. Can you see any patterns specifically from foreign jurisdictions? We talked about domestic production, and that's important for us to look at, but foreign jurisdictions that we should be focused on and potentially create consequences coming out of legislation from the Senate?

Mr. SHIVERS. So our investigations are not focused on importation. We are primarily looking for hoarding and price gouging of PPE and also counterfeit PPE. So through the course of investigation, we may discover that the PPE that we've seized is either substandard or counterfeit.

Senator TILLIS. Okay.

Mr. SHIVERS. And so we would address it after that. So we work with not just our Federal partners but State and local partners to develop those investigations. And so, again, what we've seen is some of the PPE that we've seized has been counterfeit.

Senator TILLIS. Well, I want to keep close to the time. This is just a request. You don't have to respond to it. But I want to thank Senators Blumenthal, Cornyn, and Sasse who joined on a letter to the FBI and CISA to give us a briefing on hacking. I don't know if you have seen that letter, but I think it would be very helpful for us to figure out, particularly with Chinese-affiliated hackers, some of the threats that we have there. That may be, Mr. Chairman, something we can do as a Committee, but if not, I know there are a number of Senators that would like to get together and get a briefing of the Committee on that and the threats that we should be updated on.

Mr. SHIVERS. We can coordinate that.

Senator TILLIS. Yes, if we can get that done sooner rather than later, I would like for the FBI and CISA to be represented in that meeting.

Thank you.

Chairman GRAHAM. Senator Whitehouse.

Senator WHITEHOUSE. Thank you, Chairman. If somebody could dial down my volume. There we go that's how I like it.

I want to ask about unemployment insurance, but before I do, I have to react to, Mr. Hughes, your statement about your policy for answering letters. I do not know what is going on over at the Department, but I detect a policy of not answering questions for the record from this Committee and not answering letters from this Committee. When we had Mr. Rosenstein down in the hot seat there a few days ago, I pointed out that in 17, I think it was, hearings with Department of Justice witnesses, not one question for the record from a Senator was answered afterwards. Not one. That is not a coincidence. That is a policy.

When we get questions for the record answered, it is because it is a nomination hearing and the nominee doesn't go forward until the QFRs are answered. Outside of that, the policy seems to be, "We, the Department of Justice, don't answer Committee questions for the record."

I have a similar problem with letters, so I don't believe what you have said about there being a responsible policy for getting letters answered. We have letter after letter after letter to DOJ and FBI that have gone completely unanswered. We finally got a letter out of the Antitrust Division recently by putting a hold on a piece of legislation that the Antitrust Division wanted, and the answer we got from the Antitrust Division was a blow-off. It was a nonsense answer. It did not answer the actual questions.

So I would ask you to take back to the Department, what the heck is going on? Because this exceeds the partisanship that I see

out of the Department. This is a persistent failure of response to oversight, and it is not always going to be a Republican Attorney General, it's not always going to be a Republican Chairman. Something is wrong. There is a policy someplace about not answering QFRs and not answering letters, and I am sick to death of it. So please take that back. And I see the Chairman nodding his head over there, so this is a bipartisan concern.

The letter that was raised was from Chairman Grassley. This is a bipartisan concern. This is not the time to get into this. We are going to get into this further. But somewhere there is a policy, and I want it rooted out, because it is a wrong policy.

Now, on unemployment insurance, Mr. Shivers, in your testimony, in the headings of the different elements of your testimony, you don't even mention unemployment insurance. It's not one of the topic areas. Mr. D'Ambrosio mentioned briefly unemployment insurance in his testimony, but described it as just "simple fraud."

I don't know that that is accurate, gentlemen. Just in Rhode Island, we've had 3,000 fraudulent unemployment insurance applications. Our U.S. Attorney is looking into it after the Rhode Island State Police began an investigation because they seemed to be coordinated. The damages could be in the billions, the theft could be in the billions of dollars. IP information links entities to common fraudulent claims and also to fraudulent common claims in the State of Massachusetts, in the State of Connecticut, in the State of Washington.

I think you need to step back and take a look at this as a very significant common scheme, very likely a foreign-led common scheme, and take a much harder look at this unemployment insurance fraud than you appear to be undertaking from your testimony here today. I think we're dealing with what may prove to be the crime of the decade, if not the crime of the century in terms of the amount of money that was stolen through a common scheme, run very likely by foreign crooks. And I would ask you also to take the message back that it would be really helpful if the Department of Justice and the FBI would support the bill that Treasury supports, that former Chairman Grassley and Chairman Graham support, that will peel back the ability of foreign entities to hide behind shell corporations in America, because what happens, as I think you know, is that they steal billions of dollars through these schemes, and then they launder the proceeds through shell corporations. We've seen it over and over and over again. The Department, the FBI, the Secret Service have all testified about the role of American shell corporations in hiding criminal assets. And when you look at the extent of the theft from our States through this unemployment insurance problem into which Federal money was poured in abundance as part of the COVID response, I think it's a better bet than not that at the end of the day those proceeds of theft end up behind shell corporations where it's harder for you to root them out and run them down.

So I'd be eager to have any response to the point about unemployment insurance and what you're planning to do to ramp up your response to this.

Mr. SHIVERS. Senator, there was no ill intent in not mentioning unemployment insurance.

[Voice heard off microphone.]

Mr. SHIVERS. I'm sorry. It is on. I will pull it closer.

All right. There was no ill intent in not mentioning the unemployment insurance. Just with the limited amount of time, I wanted to give an overview of some of—

Chairman GRAHAM. But here's the question that's got my interest now. Three thousand, that is a lot.

Senator WHITEHOUSE [continuing.] And that is just Rhode Island. Massachusetts, Connecticut, Washington—there are a dozen States that have this problem—

Chairman GRAHAM. But from the Secret Service point of view—

Senator WHITEHOUSE [continuing.] And probably more.

Chairman GRAHAM. Senator Whitehouse's question, is there organized effort in the country or outside the country to exploit this program versus just, you know, a handful of people misidentifying themselves? I think that is the question. What do you see from the Secret Service point of view?

Mr. D'AMBROSIO. So, Senator, first, to your first comment where you said it is a simple fraud, that really referred to the tactics and the techniques as opposed to the scope of this particular investigation. I can assure you that the Secret Service is looking at unemployment fraud as a massive amount of fraud. We do see it as an organized group. We do see connections when it comes to transnational criminal activity overseas.

Chairman GRAHAM. Well, you should have said that.

Senator WHITEHOUSE. There you go. That feels better. Thank you. Now let us make sure that these agencies respond according to that and not to the not mentioning it or calling it just "simple fraud," because it was potentially billions of dollars in fraud.

Chairman GRAHAM. Senator Hawley.

Senator HAWLEY. Thank you, Mr. Chairman. And I would also be interested in further responses to Senator Whitehouse's questions, and I am going to come back to that actually in just a second.

Let me start, though, by asking about the recent controversy involving 37 Planned Parenthood offices applying for and receiving funds under the Paycheck Protection Program despite their ineligibility. Just a quick review of the facts here. The CARES Act states that nonprofits are eligible for the program only if they and their affiliate organizations have no more than 500 employees. Now, Planned Parenthood has 16,000 employees nationwide, which is 37 times the threshold, and there is no doubt that each of the 37 Planned Parenthood offices who applied for the funds knew that they were affiliated because their own documents claim that they are affiliated. In fact, Planned Parenthood's most recent financial statement describes it as one national branch with 55 Planned Parenthood affiliates, 110 ancillary entities that are, and I am quoting now, "controlled by those Planned Parenthood affiliates."

Despite knowing all this, 37 separate Planned Parenthood entities applied for and received and, therefore, diverted \$80 million from actual small business during this global pandemic.

So let me just ask you, Mr. Hughes—I am not going to ask you to comment or reveal any details of any ongoing investigation, but let me just ask you generally, if an organization that knows it is

ineligible for a program nonetheless applies, falsely certifies its eligibility, and receives tens of millions of dollars in taxpayer money meant for somebody else, do we have a criminal conduct issue?

Mr. HUGHES. Thank you, Senator, for your question. And, again, you are right, I am unable to talk about specific investigations or the existence of specific investigations. However, the way the Department is approaching these cases is the application for these loans is pretty simple. In fact, the part you fill out is literally just two pages. And there are a number of representations on that about the number of employees you have and your monthly average payroll and the nature of your business, and then there are a couple certifications such as criminal charges and convictions over the last 5 years. I believe that is the time period.

There is some other information on there, but those inputs were specifically designed to be objective measures that could be quickly looked at and scrutinized for the purposes of determining whether an applicant intentionally misrepresented something material about their business that would allow us to proceed with charging and prosecuting swiftly.

So we go where the facts and the law command us to go in each of our investigations, and so this is just an area that, like unemployment benefits programs, we are focusing the Department's law enforcement and prosecutorial resources.

Senator HAWLEY. What you are telling us is that the application is designed to be simple, it's designed to be very factual, right? I mean, it's not supposed to be a matter of interpretation. Do you comply or not comply? Here are the standards. Tell us what the facts are. Do you meet the threshold or not? Have I got that right? I mean, that is the basic design of the application.

Mr. HUGHES. Generally, and it's not an application which receives a lot—needs to receive a lot of due diligence on the part of the lender from the beginning. Again, so really all the misrepresentation, the burden of that is on the applicant.

Senator HAWLEY. What about executives of the organization or other decisionmakers who may have known about or signed off on any fraudulent application? When I say the organization, again, I am not asking you to talk about any particular investigation to confirm or deny its existence. But, in general, if you have an organization where you have top executives who's signed off on this, would there be potential liability for them?

Mr. HUGHES. I think the traditional the traditional legal standards that apply to corporate liability and individual liability for corporate actions apply with equal force in this with respect to prosecutions of this program.

Senator HAWLEY. Very good. Well, thank you for that, and I look forward to seeing the progress of your inquiries over time.

Let me come back to the unemployment question that Senator Whitehouse was asking about. Mr. Hughes, I will direct this to you or Mr. D'Ambrosio. Do you have any sense of how much money has been lost through fraud in the unemployment insurance piece of CARES? And has DOJ had any success in recovering any of those funds to date?

Mr. D'AMBROSIO. Senator, I do not have a specific amount of what essentially has been lost. I can tell you I spoke previously

anecdotally from some of the financial institutions that we are working it with, over about 100 of them. We have been told that an alert that we put out in mid-May prevented over about a \$500 million fraud alone. So that just kind of gives you a sense of the particular scope.

We have been successful in recovering some money. We have—

Senator HAWLEY. You have been, did you say?

Mr. D'AMBROSIO [continuing.] We have been. We have been successful. We returned approximately through an investigation about \$30 million to the State of Michigan. So there are cases where this has been—we've seen some success, and we are continuing to work very diligently on these cases, one, to identify, two, to recover the funds, and then eventually prosecute these individuals for this activity.

Senator HAWLEY. Does anybody else have anything to add to that?

Mr. HUGHES. Senator, the only thing I would add is that this is a big and growing focus for the Department. We're coordinating in Senator Whitehouse's district, the U.S. Attorney's Office there, the U.S. Attorney's Offices in other jurisdictions including Washington, we are coordinating closely with both the Secret Service, the FBI, and other law enforcement. We're also coordinating with the financial industry. As the Assistant Director noted, some of the easiest, some of the quickest—the quickest tool is to get the financial institutions where these payments—that are the rails through which these payments travel to identify this activity and to work with us and State authorities to stop these payments, especially when they are traveling overseas.

Senator HAWLEY. Very good. My time has expired. I have got some additional questions on this front which I will submit to the record.

Senator HAWLEY. Thank you all for your service and being here. Thank you, Mr. Chairman.

Chairman GRAHAM. Thank you. Senator Klobuchar.

Senator KLOBUCHAR. Thank you very much, Mr. Chairman. Thank you for holding this important hearing.

I think what we do know from this pandemic is that this has brought out the best in so many people that put themselves on the front lines, but it also has brought out the worst in terms of the kinds of scams that we are talking about today.

Senator Grassley has already mentioned the letter that he and I led back in April, April 7, and we are still, Mr. Carpenito, waiting for an answer to that. And if you could—that's a long time—convey that, I'll just ask some of the questions, because we are concerned about what is happening and what investigations have actually been opened. How many investigations has the task force opened?

Mr. CARPENITO. With regards to hoarding and price gouging, we have opened several hundred investigations that are ongoing.

Senator KLOBUCHAR. And has the task force brought charges against violators—in how many cases?

Mr. CARPENITO. With regards to hoarding and price gouging, the task force has already filed eight criminal cases.

Senator KLOBUCHAR. Okay. All right. And there are 100 lawyers assigned? Is that right?

Mr. CARPENITO. The way the task force is structured is I lead the task force with the assistance of Mr. Hughes. We have three regional coordinators—one for the West out of the L.A. U.S. Attorney's Office, one in the Central out of the Chicago U.S. Attorney's Office, and one for the East out of my office. Each U.S. Attorney's Office has one representative at least. As obviously—as some district are busier than others, there are additional lawyers working on it. And each of the Department components also has a representative.

Senator KLOBUCHAR. Okay. Are they full-time then, the 100 lawyers?

Mr. CARPENITO. I would not say they are full-time. Some of them are. For example, in the early stages—

Senator KLOBUCHAR [continuing.] That is Okay. I have a lot of other questions. If we got this back in writing, we could figure it out. Again, we're just trying to push for some actual results here.

Another way to do this, in addition to what you are doing, State Attorney Generals, as you know, are doing a lot. Attorney General Ellison and I have done some work together on this since the pandemic started. And are you coordinating with them on the price gouging?

Mr. CARPENITO. We have encouraged all of the members of the task force in each of the 93 U.S. Attorney's Office and components to coordinate. I can tell you personally in New Jersey we have a very good working relationship with State Attorney General Gurbir Grewal. We have formed a joint task force with the State Attorney General. I know some other districts have done that as well. And we have had virtual daily contact about referrals, and we've worked on cases and decided which cases fit more with the State's purview or the Federal Government's.

Senator KLOBUCHAR. Okay. Your testimony indicated that the Department focuses on sellers charging "substantially higher prices than traditional market participants." I have a bill that I introduced, and cosponsoring that bill are Senators Blumenthal, Hirono, and Cortez Masto, and it would prohibit price gouging during national emergencies and targets price increases of more than 20 percent above the pre-emergency services. And States with these kind of price-gouging laws have saved targets of 10 to 25 percent. Is there a set amount or is there a minimum amount you are looking at or a target price by the task force? And would it be helpful to have this Federal law?

Mr. CARPENITO. I think it would be helpful to have that Federal law, as well as Mr. Hughes—

Senator KLOBUCHAR. That made my day. Thank you.

Mr. CARPENITO [continuing.] I am sorry?

Senator KLOBUCHAR. That made my day.

Mr. CARPENITO. I think as Mr. Hughes said, too, a sentencing enhancement for those who try to take advantage of situations like this, national disasters, I think would also be a very useful tool.

With regards to thresholds, I think that the target range you are talking about is the target range that we are talking about. The State Attorney Generals, the practices that I have looked at, the State price-gouging laws are usually in the 10-to 20-percent range.

We are certainly looking for markups of that amount or greater in our investigations.

Senator KLOBUCHAR. Okay. Last, Mr. Hughes, in your written testimony, you mentioned the Antitrust Division's joint statement with the FTC on monitoring employer collusion during the pandemic. I am very focused—I am the Ranking Member on the Antitrust Subcommittee with Senator Lee, and I am really concerned about what is going on, like the proposed Uber-Grubhub merger that there has been some discussion about, I shall say, and the fact that we're seeing more and more consolidation during the pandemic.

And on May 1, I sent a letter to the Antitrust Division and the FTC with a number of other Senators emphasizing the need for vigorous antitrust enforcement. The letter included a number of questions, and we received a response from the FTC, but we have not received anything from the Antitrust Division.

Given the importance of this issue right now, when can we expect a response?

Mr. HUGHES. Thank you for the question, Senator. I do not know the status of that particular letter. I understand and agree that the subject of it is important, and I can go back to my colleagues at the Department and—but I do assure you that the Department of Justice takes these letters seriously, and we understand that accommodation is important to the legislative process.

Senator KLOBUCHAR. It is. Just making sure that we make this a major, major piece of our consumer work right now, because it's easy just to turn an eye with these major companies saying, "Hey, let us merge. Times are tough," when, in fact, what is happening is that they are squeezing out smaller and smaller companies, and we are going to have less competition, which is the whole reason we have the antitrust laws to begin with.

The last thing, I will ask this for the record—I know my time has expired; I will ask it later—about this bill that Senator Moran and I just did on protecting seniors from scams. And we also know that a lot of seniors are targeted, and I will ask that later. So thank you.

Chairman GRAHAM. Thank you, Senator Klobuchar. Senator Blackburn.

Senator BLACKBURN. Yes, thank you, Mr. Chairman. And I want to thank our witnesses for being there today.

One of the first cases having to do with price gouging was two brothers outside Chattanooga and they were buying up hand sanitizer and then running the price up online from \$8 to I think \$70 per container. So if you would, talk to me a little bit about your participation with local and State officials and how you work with them. And I think, Mr. Shivers, this probably is best coming to you, and if you all will talk just a little bit about how you work with your State and local law enforcement partners.

Mr. SHIVERS. So one of the FBI's strengths is working with our Federal, State, and local partners, and obviously working in the COVID-19 environment it's been very challenging. But that has not deterred our ability to coordinate with our State and local partners.

There are a number of ways, and I think one of the previous questions is how does the FBI receive information relative to some of the fraud schemes. Obviously, there's a wide range, but through coordination with our State and local partners, we are receiving a lot of information relative to COVID-19 fraud. So because we operated in a task force environment in many of our offices, whether that's our Safe Streets Task Force or Violent Crime Task Force, a lot of our task forces have pivoted to address the threat of the COVID-19 fraud schemes that we are seeing.

And so, again, for us, it's just a continual practice of working very closely with our State and local partners and addressing whatever crimes are being committed within their jurisdictions.

Senator BLACKBURN. All right. That sounds great. And then when you are working with Big Tech and trying to get the information for online fraud with some of these companies, and primarily dealing with China and the fraudulent and inferior merchandise and PPE that was coming out of there, how are you working with some of our allies in this virtual space in order to get this information to shut these entities down? And does Big Tech respond quickly to your requests to shut down some of these entities and then to block them off their server systems?

Mr. SHIVERS. So as previously mentioned, our focus is not the importation of the PPE. We are primarily dealing with PPE on the front end as it pertains to hoarding and price gouging. And through the course of our investigations, we are coming across PPE that may be substandard or counterfeit.

As it pertains to working with our international partners, there are a number of fraud schemes that I think we have talked about today. Some of those fraud schemes are internet-based, and so, as appropriate, we work with our international partners to develop information leads that may have a nexus to the United States or leads that we may disseminate to our international partners. So the international partnership is very important in dealing with COVID-19 because, again, a lot of these fraud schemes are emanating from all across the world.

We have a relationship with various entities in the private sector, and I spoke a few minutes earlier about our relationship with the banking industry. We also work with the tech industry, but, obviously, you know, that requires legal service in order to receive information that may be relevant to our investigation.

Senator BLACKBURN. Thank you. I yield back. Thank you, Mr. Chairman.

Chairman GRAHAM. Thank you. Senator Blumenthal.

Senator BLUMENTHAL. Thanks, Mr. Chairman.

I would like to ask our two Justice Department representatives, have you—are you familiar with Project Airbridge?

Mr. CARPENITO. Yes, sir, I am familiar with the fact that Project Airbridge exists.

Senator BLUMENTHAL. A number of us, Senator Warren and I, began an investigation some time ago asking questions of the six major distributors involved in Project Airbridge. And our inquiry has shown that there was cronyism and political favoritism that led to tragically misallocated supplies and Government seizures of equipment that were going to providers that very much needed it.

Cronyism and incompetence that was exemplified in this program had real-life consequences, and clearly this Project Airbridge, which was a kind of pet project of Jared Kushner, was, in effect, a bridge to nowhere for the health care providers who needed that equipment. At the very least, there was incompetence, confusion, and even possible corruption.

Is there any ongoing inquiry within the Department of Justice relating to Project Airbridge?

Mr. CARPENITO. Unfortunately, Senator, I am not at liberty to discuss any ongoing nonpublic investigations of the Department.

Senator BLUMENTHAL. Will you commit to reviewing this inquiry and making it part of your investigation if there is one underway?

Mr. CARPENITO. Unfortunately, Senator, doing that would be acknowledging the existence of an investigation, and I am just not at liberty to discuss investigations of the Department.

Senator BLUMENTHAL. Well, you'll at least read the results of our investigation, correct?

Mr. CARPENITO. Once again, sir, I would be remiss to comment about an investigation. What I can tell you is we are committed to rooting out fraud with relation to any of the CARES Act programs and anything related to COVID-19 hoarding and price gouging.

Senator BLUMENTHAL. Well, Senator Schumer, Senator Warren, and I will send you the results of this investigation, and hopefully you will followup on it.

Mr. CARPENITO. Thank you.

Let me ask you about the fake cures which are part of that, I think, \$48 billion total number that Senator Feinstein mentioned, which is an astonishing and appalling number. If Americans have lost close to \$50 billion, we need really aggressive and proactive law enforcement in this area. I know you've said that you have enough resources and authority, but I think that Americans are going to be looking for results at some point. So I would suggest that maybe you would want to review whether, in fact, you do have enough authority and resources, because there can't be too much when you're investigating this kind of fraud that directly impacts people.

In a recent report, the Center for Science in the Public Interest found that at least 49 dietary supplements on Amazon with antiviral claims were making false and misleading statements. Do you have any such fake cures under investigation?

Mr. CARPENITO. I would yield to Mr. Hughes.

Mr. HUGHES. So, Senator, we have several investigations that relate to misbranded or mismarketed pharmaceuticals——

Senator BLUMENTHAL. Have you brought any actions?

Mr. HUGHES [continuing.] We have. We have brought a number of injunctions to stop the marketing of such conduct. We have filed criminal complaints against the individuals who have been marketing——

Senator BLUMENTHAL. Could you provide the details to my office, please?

Let me move on because my time is limited. In terms of unemployment insurance, you were answering some questions posed by Senator Whitehouse. What exactly is the modus operandi of these

potential scams? And are you finding actual criminal violations in any of these scams impacting Connecticut?

Mr. D'AMBROSIO. Senator, as we've seen, what it primarily is, the scam itself, is acquiring PII, stolen PII, whether it be purchased on the black market or through network intrusions and being utilized using that information and applying to the different States for the unemployment insurance. Yes, we are finding violations, and we are pursuing those cases.

Senator BLUMENTHAL. How close are you to bringing action?

Mr. D'AMBROSIO. I do not have specific information as to how close we are to prosecution.

Senator BLUMENTHAL. Do you have a dollar amount in terms of what the impact is?

Mr. D'AMBROSIO. I have stated previously, Senator, is that we published an alert in mid-May, and working with the financial institutions, because the financial institutions are the natural choke point for these payments to go, they were able to prevent, according to them, over \$500 million in payments. We've also been able to recover and return to the State of Michigan about \$30 million of fraudulent payments that were made.

Senator BLUMENTHAL. Do you have suspects, specific individuals?

Mr. D'AMBROSIO. I do not personally have that information. I know we have active investigations.

Senator BLUMENTHAL. Well, when I say "you," I do not mean you personally. I mean your agency.

Mr. D'AMBROSIO. I would have to go back and get specific information.

Senator BLUMENTHAL. Could you provide more details to my office later today? I am out of time right now, and you need more information from your agency, so I would appreciate additional information later today.

Mr. D'AMBROSIO. We will provide what we can. These are ongoing investigations that would be limited, but yes, Senator.

Senator BLUMENTHAL. Thank you.

Thanks, Mr. Chairman.

Chairman GRAHAM. Thank you. Hirono.

Senator HIRONO. Thank you, Mr. Chair.

I was very interested in the line of questioning by my colleague Senator Durbin. Mr. Carpenito, you indicated that you are now getting cooperation from Amazon, Facebook, and eBay about the selling of stolen items. So have there been any prosecutions based on the information that you have gotten from the cooperation from these three entities?

Mr. CARPENITO. I do not have any specifics about any investigations in front of me. What I can tell you is that we have done outreach with those outlets, and I am unaware of any situation where we have sought information and have not obtained it pursuant to legal process.

Senator HIRONO. Well, apparently, according to the way the situation was described by Senator Durbin, that this goes on in quite a blatant way. And if you can get information from these entities that are platforms for the sale of these stolen goods, that would be a good thing. And so I would suggest that you look at the INFORM Consumers Act that Senator Durbin referred to, which is bipar-

tisan, supported by Senators Durbin, Cassidy, myself, and Senator Perdue. That may give you more tools to go after these kinds of crimes.

I think all the panelists, you have referred to hundreds of prosecutions, thousands of investigations as a result of all the scams and fraud perpetrated because of the opportunities presented by COVID-19. And I think, Mr. Hughes, you indicated that there are serious consequences for people who commit these kinds of criminal acts. So I would like to know. Has anybody gone to prison? Are you seeking prison time? What kind of fines are you imposing on the people that you prosecute for these crimes?

Mr. HUGHES. Thank you for the question, Senator. I think for the frauds, the standard penalty, the incarceration length, applies that normally applies under non-COVID-19-related circumstances. With respect to some of the PPP fraud, for example, again, a lot of factors need to be—need to necessarily affect how long a particular defendant's prison time would be. And whether they plead and take responsibility or are convicted at trial also affects it, as does the sentencing judge.

Back-of-the-envelope calculation, just for PPP would be anywhere—the average would be between 50 months and 100 months. And that is, you know, typical for the types of frauds we are seeing where the proceeds are in the millions of dollars. Again, there are a number of different tools we bring to bear to address these problems and disrupt these schemes.

Senator HIRONO. Mr. Hughes, I am running out of time, but do you think that we should create higher consequences or steeper consequences for people who take advantage during a national crisis and a pandemic? You referred to the usual fraud kinds of consequences, but maybe we should be looking at higher levels of consequences. What do you think?

Mr. HUGHES. Senator, I think there is an honest and important debate as to the level of consequences for offenses during a national emergency. There have been discussions about proposed legislation regarding Sentencing Guidelines. Those discussions, in the Department's view, should continue, and we would be willing to have discussions about other proposed legislation in that vein.

Senator HIRONO. You have been asked the UI scam involving a Nigerian entity. So, apparently, a number of these kinds of frauds are perpetrated by foreign entities, and I'm wondering. How easy is it for you to effectively prosecute foreign entities? And do you need more tools, any of you, to go after these foreign criminals?

Mr. HUGHES. I think from a prosecution standpoint I'll defer to our law enforcement investigative colleagues with respect to investigations, but from a prosecution perspective, we have a number of tools, jurisdictional hooks which permit Federal prosecutors to charge and effectively prosecute foreign criminal organizations. And those tools in many respects are as robust as they can given certain jurisdictional and constitutional limitations. But I will defer to my Federal investigations colleagues for the investigations piece.

Mr. SHIVERS. So as I mentioned previously, working with international partners is very important for us, and so whether these fraud schemes emanate from a foreign country that touch our American citizens, we work very closely through our legal attaché

offices around the world to develop information, work in conjunction with our foreign law enforcement partners to bring charges.

Obviously, one of the potential obstacles that we would face would be matters of extradition, so those are some of the things that we have to work through. But, again, these fraud schemes, because many are internet-based, have a foreign nexus. And so with the FBI, one of the things that we have done—and this was through our elder fraud initiative that we worked with the Department of Justice over the last 2 years—is we have assigned assistant legal attachés in various countries where we know some of these fraud schemes emanate. And that gives us greater visibility, greater connection with our international partners, and enhances our ability to bring those individuals to justice.

Senator HIRONO. May I just have ask more question, a followup, Mr. Chairman?

Chairman GRAHAM. Thank you very much, Senator Hirono. We will make sure you get to do that.

Senator HIRONO. Okay.

Chairman GRAHAM. Okay. Thank you. Let us see. Senator Booker.

Senator BOOKER. I think Senator Hirono said she wanted to ask one last question.

Chairman GRAHAM. Oh, I am sorry. I misheard. Senator Hirono.

Senator HIRONO. I am sorry.

Chairman GRAHAM. No, no. I apologize. Ask anything you want to ask. I apologize.

Senator HIRONO. I think it is really hard to prosecute these kinds of crimes when the perpetrators are foreigners, and our panel explained the difficulties. And so a lot of this type of information is stolen information that is already out there, the personally identifiable information. So is there something more that States and individuals can do to protect themselves from the sort of fraud that comes about from stolen identities?

Chairman GRAHAM. Good question.

Mr. SHIVERS. I would say just kind of a basic 101, there are a number of services where individuals can have access to their credit report, and I would imagine that reviewing your credit report for anything that, you know, you may not have knowledge of would be important. But I think also taking preventive measures, and that is, obviously, the internet, there's a way that the criminals approach individuals, sending these unsolicited emails. So I would just say just using, for lack of a better word, basic common sense in how the public deals with some of these opportunities that these criminal organizations take advantage of.

So it's obviously a very difficult thing, but, again, unsolicited emails, unsolicited phone calls, where individuals are actually providing some of the PII. But, again, as we have talked about, some of that PII may be stolen. So I would just say just using some basic preventive measures.

Senator HIRONO. Thank you, Mr. Chair.

Chairman GRAHAM. Thank you. Senator Booker.

Senator BOOKER. Mr. Chairman, I think the rule of the Committee should be it is better to ask for forgiveness than permission. I know Senator Hirono knows that rule.

But I am grateful to be here, and if I can, I want to direct my questions to Mr. Carpenito, not just because he is from New Jersey, not just because he is bald, not just because Anthony Ambrose, who is both of those things, has said generous things about him. But, obviously, these issues are really impacting our State, and I would love to get some of his insights.

And so, first of all, we have seen numerous instances of retailers taking advantage of the global pandemic and gouging, charging outrageous fees for medical supplies, personal protective equipment, things that are really—we deem essential and are critical to the life, safety, and well-being of so many of our first responders and others. This behavior is immoral, frankly, and reprehensible.

My team and I have introduced the Prevent Emergency and Disaster Profiteering Act on May 7. There is no Federal law against this kind of reprehensible price gouging on essential items that are deemed critical to the health, safety, and lives of so many Americans.

And so, Mr. Carpenito, I am curious what you think of the power of having a Federal law against this kind of gouging, if you could comment on that, and then talk about the prevalence of this in New Jersey and how have you, without that law, been successful in trying to combat these issues.

Mr. CARPENITO. Thank you, Senator. So I agree with your characterization. I think New Jersey is one of the States that had one of the largest impacts from this type of conduct because, as everyone knows, New York and New Jersey were two of the most impacted States in the country by COVID-19.

We also have some of the most vulnerable victims for this as we have a very large elderly population, and we have a very large health care system.

So, thankfully, because of the invocation of the Defense Production Act and the swift movement by Attorney General Barr to set up the task force to enforce the act, we have had the tools to address hoarding and price gouging of scarce materials, those designated by the Department of Health and Human Services, and that's how we have been able to operate. I have not felt constrained as a task force leader in our tools there.

But as you mentioned, there is a—there is really a history and a record here of folks trying to take advantage of national disasters like this. We saw it in Katrina. You and I saw it in New Jersey after Hurricane Sandy. And we've seen it throughout the country on a scale that we have never seen before with COVID-19 because it is the largest health crisis we have had since the Spanish flu.

We have been unable to address certain types of price gouging because there's not a Federal statute. For example, things like toilet paper, things like, you know, meat, things like food, things like other materials that personal consumers need are better suited under the current statutory scheme to be prosecuted by State Attorney General's offices.

What we have done is I have worked with Mr. Hughes, Mr. Shivers, and we have made sure that we make those referrals to State AGs where we think they have the better tools to prosecute those individuals, because the most important thing, as always, is just to

make sure that these people are brought to justice, not who does it.

Senator BOOKER. I am grateful for that response, and I do really believe there is an urgency to give on the Federal level more tools to deal with that.

You know, on March 20 of this year, you announced the creation of the Federal-State COVID-19 Fraud Task Force with Attorney General Gurbir Grewal and our Comptroller Walsh. The task force bridges the prosecutorial efforts of the State and Federal agencies and the kind of coordination and cooperation I think is really needed in circumstances like this. And so I just want to hear a little bit more about the Federal-State task force, what kind of fraud schemes you guys have uncovered since its creation and what challenges have you all encountered in combating that fraud that you see out there.

Mr. CARPENITO. Sure, and you—we are very blessed in New Jersey. I can't speak about every State, but I think that we have heard—as task force leaders, myself and Mr. Hughes have heard similar success stories throughout the country in forming partnerships here. We have had a very good relationship during my entire tenure with Attorney General Grewal's office and, in particular, working with his first assistant, Jen Davenport, and his executive assistant, Andrew Brock. They've been in almost daily contact with our task force folks in New Jersey, sharing referrals.

Unfortunately, I cannot get into specifics of referrals because the cases that I have on my mind are not ones that are publicly available information at this time. But what I can tell you is we haven't really seen a lot of hurdles because we have put egos aside and we have focused most importantly on making sure these cases are brought.

You know, with regards to the tools, like I said, the Defense Production Act has been a powerful tool for us, and it's given us the authority to investigate price gouging and do so pretty vociferously and quickly.

Senator BOOKER. I'm over time. I'm going to submit more of a lot of our pressing questions for the record, for QFRs.

Senator BOOKER. I do have one last question for you to put you on the spot, and I apologize for doing this in advance. But my question simply is, Anthony Ambrose, is he a great police director or is he the greatest police director?

Mr. CARPENITO. He is a national treasure. I've been saying this since I came into office, and we have seen it during these riots. The fact that Newark stayed together as a community and were peaceful in their reaction to the death of George Floyd is a credit to Director Ambrose for his handling of law enforcement and a credit to Mayor Ras Baraka for his community engagement. And I saw first-hand for the past 8 to 10 days as other cities struggled with these protests, Newark thrived, and they are doing so because of the work that was done through the Newark consent decree with the leadership of Anthony Ambrose, and as I said, the community engagement and support that Mayor Baraka has shown for his police department and, quite frankly, the support that both have shown to me since I have been U.S. Attorney in focusing on violent crime

throughout Newark through not just prosecutions but by education and community engagement.

Senator BOOKER. Well, I appreciate your deference to consent decrees. I wish that the current Attorney General would actually engage and use them. They were a constructive force in the city of Newark. I appreciate you saying things about the extraordinary leadership of Ras Baraka. That is 100 percent true. And Anthony Ambrose is a treasure. He takes better care of the city of Newark than he does himself, so I hope that you will—again, I say this on the record—encourage him to get out there, exercise, and, you know, be more healthy so we have him for a few more decades.

Mr. CARPENITO. He is down 70 pounds. We are looking good.

Senator BOOKER. He is, he is, actually, in all truth.

Thank you, Mr. Chairman.

Chairman GRAHAM. Thank you. I need to call him. I am trying to lose some weight myself.

So here is the deal. We all appreciate you coming to the Committee. I asked you do you have the tools necessary, the resources. It seems like there are some tools that maybe we could utilize that you do not have. So if you can kind of get your collective wisdom, I think Senator Durbin had a bill, Senator Klobuchar, I think Senator Booker introduced legislation. So get back with us about what we can do to help you. I mean what can the Committee do to change laws or supplement laws, sentencing enhancing, whatever? Just let us know.

Thank you all for being on the front lines, and we will hold the hearing record open for the requisite amount of time for additional questions. Thank you.

[Whereupon, at 11:58 a.m., the hearing was adjourned.]

*Submitted for the Record by
Ranking Member Feinstein
June 09, 2020*

**Statement for the Record
Senate Judiciary Committee
Hearing on COVID-19 Fraud: Law Enforcement's Response to Those Exploiting the
Pandemic
June 9, 2020**

Thank you, Mr. Chairman. I understand that, today, the Committee is focusing on an issue related to the coronavirus pandemic.

However, while the issue of fraud is important, I hope that we do not lose sight of the other issues that remain of immediate importance when it comes to addressing the coronavirus pandemic.

Just last week Henry Lucero—the Executive Associate Director of Enforcement and Removal Operations at U.S. Immigration and Customs Enforcement—testified to this Committee that testing is still not widely available in immigration detention facilities.

That remains true even though the rate of infection is over 51 percent for detainees who have been tested for COVID-19.

Likewise, in one Bureau of Prisons facility in Lompoc, California, nearly the entire inmate population has tested positive for the virus. In the face of that staggering data, Bureau of Prisons Director Michael Carvajal still would not commit to universal testing of inmates.

Mr. Chairman, at a time when so many people continue to contract the virus and die from it, that's an area where I believe this Committee needs to focus more of its time and attention. We need to see that agencies within our jurisdiction respond to this crisis, and not ignore our requests for information and action.

*Submitted for the Record by
Ranking Member Feinstein
June 09, 2020*

Today, we will learn what the federal government is doing to protect consumers and state and local governments against price-gouging and fraud schemes related to the coronavirus pandemic.

The Federal Trade Commission has reported that, as of June 7, 2020, consumers have lost nearly \$48 million due to coronavirus-related fraud. This includes scam offers for vaccines, test kits, miracle cures, and air filters that were falsely advertised as capable of removing COVID-19 from the air in people's homes. These are fraudulent business practices and they must be stopped.

There have also been clear instances of unacceptable price-gouging on basic items such as hand sanitizer and disinfecting wipes. For example, at one point, bottles of Purell hand sanitizer were being sold in New York for \$25 apiece.

There have also been sophisticated schemes targeting state governments. In Washington State, for example, criminals used stolen personal information to file fraudulent unemployment claims.

Fortunately, Washington State was able to recover the \$300 million that it had paid in fraudulent claims related to one such scheme. And I am interested in hearing from our witnesses today what they know about the fraud against Washington State and whether other states are having similar problems.

States also have faced difficulty obtaining personal protective equipment – masks, gloves, gowns, and hand sanitizer – for their health care workers and first responders. They have struggled, as well, to find more sophisticated medical supplies such as ventilators.

This situation was not helped by the lack of federal coordination and leadership – with the President announcing during a March 16 conference call with governors: “Respirators, ventilators, all of the equipment—try getting it yourselves.”

*Submitted for the Record by
Ranking Member Feinstein
June 09, 2020*

The resulting race among states to find much-needed supplies “has also drawn fraudsters looking to hoard items and resell the equipment at a steep price.”

In one case, a White House team recommended that New York State use a vendor who had no background selling medical equipment. New York signed a contract to purchase ventilators for \$86 million, paying more than twice what each ventilator would have cost before the pandemic.

The ventilators never arrived. New York was able to recover the bulk of the \$69 million dollars it had already transferred to the vendor under the contract, but \$10 million dollars still has not been recovered.

Simply put, a lack of federal leadership and planning has sown confusion and helped contribute to conditions that are ripe for fraud and abuse.

This country is still facing a crisis responding to the pandemic, and there are those who fear it may get worse in the coming months.

As we focus today on the question of fraud, I hope our witnesses can also address what more this Congress and this Committee can do to ensure that vital aid gets to those in need.

Thank you, Mr. Chairman.



Department of Justice

**STATEMENT OF THE
U.S. DEPARTMENT OF JUSTICE**

**WILLIAM HUGHES
ASSOCIATE DEPUTY ATTORNEY GENERAL
OFFICE OF THE DEPUTY ATTORNEY GENERAL**

AND

**CRAIG CARPENITO
U.S. ATTORNEY FOR THE DISTRICT OF NEW JERSEY**

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

**WILLIAM HUGHES
ASSOCIATE DEPUTY ATTORNEY GENERAL**

**CRAIG CARPENITO
UNITED STATES ATTORNEY FOR THE DISTRICT OF NEW JERSEY**

**U.S. DEPARTMENT OF JUSTICE
JOINT STATEMENT
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

Good morning Chairman Graham, Ranking Member Feinstein, and members of the Committee.

Thank you for inviting us to appear before you today to discuss the Department of Justice’s (the Department) efforts to detect and prosecute those who seek to exploit the COVID-19 pandemic and the economic dislocation it has caused for personal financial gain. We have been tasked by the Attorney General and Deputy Attorney General to lead the Department’s Hoarding and Price Gouging Task Force (Mr. Carpenito) and to coordinate more generally the Department’s response to criminal conduct relating to the COVID-19 pandemic (Mr. Hughes). We want to thank the Committee for its attention to this issue and to the good work of the Department to protect the safety and security of our nation during this unprecedented crisis.

The Department is committed to detecting, investigating, and prosecuting wrongdoing related to the crisis. The Department has received reports of, is investigating, and has already commenced prosecutions of individuals and businesses using the crisis to seek windfall profits at the expense of public safety and the health and welfare of the American people, from the sale of fake cures for COVID-19 online, hoarding and price gouging with respect to critical medical supplies, and defrauding the CARES Act economic programs.

To be clear, the Department will not tolerate any bad actors who seek to treat the pandemic as an opportunity to defraud their fellow citizens or the government. In addition to the work of the task force charged with addressing hoarding and price gouging, the Department is also engaged in an effort to detect and counter fraud as well as price-fixing and other forms of market manipulation that constitute violations of antitrust law. The Department’s attorneys work side-by-side with the Federal Bureau of Investigation (FBI) and other investigative partners from a variety of federal, state, and local agencies.

Prosecuting Hoarding and Price Gouging under the Defense Production Act

Hoarding and price gouging, in particular, have the added effect of inhibiting frontline healthcare professionals, essential workers, and the public from acquiring the supplies they need to protect themselves from contracting the virus. The limited supplies of these crucial products, and associated reports of hoarding and price gouging, prompted the signing of an Executive Order by the President invoking authority under the Defense Production Act (DPA) and the subsequent formation of the anti-hoarding, anti-price gouging task force led by Mr. Carpenito.

As you are undoubtedly aware, the DPA confers broad authority on the President to combat hoarding and price gouging.¹ Under Section 101(a)(1) of the DPA, the President may require parties to accept and perform contracts deemed necessary to the national defense. Under Section 101(a)(2), the President may allocate materials, services, and facilities in such manner as deemed necessary or appropriate for the national defense. Under Section 102, the President may prohibit hoarding scarce materials in excess of the reasonable demands of business, personal or home consumption, or for the purpose of resale at prices in excess of the prevailing market price. The DPA also gives the President a range of administrative and civil enforcement tools to enforce compliance with the Act.

Section 101(b) of the DPA provides the mechanism for how the President triggers his authority under section 101(a) of the DPA. Subsection (b) provides that the President must find that (1) the material at issue “is a scarce or critical material essential to the national defense,” and (2) “the requirements of the national defense for such material cannot otherwise be met without creating a significant dislocation of the normal distribution of such material in the civilian market to such a degree as to create appreciable hardship.”²

In Executive Order 13909, issued on March 18, 2020, the President made the findings prescribed by subsection (b), thereby triggering his Section 101(a) authority. Specifically, the President determined that the “health and medical resources needed to respond to the spread of COVID-19, including personal protective equipment and ventilators, meet the criteria specified in section 101(b)” of the DPA. Executive Order 13909 further confers on the Secretary of Health and Human Services (HHS) the President’s authority under Section 101(a) “to require performance of contracts or orders (other than contracts of employment) to promote the national defense over performance of any other contracts or orders” and “to allocate materials, services, and facilities as deemed necessary or appropriate to promote the national defense,” with respect to “all health and medical resources needed to respond to the spread of COVID-19 within the United States.” The order also delegates to the Secretary of HHS the various implementation and enforcement authorities under Section 101 of the DPA with respect to health and medical resources needed to respond to the spread of COVID-19. This Executive Order thus authorizes the federal government to require the sale of needed resources either to the government or to any other party it deems appropriate.

In Executive Order 13910, issued on March 23, 2020 the President declared it the policy of the United States to prevent the hoarding of health and medical resources essential to

¹ See 50 U.S.C. § 4501 *et seq.*

² 50 U.S.C. § 4511(b).

combatting the spread of COVID-19. That order delegated to the Secretary of HHS the President's authority under Section 102 to designate materials as scarce for the purpose of prohibiting the hoarding or price gouging with respect to such materials. In Executive Order 13911, issued on March 27, 2020, the President delegated the same authority to the Secretary of Homeland Security.

On March 25, 2020, the Secretary of HHS published a notice in the *Federal Register* in which he designated fifteen categories of health and medical resources as scarce. That notice acknowledged that it is the policy of the U.S. that health and medical resources needed to respond to the spread of COVID-19, such as personal protective equipment (PPE) and sanitizing and disinfecting products, are appropriately distributed, and stated that that policy furthered the goal of protecting the Nation's healthcare system from undue strain. The materials designated as scarce include respirator face masks like the N95 mask, ventilators, sterilization services, medical gowns, Tyvek® suits, face shields, surgical masks, and surgical gloves. This notice triggered the criminal prohibitions of Section 102 of the DPA. The designations are to be periodically reviewed by HHS and are set to expire after 120 days unless a superseding notice is published.

To carry out prosecutions for violations of the criminal prohibitions under the DPA, the Attorney General announced to the Department the formation of a task force to combat hoarding and price gouging. The Attorney General appointed Mr. Carpenito to lead the task force. He further instructed each U.S. Attorney's office and the relevant Department litigating components, particularly the Antitrust Division, to designate experienced attorneys to serve as members of and provide support to the task force.

The task force's primary mission is to identify, investigate, and prosecute instances of illegal hoarding of the critical medical supplies designated by HHS. Section 103 of the DPA criminalizes the conduct prohibited by Section 102. Every violation of Section 103 requires proof of two general elements: first, that the defendant actually did something expressly prohibited, or failed to do something expressly required, by either the DPA itself, or by any rule, regulation, or order issued under the DPA; and second, that the defendant did so willfully, meaning with knowledge that his conduct was generally unlawful. Section 103 imposes criminal penalties for willful violations of the DPA and of regulations and orders issued under the Act that include up to a \$10,000 fine and imprisonment of no longer than one year for each offense.

The violations of the DPA that this task force primarily investigates are violations of Section 102 of the DPA. A willful violation of Section 102 requires proof of at least three elements in addition to the elements set forth above: first, that the defendant accumulated materials; second, accumulation of at least some of the materials took place after the materials were designated in the *Federal Register* as scarce and important to the national defense; and third, that the defendant accumulated the materials either (a) in excess of his or her reasonable needs of business, personal, or home consumption; or (b) for the purpose of resale at prices in excess of prevailing market prices.

Any charging decisions the Department makes under the DPA will take into account the larger context of the current public health crisis. The decisions the Department makes to open

investigations or to bring charges are intended to help the public health response, not hinder it. This means that, as a practical matter, the task force is focused on profiteering. We recognize that many established manufacturers and distributors of PPE have not meaningfully increased their prices since the start of the pandemic. We understand this because some of their prices are publicly available. 3M, for example, has published a price list for the many different models of N95 masks it manufactures.³ According to 3M, most of their N95 respirators should cost an end-user less than \$2.

There are resellers out there, however, who are charging substantially higher prices than these traditional market participants. When the task force sees substantially higher prices, it inquires whether the legitimate costs of the reseller are high. If, in order to turn any profit or simply break even, the reseller must set a high resale price, even a price much higher than other transactions in the market, the fact that the reseller is not profiteering is important for us to consider. It is likewise important if the reseller's costs are not particularly higher than the costs a traditional distributor incurs, but the reseller nevertheless demands a resale price substantially higher than the traditional price for the same goods. The purpose or effect of such a price is to allow that reseller to capture a profit margin that is substantially higher than what resellers generally earned prior to crisis, or are even generally earning now.

The Department's efforts have already yielded substantial results. On April 2, 2020, the Department announced the distribution of hoarded personal protective equipment (PPE), including hundreds of thousands of N95 respirator masks, to those on the frontline of the COVID-19 response in New York and New Jersey. The FBI discovered the supplies on March 30, 2020, during an investigation coordinated by the task force. The task force alerted HHS, which used its authority under the DPA to order that the supplies be sold to the U.S. In addition to the N95 respirator masks, the Department was seized a cache of hundreds of thousands of medical-grade-gloves, surgical masks, gowns, and other medical supplies. We understand that HHS was able to immediately collect that PPE and redistribute it to state and local authorities for further distribution to front line healthcare providers.

Just two weeks ago, the Department announced hoarding and price gouging charges against a man in New Jersey who allegedly attempted to defraud New York City into paying him approximately \$45 million for PPE masks at excessive prices that he did not possess and was not authorized to sell, and also brought similar charges against a licensed pharmacist in New York who allegedly sold N95 respirators to customers for up to 50% more than he paid to acquire them. These case both involved other criminal charges, including wire fraud and health care fraud.

In addition to hoarding and price gouging, the task force also is focused on identifying counterfeit and misbranded PPE imported into the U.S. from abroad. The task force has been coordinating with the FDA and the Consumer Protection Branch of the Department's Civil Division when such situations present themselves.

³ Available at <https://multimedia.3m.com/mws/media/1803670O/fraudulent-activity-price-gouging-and-counterfeit-products.pdf>.

Combating Fraud and Abuse

In addition to the work of the task force, U.S. Attorneys' Offices and many Department components, including the Criminal Division and the Civil Division, are combatting fraud relating to COVID-19.

On March 16, 2020, the Attorney General issued a memorandum directing every U.S. Attorney's Office "to prioritize the detection, investigation, and prosecution of all criminal conduct related to the current pandemic." Within days, each of the 94 U.S. Attorneys' Offices identified and appointed one prosecutor to serve as the office's Coronavirus Coordinator to ensure that those cases were given the highest priority.

Assistant United States Attorneys across the nation are committed to the mission of combatting fraud relating to COVID-19, and they work with lawyers throughout the Department to bring to bear all the criminal and civil tools necessary to investigate, prevent, and prosecute sales of fraudulent PPE and COVID-19 treatments, cures, and tests; the use of stolen identities to obtain health care, Economic Impact Payment, unemployment, or other government benefits; and loan fraud, bank fraud, money laundering, and aggravated identity theft relating to CARES Act funds. The U.S. Attorneys' Offices work with every major law enforcement agency to investigate and prosecute the fraud arising out of the pandemic; they often pair with the Criminal Division and the Civil Division to ensure that they are using every tool available to prevent and prosecute the fraud. They also have leveraged and have further strengthened relationships with State and local law enforcement counterparts in their districts, leading to more effective enforcement and more successful prosecutions.

The Criminal Division Fraud Section, working closely with the FBI and the Small Business Administration (SBA), has been focusing meaningful investigative efforts on fraud relating to the CARES Act's Paycheck Protection Program (PPP). The PPP authorizes up to \$659 billion in forgivable loans of up to \$10 million each to small businesses, nonprofits, veterans organizations, and tribal business concerns to cover employee paychecks and certain non-payroll costs during the crisis. As of June 3, 2020, the Department's prosecutors have already brought six cases charging fraud in connection with PPP loan applications:

U.S. v. Yates (Eastern District of Texas)

- Yates was charged with wire fraud, bank fraud and false statements for two fraudulent applications seeking over 5 million dollars in PPP loans from two different lenders. Falsely claiming to have hundreds of employees when in fact he had none, Yates allegedly used a publicly available random-name generator on the Internet to create lists of purported employees, and submitted them along with forged tax documents.

U.S. v. Fayne (Northern District of Georgia)

- Fayne was charged with bank fraud stemming from a PPP loan he obtained in the name of Flame Trucking with claims that he had 107 employees and an average monthly payroll of \$1,490,200. Fayne allegedly obtained a PPP loan over \$2 million and then

used over \$1.5 million of the proceeds to purchase \$85,000 in jewelry, including a Rolex Presidential watch, a diamond bracelet, and a 5.73 carat diamond ring, and to pay \$40,000 for child support.

U.S. v. Benjamin Hayford (Northern District of Oklahoma)

- Hayford was charged with wire fraud, bank fraud, false statements to a financial institution, and false statements to the SBA, in connection with allegedly fraudulently applications submitted to multiple banks seeking about \$4.4 million in PPP loans. As alleged, while Hayford certified that his company was in operation as of February 15, 2020, the company received its IRS Employer Identification Number on March 30, 2020 and registered with State of Texas on April 1, 2020. In addition, while the loan applications allegedly represented an average monthly payroll of approximately \$1.7 million for 247 employees, the supporting documentation allegedly lacked any employee information aside from internal employee numbers, and also changed representations as to whether they were contract employees or W-2 employees.

U.S. v. Rai (Eastern District of Texas)

- Rai was charged with wire fraud, bank fraud, false statements to a financial institution, and false statements to the SBA for fraudulently seeking more than \$10 million in PPP loans from two banks. In his applications, Rai fraudulently claimed to have hundreds of employees, when there were no records of Rai or his purported business paying employee wages or records of revenues from the relevant time period.

U.S. v. Staveley & Butziger (District of Rhode Island)

- Staveley and Butziger were charged with conspiring to seek over \$530,000 in PPP loans, falsely claiming to have dozens of employees earning wages at four business entities. Staveley allegedly claimed he had dozens of employees at three restaurants, two of which were not open at the time, and one of which Staveley had no role in or ownership. Butziger allegedly sought a PPP loan as the owner of an unincorporated entity named Dock Wireless with false claims that he had seven employees on Dock Wireless' payroll.

U.S. v. Sadleir (Central District of California)

- Sadleir was charged with fraudulently filing bank loan applications for a film production company that sought more than \$1.7 million dollars in forgivable PPP loans. Sadleir allegedly obtained the forgivable loans by falsely representing that the funds would be used to support payroll expenses, when, in fact, Sadleir intended to use and did use a significant portion of the funds for personal and non-business-related expenses.

In addition, the Criminal Division has also engaged in outreach to agencies tasked with implementing and overseeing CARES Act funds to design programs to detect and deter fraudulent conduct in the first instance. They are also coordinating with investigative agencies to identify key indicia of COVID-19/CARES Act related fraud schemes and to make sure

information about emerging patterns and practices of fraudsters are shared across the relevant law enforcement community. Moreover, the Criminal Division is working closely with General Services Administration OIG, Department of Defense OIG, and Department of Homeland Security OIG, to ensure that taxpayers are not defrauded as the government seeks to procure large quantities of necessary equipment and services on an urgent timeframe.

The Criminal Division has also assumed a leadership role in identifying and combating health care fraud trends emerging during the crisis, including by chairing a working group with FBI, HHS Office of Inspector General, and other law enforcement partners. Additionally, the Fraud Section has assigned 25 prosecutors to prosecute COVID-19 cases across the country, directed its Data Analytics Group to prioritize analysis of COVID-19-related billing schemes, and retained forensic accounting and other experts that will assist in investigations and prosecutions. These efforts have already led to prosecutions, including charges against a defendant in the Middle District of Florida, who, among other offenses, conspired to be paid kickbacks on a per-test basis for COVID-19 tests, provided that those tests were bundled with Respiratory Pathogen Panel tests, which reimburse at a far higher rate than COVID-19 tests.

Since February, criminal and nation-state cyber actors have been increasingly targeting U.S. pharmaceutical, medical, and biological research facilities to acquire or manipulate sensitive information, to include COVID-19 vaccine and treatment research amid the evolving global pandemic. We have also seen various forms of fraudulent activity seeking to capitalize on the attention and concern that the pandemic demands and creates, including scam websites that are designed to look like legitimate charities, government agencies, healthcare organizations, or COVID-related information sources, but which fraudulently solicit donations, trick users into revealing passwords or other personal information, or distribute malicious code. The Criminal Division's Computer Crime and Intellectual Property Section and the National Security Division are working with investigative agencies and U.S. Attorneys' Offices to combat COVID-related cybercrime and intellectual property violations, particularly those that affect the healthcare sector.

The Department has identified a variety of ongoing or potential fraudulent schemes. These include:

- Medicare beneficiaries receiving fraudulent calls, texts, and emails seeking to have the recipients disclose their personally identifiable information (PII) (e.g., social security numbers, dates of birth, and bank account routing and account numbers) under the auspices of confirming eligibility for COVID-19 tests, and then using that PII to bill health insurance programs for medically unnecessary, or not provided, services or equipment.
- Medical professionals offering free COVID-19 testing to obtain Medicare beneficiary information that can then be used to submit medical claims for unrelated and medically unnecessary – and far more expensive – tests or services, as well as the payment of kickbacks for referrals for such testing.

- Social media scams fraudulently seeking donations or claiming to provide COVID-19 relief funds if the recipient enters his or her bank account information.
- Scammers representing that they are acting on behalf of government agencies, including the SBA, U.S. Treasury, and other entities, in order to obtain money from individuals.
- Robocalls making fraudulent offers to sell respiratory masks with no intent of delivery.
- Sales of counterfeit or fake testing kits, cures, “immunity” pills, and protective equipment.
- Seeking donations fraudulently for illegitimate or non-existent charitable organizations.

Federal prosecutors around the nation have undertaken investigations and have brought, or anticipate bringing, charges in connection with all of these fraud schemes.

In addition, Department attorneys are focused on CARES Act fraud schemes connected to the Economic Impact Payments (EIP) program and state-sponsored unemployment benefit payments. The Department has received complaints of aggravated identity theft by perpetrators, including those overseas, who file false claims for EIP and unemployment benefits. The money is often routed through bank accounts and debit cards of third parties here in the U.S. From there, the proceeds are transferred to the perpetrators, many of whom are overseas.

The Department’s investigations into this conduct involve multiple law enforcement agency partners. To date, federal law enforcement has flagged payments and recovered millions of dollars before the money has left the country, and we and federal investigative agencies are working toward pursuing all the perpetrators, including those overseas. In order to prosecute perpetrators of these schemes, we can charge wire fraud, aggravated identity theft, and money laundering, among other crimes.

Consumer Protection

The Consumer Protection Branch of the Civil Division has taken action in federal court to combat fraud related to the COVID-19 pandemic by seeking to enjoin activity under Section 1345 of Title 18 of the United States Code to prevent harm to potential victims of fraudulent scams. For instance, on March 21, 2020, the Department filed suit in the Western District of Texas seeking to enjoin the operations of a website fraudulently claiming to sell COVID-19 vaccine kits purported to be from the World Health Organization. As there unfortunately is not yet a COVID-19 vaccine, the court promptly granted the Department’s request and issued a temporary restraining order requiring that the registrar of the fraudulent website immediately take action to block the public from accessing it.

Since March, the FBI’s Internet Crime Complaint Center (IC3) has received and reviewed thousands of complaints related to COVID-19 scams, referring complaints relating to websites or advertisements for fake COVID-19 vaccines and cures, fraudulent charities, and

malware to the Consumer Protection Branch for review and, if warranted, action. As a result of the ongoing cooperative efforts between federal, state, and local law enforcement, and a number of private-sector companies, including multiple Internet domain providers and registrars, the FBI Cyber Division's Cyber Initiative and Resource Fusion Unit has sent notifications on 1,000 domain names related to COVID-19 fraud, and over 800 of these domain name registrations have been suspended or otherwise mitigated. The Consumer Protection Branch, in coordination with the Food and Drug Administration (FDA), has also filed several enforcement actions seeking preliminary relief in order to protect consumers from illegal and potential harmful products being offered to treat COVID-19. These enforcement actions seek to swiftly shut down individuals and businesses selling unapproved products with misleading efficacy claims, products that are not only potentially dangerous but also may prevent those suffering from COVID-19 from receiving the healthcare they need. Federal district courts have agreed with the Department about these predatory schemes and have enjoined the unlawful sale of potentially dangerous products in several cases, including:

U.S. v. Genesis II Church of Health and Healing (Southern District of Florida)

- On April 8, 2020, the FDA and the Federal Trade Commission (FTC) issued a Warning Letter to Genesis and its principals notifying them that, by selling a product called Miracle Mineral Solution and claiming that it will cure, mitigate, treat, or prevent COVID-19, Alzheimer's, autism, brain cancer, HIV/AIDS, and multiple sclerosis, they are violating federal law by, among other things, distributing unapproved new drugs and misbranded drugs in interstate commerce. Despite this warning, Genesis continued to sell this product and expressly stated that they would not take corrective action. As a result, on April 17, 2020, the Department filed suit to enjoin Genesis from selling Miracle Mineral Solution, and the U.S. District Court for the Southern District of Florida promptly entered a temporary injunction halting its sale.

U.S. v. Purity Health and Wellness Center (Northern District of Texas)

- The Department filed suit to enjoin the Purity Health and Wellness Center (Purity) from fraudulently touting its "ozone therapy" treatment as a COVID-19 treatment. Purity and its principals agreed to be bound by a permanent injunction barring them from representing that their "ozone therapy" could be used to treat or cure COVID-19.

United States v. Gordon Pedersen, My Doctor Suggests LLC, and GP Silver LLC (District of Utah)

- The Department filed suit seeking to enjoin Pedersen, and his companies, from continuing to make false and misleading claims that Alkaline Structured Silver products, as sold by Pedersen, as a protection against and a treatment for COVID-19. The court promptly entered an injunction halting the sale of the fraudulent COVID-19 treatment.

United States v. Xephyr LLC, d/b/a N-Ergetics (Eastern District of Oklahoma)

- The Department filed suit seeking to enjoin N-Ergetics from selling an unapproved colloidal silver product purporting to cure, mitigate, or treat COVID-19, as well as other diseases including pneumonia, AIDS, and cancer. The district court entered a temporary restraining order halting the unlawful sales, which prompted the defendants to immediately take down their sales site. In addition, the defendants offered refunds to customers in response to the enforcement action.

United States v. Parris (District of Columbia)

- The Consumer Protection Branch, working with the U.S. Attorney's Office, charged a Georgia man in federal court with fraud for attempting to sell millions of nonexistent respirator masks to the Department of Veterans Affairs in exchange for large upfront payments.

Antitrust Enforcement

The Department is also aware of the potential for firms to take advantage of the pandemic to engage in anticompetitive conduct such as price fixing and bid rigging. The Department issued a press release announcing its intention to hold accountable anyone who violates the antitrust laws of the U.S. in connection with the manufacturing, distribution, or sale of public health products such as face masks, respirators, and diagnostics. The Department is also watchful for collusive practices in the sale of such products to federal, state, and local agencies. In particular, the Department's Procurement Collusion Strike Force (PCSF) is an interagency partnership leading a coordinated national response to combat antitrust crimes and related fraudulent schemes in government procurement, grant, and program funding at all levels of government. Deterrence and early detection of misconduct will be the PCSF's top priorities to help these agencies safeguard their procurement, grant, and program funding processes from collusion and corruption.

Additionally, the Department recognizes the risk to workers from anticompetitive conduct by employers. The Antitrust Division therefore issued a joint statement with the FTC noting that the nation's antitrust enforcers are closely monitoring employer collusion to disadvantage workers during the pandemic. Specifically, the agencies announced that they will protect competition for workers on the frontlines of the COVID-19 response by enforcing the antitrust laws against those who seek to exploit the pandemic to suppress or eliminate competition for compensation, benefits, hours worked, and other terms of employment.

Finally, the Department issued a joint statement with the FTC announcing an expedited procedure for reviewing proposed conduct by industry aimed at addressing responses to COVID-19 and determining whether they intend to take antitrust action in response. To date, the Department has issued three letters reviewing proposed conduct: one addressing collaborative efforts to increase the manufacturing and distribution of PPE; one aimed at increasing access to pharmaceuticals to treat the coronavirus; and a third aimed at addressing challenges faced by hog farmers.

Child Exploitation

The COVID-19 pandemic has raised other problems beyond fraud and other economic harms. The Department is gravely concerned that COVID-19 is leading to a higher incidence of online child sexual exploitation, because both offenders and children are spending more time at home and online, and because the use of videoconference platforms has increased.

The best signal we have of the growing threat is chatter we are seeing on the Dark Net, where offenders are able to speak freely. The offenders clearly see COVID-19 as creating opportunities for child exploitation. As one individual wrote on March 21, 2020, “is nobody seeing the bright side of this pandemic?? Schools are closed so kids are at home bored ... that means way more livestreams and its very clear moderators aren’t working right now since I’ve seen 3 hour streams go unbanned over the last few days where girls do whatever the f--- they want. What a time to be alive.”

The FBI recently issued a warning about “Zoom disruptions,” where individuals enter meetings taking place on videoconference platforms and broadcast child sexual abuse material. According to the FBI, in the last three months they have received more than 300 reports of Zoom disruptions throughout the U.S. and in other countries.

The Department is working with a variety of partners to try to mitigate the risk to children. For example, the FBI, in conjunction with U.S. and international law enforcement partners, has aggressively pursued leads relating to egregious child exploitation crimes, including the arrest last month of a defendant accused of enticing nearly a dozen boys online to send him sexually explicit imagery of themselves.

We have also strongly supported efforts to prevent these crimes from occurring in the first place. The Department, along with our Five Eyes partners and the tech industry developed PSAs targeted at caregivers and children to make them aware of the increased risk of child sexual exploitation. In addition, the Department has a dedicated web page with information and resources related to COVID-19 and online child sexual exploitation, including how to report such crimes. The FBI is encouraging individuals to report Zoom disruptions, and has provided guidance on how to prevent such attacks.

National Center for Disaster Fraud

The Department wants to catch perpetrators of COVID-19-related crimes as quickly as possible, so we have set up a hotline and encouraged people to call if they believe they, or someone they know, are victims of a COVID-19 scam. The hotline is set up within the Department’s National Center for Disaster Fraud (NCDF). For approximately 15 years, the NCDF has been dedicated to improving the detection, prevention, investigation, and prosecution of criminal conduct related to natural and man-made disasters and other emergencies, such as COVID-19. As a national coordinating agency within the Department of Justice, the NCDF has the resources, training, and expertise to quickly and effectively ensure that all complaints are appropriately disseminated to the relevant federal, state, or local agency for further investigation.

In the weeks since we announced the COVID-19 hotline, the Center has received thousands of contacts, most of which were addressed and referred by the hotline's automated phone system. We will be updating the National Center for Disaster Fraud's website to reflect the number of COVID-19 contacts we have received.

Conclusion

Chairman Graham, Ranking Member Feinstein, and members of the Committee, we would like to close by thanking you for this opportunity to share the good work of Department of Justice personnel all over the country to uncover and prosecute crimes associated with the COVID-19 pandemic. We look forward to answering your questions.



Michael D'Ambrosio

**Assistant Director
Office of Investigations
United States Secret Service**

**Prepared Testimony on
"COVID-19 Fraud: Law Enforcement's Response to Those
Exploiting the Pandemic"**

**Before the
United States Senate
Committee on the Judiciary
June 9, 2020**

Intro

Thank you Chairman Graham, Ranking Member Feinstein, and the Members of this distinguished Committee for holding this important hearing, and for inviting me to speak about the work of the U.S. Secret Service to counter cyber and financial crimes exploiting the coronavirus pandemic.

As early as February of this year, the U.S. Secret Service identified individuals and groups seeking to exploit the pandemic to further fraudulent schemes for their illicit profit. We published our first alert on this subject, on March 4, 2020, which focused on phishing schemes. As the pandemic continued and intensified, we have observed a proliferation and diversification of criminal schemes, particularly an increase in targeting various economic relief programs, such as those provided by the CARES Act. Countering this fraud has become a core focus of our investigative work, and I expect our investigative efforts to recover stolen assets and hold criminals accountable will continue for years.

The Secret Service, in addition to our protective mission, is responsible for the investigation of criminal violations of U.S. law pertaining to the U.S. financial system, including traditional financial crimes (such as wire fraud and money laundering), modern computer crimes (such as crimes associated with digital currencies), as well as counterfeiting of currency and other financial instruments.

As the Assistant Director of the Office of Investigations, I lead the over 160 field offices of the Secret Service, which include our network of electronic and financial crimes task forces, which conduct specialized investigations of computer and financial crimes. As a result of the pandemic, the risks to our financial system have evolved and multiplied, and we have taken swift action to adapt our work to continue safeguarding the integrity of financial systems from threats to our national and economic security.

In my testimony today, I'd like to take the opportunity to describe how these risks have evolved, what the Secret Service is doing to combat them, and how we are working with partners across the Nation, and around the globe, to safeguard the integrity of financial systems, and, ultimately, to hold criminals accountable.

The Risk of Cyber-Enabled Fraud

Major disasters have long invited fraud. From the terrorist attacks on 9/11 to Hurricanes Katrina and Maria – and indeed well before – criminals throughout history have exploited emergencies for illicit gain. The more catastrophic the event, the more active the fraudsters.

However, the fraud associated with the current COVID-19 pandemic presents a scale and scope of risks we have not seen before. While a hurricane may impact multiple states and thousands of people, this global pandemic impacts everyone. Enabled by the Internet, criminals all over the world are exploiting the fear and uncertainty of the moment for their own illicit gain. They are defrauding anxious citizens, distressed businesses, and government stimulus programs alike. And they will continue to do so throughout the course of this pandemic and the following recovery.

Over the course of the past few months, the Secret Service has observed a clear evolution of the types of frauds being perpetrated. Our first alert, on March 4, 2020, warned of increasing use of COVID-19 themes in “phishing” campaigns. Phishing is the practice of sending emails, purporting to be from reputable companies or organizations, in order to entice individuals to reveal personal information, such as passwords and credit card numbers, or to unknowingly download malicious software. Phishing is a longstanding criminal tactic online. However, as people and organizations have adapted to teleworking, people have become increasingly susceptible to fraudulent emails exploiting their concerns about this pandemic.

But phishing was just the beginning. Over the subsequent weeks, the crimes exploiting the pandemic began to diversify and substantially increase.

As communities sought out legitimate medical equipment to treat and prevent the spread of COVID-19, criminals began to peddle fraudulent medical equipment. Fraudsters engaged in “non-delivery” scams, in which payment is sent for goods and/or services, but no goods or services are ever delivered.

As anxious citizens sought out COVID-19 testing, criminals stood up sham testing sites, both to collect “fees” for fraudulent testing and to collect personal information that could later be used in identity theft and other frauds. They began peddling fake cures, substandard masks, and fraudulent tests.

As workers across the country increasingly turned to telework to increase social distancing, criminals began deploying ransomware, software designed to extort money by locking a computer system until a ransom is paid.

And they engaged in business email compromise (BEC) scams, sophisticated frauds designed to deceive businesses into sending large sums of money into the bank accounts of criminals. With workers out of the office, many of the normal oversight mechanisms that have might otherwise have prevented an organization from becoming a victim, such as in-person approval for wire transfers, made organizations especially susceptible to BECs.

Finally, as the Federal Government began to dispense stimulus funds, primarily through CARES Act programs, criminals launched a new wave of schemes aimed at defrauding U.S. and state government agencies, financial institutions, businesses, and even individuals, out of taxpayer dollars intended to support our fellow citizens, businesses, and communities in need.

The fraud related to the CARES Act is perhaps the most troubling development thus far. Congress has appropriated nearly \$3 trillion to support the American economy, the largest-ever economic stimulus package in U.S. history. Even if we assume a very low rate of fraud, of just 1%, we should still expect more than \$30 billion will end up in the hands of criminals. And that is likely an underestimation of the risk, and just one portion of the full range of risks at play. This is why countering criminal schemes seeking to exploit the COVID-19 pandemic has become a primary investigative focus for the U.S. Secret Service, and will remain so over the coming years.

Strategy

The Office of Investigations is currently focusing on four broad categories of COVID-19-related crime, and has numerous ongoing investigations related to each of these categories. These four categories are:

1. COVID-19-related scams, including the sale of fraudulent medical equipment and non-delivery scams;
2. Risks of cyber crime resulting from increased telework nationally, such as BECs;
3. Ransomware and other cyber-criminal activity that could disrupt the pandemic response; and,
4. Defrauding of government and financial institutions associated with response and recovery efforts.

It is this fourth category that I think is of particular interest to this Committee. It is an area the Secret Service is devoting extraordinary investigative effort to addressing. It is despicable that some seek to engage in fraud against U.S. government programs that aim to blunt COVID-19-induced economic harms. This includes fraud against unemployment benefits, Economic Impact Payments (EIPs), Paycheck Protection Program (PPP) funds, and other CARES Act initiatives. These criminals aren't just defrauding these programs directly, but also impeding the execution of these programs, thus denying essential aid to intended recipients in dire need of assistance.

I am pleased to report that Secret Service has already seen tremendous success emerge from our investigative efforts to date. We have initiated over one hundred criminal investigations and prevented approximately \$1 billion in fraud losses.

Among other law enforcement actions, the Secret Service has successfully disrupted hundreds of online COVID-19-related scams,¹ halted the alleged illicit sale of stolen COVID-19 test kits online,² and is participating in a nation-wide effort to counter a vast international scheme³ to defraud U.S. state unemployment systems. We have also released regular threat intelligence and alerts⁴ to provide industry, consumers and our law enforcement partners with best practices⁵ to defend themselves from the latest criminal threats.

The immediate investigative focus of the Secret Service is to disrupt and deter criminal activity that could hinder an effective response to the pandemic, to assist organizations at risk of crime, and to recover any funds stolen from Americans. Longer term, we will work to ensure that those who have criminally exploited this crisis are arrested and successfully prosecuted.

¹ <https://www.justice.gov/opa/pr/departments-justice-announces-disruption-hundreds-online-covid-19-related-scams>

² <https://www.justice.gov/usao-wdpa/pr/new-york-city-man-arrested-fraud-charges-selling-stolen-covid-19-testing-services>

³ <https://www.nytimes.com/2020/05/16/us/coronavirus-unemployment-fraud-secret-service-washington.html>

⁴ <https://www.secretservice.gov/data/press/releases/2020/20-APR/Check-Security-Features-for-Economic-Impact-Payments.pdf>

⁵ https://www.secretservice.gov/data/press/releases/2020/20-MAR/Secret_Service_Coronavirus_Phishing_Alert.pdf

Partnerships

Yet the Secret Service never operates alone. We work with a range of government and industry partners in executing our mission. In particular, the various agencies of the Department of the Treasury, including the Financial Crimes Enforcement Network (FinCEN), the Internal Revenue Service (IRS), the Treasury Inspector General for Tax Administration (TIGTA), and the various Offices of Inspectors General, including from the Department of Labor, are all critical partners in safeguarding the integrity of U.S. financial systems.

In addition, given the importance of the PPP, we are partnering with the Office of the Inspector General (OIG) of the Small Business Administration (SBA) to combat fraud against business loans. The Secret Service and SBA OIG have brought together the combined authorities, capabilities, tools, and human resources of our respective agencies in order to combat PPP-related fraud at both the national and local levels.

And, of course, to effectively coordinate across the whole of the U.S. government, we are actively engaging with the Department of Justice's COVID-19 task forces, the Federal Bureau of Investigation, Homeland Security Investigations, the Cybersecurity and Infrastructure Security Agency (CISA), and other law enforcement agencies at the state, local, and federal levels, both in the United States and abroad.

Lastly, we have dramatically expanded our outreach to industry, particularly America's financial institutions, which are responsible for distributing much of the CARES Act funds to the public. With the financial institutions, we have expanded our information sharing and other cooperation to rapidly detect fraud, freeze assets, and return money to government agencies and others who have been defrauded. This cooperation is absolutely essential, given the ability of the financial institutions to intercede quickly in the event of fraud.

Conclusion

The ongoing spate of COVID-19-related crime is in many ways a culmination of years of mounting risk within the financial sector, driven in large part by the growth of transnational cyber-crime. COVID-19-related frauds are made possible by the persistent effort by cyber-criminals to breach computer systems to steal personal information, which can subsequently be used to fraudulently apply for loans and benefits payments. Recent data breaches have allowed criminals to buy and sell this information, such as social security numbers and account passwords, which can later be used in an extensive range of frauds.

But the insecurity of the digital realm is not solely a matter of economics. These same criminals are also assisting nation-states in activities that present a very real threat to America's national security. Over the past twenty years, there has been a steady growth in transnational cyber-crime, and cooperation between these transnational criminal organizations and some foreign states. What we are seeing now with this pandemic is an acceleration of this trend, which is coinciding with a vulnerable moment for our nation and our economy. I am committed to countering this sort of criminal activity and look forward to answering your questions on how we can work together to address this threat.



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.

COVID-19 Fraud: Law Enforcement's Response to Those Exploiting the Pandemic
Hearing before the Senate Committee on the Judiciary
Questions for the Record
June 9, 2020

QUESTIONS FROM SENATOR BLUMENTHAL

Questions for Craig Carpentino

1. As discussed at the hearing, COVID-19 related fraud undermines those small businesses and households that desperately need help right now, blocking access to assistance set aside for them in the CARES Act. In his testimony, William Hughes said, "fraudsters are targeting the Payroll Protection Program, the Economic Impact Payment Program and its state unemployment benefit programs." Michael D'Ambrosio echoed this sentiment when he stated, "we have seen a surge in crimes targeting various economic relief programs, such as those provided by the CARES Act." It seems, therefore, that increased oversight and funding of the CARES Act would directly assist you in fighting these fraudulent schemes.
 - a. What increases in oversight mechanisms and other measures would enable you to protect the public from COVID-19 related fraud conducted by large businesses and foreign criminal actors?
 - b. How do Inspectors General help with your oversight and enforcement against fraud targeting relief programs? What lessons should we apply to the CARES Act?
 - c. Would harsher punishments and damages, similar to the False Claims Act, deter fraud and profiteering by large businesses and foreign criminal actors?
2. Unfortunately, child exploitation has drastically increased since the onset of COVID-19, as predators have seen the pandemic as a perfect opportunity to harm children. As even kindergarten and elementary school classes go online, more kids are sitting in front of computers alone. In your joint written testimony, you and William Hughes confirmed this grave truth, stating, "the Department is gravely concerned that COVID-19 is leading to a higher incidence of online child sexual exploitation, because both offenders and children are spending more time at home and online, and because the use of videoconference platforms has increased.

Hughes echoed this pressing issue in the hearing, stating, "the pandemic has also changed the cyber threat landscape" as "child predators on the Internet see widespread closing of schools, stay-at-home orders and the reliance on Internet platforms, as the primary means of communication, as an opportunity to prey on children." Additionally, at the hearing, Calvin Shivers stated, "in addition to fraud schemes, we are seeing crimes targeting our children. School closures have increased the presence of children, online. In addition, social distancing restrictions

and the isolation of children at home may afford terminal actors with an opportunity to sexually exploit vulnerable children.”

Predators are seeing this national crisis as an opportunity. You and Hughes made this very clear through your written testimony when you quoted an individual who posted on the Dark Web on March 21, 2020 saying, “is nobody seeing the bright side of this pandemic?? Schools are closed so kids are at home bored ... that means way more livestreams and its very clear moderators aren’t working right now since I’ve seen 3 hour streams go unbanned over the last few days where girls do whatever the f--- they want. What a time to be alive.”

- a. Do you agree that tech companies have to step up themselves to prevent and report online exploitation and abuse material on their platforms?
- b. Have the online platforms done enough during the Coronavirus pandemic to respond to this heightened risk and to stop online exploitation?

Craig Carpenito
U.S. Attorney for the District of New Jersey
Questions for the Record
Submitted June 16, 2020

QUESTIONS FROM SENATOR BOOKER

1. New Jersey ranks 7th highest in COVID-19 related fraud cases, with 1,911 FTC complaints.¹
What is the scope of the problem of COVID-19 related fraud in New Jersey and are you seeing the number of cases increase or decrease as this pandemic continues on?

¹ Federal Trade Commission, FTC COVID-19 Complaints (June 9, 2020), <https://www.ftc.gov/system/files/attachments/coronavirus-covid-19-consumer-complaint-data/covid-19-daily-public-complaints-060920.pdf>.

**Written Questions from Senator Dick Durbin
Hearing on “COVID-19 Fraud: Law Enforcement’s Response to Those Exploiting the
Pandemic”
June 16, 2020**

For questions with subparts, please answer each subpart.

Questions for U.S. Attorney Craig Carpenito

In Illinois, the most common type of COVID-19-related consumer complaint involves price gouging. It is unconscionable when profiteers use disasters to jack up the prices of items that their fellow citizens need.

Illinois has a state consumer fraud law that can be used to investigate and penalize price gouging. Also, Governor Pritzker’s COVID-19 emergency declaration specifically prohibits price gouging for COVID-related goods like PPE. These laws are enforced by our state Attorney General’s office, which to date has received over 1,700 price-gouging complaints from Illinoisans.

There is also a federal role. Federal law prohibits hoarding and price gouging of items that have been designated as scarce under the Defense Production Act, such as PPE. The Department of Justice COVID-19 Hoarding and Price-Gouging Task Force has been established under your leadership to work with state and local authorities to coordinate price-gouging investigations and enforcement actions.

1. **Since the creation of the Task Force, how many price-gouging complaints have been submitted to federal, state, and local authorities working in coordination with the Task Force, both nationally and in Illinois?**
 - a. **Are these numbers currently trending up or down?**
2. **Please break down the allocation of price-gouging complaints that are received by federal, state, and local authorities working with the Task Force, to the extent the Task Force is aware.**
 - a. **What mechanisms seem to be working most effectively for consumers to submit complaints of price-gouging to authorities?**
3. **Since the creation of the Task Force, how many price-gouging investigations have been opened by the Task Force and by state/local authorities working in coordination with the Task Force, both nationally and in Illinois?**
 - a. **Are these numbers currently trending up or down?**
 - b. **What percentage of these investigations are led at the federal level versus the state or local level?**

4. Since the creation of the Task Force, how many price-gouging enforcement actions have been conducted by the Task Force or by state/local authorities working in coordination with the Task Force, both nationally and in Illinois?
 - a. Are these numbers currently trending up or down?
 - b. What percentage of these enforcement actions are led at the federal level versus the state or local level?
5. What types of products are currently subject to the largest number of complaints regarding price-gouging, and for what products would the Task Force recommend that consumers be on highest alert for potential price-gouging activity?
6. Please discuss the extent of coordination between the Task Force and the Federal Trade Commission in investigating price-gouging complaints and taking corrective action.
7. Please discuss the extent of coordination between the Task Force and state Attorneys General in investigating price-gouging complaints and taking corrective actions.
 - a. In the Task Force's view, do state Attorneys General currently have sufficient manpower, technology, training, and resources to handle the volume of price-gouging matters that are arising during the COVID-19 pandemic, or would state Attorneys General benefit from additional resources dedicated to addressing price-gouging and related practices?
8. In the Task Force's view, are private online marketplaces that host third-party sellers currently providing optimal levels of transparency and cooperation in combating price-gouging on their platforms, or would further transparency be beneficial?
9. Has the Task Force developed and disseminated best practices for coordinating and combating price-gouging within states? If so, please discuss these best practices.
10. In the Task Force's view, what further authorities, resources, or steps would be beneficial in the effort to combat price-gouging?
11. I understand that the bulk of price-gouging complaints are received by state Attorneys General and that the lion's share of investigative work is done by those offices.

Often, when state AGs receive price-gouging complaints, their investigators contact the sellers to ask why a product's price has gotten so high. Maybe the seller can point to a legitimate reason having to do with supply costs or shortages, or maybe not. I understand that these phone calls from State AG offices generally have proved effective at persuading sellers to reduce excessively high prices.

Mr. Carpenito, it seems one of the ways we could help combat price gouging more effectively is to help State AG offices receive more training, more investigative tools, and more capability for quickly processing complaints.

Do you think bolstering the investigative resources, tools, and training used by State Attorney General offices would help the Task Force in its efforts to fight price gouging?

12. I am troubled that profiteers are able to use online marketplace platforms like Amazon and Facebook to facilitate their price-gouging schemes. There often is a lack of transparency on these websites about who the sellers are, and that enables price gougers to avoid scrutiny and to easily shut down one account and pop back up under another account.

On March 25, a group of 34 state Attorneys General wrote to Amazon, Facebook, and other online marketplaces to urge them to do more to crack down on price gouging on their platforms, including urging the companies to create mechanisms to allow consumers to report suspected price gouging.

- a. **In the Task Force's view, are online marketplaces like Facebook and Amazon currently providing optimal levels of transparency and cooperation in combating price gouging on their platforms, or does more need to be done?**
 - b. **Would it be helpful for these companies to verify the identity of and require transparency from their high-volume third-party sellers so that profiteers cannot just open and close accounts frequently to avoid scrutiny and accountability?**
13. You stated in your written testimony that "[i]n addition to hoarding and price gouging, the task force also is focused on identifying counterfeit and misbranded PPE imported into the U.S. from abroad. The task force has been coordinating with the FDA and the Consumer Protection Branch of the Department's Civil Division when such situations present themselves."
- a. **How much counterfeit or misbranded PPE has the Task Force identified so far being imported into the United States? Please provide details about the volume and types of counterfeit or misbranded PPE that have been identified so far.**
 - b. **How many enforcement actions have been undertaken with respect to counterfeit or misbranded PPE so far by the Task Force or agencies working with the Task Force?**
 - c. **In the Task Force's view, are online marketplaces currently providing optimal levels of transparency and cooperation in combating the sale of counterfeit or misbranded PPE, or does more need to be done?**

**Hearing on COVID-19 Fraud: Law Enforcement's
Response to Those Exploiting the Pandemic**

**Questions for the Record
June 16, 2020**

QUESTIONS FROM SENATOR FEINSTEIN

Questions for Mr. Carpenito

1. You mentioned in your testimony that, in the absence of a federal price gouging law, prosecutors are relying on the anti-hoarding provision of the Defense Production Act (50 U.S.C. § 4512). That provision prohibits the accumulation of scarce or threatened materials “(1) in excess of the reasonable demands of business, personal, or home consumption, or (2) for the purpose of resale at prices in excess of prevailing market prices.”
 - a. **How do you determine whether scarce or threatened materials are being resold at prices in excess of the prevailing market prices?**
 - b. **Do you apply specific, factual criteria to make this determination?**
 - c. **If so, what is it, and how did you formulate it?**
2. There are reports that doctors were prescribing massive amounts of hydroxychloroquine, a drug with no confirmed benefits for people suffering from COVID-19, for themselves and others after the President repeatedly touted it as a treatment.

As a result, patients with lupus who actually need this medicine had to wait while their refills were on back order or were provided smaller amounts of the drug than usual.

- a. **What is the COVID-19 Hoarding and Price Gouging Task Force doing to prevent the hoarding of hydroxychloroquine at the expense of patients who need it?**

QUESTIONS FOR THE RECORD**For Craig Carpenito (DOJ Hoarding and Price Gouging Task Force):**

- The Department of Justice's COVID-19 Hoarding and Price Gouging Task Force is working cases that involve the sale of fraudulent, misbranded, or stolen personal protective equipment (PPE) through online marketplaces like Amazon, eBay, and Facebook. Your testimony indicated there was, at least, some level of cooperation between DOJ and these organizations.
 - When unlawful stockpiles of PPE or other critical medical supplies are being sold online to American consumers, what are technology companies doing to provide assistance in Task Force investigations?
 - Explain the standard procedures taken by the Task Force in order to interrupt the online sale of these illicit goods. Specifically, what information or documentation is required by the technology companies (i.e. subpoenas, etc.) prior to corresponding to DOJ's request for assistance?

**WRITTEN QUESTIONS OF SENATOR CHUCK GRASSLEY FOR
SENATE JUDICIARY COMMITTEE HEARING “COVID-19
FRAUD: LAW ENFORCEMENT’S RESPONSE TO THOSE
EXPLOITING THE PANDEMIC”, JUNE 9, 2020**

Questions for Craig Carpenito

1. What difficulties or obstacles has law enforcement encountered when investigating and prosecuting cases against those who seek to exploit the COVID-19 pandemic?
2. Does law enforcement have all the tools and authorities it needs to go after COVID-19 related scams, hoarding, price gouging and other fraudulent schemes?
3. In your opinion, would a federal price gouging statute help you pursue bad actors? If so, what would you like to see in a federal price gouging statute?
4. Do you believe that existing penalties for price gouging are tough enough? What about penalties for scams and fraudulent activity related to the CARES Act Paycheck Protection Program and unemployment benefits – are they adequate or should they be strengthened?
5. What kind of legislation would you like to see Congress enact to assist you in your investigations and prosecutions of these cases? What more can we do to help prevent fraudsters and other criminals from taking advantage of Americans during the pandemic?
6. Earlier this year, China halted exports of medical supplies—including PPEs—in response to the COVID-19 pandemic. This decision caused a cascade effect around the world, where PPEs became impossible to find. In the U.S., we’ve seen shortages of medical supplies at least since February. I’m interested in developing a timeline here. At what point did the Justice Department begin to identify cases of COVID-19-related fraudulent activity? Did these cases significantly increase at any point in time?
7. It’s important that Americans know how they are at risk of falling victim to scams. What specifically is the Justice Department doing to alert and educate consumers and businesses about the different kinds of dangerous fraudulent schemes that exist during this pandemic and how to protect themselves?

8. What is the Justice Department specifically doing to ensure that hospitals are not being defrauded and sold fake PPE or other vital medical supplies?

9. What is the Justice Department doing to ensure that consumers and businesses can easily and efficiently provide you with information and file complaints should they fall victim to scams?

10. Could you please elaborate on the increase in cybercrime? What is the Justice Department doing to educate the average American on how they can prevent the spread of malware and other tools that compromise our ability to work safely from home during these times?

11. The Justice Department is using various technologies to identify and investigate fraud related to state issuance of unemployment benefits. Do states have access to these same technologies? If not, why not? Are there barriers that states report facing that keep them from guarding against fraud, or in responding to fraud that you have identified?

**Questions for Craig Carpenito
From Senator Mazie K. Hirono**

1. In Hawaii, more than 1 in 5 adults are age 60 or older. The FTC reported that as of June 4, 2020, Americans have lost at least \$46.17 million in COVID-19 related fraud. But those between ages 60 and 69 experienced the greatest amount of loss of any other age category, with \$5.67 million in loss.
 - a. Are you aware of any explanations for the higher levels of fraud loss among those age 60 and 69?
 - b. What are currently the most common COVID-19 related scams used to specifically target older Americans, and what steps are you taking to prevent such fraud?
 - c. One of the challenges in protecting older Americans from fraud is educating them about these scams. How, if at all, do you engage with community-based organizations and leaders to reach this vulnerable population?

Mr. Carpenito:

1. I'm also very concerned about price gouging and hoarding of essential PPE. How is the DOJ approaching the issue of price gouging to determine if a crime has occurred or if it is just an adjustment in the market for goods? How do you distinguish the difference? How many prosecutions has the DOJ brought so far on price gouging or hoarding?

| | |
|-------------------|-----------------------------------------------------------------------------|
| Question#: | 1 |
| Topic: | PPP and EIP Fraud |
| Hearing: | COVID-19 Fraud: Law Enforcement's Response to Those Exploiting the Pandemic |
| Primary: | The Honorable Lindsey O. Graham |
| Committee: | JUDICIARY (SENATE) |

Question: During your testimony we heard mostly about your efforts to interrupt schemes targeting unemployment insurance programs across the country. The American taxpayer is also heavily invested in additional COVID-response programs like the Paycheck Protection Program (PPP) and Economic Impact Payments (EIP).

How is the Secret Service addressing the fraud being committed against these programs? Specifically, how is the Secret Service leveraging government and agency partners in countering PPP and EIP fraud?

Response: The U.S. Secret Service, the U.S. Department of Justice (DOJ), the U.S. Department of the Treasury, and the Small Business Administration's Office of Inspector General (SBA OIG) are closely partnering on Paycheck Protection Program (PPP) and Economic Impact Payment (EIP) fraud investigations.

The SBA OIG and the Secret Service have brought together the combined authorities, capabilities, tools and human resources of our respective agencies to combat PPP and EIP-related fraud at both the national and local levels. The Secret Service Office of Investigations maintains a workforce of thousands of criminal investigators and analysts, spread across more than 100 domestic and overseas field offices. These special agents and analysts are trained in investigative techniques and technologies specifically focused on countering financial crimes, including complex cyber-enabled fraud, such as identity theft and use of ransomware, as well as more traditional violations of finance and banking law, such as counterfeiting, fraud, and money laundering. SBA OIG brings the requisite investigative expertise and authorities to combat fraud against the PPP and EIP funds. This coordination to combat an unprecedented level of fraudulent activity is a key factor in the successful oversight and enforcement of programs that disburse trillions of dollars in assistance to the American public.

The Secret Service also regularly provides best practices and alerts, and hosts events aimed at informing the general public about cyber threats and actions that can be taken to mitigate risks. This is undertaken with a variety of partners, including the Cybersecurity Information and Security Agency (CISA), and through our nationwide network of electronic and financial crimes task forces, a partnership between the Secret Service and private sector organizations, public sector departments and agencies, state and local law enforcement, and academia. The Secret Service's task forces host events and, most recently, virtual seminars and panel discussions across the country. In recent months, we have hosted virtual information sessions on issues such as Business Email Compromises (BECs), ransomware, online payment card skimming, and telework cybersecurity concerns.

| | |
|-------------------|-----------------------------------------------------------------------------|
| Question#: | 1 |
| Topic: | PPP and EIP Fraud |
| Hearing: | COVID-19 Fraud: Law Enforcement's Response to Those Exploiting the Pandemic |
| Primary: | The Honorable Lindsey O. Graham |
| Committee: | JUDICIARY (SENATE) |

In addition, the Secret Service's Global Investigative Operations Center (GIOCC) collects and analyzes cyber threat information that is then distributed through alerts to our field offices and task forces, as well as to Information Sharing and Analysis Centers (ISACs) and the public. The Service has also produced a series of PSAs that are available on the agency's website, social media platforms, and public television outlets. The topics include stimulus/Treasury check fraud, SMS-text phishing ("smishing"), BECs, ransomware, money mules, and general cybersecurity considerations.

| | |
|-------------------|-----------------------------------------------------------------------------|
| Question#: | 2 |
| Topic: | Scattered Canary Group |
| Hearing: | COVID-19 Fraud: Law Enforcement's Response to Those Exploiting the Pandemic |
| Primary: | The Honorable Diane Feinstein |
| Committee: | JUDICIARY (SENATE) |

Question: During the hearing, there were discussions of a foreign fraud ring known as “Scattered Canary” using personal information, likely obtained through prior consumer data breaches, to fraudulently obtain hundreds of millions of dollars in unemployment benefits from state governments.

This criminal scheme deprived states of the resources Congress provided them through the CARES Act. Worse, it delays the release of benefits to state residents who desperately need it as the states try to halt this fraud.

What is the Secret Service doing to stop the Scattered Canary group and its unemployment insurance scam? Is the Secret Service treating this as a criminal conspiracy rather than an isolated incident?

Response: The Secret Service is aware of industry reports that have described a group named “Scattered Canary” involved in cyber-criminal activity. It is important to note the group, as described, is not solely responsible for the fraud targeting state unemployment benefits programs. The Secret Service is coordinating multiple criminal investigations, targeting a range of fraudsters and their money mule networks.

Question: More generally, has the Secret Service seen any similar schemes, and what is being done to detect and prevent this?

Response: The mechanics of unemployment benefits fraud is similar to stolen identity refund fraud (SIRF) targeting the Internal Revenue Service tax refunds. Like SIRF cases, criminals targeting unemployment benefits simply need to obtain an individual's personal information and other basic publicly-available information to submit claims. To prevent this kind of fraud, whether SIRF or unemployment insurance fraud, government programs should utilize multiple pieces of applicant data, such as Internet Protocol (IP) address, email address, location of bank account to receive the funds, and number of benefits sent to the same bank account. Coordination between programs, financial institutions, states, and relevant government agencies is essential to ensuring that fraudsters are not using the same credentials to apply for benefits in multiple states.

To assist with this information sharing, the Secret Service is conducting joint investigations with the SBA, the Department of Labor (DOL), the Department of the Treasury, DOJ, and state, local, tribal and territorial (SLTT) law enforcement. The Secret Service also shares data with state unemployment offices that might help reduce fraud. For example, a recent Secret Service investigation identified a dark web database of approximately 500,000 identities that were

| | |
|-------------------|-----------------------------------------------------------------------------|
| Question#: | 2 |
| Topic: | Scattered Canary Group |
| Hearing: | COVID-19 Fraud: Law Enforcement's Response to Those Exploiting the Pandemic |
| Primary: | The Honorable Diane Feinstein |
| Committee: | JUDICIARY (SENATE) |

purchased online in the past six months. This database was broken down by state of victim and is in the process of being shared with each state so that they can flag the identities for potential fraud.

| | |
|-------------------|-----------------------------------------------------------------------------|
| Question#: | 3 |
| Topic: | Information to States |
| Hearing: | COVID-19 Fraud: Law Enforcement's Response to Those Exploiting the Pandemic |
| Primary: | The Honorable Diane Feinstein |
| Committee: | JUDICIARY (SENATE) |

Question: What information is the Secret Service providing to states to protect them from scams like those perpetrated by Scattered Canary, and under what circumstances does it provide that information? Please be specific as to the timing and modalities of information sharing.

Response: Secret Service special agents and analysts rapidly mobilized and responded to scams targeting COVID-19 relief. The agency leveraged existing partnerships with financial institutions and SLTT agencies, and expanded its coordination with DOL Office of Inspector General (OIG) to identify gaps in state Unemployment Insurance (UI) programs and recommend preventative measures. DOL/OIG maintains primary oversight of state UI programs. The Secret Service continues partnering with DOL/OIG to prevent further targeting.

Specifically, the Secret Service recommended that state UI programs take measures to block access to foreign and Virtual Private Network (VPN) based IP addresses, improve website security, and institute additional identity verification measures where necessary. States were further notified by the Secret Service of suspect IP addresses and email address exploits associated with this fraud scheme.

Question: What policies, practices, or procedures does the Secret Service have in place to ensure that specific, actionable information is provided to state and local government entities before they are victimized by scammers like the Scattered Canary group, particularly, but not limited to when the threat in question is under investigation by the Secret Service?

Response: The Secret Service maintains a robust set of partnerships with both public and private sectors through our network of electronic and financial crimes task forces. These task forces serve to facilitate the sharing of information and allow for an open communication line for incident reporting. These relationships are at the heart of the Secret Service's approach to investigations and once again proved successful in responding to COVID-19 related fraud, including the targeting of unemployment insurance programs. The Secret Service and our partners identified gaps in state UI programs, recommended preventative security and authentication measures, and worked with financial institutions to prevent further disbursement of funds to suspected money mules. These task forces, partnerships and liaison relationships have proved essential in preventing significant losses due to cyber-crime.

| | |
|-------------------|-----------------------------------------------------------------------------|
| Question#: | 4 |
| Topic: | Other Cyber Crimes |
| Hearing: | COVID-19 Fraud: Law Enforcement's Response to Those Exploiting the Pandemic |
| Primary: | The Honorable Diane Feinstein |
| Committee: | JUDICIARY (SENATE) |

Question: What other kinds of specific cyber crimes are you seeing that are taking advantage of the pandemic, and what is the Secret Service doing to stop them?

Response: Among other crimes—and there are many—we are seeing a rise in: 1) fraudulent pandemic-themed websites; 2) pandemic phishing schemes being used to gain unauthorized access into protected computers and accounts; 3) ransomware targeting the health sector; and, 4) cyber-criminals offering information and services to assist others in committing fraud.

The Secret Service is vigorously investigating these crimes, in collaboration with a range of federal, state and local law enforcement partners.

| | |
|-------------------|-----------------------------------------------------------------------------|
| Question#: | 5 |
| Topic: | Obstacles Encountered |
| Hearing: | COVID-19 Fraud: Law Enforcement's Response to Those Exploiting the Pandemic |
| Primary: | The Honorable Charles E. Grassley |
| Committee: | JUDICIARY (SENATE) |

Question: What difficulties or obstacles has law enforcement encountered when investigating and prosecuting cases against those who seek to exploit the COVID-19 pandemic?

Response: There are several challenges we face in investigating COVID-19 related crimes.

First, highly complex investigations, such as those involving counterfeit personal protective equipment (PPE) in the form of wire fraud investigations, require collaboration between a wide variety of law enforcement agencies and private companies. Such coordination is critical, but time consuming.

Second, much of the COVID-19 programmatic fraud, such as that targeting PPP, is targeting financial institutions and government agencies with limited law enforcement personnel or resources. The Secret Service is coordinating our investigative efforts with several Offices of Inspectors General, the Federal Bureau of Investigation, and state and local law enforcement in order to bridge this gap.

Third, criminals are rapidly identifying and exploiting system vulnerabilities and news events to defraud the American public. And, given sheer volume of this crime, it is a challenge to keep pace with the scale and diversity of the full range of criminal activity.

The challenges the Secret Service faces in investigating these matters are like the challenges involving the Internet and transnational organized criminal groups more generally. These challenges include delayed victim reporting to law enforcement, the length of time it takes to submit the required legal process and non-disclosure orders, the use of existing money mule networks and convertible virtual currency to launder proceeds, and the time required for the Mutual Legal Assistance Treaty process.

Question: Does law enforcement have all the tools and authorities it needs to go after COVID-19 related scams, hoarding, price gouging and other fraudulent schemes?

Response: The scale and scope of criminal activity exploiting the pandemic is enormous. However, the Secret Service has the tools and authorities it needs to effectively address the crisis.

| | |
|-------------------|-----------------------------------------------------------------------------|
| Question#: | 6 |
| Topic: | Existing Penalties |
| Hearing: | COVID-19 Fraud: Law Enforcement's Response to Those Exploiting the Pandemic |
| Primary: | The Honorable Charles E. Grassley |
| Committee: | JUDICIARY (SENATE) |

Question: Do you believe that existing penalties for scams and fraudulent activity related to the CARES Act Paycheck Protection Program and unemployment benefits are adequate or should they be strengthened?

Response: Higher penalties may further deter criminal activity seeking to exploit this pandemic and CARES Act programs. Higher maximum penalties for crimes committed during or in relation to a major disaster are provided by several existing statutes (18 U.S.C. §§ 1031, 1040, 1341, and 1343).

Question: What kind of legislation would you like to see Congress enact to assist you in your investigations and prosecutions of these cases? What more can we do to help prevent fraudsters and other criminals from taking advantage of Americans during the pandemic?

Response: The FY 2021 President's Budget provides for the transfer of the Secret Service to the Department of Treasury to enhance law enforcement efforts to investigate and disrupt financial crime across a range of sectors, to include fraudulent schemes capitalizing on COVID-19 and associated relief programs.

| | |
|-------------------|-----------------------------------------------------------------------------|
| Question#: | 7 |
| Topic: | Transnational Cyber-Crime Growth |
| Hearing: | COVID-19 Fraud: Law Enforcement's Response to Those Exploiting the Pandemic |
| Primary: | The Honorable Charles E. Grassley |
| Committee: | JUDICIARY (SENATE) |

Question: I'm interested in hearing more about the growth in transnational cyber-crime and the cooperation between transnational criminal organizations and foreign states. How has the COVID-19 pandemic accelerated this trend, and what can we do about it? Do you have any recommendations on how to counter this criminal activity?

Response: It is unclear if the COVID-19 pandemic has accelerated this trend. While countering this activity is a challenge, the Secret Service has sufficient existing authorities to pursue its investigations.

| | |
|-------------------|-----------------------------------------------------------------------------|
| Question#: | 8 |
| Topic: | Educate Public I |
| Hearing: | COVID-19 Fraud: Law Enforcement's Response to Those Exploiting the Pandemic |
| Primary: | The Honorable Charles E. Grassley |
| Committee: | JUDICIARY (SENATE) |

Question: It's important that Americans know how they are at risk of falling victim to scams. What specifically is the Secret Service doing to alert and educate consumers and businesses about the different kinds of dangerous fraudulent schemes that exist during this pandemic and how to protect themselves?

Response: The Secret Service regularly issues press releases, best practices, and public service announcements. We do this to keep our partners and the wider American public aware of threats and the steps that can be taken to mitigate some of the risks.

During the pandemic, we have stepped up this effort. Our investigators have been participating in media interviews and live and prerecorded public service announcements on social media, all aimed at preventing COVID-19 related fraud. In addition, the Secret Service has developed several factsheets, such as "Don't Be a Mule," "Online and Auction Fraud," and "Basic Cyber Security," for distribution via public websites and through private and public Secret Service partners.

The Secret Service maintains liaison with and has strategically assigned detailees in a number of federal and public/private partnerships, such as the National Cyber-Forensics and Training Alliance. The Secret Service has partnered with these organizations to share real time information with the private sector, as well as distribute joint public and industry-specific alerts.

Question: What is the Secret Service doing to ensure that consumers and businesses can easily and efficiently provide you with information and file complaints should they fall victim to scams?

Response: The Secret Service has partnered with both public and private sectors in an effort to share relevant information and maintain an open communication line for incident reporting. This includes partnerships with financial institutions, the healthcare sector, federal agencies, and state and local police departments. Secret Service field offices and task forces are continually conducting outreach to build trusted relationships to allow for more rapid incident reporting. In addition, Secret Service public awareness products provide information for how to report a crime. The public can also readily contact their local Secret Service field office through <https://www.secretservice.gov/contact/field-offices/>.

| | |
|-------------------|-----------------------------------------------------------------------------|
| Question#: | 9 |
| Topic: | Fake Medical Supplies |
| Hearing: | COVID-19 Fraud: Law Enforcement's Response to Those Exploiting the Pandemic |
| Primary: | The Honorable Charles E. Grassley |
| Committee: | JUDICIARY (SENATE) |

Question: What is the Secret Service specifically doing to ensure that hospitals are not being defrauded and sold fake PPE or other vital medical supplies?

Response: Since April 2020, the Secret Service has issued multiple internal alerts to our workforce of criminal investigators and analysts, spread across domestic and overseas field offices, to provide them with information about the threats of fraudulent PPE and other medical equipment to facilitate wire fraud investigations. These alerts include a list of the top threat indicators that are used by our criminal investigators and analysts to effectively prevent, detect, and respond to threats. In addition to our internal workforce audience, some of the alerts have been distributed to Secret Service partners, as well as the general American public, to provide warnings and best practices to mitigate the threat of potential criminal activity.

Through these efforts, the Secret Service has successfully investigated a number of cases of fraudulent PPE and other vital medical supplies, helping prevent tens of millions of dollars in wire fraud.

| | |
|-------------------|-----------------------------------------------------------------------------|
| Question#: | 10 |
| Topic: | Malware Spread |
| Hearing: | COVID-19 Fraud: Law Enforcement's Response to Those Exploiting the Pandemic |
| Primary: | The Honorable Charles E. Grassley |
| Committee: | JUDICIARY (SENATE) |

Question: What is the Secret Service doing to educate the average American on how they can prevent the spread of malware and other tools that compromise our ability to work safely from home during these times?

Response: The Secret Service regularly provides best practices and alerts, and hosts events aimed at informing the general public about cyber threats and actions that can be taken to mitigate risks. This effort is undertaken with a variety of partners, including the Cybersecurity Information and Security Agency (CISA), and through our nationwide network of electronic and financial crimes task forces, which are partnerships between the Secret Service and private sector organizations, public sector departments and agencies, state and local law enforcement, and academia. The Secret Service's task forces host events and, most recently, virtual seminars and panel discussions across the country. In recent months, we have hosted virtual information sessions on fraud schemes such as Business Email Compromises (BECs), ransomware, online payment card skimming, and telework concerns.

In addition, the Secret Service's Global Investigative Operations Center (GIOC) collects and analyzes cyber threat information that is then distributed through alerts to our field offices and task forces, as well as Information and Sharing Analysis Centers (ISACs) and the public. The Service has also produced a series of Public Service Announcements (PSAs) that are available on the agency's website, social media platforms, and public television outlets. The topics include stimulus/Treasury check fraud, SMS-text phishing ("smishing"), BECs, ransomware, money mules, and general cybersecurity considerations.

| | |
|-------------------|-----------------------------------------------------------------------------|
| Question#: | 11 |
| Topic: | State Technology Access |
| Hearing: | COVID-19 Fraud: Law Enforcement's Response to Those Exploiting the Pandemic |
| Primary: | The Honorable Charles E. Grassley |
| Committee: | JUDICIARY (SENATE) |

Question: The Secret Service is using various technologies to identify and investigate fraud related to state issuance of unemployment benefits. Do states have access to these same technologies? If not, why not? Are there barriers that states report facing that keep them from guarding against fraud, or in responding to fraud that you have identified?

Response: Identifying and investigating unemployment benefits fraud does not require any unique or proprietary technologies. The Secret Service primarily learns of specific fraudulent wire transfers through either financial institutions or Bank Secrecy Act data made available through Treasury's Financial Crimes Enforcement Network. Once a fraudster is identified, traditional law enforcement techniques and legal process are used to further investigations.

The Secret Service, through its National Cyber Forensics Institute, trains thousands of state and local law enforcement officers every year on how to conduct these types of investigations. Further, state and local law enforcement embedded in the Secret Service's electronic and financial crimes task forces are afforded access to all the same technologies and datasets that Secret Service agents have at their disposal to investigate unemployment benefits fraud and other similar white collar fraud schemes.

| | |
|-------------------|-----------------------------------------------------------------------------|
| Question#: | 12 |
| Topic: | Money Stolen I |
| Hearing: | COVID-19 Fraud: Law Enforcement's Response to Those Exploiting the Pandemic |
| Primary: | The Honorable Patrick Leahy |
| Committee: | JUDICIARY (SENATE) |

Question: The CARES Act provided hundreds of billions of dollars in direct payments for Americans impacted by COVID-19 and the recent economic downturn. You testified that criminals have exploited these programs, in part through the use of stolen personal information.

Do you have an estimate of how much money has been stolen through fraudulently-claimed Economic Impact Payments or unemployment benefits during this pandemic?

Response: It is currently too early to estimate exactly how much money has been lost due to fraud related to COVID-19 relief programs. However, based on fraud estimates from prior relief programs, it is estimated that fraud accounts for 1 percent up to 10 percent of disbursed funds. Assuming a similar percentage for CARES Act and other pandemic relief programs, the amount of fraud loss could total over \$100 billion dollars.

Taking just unemployment insurance programs as an example, as of June 24, 2020, the Secret Service estimates that \$550 million in defrauded funds have been returned to various state unemployment insurance programs. The Inspector General of the DOL, based on a 10 percent historic improper payment rate, estimates that "at least \$26 billion of [unemployment insurance] program funds issued under the CARES Act would be wasted, with a large portion attributable to fraud."¹

¹ Dahl, Scott S. Testimony before the U.S. Senate Committee on Finance Hearing Title: "Unemployment Insurance during COVID-19: The CARES Act and the Role of Unemployment Insurance during the Pandemic," U.S. Department of Labor, 9 June 2020. Available at: <https://www.oig.dol.gov/public/testimony/20200609.pdf>

| | |
|-------------------|-----------------------------------------------------------------------------|
| Question#: | 13 |
| Topic: | Future Programs |
| Hearing: | COVID-19 Fraud: Law Enforcement's Response to Those Exploiting the Pandemic |
| Primary: | The Honorable Patrick Leahy |
| Committee: | JUDICIARY (SENATE) |

Question: What is the Secret Service doing to ensure that future economic relief programs are not similarly susceptible to theft?

Response: The Secret Service aggressively investigates fraudsters who attempt to steal from economic relief programs. This effort both deters future criminal activity and disrupts the development of sophisticated criminal syndicates that engage in this sort of fraud. The Secret Service works closely with the Department of the Treasury, financial institutions, other federal law enforcement agencies, and with state and local law enforcement partners, to target money laundering networks that are essential for conducting this criminal scheme. The Secret Service also publishes alerts and best practices to protect against fraud to U.S. government programs. The Secret Service looks forward to continuing to work with our interagency partners to develop options to better prevent fraud against programs for disaster response and recovery.

| | |
|-------------------|-----------------------------------------------------------------------------|
| Question#: | 14 |
| Topic: | Future Cybersecurity Threats |
| Hearing: | COVID-19 Fraud: Law Enforcement's Response to Those Exploiting the Pandemic |
| Primary: | The Honorable Patrick Leahy |
| Committee: | JUDICIARY (SENATE) |

Question: As workplaces, schools, and social gatherings shut down across the country, Americans have relied on the internet more in the past several months than ever before. This has only increased Americans' exposure to cybersecurity threats and online exploitation, especially for children and the elderly.

Would federal cybersecurity requirements help reduce or prevent future recurrence of threats we have faced during this pandemic? Please explain.

Response: Effective security requires dynamic adaptation to keep pace with changes in technology, how it is used, and how criminals are exploiting it. The Secret Service has sufficient existing authorities to pursue its investigations.

| | |
|-------------------|-----------------------------------------------------------------------------|
| Question#: | 15 |
| Topic: | Shell Companies |
| Hearing: | COVID-19 Fraud: Law Enforcement's Response to Those Exploiting the Pandemic |
| Primary: | The Honorable Sheldon Whitehouse |
| Committee: | JUDICIARY (SENATE) |

Question: We know that criminals and kleptocrats use U.S. shell companies - sham companies that have no actual business operations- to launder ill-gotten criminal proceeds. However, criminals also use shell companies in schemes to defraud Medicaid and other government programs and steal millions of dollars of taxpayer money. I have worked with Chairman Graham, Senator Grassley, and Ranking Member Feinstein on a bill that would require many companies to disclose their beneficial owners, to help law enforcement see through shell companies.

Is it likely that shell companies are being used to defraud COVID relief programs?

Response: Yes. In general, shell companies play a pivotal role in cyber-enabled financial crime. The Secret Service commonly encounters both domestic and transnational crime groups using sham business enterprise models in which shell companies mask the flow of illicit funds as legitimate business. Specific to COVID-19 fraud, shell companies are being used as a primary mechanism to defraud victims by appearing as legitimate businesses for the purpose of buying and distributing COVID-19 related equipment or applying for various stimulus fund programs, like the PPP.

Question: For example, is there evidence that criminals are using shell companies to obtain PPP loans fraudulently?

Response: Yes. It appears that criminals are using shell companies to apply for PPP loans and other COVID-19 relief related programs.

| | |
|-------------------|-----------------------------------------------------------------------------|
| Question#: | 16 |
| Topic: | Money Stolen II |
| Hearing: | COVID-19 Fraud: Law Enforcement's Response to Those Exploiting the Pandemic |
| Primary: | The Honorable Sheldon Whitehouse |
| Committee: | JUDICIARY (SENATE) |

Question: Do you have a current estimate of how much COVID relief money has been lost in fraud schemes?

Response: It is currently too early to estimate exactly how much money has been lost due to fraud related to COVID-19 relief. However, based on prior relief programs, the Secret Service estimates that fraud accounts for 1 percent up to 10 percent of the funds disbursed through a relief program. Assuming a similar percentage for CARES Act and other pandemic relief programs, the amount of fraud loss could total over \$100 billion dollars.

Taking just unemployment insurance programs as an example, as of June 24, 2020, the Secret Service estimates that \$550 million in defrauded funds have been returned to various state unemployment insurance programs. The Inspector General of DOL, based on a 10 percent historic improper payment rate, estimates that “at least \$26 billion of [unemployment insurance] program funds issued under the CARES Act would be wasted, with a large portion attributable to fraud.”²

² Dahl, Scott S. Testimony before the U.S. Senate Committee on Finance Hearing Titled: “Unemployment Insurance during COVID-19: The CARES Act and the Role of Unemployment Insurance during the Pandemic,” U.S. Department of Labor, June 9, 2020. Available at: <https://www.oig.dol.gov/public/testimony/20200609.pdf>

| | |
|-------------------|-----------------------------------------------------------------------------|
| Question#: | 17 |
| Topic: | Launder Money |
| Hearing: | COVID-19 Fraud: Law Enforcement's Response to Those Exploiting the Pandemic |
| Primary: | The Honorable Sheldon Whitehouse |
| Committee: | JUDICIARY (SENATE) |

Question: Is it likely that criminals who perpetrate COVID-related fraud will use shell companies to launder their ill-gotten money?

Explain the difficulties that shell companies pose to law enforcement trying to “follow the money”?

Response: Shell companies are being used by criminal networks to create a complex and obfuscated trails of funds, which add several obstacles to law enforcement investigations. Shell companies allow criminal actors to conceal the true owner, the true purpose of the account, and the source or use of funds associated with the company. This allows illicit actors to operate in a more anonymous fashion. Given that using shell companies is a tried and true method for money laundering, it is more than likely that criminals who perpetrate COVID-related fraud will use shell companies to launder their ill-gotten money. It will allow them to take taxpayer money and efficiently launder it using layers of shell companies to assist in concealing their trail from law enforcement.

“Follow the money” is a standard investigative strategy whereby law enforcement agents start with a lead and try to follow the paper trail to uncover the entire network and masterminds behind a money laundering or other illicit finance scheme. Criminals use layers of shell companies to mislead investigators and protect themselves from investigation and prosecution. Sometimes law enforcement can find alternate routes to collect evidence against a network, only the low-end of the criminal food chain is immediately apprehended. To investigate or prosecute the entire network takes years and extensive resources, and uncovering the beneficial owner is not guaranteed. In that time, the network may use additional shell companies to cover its tracks, or may never be brought to justice.

Further there are some actors who establish shell companies on a service-for-hire basis, where they may not be fully aware of the criminal activity, but nevertheless allow criminal actors to use the established shell companies for a nominal fee. The service-for-hire actors may create hundreds of shell companies with little to no detection or scrutiny. Criminal actors are taking advantage of this situation by forming companies using stolen identities, which allows the actual criminal actors to remain anonymous.

| | |
|-------------------|-----------------------------------------------------------------------------|
| Question#: | 18 |
| Topic: | Beneficial Ownership Register |
| Hearing: | COVID-19 Fraud: Law Enforcement's Response to Those Exploiting the Pandemic |
| Primary: | The Honorable Sheldon Whitehouse |
| Committee: | JUDICIARY (SENATE) |

Question: Would having a beneficial ownership register that law enforcement could access help detect and prevent fraud and make sure taxpayer money is going to businesses and workers rather than criminals?

Response: The Secret Service currently has the investigative authorities needed to investigate fraud against COVID relief programs.

| | |
|-------------------|-----------------------------------------------------------------------------|
| Question#: | 19 |
| Topic: | Educate Public II |
| Hearing: | COVID-19 Fraud: Law Enforcement's Response to Those Exploiting the Pandemic |
| Primary: | The Honorable Sheldon Whitehouse |
| Committee: | JUDICIARY (SENATE) |

Question: Cybercriminals and other malicious actors are exploiting COVID-19 to launch cyberattacks, using the virus to induce people to expose themselves to malware and phishing schemes. For example, the new "Silent Night Zeus" bot has been deployed in scams ranging from emails promising COVID-19 financial relief to attacks against banks, and is able to log keystrokes to see what people are typing, take pictures of people's screens, and harvest passwords. On April 18, the FBI Deputy Assistant Director Tonya Ugoretz reported that the FBI has received quadruple the number of cybercrime reports compared to months before the pandemic.

What steps is the Secret Service taking to educate the public about COVID-related cyber-crime?

Response: The Secret Service regularly provides best practices and alerts, and hosts events aimed at informing the general public about cyber threats and actions that can be taken to mitigate risks. This effort is undertaken with a variety of partners, including the Cybersecurity Information and Security Agency (CISA), and through our nationwide network of electronic and financial crimes task forces, which are partnerships between the Secret Service and private sector organizations, public sector departments and agencies, state and local law enforcement, and academia. The Secret Service's task forces host events and, most recently, virtual seminars and panel discussions across the country. In recent months, we have hosted virtual information sessions on fraud schemes such as BECs, ransomware, online payment card skimming, and telework concerns.

In addition, the Secret Service's Global Investigative Operations Center (GIOC) collects and analyzes cyber threat information that is then distributed through alerts to our field offices and task forces, as well as Information Sharing and Analysis Centers (ISACs) and the public. The Service has also produced a series of PSAs that are available on the agency's website, social media platforms, and soon public television outlets. The topics include stimulus/Treasury check fraud, SMS-text phishing ("smishing"), BECs, ransomware, money mules, and general cybersecurity considerations.

| | |
|-------------------|-----------------------------------------------------------------------------|
| Question#: | 20 |
| Topic: | Bot-Schemes |
| Hearing: | COVID-19 Fraud: Law Enforcement's Response to Those Exploiting the Pandemic |
| Primary: | The Honorable Sheldon Whitehouse |
| Committee: | JUDICIARY (SENATE) |

Question: How are bots being used in fraud schemes?

Response: Botnets are primarily used as an entry point to inject malware or to gain unauthorized access to protected computers, to steal valuable data, or to deploy ransomware. Botnets are also used to perform Distributed Denial of Service (DDOS) attacks against public and private sector networks.

Question: How frequently is the Secret Service encountering bots as it investigates COVID fraud schemes?

Response: The Secret Service encounters botnets in nearly every ransomware investigation—a highly disruptive scheme during a period of increased telework. Botnets allow fraudsters to install and deploy ransomware and allow for obfuscation of high volume Internet activity. For example, such high-volume activity could include the submission of multiple fraudulent applications for unemployment insurance benefits. To quantify scope, one botnet the Secret Service has detected and is investigating has over 2.5 million victim computers in its network.

Question: Do you have an estimate on the damage bot-schemes have caused?

Response: The estimated cost of just ransomware could exceed \$1.4 billion in the United States, according to public reporting.³ When combined with the costs of DDOS attacks, fraud, identity theft, and other schemes, the total damage caused by bot-schemes likely exceeds several billion dollars annually.

³ <https://blog.emsisoft.com/en/35583/report-the-cost-of-ransomware-in-2020-a-country-by-country-analysis/>

| | |
|-------------------|-----------------------------------------------------------------------------|
| Question#: | 21 |
| Topic: | Fraud Detection |
| Hearing: | COVID-19 Fraud: Law Enforcement's Response to Those Exploiting the Pandemic |
| Primary: | The Honorable Amy Klobuchar |
| Committee: | JUDICIARY (SENATE) |

Question: Your testimony reflects the striking number and variety of coronavirus-related frauds being inflicted on the American public.

What are the most significant challenges that your agency faces in detecting illegal fraudulent schemes during this pandemic?

Response: The most significant challenge the Secret Service faces in detecting COVID-19 related fraud is the development of a robust transnational cyber criminal ecosystem, enabled by the global nature of both the Internet and the financial system. These trends, combined the present global pandemic, have created an unprecedented opportunity for transnational criminals to engage in fraud, causing substantial financial losses to victims.

Question: If you had additional resources, how would you employ them to improve fraud detection?

Response: The Secret Service will effectively use its existing resources to expand partnerships, both domestically and overseas, to address fraudulent activity across a range of sectors.

| | |
|-------------------|-----------------------------------------------------------------------------|
| Question#: | 22 |
| Topic: | CARES Oversight |
| Hearing: | COVID-19 Fraud: Law Enforcement's Response to Those Exploiting the Pandemic |
| Primary: | The Honorable Richard Blumenthal |
| Committee: | JUDICIARY (SENATE) |

Question: As discussed at the hearing, COVID-19 related fraud undermines those small businesses and households that desperately need help right now, blocking access to assistance set aside for them in the CARES Act. In his testimony, William Hughes said, “fraudsters are targeting the Payroll Protection Program, the Economic Impact Payment Program and its state unemployment benefit programs.” You echoed this sentiment when you stated, “we have seen a surge in crimes targeting various economic relief programs, such as those provided by the CARES Act.” It seems, therefore, that increased oversight and funding of the CARES Act would directly assist you in fighting these fraudulent schemes.

What increases in oversight mechanisms and other measures would enable you to protect the public from COVID-19 related fraud conducted by large businesses and foreign criminal actors?

Response: The intrinsic challenge in any disaster response is managing fraud risk while expeditiously responding to the disaster itself. However, prevention is not the only option. Criminal investigations enable the U.S. Government to recover fraudulently obtained assets and hold criminals accountable for engaging in fraud, while not impeding disaster response. Our experience in investigating fraud from other recent disasters, and economic recoveries, shows that this effort by law enforcement will extend for many years after the disaster.

Question: How do Inspectors General help with your oversight and enforcement against fraud targeting relief programs? What lessons should we apply to the CARES Act?

Response: Responding to criminal schemes seeking to exploit the COVID-19 pandemic has become a primary investigative focus for multiple offices of Inspectors General, and the Secret Service is partnering closely with them to aggressively pursue these cases where the conduct at issue falls within Secret Service financial and cyber crime jurisdiction. For example, the Secret Service is partnering closely with the Department of Labor (DOL) OIG and Small Business Administration (SBA) OIG and has put in place robust measures to work collaboratively to respond to criminal activity at both the national and local levels.

In particular, the Secret Service and SBA OIG are prioritizing cases in which criminal actors are engaging in fraud against PPP funds and other programs that aim to blunt the economic harm of the pandemic. In addition, DOL OIG and Secret Service have worked to address criminals who are exploiting state unemployment insurance programs.

The Secret Service Office of Investigations maintains a workforce of criminal investigators and analysts, spread across domestic and overseas field offices. These special agents and analysts are trained in investigative techniques and technologies specifically focused on countering financial

| | |
|-------------------|-----------------------------------------------------------------------------|
| Question#: | 22 |
| Topic: | CARES Oversight |
| Hearing: | COVID-19 Fraud: Law Enforcement's Response to Those Exploiting the Pandemic |
| Primary: | The Honorable Richard Blumenthal |
| Committee: | JUDICIARY (SENATE) |

crimes, including complex cyber-enabled fraud, such as identity theft and use of ransomware, as well as more traditional violations of finance and banking law, such as counterfeiting, fraud, and money laundering. DOL OIG and SBA OIG bring the requisite investigative expertise and authorities to combat fraud against state unemployment insurance and PPP funds.

| | |
|-------------------|-----------------------------------------------------------------------------|
| Question#: | 23 |
| Topic: | Harsher Punishment |
| Hearing: | COVID-19 Fraud: Law Enforcement's Response to Those Exploiting the Pandemic |
| Primary: | The Honorable Richard Blumenthal |
| Committee: | JUDICIARY (SENATE) |

Question: Would harsher punishments and damages, similar to the False Claims Act, deter fraud and profiteering by large businesses and foreign criminal actors?

Response: Higher penalties may further deter criminal activity seeking to exploit this pandemic and CARES Act programs. Higher maximum penalties for crimes committed during or in relation to a major disaster are provided by several existing statutes (18 U.S.C. §§ 1031, 1040, 1341, and 1343).

| | |
|-------------------|-----------------------------------------------------------------------------|
| Question#: | 24 |
| Topic: | Online Exploitation |
| Hearing: | COVID-19 Fraud: Law Enforcement's Response to Those Exploiting the Pandemic |
| Primary: | The Honorable Richard Blumenthal |
| Committee: | JUDICIARY (SENATE) |

Question: Unfortunately, child exploitation has drastically increased since the onset of COVID-19, as predators have seen the pandemic as a perfect opportunity to harm children. As even kindergarten and elementary school classes go online, more kids are sitting in front of computers alone. In their joint written testimony, William Hughes and Craig Carpentino confirmed this grave truth, stating, “the Department is gravely concerned that COVID-19 is leading to a higher incidence of online child sexual exploitation, because both offenders and children are spending more time at home and online, and because the use of videoconference platforms has increased.”

Hughes echoed this pressing issue in the hearing, stating, “the pandemic has also changed the cyber threat landscape” as “child predators on the Internet see widespread closing of schools, stay-at-home orders and the reliance on Internet platforms, as the primary means of communication, as an opportunity to prey on children.” Additionally, at the hearing, Calvin Shivers stated, “in addition to fraud schemes, we are seeing crimes targeting our children. School closures have increased the presence of children, online. In addition, social distancing restrictions and the isolation of children at home may afford terminal actors with an opportunity to sexually exploit vulnerable children.”

Predators are seeing this national crisis as an opportunity. Hughes and Carpentino made this very clear through their written testimony when they quoted an individual who posted on the Dark Web on March 21, 2020 saying, “is nobody seeing the bright side of this pandemic?? Schools are closed so kids are at home bored...that means way more livestreams and its very clear moderators aren't working right now since I've seen 3 hour streams go unbanned over the last few days where girls do whatever the f--- they want. What a time to be alive.”

Do you agree that tech companies have to step up themselves to prevent and report online exploitation and abuse material on their platforms?

Response: I agree. Tech companies perform a critical role in preventing illicit use of their platforms, and many companies can and should do more.

Question: Have the online platforms done enough during the Coronavirus pandemic to respond to this heightened risk and to stop online exploitation?

| | |
|-------------------|-----------------------------------------------------------------------------|
| Question#: | 24 |
| Topic: | Online Exploitation |
| Hearing: | COVID-19 Fraud: Law Enforcement's Response to Those Exploiting the Pandemic |
| Primary: | The Honorable Richard Blumenthal |
| Committee: | JUDICIARY (SENATE) |

Response: Data from our partners at the National Center for Missing and Exploited Children ⁴ and a June 19, 2020 report from EUROPOL ⁵ show a surge in online distribution of child sexual abuse material since the onset of this pandemic.

⁴ See <https://www.missingkids.org>

⁵ EUROPOL, "Exploiting Isolation: Offenders and Victims of Online Child Sexual Abuse During the Covid-19 Pandemic," European Union Agency for Law Enforcement Cooperation (19 June 2020). Available at: <https://www.europol.europa.eu/publications-documents/exploiting-isolation-offenders-and-victims-of-online-child-sexual-abuse-during-covid-19-pandemic>.

| | |
|-------------------|-----------------------------------------------------------------------------|
| Question#: | 25 |
| Topic: | Older Americans |
| Hearing: | COVID-19 Fraud: Law Enforcement's Response to Those Exploiting the Pandemic |
| Primary: | The Honorable Richard Blumenthal |
| Committee: | JUDICIARY (SENATE) |

Question: In Hawaii, more than 1 in 5 adults are age 60 or older. The FTC reported that as of June 4, 2020, Americans have lost at least \$46.17 million in COVID-19 related fraud. But those between ages 60 and 69 experienced the greatest amount of loss of any other age category, with \$5.67 million in loss.

Are you aware of any explanations for the higher levels of fraud loss among those age 60 and 69?

Response: Criminal networks have refined schemes for defrauding older Americans because they have proven to be highly susceptible targets. Seniors often have more available funds, such as retirement accounts, and are less likely to monitor their credit. They may also be more trusting online, more susceptible to phishing schemes, and less familiar with how to configure privacy controls on popular social media websites. Based on available data, it appears the percentage of COVID-19 related fraud victims among this age group is proportionate to non-COVID-19 related fraud schemes.

Question: What are currently the most common COVID-19 related scams used to specifically target older Americans, and what steps are you taking to prevent such fraud?

Response: Older Americans are being targeted with vaccine scams, religious or faith-based miracle cures, imposter scams to obtain Medicare identification numbers, fake work from home scams to enlist them as unwitting money mules, and phishing emails.

The Secret Service works with its law enforcement partners to aggressively investigate and prosecute fraudsters targeting seniors. The Secret Service, through its electronic fraud task forces, provides training and other outreach opportunities to educate seniors and other stakeholders on frauds and fraud prevention tips. The Secret Service is also working with Internet service providers to produce public service announcements to further educate the public on scams and prevention tips.

| | |
|-------------------|-----------------------------------------------------------------------------|
| Question#: | 26 |
| Topic: | Educate Public III |
| Hearing: | COVID-19 Fraud: Law Enforcement's Response to Those Exploiting the Pandemic |
| Primary: | The Honorable Richard Blumenthal |
| Committee: | JUDICIARY (SENATE) |

Question: One of the challenges in protecting older Americans from fraud is educating them about these scams. How, if at all, do you engage with community-based organizations and leaders to reach this vulnerable population?

Response: The Secret Service is currently working with Internet and TV service providers to distribute public service announcements to further educate the public on scams and prevention tips. Recently, Crime Support Network and Google published a website specifically focused on educating this population: <https://scamspotter.org/>.

COVID-19 Fraud: Law Enforcement's Response to Those Exploiting the Pandemic
Hearing before the Senate Committee on the Judiciary
Questions for the Record
June 9, 2020

QUESTIONS FROM SENATOR BLUMENTHAL

Questions for William Hughes

1. As discussed at the hearing, COVID-19 related fraud undermines those small businesses and households that desperately need help right now, blocking access to assistance set aside for them in the CARES Act. In your testimony, you said, "fraudsters are targeting the Payroll Protection Program, the Economic Impact Payment Program and its state unemployment benefit programs." Michael D'Ambrosio echoed this sentiment when he stated, "we have seen a surge in crimes targeting various economic relief programs, such as those provided by the CARES Act." It seems, therefore, that increased oversight and funding of the CARES Act would directly assist you in fighting these fraudulent schemes.
 - a. What increases in oversight mechanisms and other measures would enable you to protect the public from COVID-19 related fraud conducted by large businesses and foreign criminal actors?
 - b. How do Inspectors General help with your oversight and enforcement against fraud targeting relief programs? What lessons should we apply to the CARES Act?
 - c. Would harsher punishments and damages, similar to the False Claims Act, deter fraud and profiteering by large businesses and foreign criminal actors?
2. In your testimony, you said, "if you're talking just about CARES Act fraud, there is targeting the Payroll Protection Program by fraudsters, misrepresenting their small business, or the characteristics of their small business, or misrepresenting that there's a small business, at all." Whistleblowers, and whistleblower protections, are necessary in order to combat COVID-19 fraud. The CARES Act contained no anti-retaliation provisions, and did not establish any secure channels for whistleblowers to report fraud, waste, or abuse.
 - a. Do you agree that protecting whistleblowers will better enable the DOJ to bring cases against fraudulent claims related to the CARES Act, and help recover misused funds?
 - b. Have the DOJ or other agencies received whistleblower complaints during the COVID-19 crisis?

- c. What is the Department doing to encourage reporting by whistleblowers and to protect them?
3. Unfortunately, child exploitation has drastically increased since the onset of COVID-19, as predators have seen the pandemic as a perfect opportunity to harm children. As even kindergarten and elementary school classes go online, more kids are sitting in front of computers alone. In your joint written testimony, you and Craig Carpentino confirmed this grave truth, stating, “the Department is gravely concerned that COVID-19 is leading to a higher incidence of online child sexual exploitation, because both offenders and children are spending more time at home and online, and because the use of videoconference platforms has increased.

You echoed this pressing issue in the hearing, stating, “the pandemic has also changed the cyber threat landscape” as “child predators on the Internet see widespread closing of schools, stay-at-home orders and the reliance on Internet platforms, as the primary means of communication, as an opportunity to prey on children.” Additionally, at the hearing, Calvin Shivers stated, “in addition to fraud schemes, we are seeing crimes targeting our children. School closures have increased the presence of children, online. In addition, social distancing restrictions and the isolation of children at home may afford terminal actors with an opportunity to sexually exploit vulnerable children.”

Predators are seeing this national crisis as an opportunity. You and Carpentino made this very clear through your written testimony when you quoted an individual who posted on the Dark Web on March 21, 2020 saying, “is nobody seeing the bright side of this pandemic?? Schools are closed so kids are at home bored ... that means way more livestreams and its very clear moderators aren’t working right now since I’ve seen 3 hour streams go unbanned over the last few days where girls do whatever the f--- they want. What a time to be alive.”

- a. Do you agree that tech companies have to step up themselves to prevent and report online exploitation and abuse material on their platforms?
- b. Have the online platforms done enough during the Coronavirus pandemic to respond to this heightened risk and to stop online exploitation?

William Hughes
Associate Deputy Attorney General
United States Department of Justice
Questions for the Record
Submitted June 16, 2020

QUESTIONS FROM SENATOR BOOKER

1. Right now, there are no specific treatments for COVID-19 that have been scientifically validated. Despite this, there are some who are selling false hope to vulnerable people and overstating the success of possible treatments for the coronavirus. Not only are these types of fraud schemes taking advantage of the public's uncertainty surrounding the pandemic, but they are also spreading misinformation that ultimately hinders a cohesive national public health response. What steps has the Department of Justice taken to unequivocally denounce pseudo-scientific approaches to COVID-19 treatment?

**Written Questions from Senator Dick Durbin
Hearing on “COVID-19 Fraud: Law Enforcement’s Response to Those Exploiting the
Pandemic”
June 16, 2020**

For questions with subparts, please answer each subpart.

Questions for Associate Deputy Attorney General William Hughes

1. In your written testimony, you stated that “[t]he Criminal Division Fraud Section, working closely with the FBI and the Small Business Administration (SBA), has been focusing meaningful investigative efforts on fraud relating to the CARES Act’s Paycheck Protection Program (PPP).” But in your testimony you said that federal prosecutors have so far brought only six cases charging fraud in connection with PPP loan applications. The PPP authorizes up to \$659 billion taxpayer dollars in loans to businesses and other organizations, with nearly \$512 billion disbursed to date.
 - a. **How many attorneys in the Criminal Division Fraud Section are currently dedicated to “focusing meaningful investigative efforts on fraud relating to” PPP?**
 - b. **How many FBI employees are currently dedicated to “focusing meaningful investigative efforts on fraud relating to” PPP?**
 - c. **How many attorneys in U.S. Attorney’s Offices are currently dedicated to “focusing meaningful investigative efforts on fraud relating to” PPP?**
 - d. **Does each U.S. Attorney’s Office have one or more attorneys dedicated to “focusing meaningful investigative efforts on fraud relating to” PPP?**
 - e. **Has the Justice Department published guidance instructing whistleblowers with information about alleged PPP fraud on how to contact the Department?**
 - f. **Will you commit to provide this Committee with monthly updates on the number of cases brought charging fraud in connection with PPP loan applications and the dollar amounts of fraud alleged?**
2. On June 10, Treasury Secretary Mnuchin and SBA Administrator Carranza declined to publicly release the names of PPP loan recipients and the amounts they borrowed. Secretary Mnuchin said “we believe that that’s proprietary information.” This refusal to disclose this information to Congress comes despite the SBA reportedly telling the Washington Post on April 16 that the SBA “intend[s] to post individual loan data in accordance with the information presently on the SBA.gov website after the loan process has been completed.”

- a. **Please explain the process by which individual PPP loan data is shared between SBA, FBI, and DOJ.**
 - b. **Do the Department of Justice Attorneys working on investigative efforts on fraud relating to the PPP have full access to all the individual loan data under PPP?**
 - c. **Do any Inspectors General have full access to all the individual loan data under PPP? If so, which IGs have such access?**
 - d. **Do State Attorneys General working in cooperation with the Justice Department on anti-fraud task forces have full access to all the individual loan data under PPP? If not, why not?**
 - e. **Do you believe that efforts to identify and prosecute fraud in the \$659 billion PPP program would be enhanced if individual loan data were made transparent, as SBA had pledged on April 16 to do?**
 - f. **Does the lack of public transparency for PPP loan data help to explain why there have been so few cases brought so far charging fraud in connection with PPP loan applications?**
3. As part of the CARES Act, Congress created a Pandemic Response Accountability Committee composed of federal Inspectors General to prevent and detect fraud, waste, abuse and mismanagement in the federal stimulus programs.

Initially, Acting Department of Defense Inspector General Glenn Fine was tasked to lead this Accountability Committee. But shortly after his appointment, President Trump replaced Mr. Fine as well as two other IGs who were on the Committee, Acting HHS IG Christi Grimm and Acting Department of Transportation IG Michael Behm. This was part of the President's purge of Inspectors General that has seen him remove five IGs or Acting IGs since April. The President's only explanation was that he lost confidence in these IGs, several of whom were investigating sensitive matters involving the President's allies.

- a. **Do Inspectors General offices play an important role in helping to combat waste, fraud, and abuse in federal programs?**
 - b. **Are efforts to combat fraud well-served when respected, neutral IGs like Glenn Fine are summarily dismissed from service?**
4. Former Justice Department Inspector General Michael Bromwich said of the President's purge of Inspectors General, "It really is kind of a reign of terror that is unleashed for the IG community and at a time when their oversight is more needed and more necessary than frankly any time that I can remember."

Will efforts to prevent fraud in COVID-19 relief programs be hindered if IG offices are afraid to pursue investigations that might antagonize the President?

**Hearing on COVID-19 Fraud: Law Enforcement's
Response to Those Exploiting the Pandemic**

**Questions for the Record
June 16, 2020**

QUESTIONS FROM SENATOR FEINSTEIN

Questions for Mr. Hughes

1. During the hearing, there were discussions of a foreign fraud ring known as “Scattered Canary” using personal information, likely obtained through prior consumer data breaches, to fraudulently obtain hundreds of millions of dollars in unemployment benefits from state governments.

This criminal scheme deprived states of the resources Congress provided them through the CARES Act. Worse, it delays the release of benefits to state residents who desperately need it as the states try to halt this fraud.

- a. **Is this, and any similar incidents, being treated as a criminal conspiracy rather than an isolated incident(s)?**
 - b. **What is the Department of Justice doing to prosecute the Scattered Canary group and its affiliates who are running this unemployment insurance scam?**
 - c. **More generally, has the Department seen any similar schemes, and what is being done to detect and prevent this?**
 - d. **How many individuals has the Department of Justice charged for fraud in connection with applications for unemployment insurance? How many of these individuals were part of a broader conspiracy? Have any pleaded guilty or been convicted? (If so, how many?)**
2. On March 27, 2020, the CARES Act was signed into law. It provided \$2 trillion in vital economic relief related to the COVID-19 pandemic. Under that Act, Congress created two new inspector general roles: a Special Inspector General for Pandemic Recovery; and the Pandemic Response Accountability Committee, to be chaired by an existing inspector general.
 - a. **How could inspectors general augment the work that your agency is doing to identify and root out fraud and abuse?**
 - b. **What other mechanisms might Congress put into place to assist with oversight and fraud prevention?**

3. The Paycheck Protection Program (PPP), established under the CARES Act and administered by the Small Business Administration (SBA), has issued nearly 4.3 million loans since its creation. The SBA has posted on its website a “frequently asked questions” document indicating that it has decided to treat “faith-based” non-profits differently than all other non-profits in its implementation of the PPP program. [Small Business Administration, FAQs for Faith-Based Organizations, 4/3/20] Specifically, the SBA appears to have decided to waive its “affiliation rules” for faith-based non-profits. These “affiliation rules” ensure that SBA benefits are provided to small entities, not those affiliated with larger organizations. The SBA waiver appears to apply to faith-based non-profits that provide “no secular services” and those that exclusively serve their “own members or co-religionists.”
 - a. **Has the Department of Justice been told not to investigate potential fraud in the provision of PPP funds to faith-based organizations? If so, who provided that direction and what was the Justice Department told?**
 - b. **Are the affiliation rules being waived for faith-based non-profits?**
 - c. **How does the Justice Department determine whether an entity qualifies as “faith-based”?**
 - d. **Does this waiver rule apply even to faith-based non-profits that provide no secular services – in other words, that provide religious services only to their “own members or co-religionists” only?**
4. There are recent reports that the Small Business Administration has demanded that eligible Planned Parenthood organizations who were awarded these loans immediately return the money.
 - a. **What are the specific grounds for demanding return of these loans?**
 - b. **Has this criteria been applied to any other organizations? If so, please provide specific examples where other fund recipients have been treated the same as Planned Parenthood.**
 - c. **Of the 4.3 million Paycheck Protection Program loans awarded under the CARES Act, how many nonprofit organizations has the Attorney General singled out for investigation?**
5. In March, the President instructed states that they would have to bear the responsibility of getting necessary protective equipment (masks, gloves, protective gowns) and medical equipment (such as ventilators) themselves.

State and local governments responded by trying to directly purchase equipment, but it was reported that the FBI, on behalf of the Federal Emergency Management Agency, has intercepted and seized much-needed equipment, invoking the anti-hoarding provision of

the Defense Production Act (50 U.S.C. § 4512). That provision prohibits the accumulation of scarce or threatened materials “(1) in excess of the reasonable demands of business, personal, or home consumption, or (2) for the purpose of resale at prices in excess of prevailing market prices.”

For example, there were reports in May about the seizure of 500,000 N95 masks from a small medical-equipment supplier who had contracts to deliver the protective equipment to fire departments, nursing homes, and emergency medical technician departments.

- a. **What is the rationale for seizing supplies ordered directly by states?**
 - b. **How does the Department of Justice, including the FBI, determine whether the accumulation of scarce or threatened materials is in excess of the reasonable demands of business, personal, or home consumption or being resold at prices in excess of the prevailing market price?**
 - c. **Are specific, factual criteria applied to make these determinations?**
 - d. **If so, what is it, and how was it formulated?**
 - e. **If an order is going to a state or local government entity, shouldn't the presumption be against seizing it unless it's clearly part of an unlawful hoarding effort?**
 - f. **Uncertainty about available supplies, including whether or not they would be intercepted, can actually create opportunities for hoarding and price gouging. What is federal law enforcement doing to help states and local governments avoid seizure of their orders and get supplies?**
6. It has been reported that masks purchased by the California-based Movement for Black Lives Matter were temporarily “seized by law enforcement.” These masks were purchased to be used by individuals protesting the police killing of George Floyd—in an effort to protect these protestors from coronavirus infection.
- a. **Is the Department of Justice aware of this reported seizure of face masks?**
 - b. **Is the Department of Justice doing to investigate the seizure of these masks? If not, why not? If so, what steps has it taken to date? Please be specific.**
 - c. **These particular masks reportedly had the message “stop killing black people” on them. Did the message on the mask play any role in their seizure? (If the answer is “no,” please explain how you determined that was the case.)**
 - d. **What is the Department of Justice doing to make sure a seizure like this doesn't happen again?**

7. Under a program set up by the White House called “Project Airbridge,” the government was spending millions of dollars to deliver medical supplies on behalf of six major corporations in exchange for control over where some of the supplies would be delivered.

No information was given to the public—including state and local governments desperate for supplies—about how many supplies were actually delivered or where they were all sent. There are also reports that because of Project Airbridge, the government either cancelled or rerouted medical supply purchased directly by state and local governments.

- a. **Have you investigated any aspect of Project Airbridge?**
- b. **What can the Department of Justice do to ensure programs like Project Airbridge are administered fairly to companies and people selling equipment and supplies and to the states and local governments trying to purchase them?**
- c. **Would the Pandemic Response Accountability Committee, created under the CARES Act, be able to help identify any fraudulent distribution of pandemic funds or supplies?**
- d. **In your view, what can the federal government do to help identify legitimate, non-fraudulent supply sources (including reliable tests for COVID-19 and personal protective equipment)?**

8. There are reports that doctors were prescribing massive amounts of hydroxychloroquine, a drug with no confirmed benefits for people suffering from COVID-19, for themselves and others after the President repeatedly touted it as a treatment.

As a result, patients with lupus who actually need this medicine had to wait while their refills were on back order or were provided smaller amounts of the drug than usual.

- a. **What is the Department of Justice doing to prevent the hoarding of hydroxychloroquine at the expense of patients who need it?**

9. The Centers for Disease Control and Prevention recently announced that there is no antibody test that is reliable enough to serve as a basis for federal, state, or local leaders to make coronavirus-related policy decisions, yet a number of companies have advertised their antibody tests as accurate and reliable.

Unfortunately, because so many tests for COVID have been defective, the Food and Drug Administration (FDA) recently reversed its prior policy allowing these tests to be released to the market without prior FDA emergency review.

- a. **What is the Department of Justice doing to prevent fraud in the antibody testing market?**

- b. What criminal or civil options are available to protect people who purchase defective antibody tests marketed as reliable and effective?**
- c. Does the FDA's prior policy affect the Department of Justice's use of these options for any fraudulent antibody tests sold under the old policy?**

**WRITTEN QUESTIONS OF SENATOR CHUCK GRASSLEY FOR
SENATE JUDICIARY COMMITTEE HEARING “COVID-19
FRAUD: LAW ENFORCEMENT’S RESPONSE TO THOSE
EXPLOITING THE PANDEMIC”, JUNE 9, 2020**

Questions for William Hughes

1. What difficulties or obstacles has law enforcement encountered when investigating and prosecuting cases against those who seek to exploit the COVID-19 pandemic?
2. Does law enforcement have all the tools and authorities it needs to go after COVID-19 related scams, hoarding, price gouging and other fraudulent schemes?
3. In your opinion, would a federal price gouging statute help you pursue bad actors? If so, what would you like to see in a federal price gouging statute?
4. Do you believe that existing penalties for price gouging are tough enough? What about penalties for scams and fraudulent activity related to the CARES Act Paycheck Protection Program and unemployment benefits – are they adequate or should they be strengthened?
5. What kind of legislation would you like to see Congress enact to assist you in your investigations and prosecutions of these cases? What more can we do to help prevent fraudsters and other criminals from taking advantage of Americans during the pandemic?
6. Earlier this year, China halted exports of medical supplies—including PPEs—in response to the COVID-19 pandemic. This decision caused a cascade effect around the world, where PPEs became impossible to find. In the U.S., we’ve seen shortages of medical supplies at least since February. I’m interested in developing a timeline here. At what point did the Justice Department begin to identify cases of COVID-19-related fraudulent activity? Did these cases significantly increase at any point in time?
7. It’s important that Americans know how they are at risk of falling victim to scams. What specifically is the Justice Department doing to alert and educate consumers and businesses about the different kinds of dangerous fraudulent schemes that exist during this pandemic and how to protect themselves?

8.What is the Justice Department specifically doing to ensure that hospitals are not being defrauded and sold fake PPE or other vital medical supplies?

9.What is the Justice Department doing to ensure that consumers and businesses can easily and efficiently provide you with information and file complaints should they fall victim to scams?

10.Could you please elaborate on the increase in cybercrime? What is the Justice Department doing to educate the average American on how they can prevent the spread of malware and other tools that compromise our ability to work safely from home during these times?

11.The Justice Department is using various technologies to identify and investigate fraud related to state issuance of unemployment benefits. Do states have access to these same technologies? If not, why not? Are there barriers that states report facing that keep them from guarding against fraud, or in responding to fraud that you have identified?

**Questions for William Hughes
From Senator Mazie Hirono**

1. Registrations for COVID-related internet domains have skyrocketed since the outbreak of the pandemic. Studies have shown that many of these domains are being used to steal people's identities, install malware on people's computers, or commit fraud.

In April, I sent letters to a number of domain name registrars to understand what they were doing to combat this illegal activity. The responses I received were mixed. Several registrars are taking no proactive measures to ensure the domain names they register are not used for illegal purposes.

Shortly after I sent my letter, I was pleased to see the Justice Department announce that it had disrupted hundreds of domains involved in COVID-related scams.

- a. **What degree of cooperation did the Justice Department receive from domain name registrars, hosts, and other online service providers in this operation?**
 - b. **I've seen reports that the Justice Department and FBI have had trouble finding out who owns fraudulent domain names since Europe implemented its General Data Protection Regulation. Is this true? And, if so, what has the impact been on criminal investigations—particularly those involving COVID-related scams?**
 - c. **As I mentioned, several domain name registrars told me they take no action to proactively investigate companies that register domain names. They said they feared doing so would put them at risk of civil liability for copyright infringement under the Digital Millennium Copyright Act. What are the impacts of laws like the DMCA and Section 230 of the Communications Decency Act on the spread of criminal activity on the internet?**
 - d. **Are there legislative changes we should be considering to push online service providers to take a more active role in preventing or policing crime on the internet?**
2. Customs and Border Protection has seized massive quantities of counterfeit or unapproved COVID-related products at the border, including over 100,000 FDA-prohibited test kits; over 750,000 counterfeit face masks; and over 11,000 FDA-prohibited chloroquine tablets.
 - a. **While it is certainly important to seize these products before they can hurt any Americans, it is perhaps more important to trace the shipments back to their sources so they can be shut down. Are the Justice Department and FBI actively working with CBP to investigate the sellers of these products?**
 - b. **What countries are these products coming from?**
 - c. **Who are the shipments going to? Are these being shipped directly to consumers who made online purchases? Or are they going to U.S. business and infecting the supply chain? Or is it something else entirely?**

3. In Hawaii, more than 1 in 5 adults are age 60 or older. The FTC reported that as of June 4, 2020, Americans have lost at least \$46.17 million in COVID-19 related fraud. But those between ages 60 and 69 experienced the greatest amount of loss of any other age category, with \$5.67 million in loss.
 - a. **Are you aware of any explanations for the higher levels of fraud loss among those age 60 and 69?**
 - b. **What are currently the most common COVID-19 related scams used to specifically target older Americans, and what steps are you taking to prevent such fraud?**
 - c. **One of the challenges in protecting older Americans from fraud is educating them about these scams. How, if at all, do you engage with community-based organizations and leaders to reach this vulnerable population?**

Senate Judiciary Committee
“COVID-19 Fraud: Law Enforcement’s Response to Those Exploiting the Pandemic”
Questions for the Record
June 9, 2020
Senator Amy Klobuchar

Questions for Associate Deputy Attorney General William Hughes

Reports have highlighted that scams targeting seniors have increased during the current pandemic. I introduced legislation with Senator Moran to direct the Federal Trade Commission to report to Congress on these scams and make recommendations on how to prevent future scams during emergencies.

- In your view, could law enforcement efforts to combat fraudulent behavior targeting seniors during future national crises be helped by gathering additional information about what is happening to seniors during this pandemic?
- The Justice Department already has broad authority take criminal or civil action against those perpetrating frauds targeting senior citizens. What specifically is the Department doing to deter scammers from targeting seniors during the coronavirus pandemic?
- Since the start of the pandemic, how many investigations and how many criminal or civil actions has the Department brought against those who have targeted fraudulent schemes at senior citizens?

Mr. Hughes:

1. Seniors are especially vulnerable to fraud right now. That is why I've sent multiple letters highlighting the need for additional legal services for seniors through the senior legal hotline, and the need for the FTC to increase awareness about fraud. What is the DOJ doing to protect seniors during this pandemic?
2. At DOJ there is an IP task force, a China task force task force and a COVID taskforce. What is the difference between these three task forces? Do they all report to the same person?
3. Which taskforce is responsible for COVID related intellectual property theft by Chinese hackers or counterfeit PPE shipped from China?
4. What legal authority does CBP agents currently have to seize counterfeit items related to COVID-19 that do not have an infringing trademark on the item? Is this authority sufficient to stop these items at the boarder?

5. I sent a letter with Senators Cornyn and Blackburn last month asking for DOJ and DHS to brief our staff on the risk of counterfeit medical supplies and PPE to American consumers. When can we expect you to provide that briefing?

**Full Committee Hearing: COVID 19 Fraud: Law Enforcement's Response to Those
Exploiting the Pandemic
Questions for the Record
June 9, 2020**

QUESTIONS FROM SENATOR SHELDON WHITEHOUSE

Associate Deputy Attorney General Hughes:

1. We know that criminals and kleptocrats use U.S. shell companies - sham companies that have no actual business operations- to launder ill-gotten criminal proceeds. However, criminals also use shell companies in schemes to defraud Medicaid and other government programs and steal millions of dollars of taxpayer money. I have worked with Chairman Graham, Senator Grassley, and Ranking Member Feinstein on a bill that would require many companies to disclose their beneficial owners, to help law enforcement see through shell companies.
 - a. Is it likely that shell companies are being used to defraud COVID relief programs?
 - b. For example, is there evidence that criminals are using shell companies to obtain PPP loans fraudulently?
 - c. Do you have a current estimate of how much COVID relief money has been lost in fraud schemes?
 - d. Is it likely that criminals who perpetrate COVID-related fraud will use shell companies to launder their ill-gotten money?
 - e. Explain the difficulties that shell companies pose to law enforcement trying to "follow the money"?
 - f. Would having a beneficial ownership register that law enforcement could access help detect and prevent fraud and make sure taxpayer money is going to businesses and workers rather than criminals?
2. Cybercriminals and other malicious actors are exploiting COVID-19 to launch cyberattacks, using the virus to induce people to expose themselves to malware and phishing schemes. For example, the new "Silent Night Zeus" bot has been deployed in scams ranging from emails promising COVID-19 financial relief to attacks against banks, and is able to log keystrokes to see what people are typing, take pictures of people's screens, and harvest passwords. On April 18, the FBI Deputy Assistant Director Tonya Ugoretz reported that the FBI has received quadruple the number of cybercrime reports compared to months before the pandemic.
 - a. What steps is DOJ taking to educate the public about COVID-related cyber-crime?
 - b. How are bots being used in fraud schemes?
 - c. How frequently is DOJ encountering bots as you investigate COVID fraud schemes?
 - d. Do you have an estimate on the damage bot-schemes have caused?

COVID-19 Fraud: Law Enforcement's Response to Those Exploiting the Pandemic
Hearing before the Senate Committee on the Judiciary
Questions for the Record
June 9, 2020

QUESTIONS FROM SENATOR BLUMENTHAL

Questions for Calvin A. Shivers

1. As discussed at the hearing, COVID-19 related fraud undermines those small businesses and households that desperately need help right now, blocking access to assistance set aside for them in the CARES Act. In his testimony, William Hughes said, "fraudsters are targeting the Payroll Protection Program, the Economic Impact Payment Program and its state unemployment benefit programs." Michael D'Ambrosio echoed this sentiment when he stated, "we have seen a surge in crimes targeting various economic relief programs, such as those provided by the CARES Act." It seems, therefore, that increased oversight and funding of the CARES Act would directly assist you in fighting these fraudulent schemes.
 - a. What increases in oversight mechanisms and other measures would enable you to protect the public from COVID-19 related fraud conducted by large businesses and foreign criminal actors?
 - b. How do Inspectors General help with your oversight and enforcement against fraud targeting relief programs? What lessons should we apply to the CARES Act?
 - c. Would harsher punishments and damages, similar to the False Claims Act, deter fraud and profiteering by large businesses and foreign criminal actors?
2. Unfortunately, child exploitation has drastically increased since the onset of COVID-19, as predators have seen the pandemic as a perfect opportunity to harm children. As even kindergarten and elementary school classes go online, more kids are sitting in front of computers alone. In their joint written testimony, William Hughes and Craig Carpentino confirmed this grave truth, stating, "the Department is gravely concerned that COVID-19 is leading to a higher incidence of online child sexual exploitation, because both offenders and children are spending more time at home and online, and because the use of videoconference platforms has increased.

Hughes echoed this pressing issue in the hearing, stating, "the pandemic has also changed the cyber threat landscape" as "child predators on the Internet see widespread closing of schools, stay-at-home orders and the reliance on Internet platforms, as the primary means of communication, as an opportunity to prey on children." Additionally, at the hearing, you stated, "in addition to fraud schemes, we are seeing crimes targeting our children. School closures have increased the presence of children, online. In addition, social distancing restrictions and the

isolation of children at home may afford terminal actors with an opportunity to sexually exploit vulnerable children.”

Predators are seeing this national crisis as an opportunity. Hughes and Carpentino made this very clear through their written testimony when they quoted an individual who posted on the Dark Web on March 21, 2020 saying, “is nobody seeing the bright side of this pandemic?? Schools are closed so kids are at home bored ... that means way more livestreams and its very clear moderators aren’t working right now since I’ve seen 3 hour streams go unbanned over the last few days where girls do whatever the f--- they want. What a time to be alive.”

- a. Do you agree that tech companies have to step up themselves to prevent and report online exploitation and abuse material on their platforms?
- b. Have the online platforms done enough during the Coronavirus pandemic to respond to this heightened risk and to stop online exploitation?

Calvin Shivers
Assistant Director
Federal Bureau of Investigation
Questions for the Record
Submitted June 16, 2020

QUESTIONS FROM SENATOR BOOKER

1. Although the FBI has issued warnings against providing personal information to scammers, what steps has the FBI taken to detect fraudulent claims after the fact?
2. The CARES Act was passed to provide stimulus relief to Americans dealing with the economic implications of a nation-wide shutdown. Fraudsters are taking advantage of this policy and several transnational cybercriminal organizations, like the Scattered Canary Group, have been identified to illegitimately receive Economic Impact Payments.¹ How is the FBI coordinating with the IRS to oversee whether Economic Impact Payments are being sent to known cybercriminal organizations?

¹ Emma Woollacott, *African Cybercriminals Net Millions in Fraudulent COVID-19 Government Claims*, FORBES (May 20, 2020), <https://www.forbes.com/sites/emmawoollacott/2020/05/20/african-cybercriminals-net-millions-in-fraudulent-covid-19-government-claims/#471eb9b7944f>.

**Hearing on COVID-19 Fraud: Law Enforcement's
Response to Those Exploiting the Pandemic**

**Questions for the Record
June 16, 2020**

QUESTIONS FROM SENATOR FEINSTEIN

Questions for Mr. Shivers

1. During the hearing, there were discussions of a foreign fraud ring known as “Scattered Canary” using personal information, likely obtained through prior consumer data breaches, to fraudulently obtain hundreds of millions of dollars in unemployment benefits from state governments.

This criminal scheme deprived states of the resources Congress provided them through the CARES Act. Worse, it delays the release of benefits to state residents who desperately need it as the states try to halt this fraud.

- a. **What is the FBI doing to stop the Scattered Canary group and its unemployment insurance scam? Is the FBI treating this as a criminal conspiracy rather than an isolated incident?**
 - b. **More generally, has the FBI seen any similar schemes, and what is being done to detect and prevent this?**
 - c. **What information is the FBI providing to states to protect them from scams like those perpetrated by Scattered Canary, and under what circumstances does it provide that information? Please be specific as to the timing and modalities of information sharing.**
 - d. **What policies, practices, or procedures does the FBI have in place to ensure that specific, actionable information is provided to state and local government entities before they are victimized by scammers like the Scattered Canary group, particularly, but not limited to when the threat in question is under investigation by the FBI?**
2. Bad actors are marketing fake cures for COVID-19. For example, in April, federal prosecutors charged a California doctor with fraud after he emailed advertisements for “COVID-19 treatment packs.” The doctor said the packs could immunize customers from the coronavirus after six weeks and were a “100%” cure the virus. He charged \$3,995. (DOJ Press Release, April 16, 2020)
 - a. **What is the FBI doing to stop the spread of fake cures?**

- b. This doctor was brought to the attention of the FBI through a tip from the public. What is the FBI doing to ensure that these fake COVID-19 cure creators and their advertisements are quickly identified and stopped?**
- 3. It has been reported that masks purchased by the California-based Movement for Black Lives Matter were temporarily “seized by law enforcement.” These masks were purchased to be used by individuals protesting the police killing of George Floyd – in an effort to protect these protestors from coronavirus infection.
 - a. Is the FBI aware of this reported seizure of face masks?**
 - b. Does the FBI work with the U.S. Postal Service to seize materials in transit?**
 - c. If so, who makes the decision on the seizure, and what are the criteria?**
 - d. These particular masks reportedly had the message “stop killing black people” on them. Did the message on the mask play any role in any seizure? (If the answer is “no,” please explain how you determined that was the case.)**
- 4. In March, the President instructed states that they would have to bear the responsibility of getting necessary protective equipment (masks, gloves, protective gowns) and medical equipment (such as ventilators) themselves.

State and local governments responded by trying to directly purchase equipment, but it was reported that the FBI, on behalf of the Federal Emergency Management Agency, has intercepted and seized much-needed equipment, invoking the anti-hoarding provision of the Defense Production Act (50 U.S.C. § 4512). That provision prohibits the accumulation of scarce or threatened materials “(1) in excess of the reasonable demands of business, personal, or home consumption, or (2) for the purpose of resale at prices in excess of prevailing market prices.”

For example, there were reports in May about the seizure of 500,000 N95 masks from a small medical-equipment supplier who had contracts to deliver the protective equipment to fire departments, nursing homes, and emergency medical technician departments.

- a. What is the rationale for seizing supplies ordered directly by states?**
- b. How do you determine whether the accumulation of scarce or threatened materials is in excess of the reasonable demands of business, personal, or home consumption or being resold at prices in excess of the prevailing market price?**
- c. Do you apply specific, factual criteria to make these determinations?**
- d. If so, what is it, and how did you formulate it?**

- e. If an order is going to a state or local government entity, shouldn't the presumption be against seizing it unless it's clearly part of an unlawful hoarding effort?
- f. Uncertainty about available supplies, including whether or not they would be intercepted, can actually create opportunities for hoarding and price gouging. What is federal law enforcement doing to help states and local governments avoid seizure of orders and get supplies?

QUESTIONS FOR THE RECORD

For Calvin Shivers (FBI):

- A recent FBI / CISA joint announcement raised awareness about Chinese-affiliated criminals targeting U.S. healthcare organizations. Specifically, research outfits working on critical COVID-response matters like vaccines, treatments, and testing.
 - What is the FBI doing to ensure foreign actors, like the Chinese, do not inhibit the U.S. healthcare sector's pandemic response?

**WRITTEN QUESTIONS OF SENATOR CHUCK GRASSLEY FOR
SENATE JUDICIARY COMMITTEE HEARING “COVID-19
FRAUD: LAW ENFORCEMENT’S RESPONSE TO THOSE
EXPLOITING THE PANDEMIC”, JUNE 9, 2020**

Questions for Calvin Shivers

1. What difficulties or obstacles has law enforcement encountered when investigating and prosecuting cases against those who seek to exploit the COVID-19 pandemic?
2. Does law enforcement have all the tools and authorities it needs to go after COVID-19 related scams, hoarding, price gouging and other fraudulent schemes?
3. In your opinion, would a federal price gouging statute help you pursue bad actors? If so, what would you like to see in a federal price gouging statute?
4. Do you believe that existing penalties for price gouging are tough enough? What about penalties for scams and fraudulent activity related to the CARES Act Paycheck Protection Program and unemployment benefits – are they adequate or should they be strengthened?
5. What kind of legislation would you like to see Congress enact to assist you in your investigations and prosecutions of these cases? What more can we do to help prevent fraudsters and other criminals from taking advantage of Americans during the pandemic?
6. Earlier this year, China halted exports of medical supplies—including PPEs—in response to the COVID-19 pandemic. This decision caused a cascade effect around the world, where PPEs became impossible to find. In the U.S., we’ve seen shortages of medical supplies at least since February. I’m interested in developing a timeline here. At what point did the FBI begin to identify cases of COVID-19-related fraudulent activity? Did these cases significantly increase at any point in time?
7. It’s important that Americans know how they are at risk of falling victim to scams. What specifically is the FBI doing to alert and educate consumers and businesses about the different kinds of dangerous fraudulent schemes that exist during this pandemic and how to protect themselves?

8.What is the FBI specifically doing to ensure that hospitals are not being defrauded and sold fake PPE or other vital medical supplies?

9.What is the FBI doing to ensure that consumers and businesses can easily and efficiently provide you with information and file complaints should they fall victim to scams?

10.Could you please elaborate on the increase in cybercrime? What is the FBI doing to educate the average American on how they can prevent the spread of malware and other tools that compromise our ability to work safely from home during these times?

11.Based on my understanding, the FBI is a member of Operation Stolen Promise. Can you tell us what the FBI's role is and how it is collaborating with its interagency partners and field offices to prevent COVID-19-related fraud?

12.The FBI is using various technologies to identify and investigate fraud related to state issuance of unemployment benefits. Do states have access to these same technologies? If not, why not? Are there barriers that states report facing that keep them from guarding against fraud, or in responding to fraud that you have identified?

**Questions for Calvin A. Shivers
From Senator Mazie Hirono**

1. Registrations for COVID-related internet domains have skyrocketed since the outbreak of the pandemic. Studies have shown that many of these domains are being used to steal people's identities, install malware on people's computers, or commit fraud.

In April, I sent letters to a number of domain name registrars to understand what they were doing to combat this illegal activity. The responses I received were mixed. Several registrars are taking no proactive measures to ensure the domain names they register are not used for illegal purposes.

Shortly after I sent my letter, I was pleased to see the Justice Department announce that it had disrupted hundreds of domains involved in COVID-related scams.

- a. **What degree of cooperation did the FBI receive from domain name registrars, hosts, and other online service providers in this operation?**
 - b. **I've seen reports that the Justice Department and FBI have had trouble finding out who owns fraudulent domain names since Europe implemented its General Data Protection Regulation. Is this true? And, if so, what has the impact been on criminal investigations—particularly those involving COVID-related scams?**
 - c. **As I mentioned, several domain name registrars told me they take no action to proactively investigate companies that register domain names. They said they feared doing so would put them at risk of civil liability for copyright infringement under the Digital Millennium Copyright Act. What are the impacts of laws like the DMCA and Section 230 of the Communications Decency Act on the spread of criminal activity on the internet?**
 - d. **Are there legislative changes we should be considering to push online service providers to take a more active role in preventing or policing crime on the internet?**
2. Customs and Border Protection has seized massive quantities of counterfeit or unapproved COVID-related products at the border, including over 100,000 FDA-prohibited test kits; over 750,000 counterfeit face masks; and over 11,000 FDA-prohibited chloroquine tablets.
 - a. **While it is certainly important to seize these products before they can hurt any Americans, it is perhaps more important to trace the shipments back to their sources so they can be shut down. Are the Justice Department and FBI actively working with CBP to investigate the sellers of these products?**
 - b. **What countries are these products coming from?**
 - c. **Who are the shipments going to? Are these being shipped directly to consumers who made online purchases? Or are they going to U.S. business and infecting the supply chain? Or is it something else entirely?**

3. In Hawaii, more than 1 in 5 adults are age 60 or older. The FTC reported that as of June 4, 2020, Americans have lost at least \$46.17 million in COVID-19 related fraud. But those between ages 60 and 69 experienced the greatest amount of loss of any other age category, with \$5.67 million in loss.
 - a. **Are you aware of any explanations for the higher levels of fraud loss among those age 60 and 69?**
 - b. **What are currently the most common COVID-19 related scams used to specifically target older Americans, and what steps are you taking to prevent such fraud?**
 - c. **One of the challenges in protecting older Americans from fraud is educating them about these scams. How, if at all, do you engage with community-based organizations and leaders to reach this vulnerable population?**

Senate Judiciary Committee
“COVID-19 Fraud: Law Enforcement’s Response to Those Exploiting the Pandemic”
Questions for the Record
June 9, 2020
Senator Amy Klobuchar

Questions for FBI Assistant Director Calvin Shivers and Secret Service Assistant Director Michael D’Ambrosio

Your testimony reflects the striking number and variety of coronavirus-related frauds being inflicted on the American public.

- What are the most significant challenges that your agency faces in detecting illegal fraudulent schemes during this pandemic?
- If you had additional resources, how would you employ them to improve fraud detection?

**Written Questions for Calvin Shivers
Submitted by Senator Leahy
June 16, 2020**

1. Amid the COVID-19 pandemic there has been a wave of scams related to healthcare products and services, including the sale of fake test kits, treatments, and cures. I am concerned that these schemes will only become more prevalent as the disease continues to impact more people, and the demand for test kits and treatments becomes greater.
 - a. **What is the FBI doing to eradicate these schemes and protect Americans from unknowingly purchasing fake testing or treatment products?**
 - b. **Is the FBI working with retail or ecommerce companies to stop the sale of fake or mislabeled testing and treatment products? What have these companies been doing to address this problem?**
2. As workplaces, schools, and social gatherings remain restricted across the country, Americans have relied on the internet more in the past several months than ever before. This has only increased Americans' exposure to cybersecurity threats and online exploitation, especially for children and the elderly.
 - a. **Have you observed an increase in attempted or successful data breaches during the COVID-19 pandemic?**
 - b. **Would federal cybersecurity requirements help reduce or prevent future recurrence of threats we have faced during this pandemic? Please explain.**
 - c. **In what ways has the FBI worked with internet companies to increase protections against exploitation and PII theft for vulnerable populations? What measures are these companies taking in response to the spike in cybercrime? In your view, what else should internet companies be doing?**

Mr. Shivers:

1. What the most common counterfeit items you are seeing related to the COVID pandemic? We are all hopeful that at home rapid test kits will be available soon and eventually a vaccine. What is the risk to public safety of these counterfeit items?
2. Are you working with any private retailers—such as Amazon—to identify and intercept counterfeit COVID supplies?
3. I believe the FBI has imbedded agents at the Intellectual Property Rights Center at DHS. Can you discuss the importance of the IPR center in gathering and intercepting counterfeit goods?

**Full Committee Hearing: COVID 19 Fraud: Law Enforcement's Response to Those
Exploiting the Pandemic
Questions for the Record
June 9, 2020**

QUESTIONS FROM SENATOR SHELDON WHITEHOUSE

Assistant Director Shivers:

1. We know that criminals and kleptocrats use U.S. shell companies - sham companies that have no actual business operations- to launder ill-gotten criminal proceeds. However, criminals also use shell companies in schemes to defraud Medicaid and other government programs and steal millions of dollars of taxpayer money. I have worked with Chairman Graham, Senator Grassley, and Ranking Member Feinstein on a bill that would require many companies to disclose their beneficial owners, to help law enforcement see through shell companies.
 - a. Explain the difficulties that shell companies pose to law enforcement trying to detect and prevent fraud and "following the money" trying locate criminal proceeds.
 - b. Would having a beneficial ownership register that law enforcement could access help detect and prevent fraud and make sure taxpayer money is going to businesses and workers rather than criminals?
2. Cybercriminals and other malicious actors are exploiting COVID-19 to launch cyberattacks, using the virus to induce people to expose themselves to malware and phishing schemes. For example, the new "Silent Night Zeus" bot has been deployed in scams ranging from emails promising COVID-19 financial relief to attacks against banks, and is able to log keystrokes to see what people are typing, take pictures of people's screens, and harvest passwords. On April 18, the FBI Deputy Assistant Director Tonya Ugoretz reported that the FBI has received quadruple the number of cybercrime reports compared to months before the pandemic.
 - a. What steps is the FBI taking to educate the public about COVID-related cyber-crime?
 - b. How are bots being used in fraud schemes?
 - c. How frequently is the FBI encountering bots as it investigates COVID fraud schemes?
 - d. Do you have an estimate on the damage bot-schemes have caused?