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 (GIOC) 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 is 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 loses 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/.