U.S. Immigration and Customs Enforcement

TESTIMONY OF

STEVE FRANCIS
ASSISTANT DIRECTOR FOR GLOBAL TRADE INVESTIGATIONS DIVISION AND
DIRECTOR OF
THE NATIONAL INTELLECTUAL PROPERTY RIGHTS COORDINATION CENTER

HOMELAND SECURITY INVESTIGATIONS
U.S. IMMIGRATION AND CUSTOMS ENFORCEMENT
U.S. DEPARTMENT OF HOMELAND SECURITY

REGARDING

"Part I: Oversight of the Administration's Effort to Protect the Integrity of Our Nation's Medical Supply Chain."

BEFORE THE

UNITED STATES SENATE
COMMITTEE ON FINANCE

TUESDAY, JULY 28, 2020
10:15 AM
215 DIRKSEN SENATE OFFICE BUILDING

INTRODUCTION

Chairman Grassley, Ranking Member Wyden, and distinguished members of the Committee.

Thank you for the opportunity to testify before the committee on U.S. Immigration and Customs Enforcement (ICE) Homeland Security Investigations (HSI) response to those exploiting the Coronavirus Disease 2019 (COVID-19) pandemic.

As the largest investigative agency within the U.S. Department of Homeland Security (DHS), HSI investigates and enforces more than 400 federal criminal statutes, including the U.S. customs laws under Title 19 of the United States Code, and general federal crimes under Title 18 of the United States Code, as well as many others. HSI Special Agents use this unique and broad statutory authority to investigate all types of cross-border criminal activity and work in close coordination with our federal, state, local, tribal, and international partners in a unified effort to target those nefarious actors trying to capitalize on the COVID-19 pandemic through fraud.

COVID-19 is a worldwide pandemic affecting nearly every country in the world. Despite widespread illness and death caused by COVID-19, individuals and organizations operating around the globe are actively seeking to exploit the pandemic for illicit financial gain. The illicit schemes these entities employ compromise legitimate trade and financial systems, threaten the integrity of the U.S. border, and endanger the safety and security of the American public. In April 2020, HSI launched Operation Stolen Promise to utilize the agency's unique authorities, robust cyber capabilities, and strategic partnerships worldwide to protect the Homeland from the increasing and evolving threat posed by COVID-19-related fraud and criminal activity.

COVID-19-Related Criminal Activity

As the COVID-19 pandemic has evolved and intensified, concerned Americans have sought to acquire test kits, personal protective equipment (PPE), medicines, hygiene products, and other medical equipment and supplies to protect themselves from the virus. Criminal networks and nefarious individuals worldwide are capitalizing on this sudden global demand, and are flooding the internet with fraudulent, counterfeit, substandard, or unapproved products. Illicit websites are selling fake goods defrauding consumers, degrading the integrity of legitimate commerce and trade, and endangering the lives of U.S. consumers. As new kits to test for COVID-19 and drugs to treat the virus have been developed and tested, criminal actors have shifted their operations accordingly; and they continue to sell counterfeit, unapproved, and substandard kits and pharmaceuticals, predominantly in online marketplaces.

Criminal organizations that historically have been engaged in financial scams such as bank and loan fraud, romance scams, Internal Revenue Service (IRS) scams, investment opportunity scams, and business email compromise are now pivoting to exploit this pandemic and associated lending opportunities and stimulus packages for illegal financial gains. At the same time, crimes of victimization continue to persist, with vulnerable populations being exploited by financial fraud schemes and offers of counterfeit, substandard, or non-existent PPE. As the pandemic has continued to take grip, financial fraud scams involving financial relief, paycheck protection program, and stimulus checks have also surged. In addition to the financial industry, these fraud scams also impact government public benefit agencies that are in the process of distributing aid

and providing assistance.

HSI Response

Since March 2020, HSI offices domestically and internationally have seen a significant increase in COVID-related fraud and other criminal activity. In response, HSI has intensified collaboration and partnership with multiple federal departments and agencies, along with business and industry representatives, to ensure the surging criminal activity surrounding the COVID-19 pandemic is met with an equally robust investigative response. Together, HSI and its partners are actively targeting those who attempt to sell counterfeit, substandard or otherwise unlawful pharmaceuticals and medical supplies and exploit this pandemic for illicit financial gain, as well as the platforms and internet provider accounts enabling this illicit activity. Additionally, HSI special agents are working alongside domestic and foreign law enforcement, regulatory agencies, financial institutions, and non-governmental organizations to identify and investigate COVID-19 related financial schemes targeting both the public and private sectors, to include government, businesses, and individuals. Taking a victim-centered approach, HSI endeavors to remedy, as much as possible, financial losses to individuals, businesses, and public and private institutions by ensuring that money acquired through fraud is returned to victims. As of July 24, 2020, HSI efforts have disrupted illicit transactions and recovered victims' funds of approximately $17.9 million.

Operation Stolen Promise Overview

In April 2020, HSI officially launched Operation Stolen Promise to protect the Homeland from the increasing and evolving threat posed by COVID-19-related fraud and criminal activity. Operation Stolen Promise is a strategic plan which combines HSI's expertise in global trade, financial fraud, international operations and cyber-crime to investigate financial fraud schemes, the importation of unlawful pharmaceuticals and medical supplies, websites defrauding consumers, and any other illicit criminal activities associated with the virus that compromises legitimate trade or financial systems and endangers the public.

Since the launch of this operation, HSI has opened over 570 investigations nationwide, seized over $7 million in illicit proceeds; made 53 arrests; executed 75 search warrants; analyzed over 50,000 COVID-19-related domain names and worked alongside U.S. Customs and Border Protection (CBP) to seize over 900 shipments of mislabeled, fraudulent, or unauthorized COVID-19 test kits, treatment kits, homeopathic remedies, purported anti-viral products, and PPE.

Operation Stolen Promise was built around four central pillars: partnership, investigation, disruption, and education. Each represents a core element of the HSI approach to addressing COVID-19 fraud. Since the operation's inception, HSI has implemented key actions under each of these pillars to take a comprehensive, multi-faceted approach to combatting COVID-19-related fraud across multiple fronts.

Operation Stolen Promise Central Pillars

Partnership

HSI, using its network of 80 Attaché offices in 50 countries, is partnering with both government and private sector partners around the world to comprehensively and effectively prevent and investigate criminal activity surrounding the pandemic. Strong partnerships are critical to strengthening global supply-chain security and will ultimately protect the American public from victimization.

HSI works alongside CBP on a daily basis to identify and investigate the illegal import and export of unlawful pharmaceuticals and medical supplies. As of July 24, 2020, HSI and CBP have collaborated to seize over 900 shipments of mislabeled, fraudulent, or unauthorized COVID-19 test kits, treatment kits, homeopathic remedies, purported anti-viral products, and PPE.

HSI also works closely with the Food and Drug Administration (FDA), the IRS, the U.S. Postal Inspection Service (USPIS), the Small Business Administration (SBA), the Federal Bureau of Investigation, the Department of Justice (DOJ) Consumer Protection Branch, the DOJ Computer Crime and Intellectual Property Section, U.S. Attorney's Offices around the country, and other federal, state, and local agencies to investigate and prosecute all forms of COVID-19 related fraud and criminal activity. These collaborative efforts span across multiple HSI components, including the National Intellectual Property Rights Coordination Center (IPR Center), the National Targeting Center – Investigations (NTC-I), the Illicit Finance and Proceeds and Crime Unit (IFPCU), the Cyber Crimes Center (C3), and HSI International Operations. The IPR Center also receives funding from the Department of State to deliver training and technical assistance to foreign law enforcement partners designed to strengthen their ability to cooperate with us.

With over 80 international offices in more than 50 countries, HSI has one of the largest international footprints in U.S. law enforcement. Positioned within embassies, consulates, and combatant commands around the world, HSI personnel abroad are leveraging relationships with other nations to exchange information and to jointly investigate illicit COVID-19 fraud schemes. On a daily basis, HSI special agents worldwide are engaging foreign law enforcement and customs partners to prevent shipments of unlawful pharmaceuticals and medical supplies from reaching the U.S.; to disrupt or dismantle illegal supply networks at the point of origin; to thwart illicit financial fraud as it occurs; and to assist in repatriating funds to victims. To date, the Five Eyes Law Enforcement Working Group has been a core component to HSI's international efforts on Operation Stolen Promise.

The HSI-led IPR Center, which stands at the forefront of the United States Government's response to combatting global intellectual property (IP) theft and enforcing international trade laws, is working with its 25 federal and industry partners to identify, interdict, and investigate individuals, companies, and criminal organizations engaging in the illegal importation of COVID-19 related products. As part of this effort, on May 5, 2020, industry leaders from Pfizer, 3M, Citi, Alibaba, Amazon, and Merck announced that they joined forces with the IPR Center in an unprecedented public-private partnership to combat fraud and other illegal activity surrounding COVID-19. Additionally, HSI is working closely with banks, money services businesses, and other financial institutions to identify, target, and disrupt COVID-19 financial fraud schemes, and is leveraging its partnerships with the cyber security industry and its cyber threat intelligence capabilities to identify and take down websites being utilized to facilitate COVID-19 related fraud and criminal activity.

Investigation

HSI and its partners are developing and pursuing actionable intelligence and investigative leads into those criminally exploiting the pandemic. These efforts are led by HSI special agents in domestic and international field offices and are being spearheaded by HSI's IPR Center, NTC-I, C3, and IFPCU. Investigative efforts center on global trade investigations, financial investigations, and cyber investigations.

The IPR Center and the NTC-I lead the U.S. government's response to combatting global IP theft and enforcement of its international trade laws and serve as the primary HSI entities for the exchange of information and intelligence related to COVID-19 illicit criminal activity. Through established relationships with government and private sector partners, the IPR Center and NTC-I are spearheading efforts to identify, interdict, and investigate individuals, companies, and criminal organizations engaging in the illegal importation of COVID-19 related pharmaceuticals and medical items, such as test kits and PPE.

HSI's investigative efforts pursuant to Operation Stolen Promise have revealed that the degree of fraud being perpetrated is representative of the panic resulting from the pandemic. As information on potential cures, tests, PPE, etc., spreads to the public, the types of fraud quickly change to meet these perceived new needs. This was true, for example, with hydroxychloroquine.

Many of the items detained by CBP and HSI have not been approved or otherwise authorized by the FDA or the Environmental Protection Agency. Unfortunately, consumers have no way to know if these items are in fact legitimate or if they will work if ordered from third-party marketplaces or non-medical websites. Based on the seizures made in conjunction with HSI's partners at CBP, approximately 56 percent of seizures originate in China and Hong Kong. The largest percentage of seizures have been COVID test kits at 45 percent, followed by pharmaceuticals at 27 percent, viral lanyards at 16 percent, and PPE at 10 percent. While all products are not necessarily counterfeit, they may not meet U.S. regulatory standards nor provide the medical benefits they claim. To date, HSI has seen a substantial number of inbound COVID-19 test kits going to residential addresses. Acting upon information obtained through CBP seizures, HSI has leverged our longstanding relationships with foreign customs and law enforcement officials to provide actionable intelligence which has resulted in arrest and seizures overseas. These arrests and seizures have prevented substandard and unregulated pharmaceuticals, PPE, and test kits from entering the domestic medical supply chain.

Since the launch of Operation Stolen Promise, the HSI IFPCU has worked closely with HSI field offices around the world and with its key partners to initiate, pursue, and support HSI investigations related to COVID-19 fraud. HSI has seen that scammers have attempted to profit from the pandemic through a number of means, including bank and loan fraud, fraudulent fundraising for fake charities, various medical scams and online sales of counterfeit medicines, medical supplies, testing kits, and PPE. Additionally, HSI has directed agents to pursue criminals who are engaged in crimes of victimization, with a particular focus on those who exploit vulnerable populations including the elderly.

To date, reporting from HSI domestic and international field offices and from the Federal Trade Commission all suggest that previously existing online fraud schemes and mass marketing scams have pivoted to exploit the COVID-19 pandemic. HSI is working closely with numerous federal agencies including the DOJ, IRS, USPIS, the Treasury Inspector General for Tax Administration, and the SBA Office of the Inspector General to analyze data associated with individuals and businesses attempting to exploit the economic stimulus package and defraud the United States Government.

Through an HSI-led COVID-19 Virtual Task Force, respective agencies provide guidance and direction to field agents to collaborate with members in order to identify vulnerabilities and provide resources and expertise to effectively combat illicit actors engaged in financial fraud activities. HSI has integrated its Office of Intelligence and Innovation Lab into this effort to support ongoing activities by HSI and its partners to research and track investigative leads related to COVID-19 fraud. These leads are being sent to HSI field offices and to the COVID-19 Fraud Task Force partners for further investigation. As of July 24, 2020, Operation Stolen Promise has led to the seizure of over $2.2 million related to CARES Act fraud.

The HSI C3 and its cybersecurity partners have continued to use the full extent of their investigative, analytical, and technical resources to collaboratively process and enrich data to target individuals and criminal organizations attempting to exploit this pandemic for illegal financial gains via fraudulent schemes. As Operation Stolen Promise has unfolded, C3 has committed to increasing enforcement by targeting online platforms and dark web sites enabling the sale and distribution of illicit materials related to COVID-19 and victimizing the American people. In addition to investigating the criminal elements operating illegally on the web, C3 has achieved significant success within the third pillar of Operation Stolen Promise, disruption. These efforts will be further described soon.

Disruption

Since launching Operation Stolen Promise, HSI has utilized the full breadth of its authorities to disrupt and dismantle fraud schemes; takedown illicit websites and other illegal online marketplaces; seize counterfeit or illicit pharmaceuticals and medical devices; and arrest and dismantle the organizations responsible. As of July 24, 2020, HSI special agents have seized over $7 million in illicit proceeds; made 53 arrests; executed 75 search warrants; conducted 42 disruptions of potential criminal activity; took appropriate disruption activity on thousands of illicit websites, and seized over 900 shipments of unlawful pharmaceuticals or medical supplies. Furthermore, HSI disrupted the flow and blocked the transfer of approximately $18 million being sent to fraudulent entities which were offering goods, services, or financial support under the guise of COVID-19 relief, protecting those consumers who were being defrauded.

A key element to HSI's disruption activities under Operation Stolen Promise are C3's efforts in the cyber realm. C3 leads the agency's response to preventing transnational criminal organizations, nefarious individuals, and malicious actors from exploiting this pandemic through online fraudulent schemes and the sale and distribution of illicit COVID-19 materials through nefarious online markets and the darknet.

Pursuant to Operation Stolen Promise, C3 has partnered with public/private and cybersecurity partners as well as other federal law enforcement agencies to identify and analyze

fraudulent websites, social media platforms and other online forums responsible for the advertisement of illicit COVID-19 related material. C3 and HSI special agents in the field work with website hosts and U.S. registrars to disrupt these illicit sites and to prevent the flow of dangerous items as quickly as possible, while still maintaining evidence for potential criminal investigation and prosecution. Once a suspected fraudulent domain is identified, it is referred to a field office for criminal investigation or referred to internet governance partners for appropriate action.

To date, C3 has analyzed over 50,000 COVID-19 suspected fraudulent domains for appropriate disruption action. These included phishing websites impersonating legitimate businesses selling COVID-19 supplies and charitable organizations conducting COVID-19 fundraising. Additional websites have been set-up for the purpose of executing malware and for selling COVID-19 related supplies that the sellers never intend on sending to the customer.

Education

One of the main goals of Operation Stolen Promise is to educate the public on the various types of fraudulent activity associated with the pandemic. To that end, HSI launched a robust public awareness campaign – *S.T.O.P COVID-19 Fraud* – to relay critical information to the public on COVID-19 fraud and criminal activity. Through this initiative, HSI is able to provide facts, tips, and red flags on pandemic-related crime and to guide the public on how to recognize potential fraud, protect themselves from it, and report it to authorities. HSI has developed outreach materials specifically for this effort, which are posted online in English and Spanish, and are available for HSI personnel to share with both public and private sector partners at meetings and other outreach events.

Additionally, HSI launched a dedicated COVID-19 webpage on ICE.GOV to provide information to the public on COVID-19 related fraud schemes. The page highlights the investigative efforts the agency is taking to counter the threats posed by individuals and criminal organizations seeking to exploit the pandemic for illicit financial gain and what HSI and its partners are doing to protect the public during the COVID-19 pandemic. HSI's *S.T.O.P COVID-19 Fraud* campaign is also highlighted on that page.

CONCLUSION

In the midst of a relentless global pandemic, the American people are counting on law enforcement to safeguard the public and ensure that our states, cities, and communities are protected from individuals and organizations intent on exploiting the pandemic through fraud. This is why HSI launched Operation Stolen Promise, and why the men and women of HSI have worked day in and day out to identify, disrupt, and dismantle these schemes rapidly and effectively utilizing the unique and extensive tools at HSI's disposal.

HSI's work through Operation Stolen Promise has yielded tremendous statistical results in just a matter of months. These actions have kept unlawful pharmaceuticals, testing kits, and medical supplies out of the hands of American consumers; have prevented Americans from being victimized by financial scams; and have helped secure the integrity of the U.S. financial and trade systems. Despite being faced with an unprecedented global health crisis, HSI personnel throughout the country and around the world have remained dedicated to carrying out this

important mission. HSI is proud of its role in responding to COVID-19 fraud and on the impact Operation Stolen Promise has made on the lives of the American public, which the men and women of HSI have sworn to protect and serve.

Thank you again for the opportunity to submit this testimony for the record.